T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Mekatronik Mühendisliği Anabilim Dalı

OTONOM ARAÇLARIN RADYO FREKANS SALDIRILARINA KARŞI GÜVENLİĞİ

Yüksek Lisans Tezi

Hasan YILDIRIM

Danışman
Dr. Öğr. Üyesi Cansu NOBERİ

İstanbul – 2024

TEZ TANITIM FORMU

Yazar Adı Soyadı : Hasan YILDIRIM

Tezin Dili : Türkçe

Tezin Adı : Otonom Araçların Radyo Frekans Saldırılarına Karşı Güvenliği

Enstitü : İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsü

Anabilim Dalı : Mekatronik Mühendisliği

Tezin Türü : Yüksek Lisans

Tezin Tarihi : 24.07.2024

Sayfa Sayısı : 83

Tez Danışmanları : Dr. Öğr. Üyesi Cansu NOBERİ

Dizin Terimleri : Siber güvenlik, Elektronik haberleşme, HackRf One, Gnu Radio, Şifreleme, Otonom sistemler,

Türkçe Özet : Otonom araçların içerdiği sistemlerden en önemli olanları haberleşme sistemleridir. İnsan gücü olmadan kendi kendilerine karar verebilen otonom araçlar uzaktan takip edilmekte ve sistemlerinde kablosuz iletişim yapılmaktadır. Araç anahtar haberleşmesi bu sistemlerdendir. Bu sistemler kablosuz iletişim yaparak radyo dalgaları kullanılarak gerçekleştirilmektedir. Elektromanyetik dalgalar olan radyo dalgaları alıcı ve verici cihazlar arasında iletilerek sistemlerin çalışmasını sağlamaktadır. Araçlar üzerinde kapıların açılması için butona basıldığında giden sinyal araca iletir. Araç sinyalin işlenmesiyle kapıların açılmasını sağlamaktadır. Bu sistem çalışırken hackrf one kullanılarak radyo dalgalarına yapılan sinyal saldırısında kapının açılmak için gönderilen sinyali yakalanmıştır.

Yakalanan sinyal araca tekrar iletildiğinde aracın kapılarının açıldığı gözlenmiştir. Bu durumda dışarıdan müdahale ile araçlara erişim mümkün olmuştur. Dışarıdan erişimin mümkün olmasıyla araçların hırsızlık riskleri artabilmektedir. Bu duruma çözüm olarak çalışma kapsamında sinyalin şifrelenmesi amaçlanmıştır. Araçtaki sistem ile anahtar üzerinde bulunan sistemde gönderilen sinyalin tek bir formda olması aracın haberleşme yapısında güvenlik açığı oluşturmuştur. Anahtar içerisindeki sistem yazılımı geliştirilerek sinyal şifrelenmiş ve araca iletilmiştir. Anahtar içerisindeki sistem yazılımı araç içerisindeki sistem yazılımına uyumlu olarak geliştirilmiştir. Araca gelen şifreli sinyal tanımlanmıştır. Tanımlanan sinyal algoritmaya uygun olarak kapının açılmasını veya kapanmasını sağlamıştır. Bu durum için benzer haberleşme yapısını kullanan sistemlere bakılmıştır. Bir çok alanda radyo dalgalarıyla haberleşen sistemlerin bu durumda siber güvenlik açığı bulunmaktadır. Bu çalışmanın örnek olması amacında sinyal saldırısı yapılmış ve bu güvenlik açığına çözüm getirilmiştir.

Dağıtım Listesi **:** 1. İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsüne
2. YÖK Ulusal Tez Merkezine

İmzası
Hasan YILDIRIM

T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Mekatronik Mühendisliği Anabilim Dalı

OTONOM ARAÇLARIN RADYO FREKANS SALDIRILARINA KARŞI GÜVENLİĞİ

Yüksek Lisans

Hasan YILDIRIM

Danışman
Dr. Öğr. Üyesi Cansu NOBERİ

İstanbul – 2024

BEYAN

Bu tezin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez olarak sunulmadığını beyan ederim.

Hasan YILDIRIM

24.07.2024

T.C.

İSTANBUL GELİŞİM ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Hasan YILDIRIM' ın **"Otonom Araçların Radyo Frekans Saldırılarına Karşı Güvenliği"** adlı tez çalışması, jürimiz tarafından Mekatronik Mühendisliği Anabilim Dalı Mekatronik Mühendisliği Bilim Dalı YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan _____

Prof. Dr. Mustafa Emre AYDEMİR

Üye _____

Dr. Öğr. Üyesi Cansu NOBERİ

(Danışman)

Üye _____

Dr. Öğr. Üyesi Serkan GÖNEN

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

.... / .... / 2024

Prof. Dr. İzzet GÜMÜŞ

Enstitü Müdürü

ÖZET

Otonom araçların içerdiği sistemlerden en önemli olanları haberleşme sistemleridir. İnsan gücü olmadan kendi kendilerine karar verebilen otonom araçlar uzaktan takip edilmekte ve sistemlerinde kablosuz iletişim yapılmaktadır. Araç anahtar haberleşmesi bu sistemlerdendir. Bu sistemler kablosuz iletişim yaparak radyo dalgaları kullanılarak gerçekleştirilmektedir. Elektromanyetik dalgalar olan radyo dalgaları alıcı ve verici cihazlar arasında iletilerek sistemlerin çalışmasını sağlamaktadır. Araçlar üzerinde kapıların açılması için butona basıldığında giden sinyal araca iletir. Araç sinyalin işlenmesiyle kapıların açılmasını sağlamaktadır. Bu sistem çalışırken hackrf one kullanılarak radyo dalgalarına yapılan sinyal saldırısında kapının açılmak için gönderilen sinyali yakalanmıştır. Yakalanan sinyal araca tekrar iletildiğinde aracın kapılarının açıldığı gözlenmiştir. Bu durumda dışarıdan müdahale ile araçlara erişim mümkün olmuştur. Dışarıdan erişimin mümkün olmasıyla araçların hırsızlık riskleri artabilmektedir. Bu duruma çözüm olarak çalışma kapsamında sinyalin şifrelenmesi amaçlanmıştır. Araçtaki sistem ile anahtar üzerinde bulunan sistemde gönderilen sinyalin tek bir formda olması aracın haberleşme yapısında güvenlik açığı oluşturmuştur. Anahtar içerisindeki sistem yazılımı geliştirilerek sinyal şifrelenmiş ve araca iletilmiştir. Anahtar içerisindeki sistem yazılımı araç içerisindeki sistem yazılımına uyumlu olarak geliştirilmiştir. Araca gelen şifreli sinyal tanımlanmıştır. Tanımlanan sinyal algoritmaya uygun olarak kapının açılmasını veya kapanmasını sağlamıştır. Bu durum için benzer haberleşme yapısını kullanan sistemlere bakılmıştır. Bir çok alanda radyo dalgalarıyla haberleşen sistemlerin bu durumda siber güvenlik açığı bulunmaktadır. Bu çalışmanın örnek olması amacında sinyal saldırısı yapılmış ve bu güvenlik açığına çözüm getirilmiştir.

Anahtar Kelimeler: Siber güvenlik, Elektronik haberleşme, HackRf One, Gnu Radio, Otonom sistemler,

SUMMARY

The most important systems in autonomous vehicles are communication systems. Autonomous vehicles that can make decisions on their own without human power are remotely monitored and wireless communication is performed in their systems. Vehicle key communication is one of these systems. These systems are realized using radio waves by wireless communication. Radio waves, which are electromagnetic waves, are transmitted between the receiver and transmitter devices and ensure the operation of the systems. When the button is pressed to open the doors on the vehicles, the outgoing signal is transmitted to the vehicle. The vehicle ensures that the doors are opened by processing the signal. While this system was working, the signal sent to open the door was captured in the signal attack on radio waves using hackrf one. When the captured signal was transmitted back to the vehicle, it was observed that the doors of the vehicle were opened. In this case, access to vehicles was possible with external intervention. With the possibility of external access, the risk of theft of vehicles may increase. As a solution to this situation, it is aimed to encrypt the signal within the scope of the study. The fact that the system in the vehicle and the signal sent in the system on the key are in a single form has created a security gap in the communication structure of the vehicle. By developing the system software in the key, the signal was encrypted and transmitted to the vehicle. The system software in the key was developed compatible with the system software in the vehicle. The encrypted signal received by the vehicle was identified. The identified signal enabled the door to open or close in accordance with the algorithm. For this case, systems using similar communication structure were examined. Systems that communicate with radio waves in many areas have cyber security vulnerabilities in this case. For the purpose of this study to be an example, a signal attack was made and a solution was brought to this vulnerability.

Keywords: Cyber security, Electronic communications, HackRf One, Gnu Radio, Autonomous systems,

İÇİNDEKİLER

ÖZET ..... **i**
SUMMARY ..... **ii**
KISALTMALAR ..... **v**
ŞEKİLLER LİSTESİ ..... **vi**
ÖNSÖZ VE TEŞEKKÜR ..... **vii**
GİRİŞ **1**
BİRİNCİ BÖLÜM **3**
1.1. Geçmişten Günümüze Otomotivdeki Gelişmeler 3
1.2. Geçmişten Günümüze Mekatronik Kavramı 5
1.3. Otonom Kavramı 7
1.3.1. Otonom Araçların Tarihi 8
1.4. Otonom Araçların Güvenliği 11
İKİNCİ BÖLÜM **14**
2.1. Hackrf One 14
2.2. GNU Radio 17
2.3. 3D Yazıcı 19
2.4. Gömülü Sistem 22
2.4.1. Arduino Uygulama Geliştirme Kartı 23
ÜÇÜNCÜ BÖLÜM **26**
3.1. Otonom Araç Tasarımı 26
3.2. Otonom Araç Elektronik Şeması 28
DÖRDÜNCÜ BÖLÜM **31**
4.1. Mevcut Araç Anahtar Yazılım 31
4.2. Geliştirilen Araç Anahtar Yazılımı 32
4.2.1. Araç Kumandası Radyo Frekans Verici Donanım Yazılım 33
4.2.2. Araç İçerisinde Radyo Frekans Alıcı Donanım Yazılım 38
BEŞİNCİ BÖLÜM **43**
5.1. Araç ve Kumanda Haberleşmesinde Gönderilen Sinyalleri Yakalama 43
5.2. Araç ve Kumanda Haberleşmesinde Yakalanan Sinyali İşleme 48
ALTINCI BÖLÜM **50**
6.1. Mevcut Araç Anahtar Yapısına Sinyal Saldırısı 50
6.1.1. Kumandadan Gönderilen Kapı Açma Sinyalini Yakalamak 50
6.1.2. Yakalanan Sinyali Alıcıya İletmek 54
6.2. Geliştirilen Araç Anahtar Yapısına Sinyal Saldırısı 58
YEDİNCİ BÖLÜM **59**
7.1. Askeri 59
7.2. Sağlık 60
7.3. Taşımacılık 61

SEKİZİNCİ BÖLÜM 63
8.1. Sonuçlar 63
8.2. Sınırlılıklar 64
8.3. Öneriler 65

KISALTMALAR

TDK	**:**	Türk Dil Kurumu
GPS	**:**	Küresel Konumlama Sistemi (Global Position System)
STL	**:**	Standart Triangle Language
PLA	**:**	Polilaktik Asid
ABS	**:**	Akrilonitril Bütadiyen Stiren
FDM	**:**	Fused Deposition Modeling
SLS	**:**	Selective Laser Sinterin
IDE	**:**	Integrated Development Environment
ECU	**:**	Elektronik Kontrol Ünitesi
ABS	**:**	Anti Block System
CAN	**:**	Controller Area Network
SİHA	**:**	Silahlı İnsansız Hava Aracı

ŞEKİLLER LİSTESİ

ŞEKİL 1.1 OTONOM ARAÇ SÜRÜŞ TEKNOLOJİLERİ (GÜRTAŞ, 2020) 9
ŞEKİL 1.2 OTONOM ARAÇLARIN SÜRÜŞ SEVİYELERİ (BAKİOĞLU, ATAHAN, 2021) 10
ŞEKİL 2.1 HACKRF ONE 15
ŞEKİL 2.2 HACKRF ONE ANTEN 15
ŞEKİL 2.3 HACKRF ONE CİHAZI VE ANTEN TAKILMASI 16
ŞEKİL 2.4 GNU RADİO ARAYÜZÜ 18
ŞEKİL 2.5 GNU RADİO BLOK MENÜSÜ 19
ŞEKİL 2.6 CREALİTY ENDER 5S 3 BOYUTLU YAZICI 21
ŞEKİL 2.7 3 BOYUTLU YAZICI PARÇA BASIMI 22
ŞEKİL 2.8 ARDUİNO UYGULAMA GELİŞTİRME KARTI 24
ŞEKİL 3.1 ARAÇ SAĞ VE SOL KAPILARI TASARIMLARI 26
ŞEKİL 3.2 ARAÇ TASARIMI ÖN ÇAPRAZ GÖRÜNÜMÜ (A) VE ARAÇ TASARIMI ARKA ÇAPRAZ GÖRÜNÜMÜ (B) 27
ŞEKİL 3.3 ARAÇ ARKASI GÖRÜNÜM (A) VE ARAÇ ÖN ÇAPRAZ GÖRÜNÜM (B) 28
ŞEKİL 3.4 ARAÇ KUMANDA ELEKTRONİK ŞEMASI 29
ŞEKİL 3.5 ARAÇ İÇİ ELEKTRONİK ŞEMASI 30
ŞEKİL 4.1 ARAÇ ANAHTAR YAPISI 31
ŞEKİL 4.2 ARAÇ KAPI KİLİT YAPISI 32
ŞEKİL 4.3 ALICI YAZILIM KÜTÜPHANELERİ 33
ŞEKİL 4.4 VERİCİ YAZILIM DEĞİŞEN TANIMLAMA 33
ŞEKİL 4.5 VERİCİ YAZILIM KAPI AÇMA ALGORİTMASI 35
ŞEKİL 4.6 VERİCİ YAZILIM KAPI KAPATMA ALGORİTMASI 36
ŞEKİL 4.7 VERİ ÜRETME TANIMLAMA 37
ŞEKİL 4.8 KUMANDA KAPI AÇMA BUTON SORGULAMASI 37
ŞEKİL 4.9 ALICI YAZILIM KÜTÜPHANE VE TANIMLAMA 38
ŞEKİL 4.10 ALICI YAZILIMDA GİRİŞ PORTLARI BELİRLEME 39
ŞEKİL 4.11 ALICI YAZILIM KAPI AÇMA ALGORİTMASI 40
ŞEKİL 4.12 ALICI YAZILIM KAPI KAPAMA ALGORİTMASI 41
ŞEKİL 5.1 SİNYAL YAKALAMA AKIŞ DİYAGRAMI 45
ŞEKİL 5.2 YAKALANAN SİNYALİ İLETME AKIŞ DİYAGRAMI 48
ŞEKİL 6.1 SALDIRIDAN ÖNCE ARAÇ DURUMU 50
ŞEKİL 6.2 SANAL İŞLETİM SİSTEMİ – UBUNTU 51
ŞEKİL 6.3 GNU RADİO AÇILIŞ ARAYÜZÜ 51
ŞEKİL 6.4 GNU RADİODA SİNYAL YAKALAMADA KULLANILAN BLOKLAR 52
ŞEKİL 6.5 SİNYAL GÖSTERİMİ 53
ŞEKİL 6.6 YAKALANAN SİNYAL GÖSTERİMİ 54
ŞEKİL 6.7 YAKALANAN SİNYALİ ALICIYA İLETEN AKIŞ DİYAGRAMI 55
ŞEKİL 6.8 YAKALANAN SİNYALİ İLETİRKEN OLUŞAN GRAFİK GÖRÜNTÜSÜ 56
ŞEKİL 6.9 ARAÇ SALDIRI SONRASI DURUMU 57
ŞEKİL 6.10 GELİŞTİRİLEN SİSTEMİN İZİNSİZ GİRİŞ ALGILAMASI 58

ÖNSÖZ VE TEŞEKKÜR

Bu tez çalışmasında, günümüzün yaygın teknolojilerinden olarak otonom araçların, bir sinyal saldırısına karşı yeteri güvenlik önlemlerinin bulunup bulunmadığı incelenmiştir. İncelemeler sonucunda sinyal saldırısı yapılarak, otonom araçlara uzaktan erişim mümkün olmuş ve bu saldırıya önlem alınmıştır. Alınan önlemle birlikte amaçlanan, yeni teknolojiler arasında olan otonom araçların çalınma riskini azaltmaktır. Tez çalışması için bu konunun seçilmesi, aslında günümüz teknolojisinin yaşadığı olarak nitelendirilmektedir.

Öncelikle tez konusunu seçerken isteklerimi göz önünde bulundurup bana yardımcı olan, ilk kez böyle bir çalışma içerisinde bulunduğum için yaşadığım zor durumlarda dahi bana her anlamda destek olan tez danışmanım Dr. Öğr. Üyesi. Cansu NOBERİ hocama teşekkürlerimi sunarım.

Tez çalışması için desteklerini esirgemeyen başta Bilimsel Araştırma Projeleri Koordinatörü Dr. Öğr. Üyesi Serap YEŞİLKIR BAYDAR hocama ve malzeme tedarik konusunda yardımlarını esirgemeyen Bilimsel Araştırma Projeleri Koordinatörlüğü ekibine teşekkürlerimi sunarım.

Tez çalışmam için ihtiyaç duyduğum gerek malzeme desteği ile kullanılan yöntemler gerek ise değerli bilgilerini ve zamanını esirgemeyerek desteklerini gösteren Dr. Öğr. Üyesi Serkan GÖNEN hocama teşekkürlerimi sunarım.

Bu zorlu tez sürecinde benden desteğini bir an için bile esirgemeyen değerli arkadaşım, Ahmet Faruk GÖRMÜŞ'e, tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen her zaman yanımda olan sevgili aileme teşekkürlerimi bir borç bilirim.

GİRİŞ

Otomotiv teknolojisi, günümüzde kullanılan boyutlara gelene kadar birçok denemelerden geçmiştir. Bu denemelerden ilki, tarih kayıtlarına göre 1769 yılında Fransız Yüzbaşı Nicholas Joseph Cugnot tarafından gerçekleştirilmiştir. O dönemde bulunan cephelere silah taşımak için buhar gücü kullanarak tasarlamış, ancak yeterli hıza çıkamadığı için verim alınamamıştır. Bundan 30 yıl sonrasında ise İngiliz mucit olan Richard Trevithick ile Amerikalı mucit Oliver Evans'ta bu çalışmaların devamlılığında bulunmuş ancak onlarda başarılı olamamıştır. 1829 yılında, diğer bir İngiliz mucit S. Goldswort Guyney tarafından buhar gücüyle çalışan ve 20-30 km hızları arasına ulaşan ilk araç üretilmiştir. Ancak 1860 yılında, günümüzde kullanılan içten yanmalı motor keşfedilmiş ve sonrasında 1876 yılında benzin kullanılarak çalıştırılmıştır (Bedir, 2002). 1886 yılında ise Carl BENZ tarafından yapılmıştır. 3 tekerlekli olan bu otomobil, içten yanmalı benzinli bir motora sahip olup bir devrim niteliğinde olmaktadır. O dönemlerde buharlı motorla çalışan sistemlerden çok farklı olarak kendine has yapısı ve kullanılan sistemlere göre çok daha verimli olmaktadır. Dolayısıyla birçok kişi tarafından tarihteki ilk otomobil olduğu düşünülmektedir (Rojteur, 2023).

Bu otomobillerin kullanımının artması ve üretilebilirliği, o dönemlerde otomotiv sanayisinin başlangıcını oluşturmuştur. 1900'lü dönemlerde kullanılan at arabasına benzer tekerlekli araçların yerini motorlu araçlar almakta, hatta üretim tesisleri de motorlu araçlar üretimine doğru evirilmiştir. O dönemde bu tesislerden en bilinenler arasında olan Ford, araç üretimini günümüze kadar sürdürmüştür. Hızla gelişen otomotiv sanayisi, ilk sürücü belgeleri ve servis istasyonlarının oluşmasına neden olmuştur. Oluşan bu yenilikler, yavaşça dünya piyasasında yerini almıştır. 1900'lü dönemlerde satış alt yapısının oluşturulmaya başlanmasına eş olarak Ford'un ünlü modeli olan T piyasaya sürülmüştür. Bu araçların ortaya çıkması ve otomotiv sanayisinin gelişmesi, ülkeler için otomotiv altyapısı altında diğer çalışmaları da beraberinde getirmiştir. Bu çalışmalar, araçların kullanımı için yol çalışmalarını ve trafik kurallarının temelini oluşturmaya başlanmıştır (Yulu, 2018).

Bu çalışma da amaç, artık günümüz araçlarda çok sık görülmeye başlayan otonom araçların sahip olduğu yazılımlarda anahtar ve araç arasındaki haberleşme

yapısının güvenlik açığını incelemek ve önlemek olmaktadır. Geçmişten günümüze otomotiv alanı, tahmin edilemeyecek boyutlarda ilerlemiştir. Bu ilerlemeyle eş olarak güvenlik problemleri de ortaya çıkmakta ve bu problemler yüksek risklerde olmaktadır. Geçmişte kullanılan donanım veya sensörler ile günümüzdeki sistemler farklılık göstermektedir. Dolayısıyla, bu güvenlik problemlerinin çözümü içinde eş zamanlı çalışmalar yapılması gerekmektedir.

BİRİNCİ BÖLÜM

Bu çalışma kapsamında bulunan teknolojilerin ilk prototiplerinden günümüze kadar olan gelişmeleri gözlemlenmiştir.

1.1. Geçmişten Günümüze Otomotivdeki Gelişmeler

1885 - Yılında Carl Frederich Benz tarafından ilk kez içten yanmalı motor kullanılarak benzinle çalışan bir otomobil yapılmıştır.

1890 – Yılında çalışma esnasında oluşan bir kaza sonucunda Herbert Akroyd Stuart, bir gaz yağının yüksek sıcaklı bir yere değmesi ve hava ile temas etmesi sonucunda yandığını gözlemlemiştir. Bir odacık içerisinde havanın sıkışıp ısınmaktadır. Sonrasında odacık içerisine yanıcı ve patlayıcı olan bir karışım gönderilmektedir. Bu karışımın yanması içinde bir ön yanma odası bulunur ve bu oda da dışarıdan bir alev ile ısıtılmaktadır.

1890 – Yılında bulunan otomobillerin çoğu yokuş çıkmakta zorlanmaktadır. Çünkü günümüzde olduğu gibi o zamandaki otomobillerde bir şanzıman sistemi bulunmamaktadır. Dolayısıyla yokuşta bir süre sonra durup geri gitmektedir. Benz Victoria markalı bir otomobilde, 1893 yılında otomobillerin yokuş yukarı tırmanmasını sağlamak için manivelada alabileceği gücü yükseltmek amaçlı deri kayışı oldukça küçük bir kasnağa takılan bir kol kullanıldı.

1892 – 1897 Yıllarında Rudolf Diesel dizel motoru yaptı. Okuduğu okul Münih Yüksek Teknik Okulunda yaptığı bu dizel motoru geliştirdi.

1893 – Yılında Charles Duryea ve abisi Frank Duryea tarafından Amerika'ya ait ilk otomobil yapıldı.

1894 – Yılında otomotiv alanıyla ilgili olarak ilk kez resmi otomobil yarışı düzenlendi.

1902 – Yılında Ferdinand Porsche, Mixte-Wagen adını verdiği, günümüzde hibrit diye tanımladığımız hem elektrikle hem de benzinle çalışabilen aracını üretti.

1905 – Yılında Alfred Büchi, otomobillerden çıkan egzoz gazlarını kullanarak bir türbin tasarladı. Bu türbin sonucunda motora giren havanın miktarını arttırdı.

1908 – Yılında otomotiv sektöründe devrim niteliğinde olacak olan seri üretime geçildi. ABD'li Henry Ford'un yaptığı ilk seri üretim otomobili, 1913 yılında günde 1000 adet üretiliyordu.

1918 – Yılında dizel sistemler Royal Aircraft Establisment fabrikaları tarafından geliştirilerek günümüzde kullanılan yüksek devirli dizel motorları oluşturuldu.

1919 – Yılında ilk kez Avrupa tarafından Type A otomobili seri üretim ile piyasalara sunuldu.

1924 – Yılında ilk kamyon, MAN markanın direkt enjeksiyonlu dizel motoru kullanmasıyla üretildi.

1934 – Yılında Citroen artık seri bir şekilde önden çekiçli otomobilleri üretmeye başladı.

1938 – Yılında Citroen tarafından hidropnömatik süspansiyon icat edildi.

1938 – Yılında Saurer tarafından ilk kez turbo motorlu kamyon üretildi.

1954 – Yılında Felix Wankel tarafından döner pistonlu motor geliştirildi.

1967 – Yılında ilk kez otomobillere ABS sistemi uygulanmaya başladı.

1984 – Yılında ilk kez Garett Intercooler tarafından turbo soğutucusu üretildi.

1993 – Yılında düşük motor devirlerinde diğer turbolardan farklı geometri yapısına sahip olmasıyla turbonun verimini arttıran sistem ilk kez Fiat Croma TdiD otomobilinde kullanıldı.

2004 – Yılında BMW 535d markalı araca o dönemde ilk kez uygulanan çift turbolu seri üretim dizel motoru oldu.

2005 – Yılında Cenevre otomobil fuarında, Mercedes tarafından üretilmiş olan 3 turbolu v6 dizel motoru olan araç gösterime sunuldu (Otomotiv Sektör, 2009).

1800'lü yıllardan günümüze kadar olan otonom araçlarının gelişim sürecine bakıldığında, teknolojinin üzerine eklenerek ilerlemiştir. Bu ilerleme, çoğu durumlarda çalışma alanları dışına çıkılarak ortak çalışmalara sebep olmuştur. Buna örnek olarak, dünyanın teknolojisi geçmişin ilk gelişimlerinden olan ve sadece buhar gücüyle çalışan dıştan yanmalı bir motor üretilmiş ve üretilen bu motor, günümüzde elektrikli motor olarak yeniden tasarlanmıştır. Yıllar boyu süren bu gelişmenin tarihine

bakıldığında, aslında çalışmaların süreci evrimleşerek devam etmiştir. Örneğin, dıştan yanmalı motorların verimleri içten yanmalı motorlara göre oldukça düşüktür. Dolayısıyla, daha iyi bir verim alınması ihtiyacı duyulduğu için bilim insanlarının çalışmaları sonucunda içten yanmalı motorlar tasarlanmıştır. İstenilen amaca ulaşılıp ulaşılmadığı ise mevcut oldukları teknolojiden daha iyi bir sonuç almaları karşısında anlaşılmıştır. İçten yanmalı motorları üretirken de mekanikle birlikte elektrik yapısı da kullanılmıştır. Mekanik ve elektrik alanları birbirinden farklı konular olmasına rağmen birlikte kullanılmasıyla yeni bir icadın veya devrin başlangıcına neden olmuştur. Farklı alanların sentezlenmesi kullanılarak birden fazla sektörde kullanılan faydalı sistemler üretilmiştir. Bu sentezlenmeler, günümüzde de devam etmekte olan mekatronik kavramını ortaya çıkarmıştır. Gelişen teknoloji ile oluşan ihtiyaçların çözümü için mekanik, elektrik, yazılım vb. alanlar uyum içerisinde çalışarak mekatronik sistemlerini meydana getirmiştir. Böylelikle mekatroniğin ilk adımları bu dönemlerde oluşmaya başlanmıştır.

1.2. Geçmişten Günümüze Mekatronik Kavramı

Geçmişe bakıldığında, mekatronik kavramı ilk kez Japonya'da meydana gelmiştir. 1960'lı yılların sonlarında, elektrik şirketinde çalışan bir mühendis, bilgisayar ile elektrik alanlarının birlikte kullanılması için çalışmalar yapmıştır. Elektrik motorlarının kontrolüne ihtiyaç duyan mühendis, bu motorların kontrolünü bir bilgisayar ile kontrol edebileceğini düşünmüş ve çalışmalara başlamıştır. Bu çalışma, tarihte 2 farklı alanın birleşmesiyle mekatronik mantığının oluşmasını sağlayan ilk çalışmadır. Japonya'da yapılan bu çalışma, tüm dünyaya örnek olarak yeni çalışmaların temelini atmalarını sağlamıştır. Birçok alanların sentezlenmesi, uyum içerisinde çalışması ve sürekli gelişimi vb. amaçlar doğrultusunda, üniversitelerde eğitim olarak görülmeye başlanmıştır. İlerleyen yıllarda, insan hayatını kolaylaştıran birden fazla sektörde görülmüş ve dolayısıyla araştırma geliştirme çalışmaları hız kazanmıştır. 1980 yıllarını takiben, mühendislerin çalışmaları sonucu mikroişlemciler oluşturulmaya başlanmıştır. Mikroişlemciler, genel olarak içerisine tanımlanan algoritmaları yine içerisinde tanımlanan şartlara göre tasarlanan çok küçük boyutlu cihazlardır. Otomotiv üzerinde ABS (Anti-Lock System) fren sistemlerin, hava yastığı sistemlerinde kullanılmaya başlanmıştır. Ayrıca, mikroişlemci

teknolojisinin gelişmesi ile birlikte, günümüzde çalışmaları sürmeye devam eden robotik uygulamalarında ilk adımları atılmıştır (Coşkun, 2003).

Mekatroniğin teknoloji gelişim sürecine olan faydaları oldukça fazladır. Ancak, hem kullanılan parçaların küçük ve hafif olması hem de sistemlerin tek bir noktadan kontrol edilmesi yönleri en önemlilerdendir. Uçak, gemi, otomotiv, sanayi üretim hatları vb. organize çalışarak takibi zor olan sistemler, aslında mekatronik uygulamaları sayesinde oldukça basitleştirilmiştir. Dolayısıyla, zorlayıcı veya karışık olan bir sistemin dahi tek noktadan kontrol edilmesi, insan hayatını kolaylaştırmıştır. Pratik bir şekilde sistemlerin yönetilmesiyle zamandan tasarruf edilmektedir. Mikroişlemciler, bu yönüyle sanayide istihdam, üretim hızı, üretim kalitesi vb. durumları etkilemiştir. Ayrıca, birçok sistemi kolaylaştıran mikroişlemcilerin gelişimiyle sanayide kullanılan yeni kavramlar türetilmiştir. Bu kavramlardan günümüzde en yaygın olan otonom kavramıdır. Otonom kavramının TDK (Türk Dil Kurumu)'da geçen tanımı, "kendi kendini yönetme gücüyle hareket etmek" idir.

Günümüzde bulunan birçok sistem artık otonom olarak çalışmaktadır. Örneğin, mutfaklarda kullanılan beyaz eşyalarda, mikrodalga fırınlar istenilen sıcaklığa veya saate göre ayarlandığında, sistem buna uyum sağlar. Belirtilen şartların dışına çıkmaz. İstenilen şartlar değişmediği sürece aynı şekilde çalışmasını devam ettiren bu sistemler, otonom olarak çalışan sistemler için en basit örneklerdendir. Dolayısıyla, otonom kavramı, mikroişlemcilerin içerisine tanımlanan çalışma şartlarıdır denilebilir. Çünkü mekatronik açıdan bir sistemin çalışması için gerekli gücün şiddeti, miktarı vb. parametreler doğrultusunda çalışmasının kararını verecek olan parçalar mikroişlemcilerdir. Bu yüzden mikroişlemciler, mekatronik sistemlerin beynidir. Beyin işlevi gibi çalışan mikroişlemcilerin otonom yetkinliği de içerisinde ki tanımlamaya göre olmaktadır. Aslında bu örneğe bakılarak, buna benzer veya daha da gelişmiş sistemlerin birlikte çalışması sonucunda otonom kavramının varlığı oluşmaktadır (Şahinoğlu, 2006). Otonom kavramının zaman içerisinde gelişerek günümüze yerleşmesiyle, birden fazla sektörde kullanılmasına sebep olmuştur. Günümüzde otonom kavramı içerisinde çalışan bu sistemlere akıllı sistemlerde denilebilmektedir. Dolayısıyla, ihtiyaca göre çeşitlenen teknolojiler yeni yaşam alanları oluşturmuştur. Bu alanlara bakıldığında Akıllı evler, akıllı şehir, akıllı robot vb. kavramlar meydana gelmiştir. Bu kavramlarda mekatronik açıdan çalışan

sistemlere bakıldığında; Şehirler, iş yerleri, evler vb. meskenlerde sensörler ile harekete duyarlı aydınlatma sistemleri kullanılmaktadır. Harekete duyarlı, otonom olarak çalışan bu sistemler, minimum enerji ile tasarruf etmeyi de mümkün kılmıştır.

Binalar, akıllı sistem olarak kullanılan kameralar ile hırsızlık, yangın vb. durumların takibi yapılabilmektedir. Kendi içerisinde otonom olarak çalışan bu sistemlerin kontrolü ise günümüzde bir telefondan yapılabilmektedir (Akçay, Canbaz, Diş, 2022).

Kamera sistemlerine ek olarak, tıp biliminde tanı aracı (radyografi vb.) olarak veya tıp alanında kullanılan cihazların üretimi için kullanılmaktadır (Demirkesen, 2012). Birçok hastalığa veya sağlık alanında ki yetersizliklere bakıldığında, otonom çalışan mekatronik sistemlerin kullanımı gün geçtikçe artmıştır. Doğru tanı, reçeteleme, hasta takip sistemi vb. kullanım alanları meydana gelmiştir (Hakverdi, 2021).

Otonom sistemler, günümüzde ki araçlarda da artık sıkça görülür hale gelmiştir. Demirkesen, insan müdahalesi olmadan sürüş gerçekleştirebilen bu araçların, çevresel şartlara ve trafik kurallarına uyumlu olarak çalıştığını belirtmiştir. Otonom kavramının günümüzden itibaren daha da geliştirileceği ve insan hayatında ki çoğu durumlarda vazgeçilmez olacağı tahmin edilmektedir.

1.3. Otonom Kavramı

Otonom kelimesi, Fransızcadan dilimize gelmiş ve anlamı bağımsız olan kelimedir. Anlamına uygun olarak, otonom sistemlerde bir insan gücü olmadan kendi kendine çalışan sistemlerdir (Bilban, 2020). Otonom kelimesinin ilk ortaya çıkış çalışmaları aslında matematiğe dayanmaktadır. Ancak günümüzdeki modern kullanımda araçlar ve cihazlarla birleşmiştir. Araçlarda bulunan donanımsal parçalar ile bu parçaların kontrolünü, yazılımsal tabanlı mikroişlemcilerle birlikte sağlayarak uyum içerisinde çalışmaktadırlar. Bilban, hava araçları, kara araçları, deniz araçları, haberleşme sistemleri vb. alanlarda bulunan sistemlerin kendi kendini yönetme yetkinlikleri bulunduğunu ifade etmektedir. Bu yetkinlikler, her alanda farklı şartlar meydana getirmektedir. Bunun örneği olarak, bir hava aracı hava şartlarıyla ilgili parametrelerle iletişimde kalabilirken, kara araçlarında otonom araçlar insan, çevre, trafik, şeritler vb. birçok parametre ile etkileşimde olmaktadır. Bu durumlar karşısında

vereceği kararlar, otonom araçlarda tartışmalara neden olmuştur. Karşılaştıkları engeller sonucunda çevreye veya içerisinde bulunan sürücüye zarar verme durumları büyük ölçüde risk taşımaktadır. Dolayısıyla, otonom kavramı, geçmişten günümüze kadar araçlarda da güvenli bir şekilde kullanılması için çalışmaların süreci her geçen gün artmaktadır.

1.3.1. Otonom Araçların Tarihi

1955 – Yılında Cenevre otomotiv fuarında tanıtılan araç Fiat 600, ilk arkadan itiş motorlu araç olmasıyla birlikte buz çözme özelliğine sahiptir.

1958 – Yılında, günümüzde kullanılan hız sabitleme sisteminin mekaniksel olarak ilk kez Chrysler marka araçta kullanılmış ve o dönemlerde otomatik pilot olarak isimlendirilmiştir.

1960 – Yılında, modern otomobillerin içerdiği karma yapılı sistemler, tasarım, biçim veya sahip olduğu teknolojik yenilikler vb. bakımından günümüzde kullanılan araçların ilk ortaya çıkış yılları olarak kabul edilmektedir.

1971 – Yılında, uçak sanayisinde farklı türlerde kullanılan sistem olan ABS(Anti-Lock Breaking System) ilk kez Chrysler Imperial araçlarında kullanılmak üzere tasarlanmıştır. Kaygan zeminlerde veya yüksek hızlarda aniden fren yapıldığında aracın kaymasını engellemektedir.

1987 – Yılında, genelde uçaklarda hava yastığı sistemi kullanılmaktadır. Uçak sanayisinden otomotivde de kullanıma geçen hava yastığı sistemi, Porsche markası tarafından araç içerisinde bulunan tüm koltuklara uygulanmıştır.

2003 – Yılında, sürücüler araçlarını kendi kontrolüyle park edilirken 2003 yılında otomatik park sistemi geliştirildi. Bu sistem, sürücüye gerek duymadan aracın dış dünyayla olan iletişim sonucunda park edebilmesini sağlayan sistemdir.

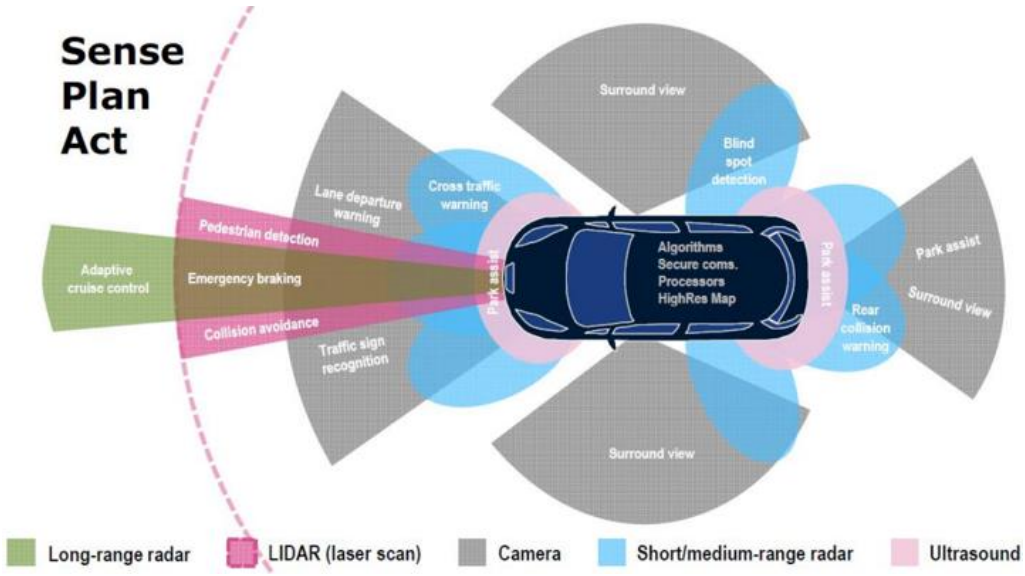
2010 – Yılında, otomatik park sistemi gibi bir çok benzer sistemler oluşmuştur. Fren, şerit takip, yokuş kalkış vb. amaçlar doğrultusunda tasarlanan sistemler, otomatik pilotun ilk adımları sayılabilmektedir. Dolayısıyla, otonom kavramı belirginleşmeye başlamıştır.

2014 – Yılında, Tesla firmasının üretmiş olduğu oto pilot etrafındaki bir çok nesneyi algılayabilen ve gerekli durumlarda onların durumuna göre araca tepki

gösteren sistemlerden oluşturulmuştur. Örneğin, önüne aniden bir yayanın veya cismin geldiğini gören Tesla Oto Pilot, sürücü fark etmeksizin ani fren yapabilmektedir.

2020 – Yılında, otonom araçlar artık kendi kendini araç içerisinde bir sürücü olmadan da yönetebilmektedir. GPS, sensörler, sensör haberleşmesi, cihazlardaki gömülü yazılımlar aracılığıyla otonom araçların seyahat etmesi için insan gücüne olan ihtiyaç ortadan kalkmıştır (Ardatürk, 2022).

Günümüz itibariyle, otonom araçlarda yaygın olarak park sensörleri, ateşleme sistemleri, konum sensörleri vb. Kullanılmaktadır. Bu sistemlere ek olarak, otonom araçlar için en önemli sistemlerden biri lidar sistemleridir. Lidar sistemi, otonom araçların çevre ile iletişimini sağlamaktadır. Araç etrafında bulunan engellerin konumu tespit edip aracı bilgilendirmektedir. Lidar sensörden gelen bu verilerle araç, uyarıcı etkiyi alıp içerisinde bulunan şartlar doğrultusunda çalışmaktadır. Lidar sistemine ek olarak, kızıl ötesi kameralar veya ultrasonik sensörlerde bu işlevlerde çalışmaktadırlar. Otonom araçların çevreyle iletişimleri kendilerini yönetmek için önemlidir. Dolayısıyla bulunduğu çevredeki nesne veya canlıları iyi tanımlaması araçların karar verme algoritmalarının doğruluğunu artırmaktadır. Bu algoritmalara örnek olarak otonom araçların hız ayarlama sistemleri (Cruise Control) ile GPS(konum algılama) sistemiyle birlikte çalışarak aracın hızını ayarlayabilmektedir (Gökozan, Taştan, 2018).



Şekil 1.1 Otonom Araç Sürüş Teknolojileri (Gürtaş, 2020)

Aracın çevresinde bulunan sensörler ile çevresiyle sürekli etkileşim içerisindedir. Dolayısıyla, otonom araçların karar verme algoritmaları bu etkileşimlere göre oluşmaktadır. Verilen kararlar doğrultusunda, otonom aracın kendini yönetme yetkinliği bu yapı içerisinde çalışır. Aracın karşısına bir engel çıktığında frenleme veya yönünü değiştirme kararı, içerisinde tanımlanan yazılımsal donanımla belirlenmektedir. Farklı bir örnek olarak, otonom araçlar, otomatik park yaparken geri hareket esnasında bir cisimle karşılaştığında ne zaman fren yapması gerektiğini, yine içerisinde bulunan yazılımsal donanıma göre belirlemektedir. Sonuç olarak, otonom araçların karar verme algoritmalarına bakılarak güvenli olup olmadığı hala tartışma konusudur. Bundan dolayı, otonom araçların kullanımına göre dünya üzerinde uygulanan kanunlar bulunmaktadır.



Şekil 1.2 Otonom Araçların Sürüş Seviyeleri (Bakioğlu, Atahan, 2021)

Şekil 1.2'de görülen seviyeler, otonom araçlar için geçerlidir. Dünya üzerinde ki birçok ünlü otomotiv markası 3. seviyededir. 5. Seviye, otonom araçlar için en üst

seviyedir. Bu seviyede sürüşün tüm kontrolleri araca ait olmaktadır. Dolayısıyla, hala birçok ülke bu seviyeye geçmek için hazır değildir.

Tüm kontrollerin araca ait olması, insana ihtiyaç olmaması anlamına gelmektedir. Dolayısıyla, bu durum aracın etrafındaki tüm nesnelerle etkileşimde kalmasını gerektirir. Sürekli haberleşme içerisinde olan otonom araçlar, kendi içlerindeki donanımlar, hatta etrafındaki diğer araçlarla dahi etkileşimde olmaktadır. Bu haberleşme yapılarından doğan etkileşim, kablosuz bağlantı olarak dahi yapılabilmektedir. Örneğin, GPS sensörlerinin çalışması için uyduya bağlanılması gerekmektedir. Uyduya bağlanmak içinse radyo dalgaları kullanılmaktadır. Metal tel üzerinden akım geçmesiyle radyo frekansı oluşmaktadır. Bu frekansların dalgaları ise elektromanyetik dalgalardır. Bu dalgalar atmosfer ortamında yayılarak haberleşmeyi mümkün kılmaktadır. Kablosuz iletişimi sağlayan radyo dalgaları ile otonom araçlar, GPS gibi bir çok sistemde diğer sistemlerle haberleşmeyi mümkün kılmaktadır. Farklı bir örnek olarak, araçlar kapı kilit sistemlerini açmak için anahtarları ile sürekli etkileşim içerisindedir. Bu etkileşim radyo dalgaları kullanılarak yapılmaktadır. Dolayısıyla, otonom araçların en önemli kullanım alanlarından olan radyo dalgaları da bu teknoloji ile birlikte gelişmeye devam edecektir.

1.4. Otonom Araçların Güvenliği

Otonom araçlar ve IoT sistemleri üzerinde yapılan araştırmalar, güvenlik ve performans iyileştirmeleri konularında önemli ilerlemeler sağlamaktadır. Aşağıda, bu alandaki literatür özetlenmiştir.

Li ve arkadaşları (2024), derin sinir ağı (DNN) tabanlı kamera yeniden konumlandırma modülünün özerk araçlarda kullanımını kolaylaştırmak amacıyla bir kenar bulut işbirliği çerçevesi önermişlerdir. Bu çerçeve, belirli modüllerin sunucuya aktarılması ve farklı ağ segmentasyonu şemaları altında veri çerçevelerinin çıkarım süresinin değerlendirilmesi ile ilgili kararları yönlendirmektedir. Deneysel sonuçlar, önerilen çerçevenin etkinliğini doğrulamaktadır (Li et al., 2024). Özerk araçların navigasyon ve kontrol sistemleri üzerine yapılan araştırmalar, bu araçların şehir içi karmaşık ortamlarda daha etkili ve güvenli bir şekilde hareket etmelerini sağlamayı amaçlamaktadır. Bu bağlamda, Ghintab ve Hassan (2024) tarafından yapılan çalışmada, araç kontrolü için orantılı türevsel entegral benzeri tip 2 bulanık mantık

kontrolörü (PID-like IT2FLC) kullanılarak, araçların hareket kontrol stabilitesinin, hassasiyetinin ve verimliliğinin artırıldığı belirtilmiştir. Araştırma, araçların yerleşimini daha doğru bir şekilde lokalize etmek için kullanılan minimal konvolüsyonel sinir ağı (CNN) ve A* algoritmasının etkinliğini vurgulamaktadır.

Diğer bir çalışma olan Li ve arkadaşlarının (2024) araştırması, özerk araçlar için DNN tabanlı kamera yeniden konumlandırma modülünün sunucu tarafı hesaplama ile geliştirilmesine odaklanmıştır. Bu çalışma, araçlarda yerleşik yüksek performanslı hesaplama donanımlarına olan ihtiyacı azaltmayı ve kenar bulut işbirliği çerçevesi kullanarak hesaplama yükünü sunucu tarafına aktarmayı amaçlamaktadır

Ek olarak, Naiseh ve arkadaşları (2024) tarafından yapılan çalışma, özerk araçların toplum tarafından kabul edilmesi üzerine odaklanmış ve sosyal etkiler ile başlangıçtaki güvenin bu kabulde önemli belirleyiciler olduğunu ortaya koymuştur. Bu çalışma, özerk araçlarla insan etkileşimlerinin davranışsal yönlerini ve teknolojiyi benimseme süreçlerini detaylı bir şekilde ele almaktadır.

Son olarak, anonimlik ve güvenlik, heterojen bağlantılı araç ağlarında önemli bir yere sahiptir. Bu konuda yapılan çalışmada, kimlik doğrulama şemaları ve anonim kimlik doğrulama çerçevesi üzerinde durulmuş, araçlar arası iletişimde güvenliğin nasıl sağlanabileceği üzerine çeşitli yöntemler sunulmuştur (Sivasankari ve d., 2024).

Bu tezin bilime katkıları aşağıda sunulmuştur.

Radyo Frekans Saldırılarına Karşı Güvenlik Önlemleri: Bu çalışma, otonom araçların radyo frekans (RF) saldırılarına karşı nasıl korunabileceği konusunda detaylı analizler ve çözümler sunmaktadır. Bu, otonom araçların güvenliğini artırmak için önemli bir katkıdır.

RF Saldırı Tespit ve Önleme Yöntemleri: Bu çalışma, RF saldırılarını tespit etmek ve önlemek için çeşitli yöntemler geliştirmiştir. Bu yöntemler, sadece otonom araçlar için değil, diğer radyo frekans ile çalışan cihazlar için de uygulanabilir, bu da daha geniş bir güvenlik çözümü sunar.

Teknik Gelişmeler ve Uygulamalar: Çalışmada kullanılan teknikler ve geliştirilen yazılımlar, RF saldırılarını daha etkili bir şekilde tespit etme ve önleme kapasitesine sahiptir. Bu teknikler ve yazılımlar, mekatronik mühendisliği alanında önemli bir yenilik olarak değerlendirilebilir.

Pratik Uygulama ve Deneysel Sonuçlar: Tez, teorik bilgileri pratiğe dökerek deneysel sonuçlarla desteklemiştir. Bu, teorik çalışmaların gerçek dünya uygulamalarında nasıl performans gösterdiğini gösterir ve diğer araştırmacılara bu alanda yol gösterici olur.

Otonom Araç Teknolojilerinin Gelişimi: Otonom araçlar, geleceğin ulaşım teknolojilerinde önemli bir rol oynayacaktır. Bu çalışma, bu araçların güvenliğini artırarak, teknolojinin daha güvenli ve yaygın bir şekilde benimsenmesine katkıda bulunur.

İKİNCİ BÖLÜM

Çalışma içerisinde kullanılan sistemleri ve tanımlamaları bu bölümde verilmektedir. Teknik özellikleri ve genel özellikleri tanıtılarak donanımlar açıklanmıştır.

2.1. Hackrf One

Hackrf one yazılım tanımlı radyo sinyal cihazıdır (Gummineni, Polipalli, 2020). Half-Duplex (Yarı zamanlı) olarak çalışmaktadır. Yarı zamanlı çalışma, hackrf one cihazının aynı anda sinyalleri alırken verememesi veya verirken alamamasıdır. Hackrf one cihazı alıcı durumunda çalışıyorsa, sadece alıcı işlevi görmektedir. Verici durumunda çalışıyorsa, sadece verici işlevi görmektedir. Bu durum yazılım tanımlı radyo sinyal cihazları arasında yarı zamanlı çalışma olarak geçmektedir. Bunun haricinde, tam zamanlı olarak çalışan diğer çeşitleri de mevcuttur. Tam zamanlı çalışma algoritmasına sahip olan yazılım tanımlı radyo sinyal cihazları, herhangi parametreler doğrultusunda, sinyal alıcı olarak çalışırken aynı zamanda verici işlemini de yapabilmektedir. Örneğin, bir istasyondan sinyali alıp başka bir konuma sinyali eş zamanlı olarak iletebilmektedirler. Bu tip çalışma şekline ise tam zamanlı çalışma denmektedir. Gummineni ve Polipalli, hackrf one yazılım tanımlı radyo sinyal cihazı saniyede maksimum 20 milyon örnekleme frekansı (Samp rate) gönderebildiğini ifade etmektedir. Örnekleme frekansı, 1 saniyede toplanılan veriyi ifade etmektedir. Hackrf one cihazı saniyede 20 milyon sinyal formunda veriyi yakalayabilmektedir. Örnekleme hızının yüksek olması sinyallerin kalitesinde artış göstermektedir. Ancak kalite artışı ise bilgisayarların işlem gücünü oldukça fazla zorlamaktadır. Hackrf one cihazı, 1 Mhz ile 6 Ghz frekans aralığında bulunan sinyalleri yakalayıp işleyebilmektedir. Frekansların işlenmesinde hassasiyet oldukça önemli olmaktadır. Dolayısıyla, yüksek frekanslara çıkılması daha az hassasiyet alınmasına neden olmaktadır.



Şekil 2.1 Hackrf One

Şekil 2.1'de hackrf one cihazının genel görünümü gösterilmektedir. Kırımızı kapaklı olan kısımlar port kısımlarıdır. Şekil 2.1'de sağ uçta bulunan iki port, zamanlama portu olmaktadır. Genel olarak hassas zamanlama gerektiren işlemlerde kullanılmaktadır. Sol kısımda bulunan port ise anten portu olmaktadır. Hackrf one cihazına radyo sinyallerini algılamak veya iletmek için mesafesini artırmak amacıyla anten takılabilmektedir.



Şekil 2.2 Hackrf one anten

Hackrf one cihazına takılan anten şekil 2.2'de görülmektedir. Antenin cihaza takılması, cihazın alıcı gücünü artırmaktadır. Ayrıca antenlerin yapısına özel olarak, şekil 2.2'de görülenden daha uzun bir hale gelecek yapıya sahip olmaktadır. Dolayısıyla, antenin uzunluğuna oranla cihazın sinyalleri algılama veya iletme mesafesi artmaktadır.



Şekil 2.3 Hackrf one cihazı ve anten takılması

Şekil 2.3'te hackrf one cihazına anten takılarak cihazın sinyali algılama mesafesi arttırılmıştır. Antenin uzunluğu, çalışmaya uygun olarak artacak veya azalacaktır.

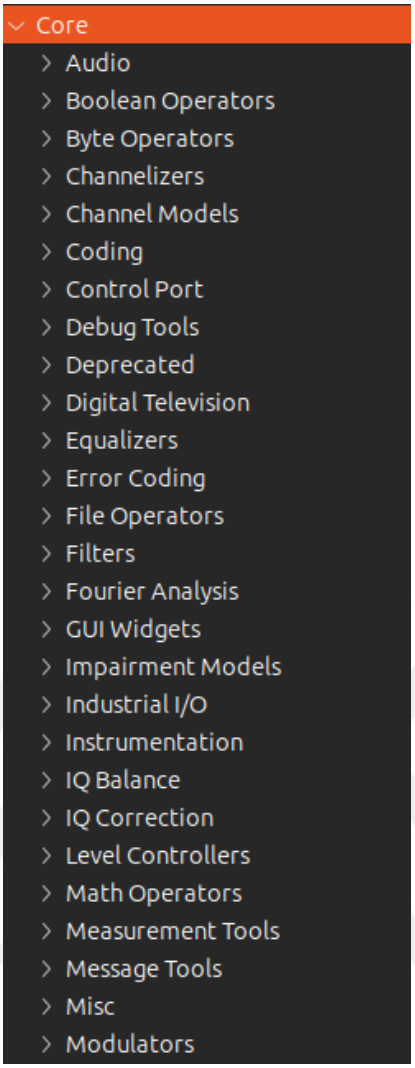
2.2. GNU Radio

Gnu radio, açık kaynak kodlara sahip yazılım tanımlı donanımların geliştiricisidir. Radyo sinyallerinin işlenmesi, sinyalleri yakalanması için gerekli parametrelerin belirlenmesi veya yakalanan sinyallerin gerekli parametrelerde tekrar iletilmesi gibi radyo sinyalleri üzerinde birçok işlemin yapılmasını sağlamaktadır. Örneğin, radyo dalgaları ile kablosuz olarak iletişimde bulunabilen cihazların ilettikleri ve aldıkları sinyallerin özellikleri farklı değerlerde olmaktadır. Ayrıca, sinyallerin iletiminde çevresel veya varsa cihazlardaki radyo dalgaları da mevcut olabilmektedir. Bunlar istenmeyen radyo dalgaları oldukları için bu dalgalara gürültü adı verilmektedir. Çünkü istenilen frekansın yakalanmasında engelleyici bir etkide bulunmaktadır. Dolayısıyla, alınması istenilen radyo dalgalarına karışan gürültü sinyalleri, Gnu Radio kullanılarak filtrelenebilmektedir. Sinyallerin yakalanması için uygun parametre değerlerinin ayarlanmasında ve aynı şekilde sinyali iletirken de aynı parametre değerlerini ayarlayarak iletmesini mümkün kılmaktadır (Haritha, Seethal, Gandhiraj, 2017). Bu işlemleri oluşturmak için içerisinde bulunan blokları kullanmaktadır. Blokların kullanılmasıyla oluşan diyagram, yazılım tanımlı radyo cihazları içerisinde çalışmaktadır. Bu cihazlara örnek olarak, hackrf one cihazı oluşturulan blok diyagramını çalıştırabilmektedir. Gummineni ve Polipalli, hackrf one cihazı C++ ve python ile kodlanıp kullanılabilmektedir. Gnu radio arayüzü ise Hackrf one cihazının kullanılmasını modüller aracılığıyla yapmaktadır. Gnu radio arayüzünde bulunan araçların, senkronize çalışması modül oluşturmaktadır. Bu modüller arka planda python kodlarını çalıştırmaktadır. Arayüzün asıl amacı sinyal işleme, birleştirme vb. işlemler için basit bloklar oluşturarak kullanılmasıdır. Gnu radio içerisinde birçok uygulama hazır olarak mevcuttur. Bu uygulamalar amaca göre hazır araçlar olarak kullanılabilmektedir (Schmid, 2006).



Şekil 2.4 Gnu radio arayüzü

Şekil 2.4'te gnu radio akış diyagram arayüzü görülmektedir. Arayüzde yapılan blokların yazılım tanımlı radyo sinyallerinde çalışması bu arayüzde oluşturulmaktadır. Üzerlerinde yapılacak herhangi parametre değişikliği de bu arayüzde yapılacak olan akış diyagramında değişebilmektedir.



Şekil 2.5 Gnu radio blok menüsü

Şekil 2.5 de gnu radio için kullanılacak olan bloklar gözükmektedir. Kategori halinde ayrılan blokların işlevleri birbirlerinden farklı olmaktadır. Örneğin, ses sinyalleri için kullanılacak bloklar audio kategorisinde iken, filtreleme işlemleri için kullanılan bloklar filter kategorisinde olmaktadır.

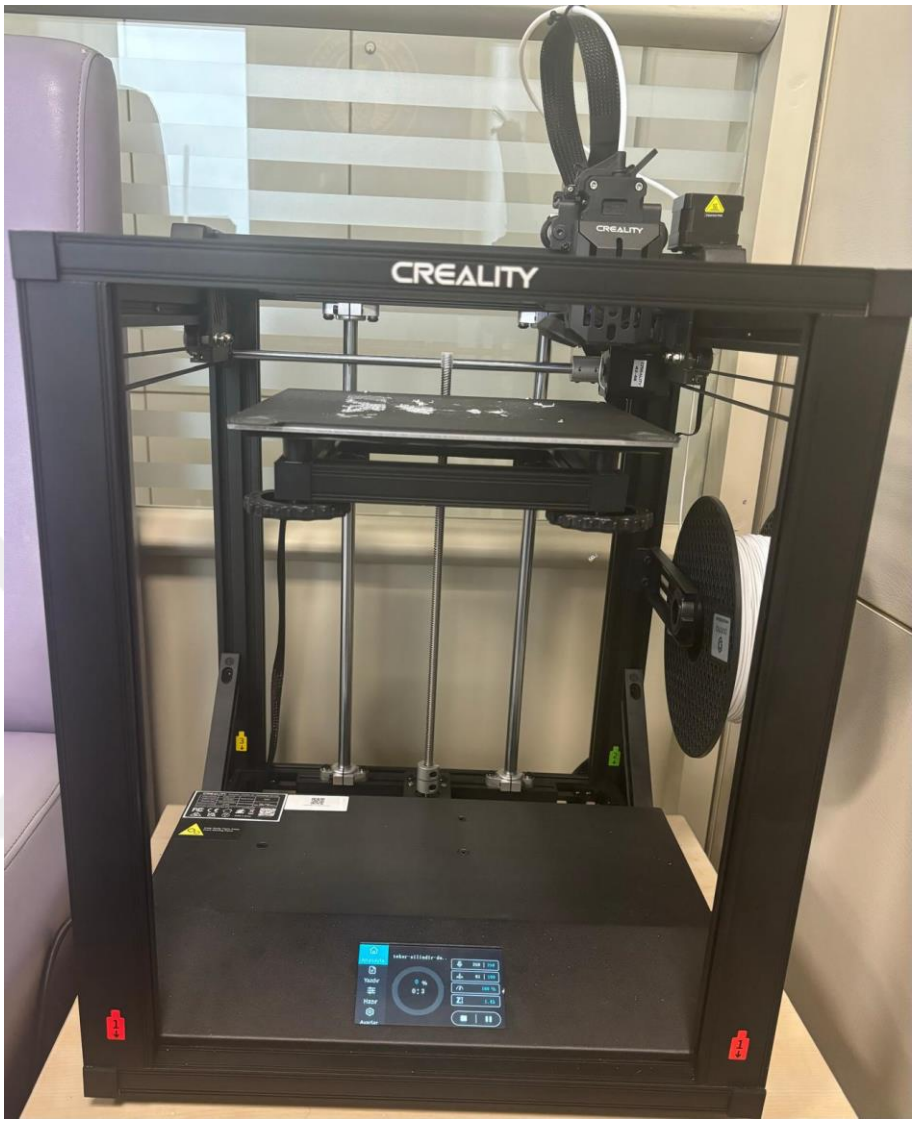
2.3. 3D Yazıcı

3 boyutlu yazıcıların (3d) ilk adımları 1980'li yıllara kadar uzanmaktadır. Sanayinin gelişmesiyle birlikte talaşlı imalatta bir ürünün oluşturulması için malzemenin çoğunluğu talaş olarak belirlenir. Ayrıca, malzeme üzerinde yapılacak olan bir hatanın geri dönüşü olamadığı içinse malzemenin çöp olma ihtimalide bulunmaktadır. Bir ürün için ilk prototip, sanayide oldukça önem arz etmektedir.

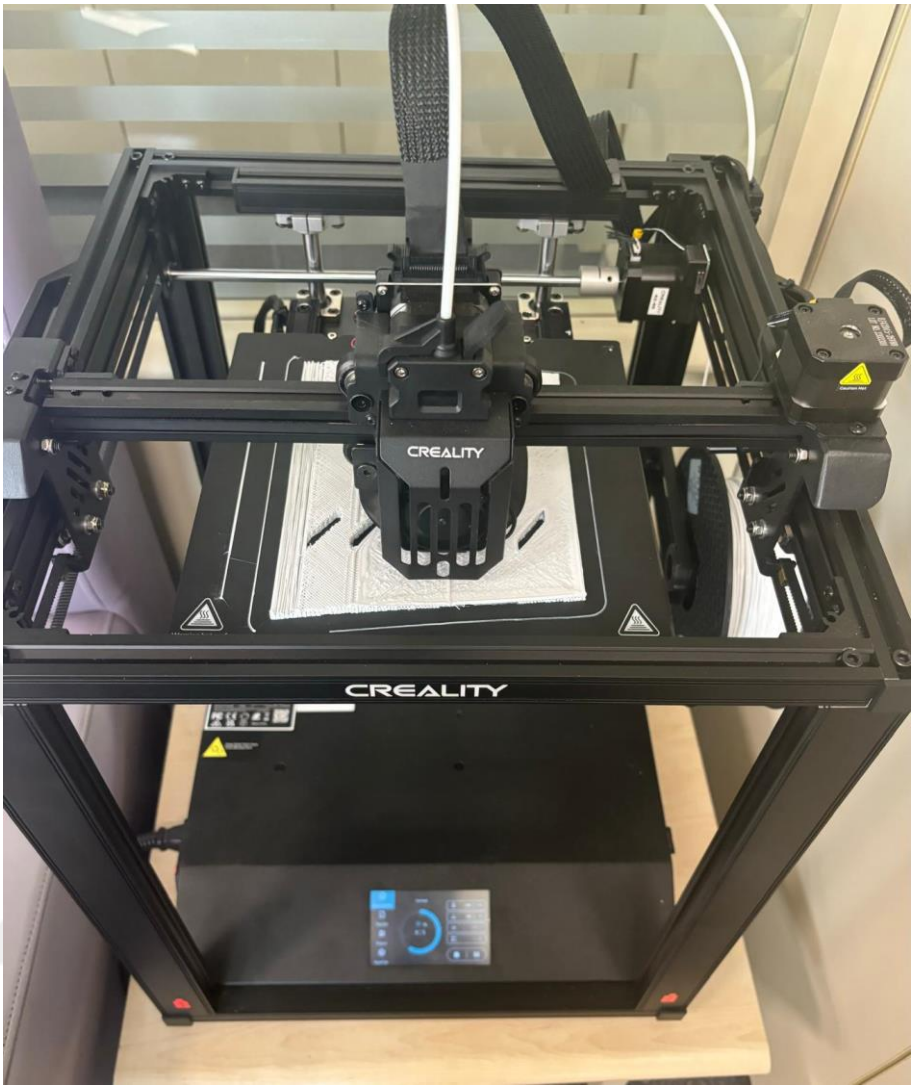
Çünkü prototip sayesinde ürünün istenilen özelliklerde olup olmadığı veya tasarımında ya da üretiminde herhangi sorunla karşılaşılması durumları analiz edilebilmektedir. Dolayısıyla, ilk prototip ürünün yeri oldukça önemlidir. Buna göre, bu prototipin üretilmesi için yapılacak olan işlemler pahalı olabilmektedir. Pahalı olabildiği gibi, ürünlerin üretim süreci çok uzun olabilmektedir. Üstelik, bu süreçte yapılacak veya tasarımda yapılacak bir hata sonucu tüm işlemlerin baştan yapılması gerebilir. Bu duruma istinaden, bilgisayar destekli tasarım programları aracılığıyla tasarım ve imalatın gelişmesiyle 3 boyutlu yazıcılar geliştirilmiştir. 3 boyutlu yazıcılar herhangi bir kesme veya delme işlemi yapmaz (Yılmaz, Arar, Koç,2013). Bilgisayar destekli tasarım programları ile oluşturulmak istenen ürün tasarlanır. Tasarlanan model 3 boyutlu yazıcıya verilmeden önce 3 boyutlu yazıcının uyumlu olduğu tasarım programında tanımlanır. Ürünün kıvrımları, kenarları, köşeleri gibi sahip olduğu geometriyi oluşturması için önce bilgisayarda çözümlenir. 3 boyutlu yazıcılar için yapılan tasarımları açabilen dosyaların formatı genellikle STL olmaktadır. Programda tanımlanan 3 boyutlu model yazıcıya aktarıldığında, yazıcı içerdiği malzemeyi eriterek katmanlar halinde üst üste enjekte etmektedir (Güleryüz, 2021). 3 Boyutlu yazıcılarda ABS veya PLA vb. plastikler kullanılmaktadır. Malzemelerin kullanım alanlarına göre birbirlerinden farklı avantajları ve dezavantajları bulunmaktadır (Günay, Gündüz, Yılmaz, Yaşar, Kaçar, 2020).

3 boyutlu yazıcılar geliştikçe birçok sektörde kullanılmaya başlanmıştır. Otomotiv sanayisi, tıp, inşaat vb. birçok alanda faaliyet göstermektedir. Kullanılan alanlara göre ise malzemeler ve 3 boyutlu yazıcıların özellikleri değişmektedir. Yılmaz vd. 3 boyutlu yazıcılar teknolojinin gelişmesiyle farklı üretim teknikleri ortaya çıktığını ifade etmektedir. Örneğin, FDM (Fused Deposition Modeling) plastik gibi malzemeler 3 boyutlu yazıcının nozul kısmında ısınarak eritilir. Eritilen malzeme, nozuldan basınç yaparak çıkmasıyla sertleşmeye başlar. Sertleşmesinden hemen sonra malzemeyi sıkıştırarak katmanlar oluşturur. Katmanların sonucunda ise istenilen ürün ortaya çıkmaktadır (Kun, 2016). Diğer bir üretim tekniği ise SLS (Selective Laser Sinterin) üretim tekniği olmaktadır. Bu üretim tekniği, ürünün oluşturulması için toz halinde olan maddeyi, lazer ışını kullanarak yüksek sıcaklık veya basınçta katman halinde birleştirmektedir. Ürün oluşturulana kadar bu işlem katmanlar halinde devam

etmektedir. Bu teknik, karmaşık geometriler için idealdir ve ayrıca metal üretimde yapabilmektedir (Hussain, Khan, Ashraf, Ahmad, Ahmad, Imran, 2019).



Şekil 2.6 Creality Ender 5S 3 boyutlu yazıcı



Şekil 2.7 3 Boyutlu yazıcı parça basımı

2.4. Gömülü Sistem

Gömülü sistemlerin ilk çalışmaları 1961 yılında yapılmaktadır. Yıllar boyunca gelişmekte olan ve teknolojinin temel yapısını oluşturan gömülü sistemler, günümüzde birçok alanda kullanılmaktadır. Günlük hayatta karşımıza çıkan ATM cihazları, araçlar, yazıcılar, bilgisayarlar vb. birçok cihazda kullanılmaktadır. Gömülü sistemlerin bu cihazlara verdiği ortak özellik ise bir algoritma oluşturulmasını sağlamaktır. Bu algoritmanın oluşturulmasıyla, istenilen cihaza istenilen işlevin yaptırılması mümkün olabilmektedir. Örnek olarak, trafik ışıklarının ne kadar süre ile yeşil veya kırmızı ışığı göstermesi, sahip olduğu gömülü sistemin içerisindeki algoritma ile belirlenmektedir. Bir insan gücüne ihtiyaç duymadan bu işlevi

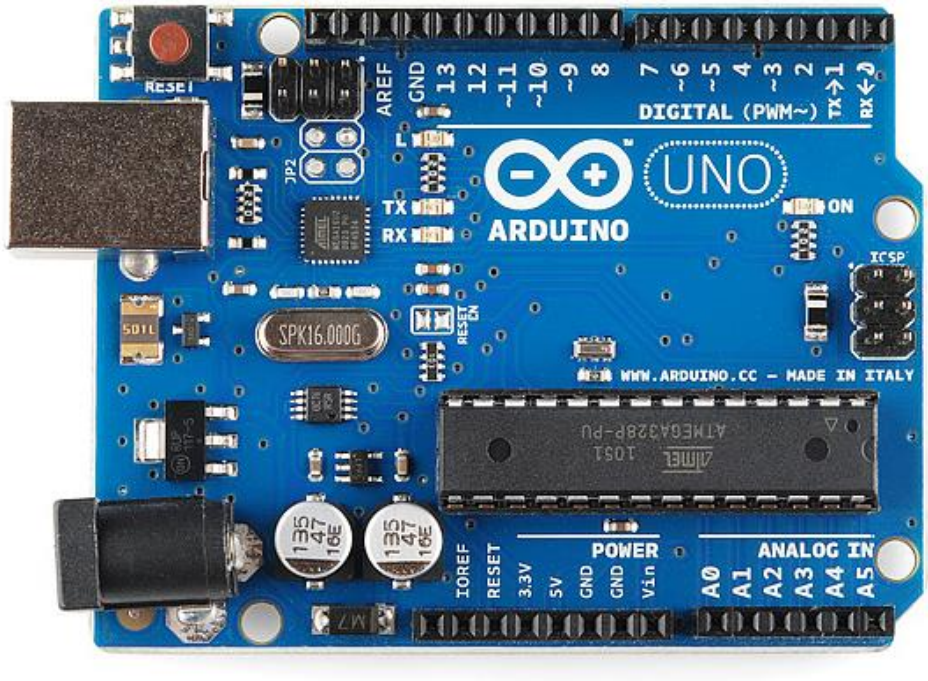
tekrarlamaktadır. Dolayısıyla gömülü sistemler, herhangi bir işlemi gerçekleştirmek veya sorgulamak için kullanılan sistemlerdir. Bu sistemler, fiziksel araçlara entegre edilebilmektedir. Gömülü sistem içerisinde ki algoritmalar, bir karar aşamasına bağlı çalışmaktadır. Bu kararların belirlenmesi için algoritma oluşurken belirli şartlar girilmektedir. Bu şartlar, sistemin nasıl çalışacağını belirlemektedir. Kısacası, gömülü sistemler bir akış diyagramı oluşturarak bu diyagramın dışına çıkamamaktadır (Doğru, 2012). Bu algoritmaların çalışmasıyla sistemler yönetilir. Sistemlerin yönetilmesini sağlayan donanım ve algoritma yazılımların iletişimini sağlayan genel sisteme ise işletim sistemi denilmektedir. İşletim sistemi, donanımların ve yazılımların haberleşmesini sağlayan bir arayüz görevi görmektedir. Belirtilen şartlar içerisinde koordineli ve sürekli olarak çalışmasını sağlamaktadır. İşletim sistemi içerisindeki yazılımların programlaması içinse uygulama programlama ara yüzleri kullanılmaktadır. Ayrıca, işletim sisteminin kullanılacağı alanlara göre içerdiği uygulama alanları da farklı olacağından dolayı programlara arayüzleride farklılık gösterebilmektedir (Boyaci, 2010).

Bu çalışma için üretilecek olan algoritma yazılımlarının donanımlarla iletişimi sağlamak için arduino gömülü sistem uygulama geliştirme kartı kullanılacaktır. Arduino uygulama geliştirme kartı için kullanılacak olan yazılım arduino IDE yazılımıdır. IDE (Integrated Development Environment) tanımı entegre geliştirme ortamı olarak tanımlanmaktadır. Arduino uygulama geliştirme kartının programlanması için kullanılmaktadır.

2.4.1. Arduino Uygulama Geliştirme Kartı

Arduino, günlük hayatta karşılaşabileceğimiz elektromekanik sistemlerin programlanmasında kullanılan uygulama geliştirme kartlarının en basit sistemlerindendir. Genel olarak bulunabilirliği ve kolaylığı açısından eğitim amaçlı olarak kullanılmaktadır. Arduino geliştirme kartları, benzer olarak diğer geliştirme kartlarının yapabildiği birçok işlevi yapabilmektedir. Bilgisayarlarla iletişim kurabilen veya internete erişimine mümkün olmaktadır. Görüntü, ses, ışık, sensör çalışmalar vb. durumların kontrol edilmesini veya işlemesini sağlayabilmektedir. Örneğin, bir kameradan veri alabilir ve aldığı veriyi işleyerek güvenlik çalışmalarında kullanılabilmektedir. Diğer bir kullanım örneği olarak, bir ortamın sıcaklığını kontrol ederek gerekli durumlarda klimayı açıp kapatabilmektedir (Koçak, Kırbaş, 2016).

Bunun gibi birçok çalışmaları yerine getirebilmektedir. Bu çalışma kapsamı için örnek vermek gerekirse, araçlardaki cam açıp kapama veya araç kapılarının kilitlerini açıp kapama işlemini yapabilmektedir. Arduino üzerinde ATmega328 mikrodenetleyici bulunmaktadır. Mikrodenetleyiciler, bir işlevi yerine getirmek için programlanabilen çipler olmaktadır. Arduino üzerinde bulunan portların yönetimi mikrodenetleyici çip ile gerçekleştirmektedir. Portlara bağlanan donanımların çalışması ise farklılık göstermektedir. Kontrol etme görevine sahip sensörler, input (Giriş) olarak tanımlanırken, herhangi bir işlevi gerçekleştirecek olan donanımlar output (Çıkış) olarak tanımlanmaktadır. Inputlar, takılan donanımın özelliğine göre arduino da işlenmesi için veri girişi yapmaktadır. Outputlar ise arduino da işlenen verilere göre işlevi gerçekleştirmektedir.



Şekil 2.8 Arduino Uygulama Geliştirme Kartı

Şekil 2.8 de arduino uygulama geliştirme kartı görülmektedir. Kart üzerinde 13 adet dijital çıkış bulunmaktadır. 6 adet analog girişi bulunmaktadır. Analog girişler input olarak çalışmaktadır. Alınan verileri arduino içerisine taşımaktadırlar. Dijital çıkışlar ise output olarak çalışmaktadır. Arduino da verinin işlenmesine göre bir sistemi çalıştırabilirler. Örneğin, bir led lambayı yakıp söndürebilirler. Dijital çıkışlardan 3,5,6,10,11 numaralı çıkışlar analog çıkış olarak da kullanılabilmektedir.

Bu çıkışların analog olarak çalışması ise yanlarındaki analog çizgisinden anlaşılmaktadır. Örneğin, ortamın sıcaklığını ölçen sensör analog girişinden veriyi arduinoya iletir. Arduino, veri girişini işleyerek analog çıkışların bağlı olduğu fanın çalışma hızını belirleyebilmektedir. Arduino üzerinde topraklama (GND) ve besleme (5V) portları bulunmaktadır. Sisteme güç vermek için bu portlar kullanılmaktadır. Arduino maksimum 5V olarak çalışmaktadır. Dolayısıyla outputlara takılan donanımların çalışma voltaj aralığı 5V alında olmalıdır.

ÜÇÜNCÜ BÖLÜM

Çalışma kapsamında gerçekleştirilen otonom araçlara yönelik prototip tasarlanmıştır. Bu tasarımla birlikte aracın içerisine elektronik devre entegre edilmiştir.

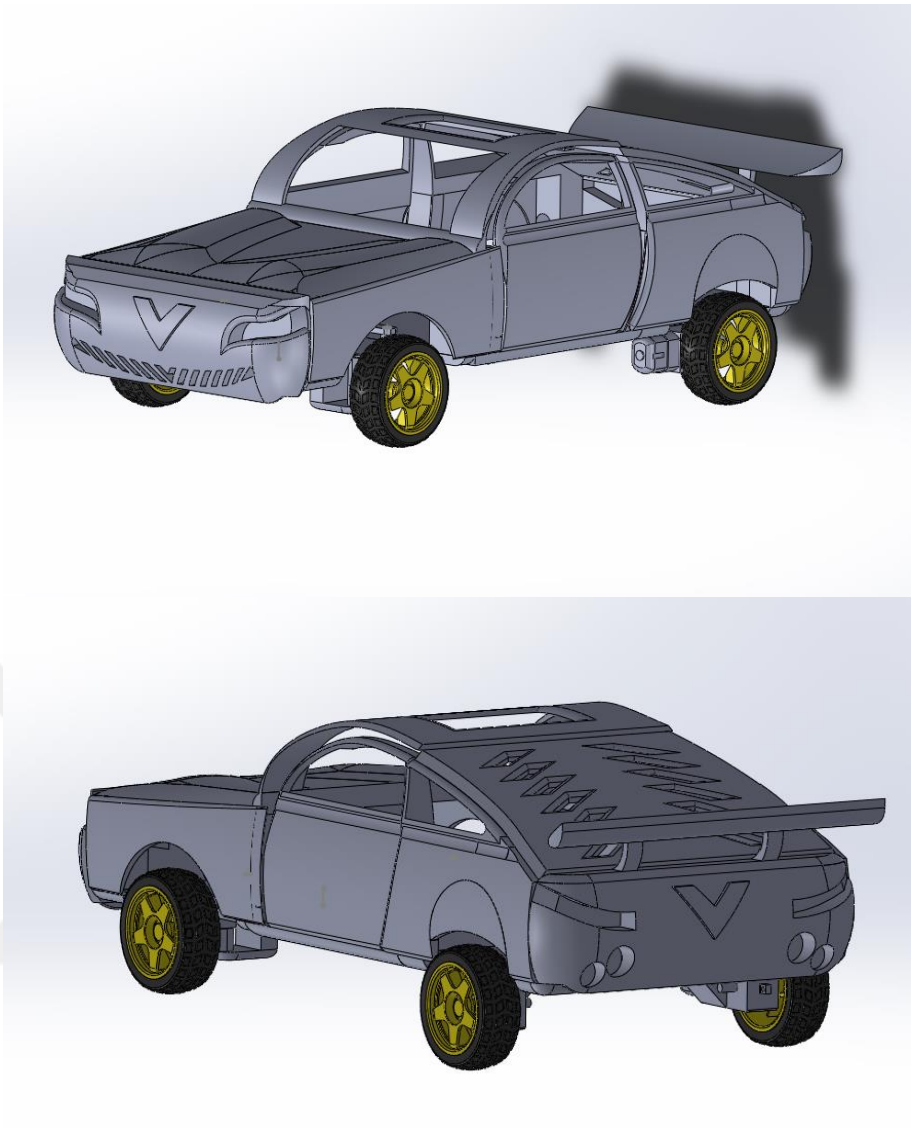
3.1. Otonom Araç Tasarımı

Çalışma için üretilen prototip araç, solidworks 3 boyutlu tasarım programında tasarlanmıştır. Tasarımın oluşturulma aşamasında, elektronik sistemin içerisine eklenmesi düşünülmüştür. Dolayısıyla, araç parçalarının öncelik olarak parça parça çizimi tamamlandıktan sonra sistem üzerinde montajlanması yapılmıştır. Tasarım aşaması, aracı oluşturmak için önemli rol oynamaktadır. Çünkü tasarım aşamasında aracın yapılması esnasında oluşabilecek hatalar öngörülebilmektedir. Dolayısıyla, solidworks bilgisayar destekli tasarım programı çalışma için kullanılmıştır.



Şekil 3.1 Araç sağ ve sol kapıları tasarımları

Şekil 3.1 de üretilen prototip aracın kapı tasarımlar verilmiştir. Araç parçaları şekil 3.1 de olduğu gibi birbirinden ayrı olarak tasarlanmış ve montajlanmıştır.



Şekil 3.1 Araç tasarımı ön çapraz görünümü (a) ve araç tasarımı arka çapraz görünümü (b)

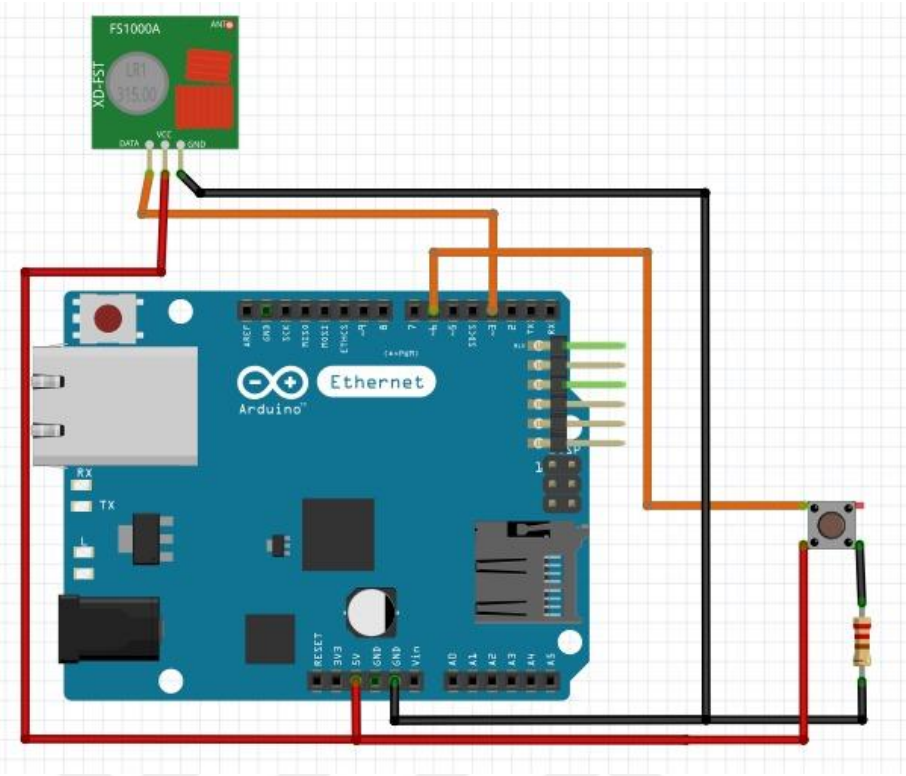
Şekil 3.2 de prototip aracın, parçaların tasarımı bittikten sonra montajlanmış hali görülmektedir.



Şekil 3.3 Araç arkası görünüm (a) ve araç ön çapraz görünüm (b)

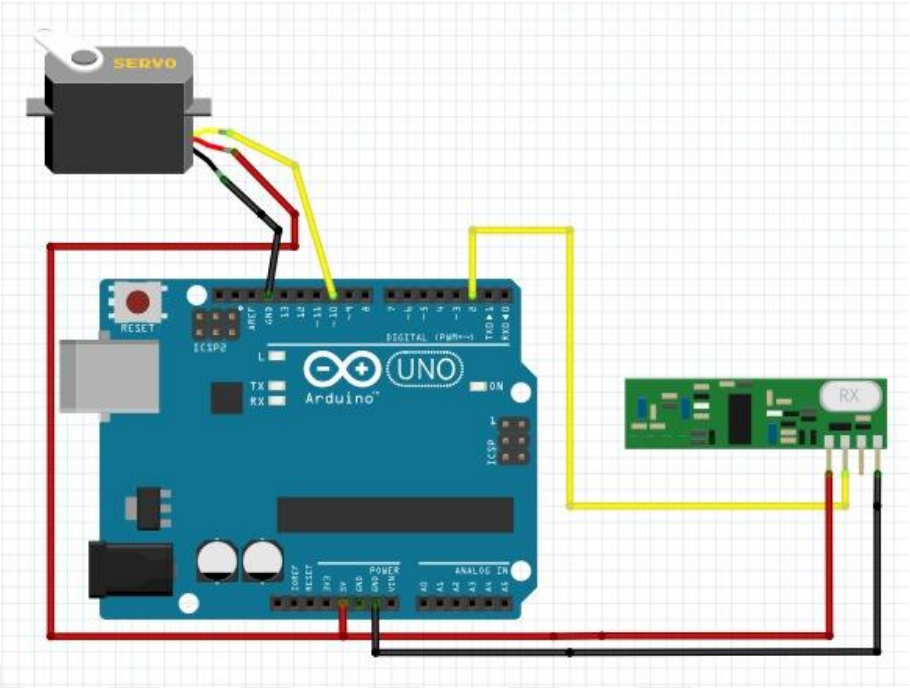
3.2. Otonom Araç Elektronik Şeması

Araçlarda kullanılan elektronik sistem oluşturulmuştur. Araç kapı kilitlerine bağlı motor, araçta bulunan arduinoya bağlanmıştır. Arduino kumandadan aldığı sinyaller ile motoru çalıştırmaktadır.



Şekil 3.4 Araç kumanda elektronik şeması

Aracın kumandasında kullanılan arduino kartına, 433 Mhz frekansta çalışan radyo frekans vericisi takılmıştır. Ayrıca, aracın kapılarının açılıp kapanması için buton konulmuştur. Butona basıldığında, aracın kapısının açılması için sinyal gönderim işlemi başlamaktadır. Sinyal, 433 Mhz frekans verici aracılığıyla aracın alıcısına iletilmektedir.



Şekil 3.5 Araç içi elektronik şeması

Şekil 3.5 de araç içerisindeki elektronik şema görülmektedir. Kumanda tarafından gönderilen sinyal 433 Mhz frekans alıcısında algılanmaktadır. Algılanan sinyalin işlemine göre aracın kapılarının açılması için motoru harekete etmektedir.

DÖRDÜNCÜ BÖLÜM

4.1. Mevcut Araç Anahtar Yazılım

Araçlarda kullanılan araç anahtar arasındaki haberleşme, radyo frekansları kullanılarak yapılmaktadır. Kullanıcı, aracın kapısını açmak için anahtarı üzerindeki tuşa bastığında, araca sinyal gönderilmektedir. Gönderilen sinyalle aracın kapılarının açılması üzerine olan sinyali algılayıp kapıları açacaktır. Her araç için birbirinden farklı parametrelerde olan bu sinyaller, bir başka araç için işlevsiz olmaktadır. Ancak, parametrelerin doğruluğunun sağlanmasıyla başka araçlarında bu sinyali işlemesi mümkün olmaktadır. Bu çalışma kapsamında, araçların anahtarları ile arasındaki haberleşme sistemi yapısı, arduino ve 433 Mhz alıcı verici cihazı kullanılarak yapılmıştır.

```
int default_ac = 7;
int default_kapat = 8;
bool default_acOnce = false;
bool default_kapatOnce = false;
void setup() {
  pinMode(default_ac, INPUT);
  pinMode(default_kapat, INPUT);
  mySwitch.enableTransmit(3);
}
void loop() {
 if (digitalRead(default_ac) == HIGH && !default_acOnce) {
    mySwitch.send(3000, 24);
    delay(500);
    default_acOnce = true;
  }
  if (digitalRead(default_kapat) == HIGH && !default_kapatOnce )
  {
    mySwitch.send(4000, 24);
    delay(500);
    default_kapatOnce = true;
  }
}
```

Şekil 4.1 Araç anahtar yapısı

Şekil 4.1 de aracın kumandasında bulunan sistem görülmektedir. Anahtar üzerindeki kapıları açma veya kapatma tuşlarına basıldığında birbirinden farklı

parametreler gönderilmektedir. Araç bu parametreleri tanımlayarak kapılar üzerindeki işlevini yapabilmektedir.

```
#include <Servo.h>
int servoPinSag = 10;
int servoPinSol = 8;
Servo servoMotorSag;
Servo servoMotorSol;
RCSwitch mySwitch = RCSwitch();
void setup() {
  pinMode(sag_kapi, OUTPUT);
  pinMode(sol_kapi, OUTPUT);
  servoMotorSag.attach(sag_kapi);
  servoMotorSol.attach(sol_kapi);
  mySwitch.enableReceive(0);
}
void loop() {
      if (receivedValue == 3000 ) {
       servoMotorSag.write(90);
       servoMotorSol.write(90);
       mySwitch.resetAvailable();
       delay(1000);
      }
      if (receivedValue == 4000 ) {
       servoMotorSag.write(0);
       servoMotorSol.write(0);
       mySwitch.resetAvailable();
       delay(1000);
      }
```

Şekil 4.2 Araç kapı kilit yapısı

Şekil 4.2 de aracın kapıları açan veya kapatan algoritma görülmektedir. Aracın kapılarına servo motor bağlanmıştır. Servo motor, yazılımı oluşturmak için kütüphanesi arduino içerisinde eklenmiştir. Anahtardan gelen sinyali algılayıp içerisinde işleyen araç yapısı, sinyalin yapısına göre kapılar üzerinde ki işlevini tamamlamaktadır.

4.2. Geliştirilen Araç Anahtar Yazılımı

Geliştirilen sistem alıcı ve verici olmak üzere iki bölümden oluşmaktadır.

4.2.1. Araç Kumandası Radyo Frekans Verici Donanım Yazılım

Araç ile anahtar arasındaki sinyal haberleşmesinin güvenliği için geliştirilen yazılımda donanımsal cihazlardan dolayı bazı yazılım kütüphaneleri kullanılmıştır.

```
#include <RCSwitch.h>
RCSwitch mySwitch = RCSwitch();
```

Şekil 4.3 Alıcı yazılım kütüphaneleri

Şekil 4.3'te, araç anahtar içerisinde bulunan yazılımda RC Switch kütüphanesi kullanılmıştır. Anahtar içerisinde bulunan sinyal gönderici donanımın çalışması için arduino gömülü sistemde bu kütüphanenin kurulması gerekmektedir.

```
#include <RCSwitch.h>
RCSwitch mySwitch = RCSwitch();
int kapi_ac = 5;
int kapi_kilit = 6;
bool kapi_acOnce = false;
bool kapi_kilitOnce = false;
unsigned long kapi_ac_dizi[200];
unsigned long kapi_kilit_dizi[200];
int kapi_ac_dizi_sayi = 0;
int kapi_kilit_dizi_sayi = 0;
void setup() {
  pinMode(kapi_ac, INPUT);
  pinMode(kapi_kilit, INPUT);
  mySwitch.enableTransmit(3);
  randomSeed(analogRead(A0));
  Serial.begin(9600);
}
```

Şekil 4.4 Verici yazılım değişen tanımlama

Şekil 4.4'te, anahtar sistemi içerisinde bazı parametreler tanımlanmıştır. Anahtar sistemi için 2 adet buton bulunmaktadır. Bunlardan biri araç kapılarının kilidini açmak için diğeri ise araç kapılarının kilidini kapatmak için kullanılmaktadır. Yazılım içerisinde arduino kartının 5 numaraları dijital çıkışı kapıların açılmasını sağlayan butona, 6 numaralı dijital çıkışı ise kapının kilitlenmesini sağlayan butona

tanımlanmıştır. Bu butonlara basılıp basılmamasını kontrol etmek için ise bool (boolean) komutu kullanılarak sorgulanmaktadır.

Sisteme tanımlanan diğer bir bölüm ise dizi algoritmasıdır. Bunun için kapi_ac_dizi ve kapi_kilit_dizi adında 200 karakter içerebilen 2 adet dizi tanımlanmıştır. Bu dizilerinin içerisinde ne kadar değişken olduğunun gösterilmesi içinse kapi_ac_dizi_sayi ve kapi_kilit_dizi_sayi adında 2 adet değişken tanımlanmıştır.

Arduino uno içerisinde tanımlanan kapi_ac ve kapi_kilit değişkenleri, sistemde INPUT modu olarak tanımlanmıştır. Tanımlanan kapi_ac ve kapi_kilit değişkenleri, butona bağlı olduğundan dolayı butonun aktif olup olmamalarını sisteme bildirmektedir. Dolayısıyla, sisteme bir veri göndereceği için INPUT modunda çalışması gerekmektedir. Tanımlanan parametrelere ek olarak, mySwitch.enableTransmit(3) kod satırı ise anahtar içerisinde sinyal gönderecek olan donanımın çalışması için kullanılmıştır. 433 Mhz frekansında çalışan bu donanımın çalışması için arduino unonun 3 numaralı dijital çıkışına tanımlanmıştır. Sistemde değişken üretilmesi için randomSeed komutu kullanılmıştır. Bu komut ile rastgele veri üretimi sisteme tanımlanmıştır. Sistemin veri üretmesi ise sonraki komutlarda belirlenen değerler arasında olacaktır. Üretilen verilerin görüntülenmesi için ise Serial.begin komutu kullanılmıştır. Böylelikle sisteme gerekli tüm parametreler tanımlanmıştır.

```
void loop() {
  if (digitalRead(kapi_ac) == HIGH && !kapi_acOnce) {
    int sinyal = random(10, 1000);
    Serial.println(sinyal);
    if (sayi_kontrol(sinyal, kapi_ac_dizi, kapi_ac_dizi_sayi)) {
      while (true) {
        sinyal = generateRandomnumber(10, 1000);
        if (!sayi_kontrol(sinyal, kapi_ac_dizi, kapi_ac_dizi_sayi)) {
          break;
        }
      }
    }
    kapi_ac_dizi[kapi_ac_dizi_sayi] = sinyal;
    kapi_ac_dizi_sayi++;

    if (kapi_ac_dizi_sayi >= 200) {
      kapi_ac_dizi_sayi = 0;
    }
    mySwitch.send(sinyal, 24);
    kapi_acOnce = false;
    delay(500);
  }
```

Şekil 4.5 Verici yazılım kapı açma algoritması

Şekil 4.5'te, araç kapısının açılması için butona basıldığında, sistem ilk olarak butonun aktif olup olmadığını sorgulamaktadır. Sistem butonun aktif olduğunu algıladıktan sonra içerisinde sinyal adında bir değişken üretmektedir. Bu değişken, 10 ile 1.000 arasında bir sayı olmaktadır. Üretilen bu değişken, ilk olarak daha önce tanımlanan kapi_ac_dizi adındaki dizi içerisinde sorgulanmaktadır. Eğer üretilen bu değişken, dizi içerisinde yoksa dizi içerisine eklenmektedir. Diziye eklendikten sonra, 433 Mhz frekansta çalışan donanım sayesinde radyo dalgaları olarak iletimi sağlanmaktadır. Ancak, eğer ki üretilen bu sinyal adındaki değişken, dizi içerisine daha önceden eklenmiş ise sistem bunu algılayarak yeni bir değişken üretmektedir. Buradaki amaç, üretilen değişkenin birbirinden bağımsız olması gerekmektedir. Dolayısıyla, değişkenin daha öncesinde üretmemiş olduğu bir parametre olması gerekmektedir. Değişkenin özgünlüğünün sağlanması için sistem aktif olduğunda, sürekli olarak bir sorgu hali içerisinde olmaktadır. Dolayısıyla, sorgulamanın sonunda sistemde üretilmiş olan sinyal adındaki değişken, kapi_ac_dizi içerisinde olmayan bir değişken olmaktadır. Sonrasında bu değişken, 433 Mhz frekansta çalışan donanım ile

verici sisteme iletilmektedir. Buton basıldıktan sonra sistemin çalışması bu şekilde olmaktadır. Bu sisteme ek olarak önemli bir husus ise sistem yalnızca buton aktif olduğu süre içerisinde çalışmaktadır. Dolayısıyla, butona basılma süresi genel olarak bakıldığında 1 veya 2 saniye arasında olmaktadır. Çalışma içerisinde ki tüm eylemler bu süre içinde gerçekleşmektedir. Eğer butona basıldıktan sonra süre fark etmeksizin çalışması, sinyalin sürekli olarak gönderilmesini sağlamaktadır. Sürekli sinyalin gönderilmesi ise verici sistemde karışıklığa yol açabilmektedir. Dolayısıyla sistemin sadece butona basarken çalışması önem arz etmektedir.

```
if (digitalRead(kapi_kilit) == HIGH && !kapi_kilitOnce) {
  int sinyal = random(1001, 2000);
  Serial.println(sinyal);
  if (sayi_kontrol(sinyal, kapi_kilit_dizi, kapi_kilit_dizi_sayi)) {
    while (true) {
      sinyal = generateRandomnumber(1001, 2000);
      if (!sayi_kontrol(sinyal, kapi_kilit_dizi, kapi_kilit_dizi_sayi)) {
        break;
      }
    }
  }
  kapi_kilit_dizi[kapi_kilit_dizi_sayi] = sinyal;
  kapi_kilit_dizi_sayi++;

  if (kapi_kilit_dizi_sayi >= 200) {
    kapi_kilit_dizi_sayi = 0;
  }
  mySwitch.send(sinyal, 24);
  kapi_kilitOnce = true;
}

if (digitalRead(kapi_ac) == LOW) {
  kapi_acOnce = false;
}
if (digitalRead(kapi_kilit) == LOW) {
  kapi_kilitOnce = false;
}
```

Şekil 4.6 Verici yazılım kapı kapatma algoritması

Şekil 4.6'te, aracın kapısının açıldıktan sonra kapanması için çalışılan algoritmadır. Aracın kapısının kilitlenmesi için butona basıldığında, sistem butonun çalışıp çalışmadığını sorgulamaktadır. Sistem butonun aktif olduğunu algılandıktan sonra, 1.001 ile 2.000 arasında sayı üretmektedir. Bu sayı, sinyal adlı değişkene

atanmış olmaktadır. Üretilen değişken, sistemde tanımlanmış olan kapi_kilit_dizi adlı dizide sorgulanmaktadır. Eğer ki değişken bu dizi içerisinde daha önceden eklenmemiş ise dizinin içerisine eklenmektedir. Dizi içerisine eklendikten sonra, 433 Mhz frekansta çalışan donanım ile alıcı sisteme iletilmesi için yayılmaktadır. Ancak eğer ki üretilen değişken, daha öncesinde sistem içerisine eklenmiş ise sistem yeni değişken üretmektedir. Üretilen bu değişkenlerde kapı_kilit_dizi içerisinde mevcutsa sistem yeni değişken üreterek özgün bir değişken yakalamaktadır. Sistemin benzersiz bir değişkene sahip olması önem arz etmektedir. Dolayısıyla, sistem içerisinde benzersiz değişken olana kadar değişken üretilmesi devam etmektedir. Değişken benzersiz olduktan sonra ise tekrardan dizi içerisine eklenmektedir. Dizi içerisine eklendikten sonra yine 433 Mhz frekansta çalışan donanımsal cihaz ile alıcı sisteme gönderilmesi için gönderilmektedir.

```
unsigned long generateRandomnumber(long minVal, long maxVal) {
  return random(minVal, maxVal);
}
```

Şekil 4.7 Veri üretme tanımlama

Şekil 4.7'te sistemin veri üretmesi için oluşturulan algoritma tanımlanmıştır. Sistemde random olan komutlarda minimum değer(minVal) ve maksimum değer(maxVal) belirlenmektedir. Belirlenen değer aralığında veri üretimi yapılmaktadır.

```
bool sayi_kontrol(unsigned long sayi, unsigned long dizi[], int dizi_boyutu) {
  for (int i = 0; i < dizi_boyutu; i++) {
    if (dizi[i] == sayi) {
      return true;
    }
  }
  return false;
}
```

Şekil 4.8 Kumanda kapı açma buton sorgulaması

Şekil 4.8'te, sistemde kullanılan dizilerin içerisinde belirtilen parametrelerin bulunup bulunmaması durumunu sorgulamamaktadır. Dizi içerisinde belirtilen

parametrenin bulunması durumunda sisteme var olduğu bilgisini göndermektedir. Bulunmaması durumunda ise sisteme bulunmadığı bilgisini göndermektedir. Algoritmanın içerisinde yapılan sorgu komutu şekil 4.8 gösterilen komut aracılığıyla çalışmaktadır.

4.2.2. Araç İçerisinde Radyo Frekans Alıcı Donanım Yazılım

```
#include <RCSwitch.h>
#include <Servo.h>
#define MAX_DATA_COUNT 200
int servoPinSag = 10;
int servoPinSol = 8;
Servo servoMotorSag;
Servo servoMotorSol;
RCSwitch mySwitch = RCSwitch();
bool intrusionDetected = false;
unsigned int acilan_kapi[MAX_DATA_COUNT];
unsigned int kilitlenen_kapi[MAX_DATA_COUNT];
int acik_kapi = 0;
int kapali_kapi = 0;
```

Şekil 4.9 Alıcı yazılım kütüphane ve tanımlama

Şekil 4.9'da araç üzerinde bulunan alıcı sistem içerisinde kullanılan kütüphaneler gösterilmektedir. Aracın kapılarının açılması sebebiyle gönderilen sinyalin tanınması için alıcı sistem üzerinde de RC Switch kütüphanesi kullanılmaktadır. Frekansları gönderen ve tanımlayan sistemlerin çalışmasında, kütüphanenin kullanılması zorunlu olmaktadır. Dolayısıyla, kütüphane bulunmadığı sürece gelen sinyal algılanamayacaktır. Algılanamayan sinyaller sistem içerisinde işlem göremeyeceğinden dolayı sistemi çalıştırmayacaktır. Sistemde gelen verilerin kayıt olması için kullanılacak olan dizilerin maksimum alabileceği veri sayısı 200 olarak belirlenmiştir. 200 veri define komutu ile sistemde tanımlanmış ve sabitlenmiştir. Sistemde kullanılan kapı kilit sistemi için servo motor kullanılmıştır. Servo motorların kullanımı içinse sistemde kütüphane kullanılmaktadır. Servo motorların bağlantısı, sağ kapı için arduino 10 numaralı dijital çıkışına, sol kapı için ardino 8 numaralı dijital çıkışına tanımlanmıştır. Şekil 4.9'da servo terimi, servo kütüphanesinin içinde bulunduğu tanımından gelmektedir. Servo terimi kullanılacak olan değişkenin elektronik olarak çalışan bir motor türü olduğunu belirtmektedir. Şekil

4.9’da kullanılan bool terimi ise aracın kapılarının açılması için kumanda da bulunan sinyal gönderici donanım tarafından bir RF sinyali alınıp alınmadığını sorgulamaktadır. Sorgulama sonucunda sinyal alınması durumunda sistem alındı bilgisini vermektedir. RF sinyallerinin alınmasından sonrada servo motorların çalışması mümkün olmaktadır. Aracın sisteminin açılma ve kapanma sinyallerini kayıt eden 2 adet dizi bulunmaktadır. Alıcı kumandadan gelen verilerle bu sinyaller tanımlanmalara göre acilan_kapi veya kilitlenen_kapi dizilerine eklenecektir. Bu dizilerin içerdiği verilerin sayısı ise acik_kapi ve kapali_kapi olarak tanımlanmıştır. Dolayısıyla, dizi içerisine veri girişi oldukça sistemde ne kadar verinin bulunduğu bu şekilde belirlenebilecektir. Diziler, sistemde güvenliği sağlamak için veri tabanları görevi görmektedir. Veri tabanları, bu verilerin daha önceden içermiş olması veya olmaması ile ilgili işlemleri gerçekleştirebilecektir.

```
void setup() {
  pinMode(servoPinSag, OUTPUT);
  pinMode(servoPinSol, OUTPUT);
  servoMotorSag.attach(servoPinSag);
  servoMotorSol.attach(servoPinSol);
  Serial.begin(9600);
  mySwitch.enableReceive(0);
  servoMotorSol.write(90);
  servoMotorSag.write(0);
}
```

Şekil 4.10 Alıcı yazılımda giriş portları belirleme

Şekil 4.10’da, araç üzerindeki alıcı sistem içerisinde arduinonun 10 ve 8 numaralı dijital çıkışına tanımlanan servo motor pileri output olarak belirtilmiştir. Böylelikle, servo motorların radyo frekanslarının alınmasına uygun olarak çalışması, output pini aracılığıyla olmaktadır. RF sinyallerine uyumlu olarak çalışabilmesi için ise servoMotor.attach komutu kullanılmıştır. Bu komut aracılığıyla, servoMotor adlı cihazın servopini ile bağlantı kurulmuştur. Serial begin olarak tanımlanan komut, seri haberleşmenin hızı olmaktadır. Sisteme saniyede 9600 bit gönderimi yapılmaktadır. Bir sonraki komut, mySwitch.enableReceive ile araçtaki radyo frekans alıcı sisteminin girişi arduinonun 0 numaralı dijital çıkışına tanımlanmıştır. Tanımlamaların yapılması

ile sisteme gelen radyo frekans sinyalleri, tanımlanıp işlenmeye hazır durumda olmaktadır.

```
void loop() {

  if (mySwitch.available()) {
    unsigned long receivedValue = mySwitch.getReceivedValue();
    if (receivedValue >= 10 && receivedValue <= 1000 && acik_kapi < MAX_DATA_COUNT) {
      bool acilan_kapi_mevcut_veri = false;
      for (int i = 0; i < acik_kapi; i++) {
        if (receivedValue == acilan_kapi[i]) {
          acilan_kapi_mevcut_veri = true;
          break;
        }
      }
      if (!acilan_kapi_mevcut_veri) {
        acilan_kapi[acik_kapi] = receivedValue;
        acik_kapi++;
        servoMotorSag.write(0);
        servoMotorSol.write(90);
        Serial.println(mySwitch.getReceivedValue());
        mySwitch.resetAvailable();
        delay(1000);
      } else {
        Serial.println(receivedValue);
        Serial.println("Sisteme İzinsiz Erişim Denemesi Algılandı!");
        delay(1000);
      }
    }
```

Şekil 4.11 Alıcı yazılım kapı açma algoritması

Şekil 4.11'de, tanımlamalardan sonra alınan sinyallerin işlendiği komutlar bulunmaktadır. Kumanda vericisinden gelen sinyal, araçtaki alıcı sistem tanımlayıp, aracın kapısının kilitlenip açılmasını işlemektedir. Şekil 4.11'de, kumanda vericisinden gelen kapının açılması sinyali algılanacaktır. Verici sistemde belirtilen parametreler arasında olduğu belirlendikten sonra sistemin içerisindeki algoritma çalışacaktır. Algoritma, ilk olarak sinyalin sayılardan oluşan bir veri olduğunu bir değişkene tanımlayacaktır. Tanımlanan veri, dizilerin, bu verinin daha önce algılanmadığı varsayılarak false parametresiyle çalışacaktır. Her iki dizi içerisinde de bulunmadığı varsayılmaktadır. Şekil 4.11'de, verinin kapının açılması için gönderilen sinyal olduğu bilinmektedir. Bunun için sistem, sinyalin kapının açılması için gönderildiğini algılayarak algoritmayı döndürmeye başlamaktadır. Algoritmanın ilk adımı, bu verinin daha önce veri tabanı içerisinde olup olmadığını sorgulamaktır. Veri tabanında sorgulanması sonucunda sistemde algoritma 2 farklı şekilde çalışmaktadır.

Eğer sistemde verinin daha önce var olduğu tespit edildiyse, sinyalin işlenmesi için ilk sisteme girdiği veri true olarak tekrardan tanımlanacaktır. Tekrardan tanımlanan sistem farklı bir sorgulamaya girerek sisteme izinsiz erişim denemesi olduğunu bildirecektir. Bu bilgilendirmeyle sisteme daha önceden tanımlanmış bir sinyalin gönderildiğini ve bu sinyalin verici kumanda tarafından gönderilmediği anlaşılacaktır. Dolayısıyla, izinsiz erişim denemesi olarak tahmin edilecek ve gerekli güvenlik önlemleri alınabilecektir. Ancak, eğer algılanan sinyal daha önce veri tabanı içerisine eklenmediyse, algoritma farklı bir yöntemde ilerleyecektir. Veriyi ilk olarak veri tabanı içerisine ekleyecek ve daha sonra içerisinde kütüphaneleriyle tanımlanan servo motorları belirtilen koşullarda çalıştıracaktır. Servo motorlarının çalışması ile araç kapılarının kilidi açılacaktır. Aracın kapısının açılması için sinyali tanımlaması gerekmektedir. Dolayısıyla aracın kumandası, yalnızca aracın içerisinde ki donanımın tanımlayacağı şekilde sinyali üretip alıcı sisteme gönderebilmektedir. Bu duruma eş olarak, kapının kilitlenmesi prensibi ise aynı durumda çalışmaktadır.

```
else if (receivedValue >= 1001 && receivedValue <= 2000 && kapali_kapi < MAX_DATA_COUNT) {
  bool kapanan_kapi_mevcut_veri = false;
  for (int i = 0; i < kapali_kapi; i++) {
    if (receivedValue == kilitlenen_kapi[i]) {
      kapanan_kapi_mevcut_veri = true;
      break;
    }
  }
  if (!kapanan_kapi_mevcut_veri) {
    kilitlenen_kapi[kapali_kapi] = receivedValue;
    kapali_kapi++;
    servoMotorSag.write(70);
    servoMotorSol.write(0);
   Serial.println(mySwitch.getReceivedValue());
    mySwitch.resetAvailable();
    delay(1000);
  } else {
    Serial.println(receivedValue);
    Serial.println("Sisteme İzinsiz Erişim Denemesi Algılandı!");
    delay(1000);
  }
}
```

Şekil 4.12 Alıcı yazılım kapı kapama algoritması

Şekil 4.12'de, kapının kapanması için gönderilen sinyalin çalışma algoritması görülmektedir. Aracın açılması için gönderilen sinyalin işlenmesine benzer yapıda çalışmaktadır. Sisteme giriş yapan sinyalin kapıların açılması için gönderilen sinyal değil tam aksine sistemin kapıların kapanması için gönderilen sinyal olduğu

sorgulamada tespit edilmektedir. Sinyalin kapıların kapatılması için gönderilen sinyal olduğu tespit edildikten sonra veri tabanı içerisinde, bu verinin daha önceden eklenip eklenmediği sorgulanmaktadır. Sorgulanan veri, eğer daha öncesinde sistem içerisinde mevcutsa algoritma bunu tespit etmektedir. Tespit edilen veri dizi içerisinde daha önceden eklendiği için bağlı olduğu değişkeni true olarak çalıştırmaktadır. True olarak çalışan değişken, algoritmadaki farklı bir sorgulamaya giderek sisteme izinsiz erişim denemesinin olduğunu saptamaktadır. Böylelikle sisteme dışarıdan bir saldırı olduğu düşünülerek gerekli güvenlik önlemleri alınabilecektir. Ancak sistemde veri girişinin daha önceden olmadığı tespit edildiğinde, algoritma farklı şekilde çalışacaktır. Bu yöntemde de ilk olarak veriyi veri tabanına ekleyecek ve daha sonra servo motoruları çalıştıracaktır. Servo motorların çalışmasıyla aracın kapılarının kilitleri hareket edecek ve araç kilitli durumda olacaktır.

Radyo sinyalleriyle yapılan bu haberleşmenin sömürülmesiyle, sisteme kolayca erişilmesi mümkün olmaktadır. Otonom araçlar gibi farklı birçok siber fiziksel sistemlerde de bu yapıların kullanıldığı göz önüne alındığında, aslında gelecek açısından önemli bir güvenlik problemi sorunu olmaktadır. Dolayısıyla, radyo frekanslarının güvenliğinin artması birçok güvenlik yönünden önem arz etmektedir.

BEŞİNCİ BÖLÜM

Araçtaki sisteme yönelik sinyal saldırı gerçekleştirilmesi için öncelikli olarak sinyal yakalama ve sonrasında sinyal iletimi yapılmaktadır. Bu işlemlerin yapılabilmesi için ise parametrelerin belirlenip ayarlanması gerekmektedir.

5.1. Araç ve Kumanda Haberleşmesinde Gönderilen Sinyalleri Yakalama

Günümüz araçların sahip olduğu elektromekanik donanımların kullanılması için aracın beyni olarak da sayılabilen bir sistem geliştirilmiştir. Bu sistem, ECU (Elektronik Kontrol Ünitesi) olmaktadır. Araçların otonom olarak gerçekleştirmesi veya onların kontrolünü sağlaması gerektiği durumlar ECU tarafından yapılmaktadır. Hava yastığı, ABS frenleme sistemi, silindir içi yanma zamanlamaları, hava yakıt karışım kontrolü, vb. sistemlerin çalışmasını ve kontrolünü sağlamaktadır. Bu sistemlerin çoğu, sürücü istemi dışında tetiklenerek çalışan sistemlerdir. Örneğin, kaza anından hemen önce hava yastığının açılması için ECU aracılığıyla hava yastığının açılıp açılmama şartlarının kontrolü sağlanabilmektedir. Ayrıca, silindir içerisine girecek olan hava-yakıt karışımın kontrolü de ECU aracılığıyla sağlanabilmektedir. Bu sistemleri çalıştırırken veya kontrolünü sağlarken, her birini eş zamanlı olarak yapabilmektedir. Dolayısıyla araç için önemli durumları belirleyen ECU, aracın beyni olarak nitelenebilmektedir.

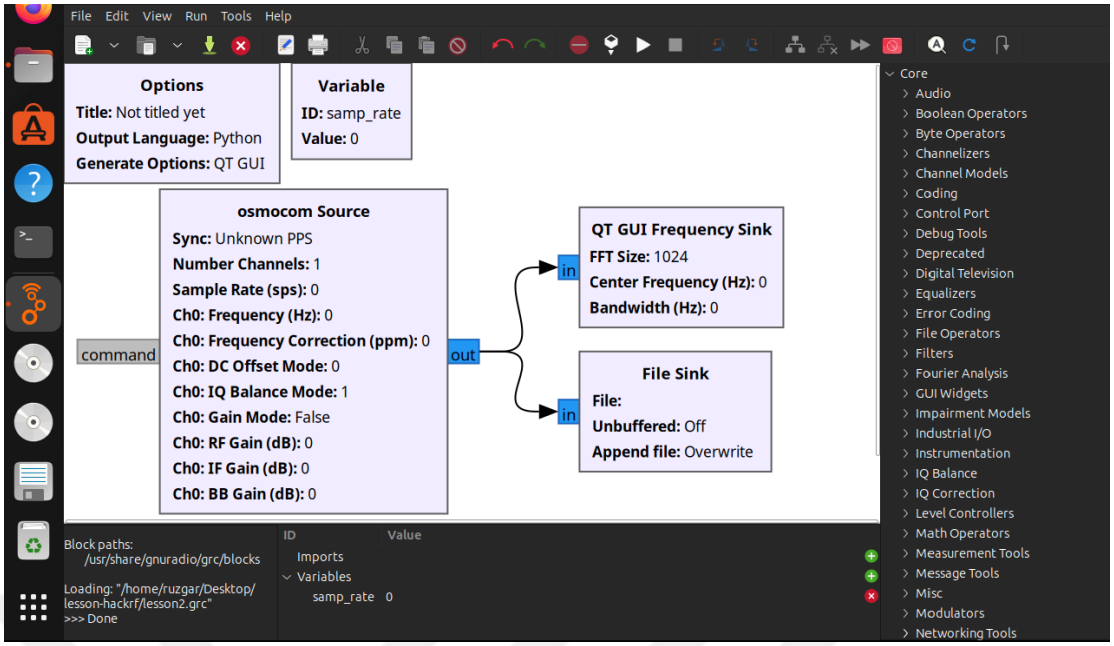
Bu sistemlerin çalışma prensipleri, araç içi olduğu gibi araç dışı çalışma ile de olabilmektedir. Örneğin, ABS fren sisteminin çalışabilmesi için uygun şartlar sağlanması ile araç içinde eyleme geçilmektedir. ABS, Aracın yol üzerinde kaymasının önlenmesi için sık ve aralıklı olarak frenleme yapılmaktadır. Ancak aracın anahtarı, araç içerisinde herhangi bir bağlantı olmadan radyo frekansları kullanılarak birbirlerine bağlı olmaktadır. Dolayısıyla, radyo frekansları da somut bir kablo olmadan sistemler arası kablo görevi görmektedir. ECU, bu sistemlerle sürekli olarak haberleşme içerisinde olmaktadır (Kara, 2009). Bu haberleşme için otomotiv sektöründe yaygın olarak kullanılan CAN haberleşme protokolü kullanılmaktadır. CAN haberleşme protokolü, seri haberleşme protokolüdür. CAN haberleşme protokolü kısaca, araç içerisinde çalışılan veya kontrol edilen tüm donanımlara eş zamanlı ileti yollayabilmektedir. Sonrasında ileti sonuçlarını alarak analiz etmektedir.

Sonuçlara göre çalıştırabileceği bir sistem olup olmadığını kontrol etmektedir. Analiz sonucu yine gerekli durumlarda yapılması gereken eylemleri göndermektedir. CAN haberleşme protokolünde gönderilen iletiler, alıcı yoluna bağlı tüm alıcılar tarafından alınır. Çalışma yapısına bakıldığında, eğer yapılması gereken bir işlev varsa CAN haberleşme protokolü aracılıyla ECU'ya iletilir ve ECU da gerekli işlemleri yapması için iletiler gönderir (Baki, Tutkun, 2021). Gönderilen bu iletilerin radyo sinyalleri de aynı olmaktadır. Dolayısıyla, her seferinde aynı frekansta ve aynı parametrelerde gönderilen bu sinyallere herhangi bir şifreleme veya yetkilendirme olmadığı içinde alıcıların takibini yapmak zor olmaktadır. Çünkü sisteme saldırı yapmayı başaran bir siber saldırgan, sistemin içerisinde ki çalışma koşullarını görebilmektedir. Sonrasında bu çalışma yapısına bağlı olarak, kendi saldırı planını işleme sokabilmektedir. Araçların anahtar kilit sistemleri de bu çalışma yapılarına örnek olmaktadır.

Özgün olarak tasarlanan prototip aracın elektromekanik donanımları, araç içerisine monte edilmiştir. Araç içerisinde arduino kartı kullanılmaktadır. Aracın beyni niteliği sayılabilecek olan sistem, arduino gömülü kartı olmaktadır.

Otonom aracın yönlendirilmesi veya kontrol edilmesi kumanda aracılığıyla yapılmaktadır. Kumandanın üzerine bulunan tuş takımları; 1. Olan tuş aracın CAN haberleşme protokolü kullanarak sistemi çalıştıran buton olmaktadır. Öncelik olarak sistemin açığını saptamak için sistem aracın içerisinde monte edilmiştir. Dolayısıyla 1. Butona basıldığında sistem çalışmış olacaktır.

Bir sonraki adım, çalışan bu sisteme bir siber saldırı uygulamak olacaktır. Siber saldırılar, sistemlerde bulunan açıkların sömürülmesiyle başarılı sonuçlara ulaşmaktadır. Sömürülerek sızma girişiminin başarılı olması halinde sistemdeki veri akışı izlenebilir. Sistemin çalışması değiştirilebilmektedir. Bu tür siber saldırılar, aslında sistem içerisinden yapılmaktadır. Bu çalışma için sisteme yapılacak olan saldırı, bir frekans saldırı olacaktır. Sürücü sistemi çalıştırdıktan sonra gönderdiği frekans yakalanmaktadır. Frekansın yakalanabilmesi için hackrf one cihazı kullanılmıştır. Kullanılan bu cihaz açık kaynaklı kodlardan oluşmaktadır. Cihazın kontrolünü sağlamak içinse gnu radio kullanılmıştır. Gnu radio aslında blok diyagramlardan oluşan yazılım tabanlı radyo frekans arayüz sistemidir. Dolayısıyla uygun bloklar kullanılarak araç ile anahtar arasında bulunan radyo frekanslarının yakalanması yapılmıştır. Bu saldırı için aşağıda bulunan blok diyagram kullanılmıştır.



Şekil 5.1 Sinyal yakalama akış diyagramı

Şekil 5.1'de gösterilen gnu radio arayüzünde bloklar kullanılarak bir akış grafiği bulunmaktadır. Bu akış grafiğinin çalışma amacı, belirtilen frekansta ve parametrelerde olan sinyalleri yakalamaktır. Sinyalleri yakalamak için ise akış grafiği, donanımlarla iletişim kurmada en yaygın olan osmocom source bloğu kullanılmıştır. Osmocom source bloğu, farklı donanım cihazlarıyla iletişim kurulmasını sağlayan bir soyutlama katmanıdır. Yakalanması istenilen radyo frekanslarının sahip olduğu parametreler, osmocom source kısmında belirtilmelidir. Çünkü osmocom source öncelikle hackrf one cihazını çalıştırarak belirtilen parametre ve frekansta alıcı eyleminde bulmasını sağlar. Hackrf one alıcı eyleminde bulunurken sadece girildiği frekansta en verimli sinyalleri toplar. Bu çalışma için saldırı yapılacak olan sinyal 433 Mhz olmaktadır. Aracın kapı kilit sistemi ve aracın kilidini açan kumanda sistemi 433 Mhz frekansında çalışmaktadır. Dolayısıyla, 433 Mhz frekanstan yönü farketmeksizin uzaklaşılırsa araç kapısının açılması için üretilen sinyaller yakalanamaz.

Akış grafiği üzerinde bulunan Variable (değişken) bloğunda Samp Rate(örnekleme hızı) belirtilir. Belirtilen örnekleme hızına ID atanır ve akış grafiğindeki diğer bloklarla kullanılabilir. Değişken bloğunun kullanılması diğer bloklarda aynı esnada örnekleme hızı değişkeninin değişmesini pratikleştirmek amaçlı kullanılmaktadır. Bu değişkenler örnekleme hızı dışında belirtilecek olan farklı

parametrelerde olabilir. Sample Rate parametresi örnekleme hızı olmaktadır. Örnekleme hızı, analog sinyallerin dijital formlara dönüşmesi esnasında bir saniyede alınan örnek sayısını belirten terim olmaktadır. Akış grafiğinde bulunan örnekleme hızı 10 milyondur. Saniyede 10 milyon örnek frekans aldığı belirtilmektedir. Örnekleme hızının artması yüksek çözünürlük ve daha geniş bant genişliği oluşturmaktadır. Alıcının aldığı frekansların doğruluğunu daha verimli olarak belirleyebilmektedir. Ancak, bu yüksek örnekleme hızı daha fazla işlem gücü gerektirmektedir. Dolayısıyla, alıcı cihazların ve kullanılan işlemcilerin bu gücü kaldırabilecek boyutta olması gerektirmektedir Bu çalışmada kullanılan hackrf one cihazı, maksimum olarak 20 milyon örnekleme hızı yetkinliğine sahip olmaktadır. Örnekleme hızının düşük olması durumunda ise daha az işlem gücü kullanılmaktadır. Ancak yüksek örnekleme hızından ziyade daha az çözünürlük ve detay sağlamaktadır. Düşük örnekleme hızının sonuçları olarak belirtilen parametreler ve frekanslar doğru girilmiş olsa da alınan frekanslar detaylı olamayacağı için tekrar sisteme gönderildiğinde saldırı başarısız olabilmektedir. Uygun parametreler ve uygun frekansların yakalanması için her sistemin çalışma parametreleriyle birlikte frekans aralıklarında yapılacak olan çalışmalar gerçekleştirilebilir. Böylelikle en doğru sinyali yakalamak için bulunan frekansın ve doğru parametreler saptanabilir.

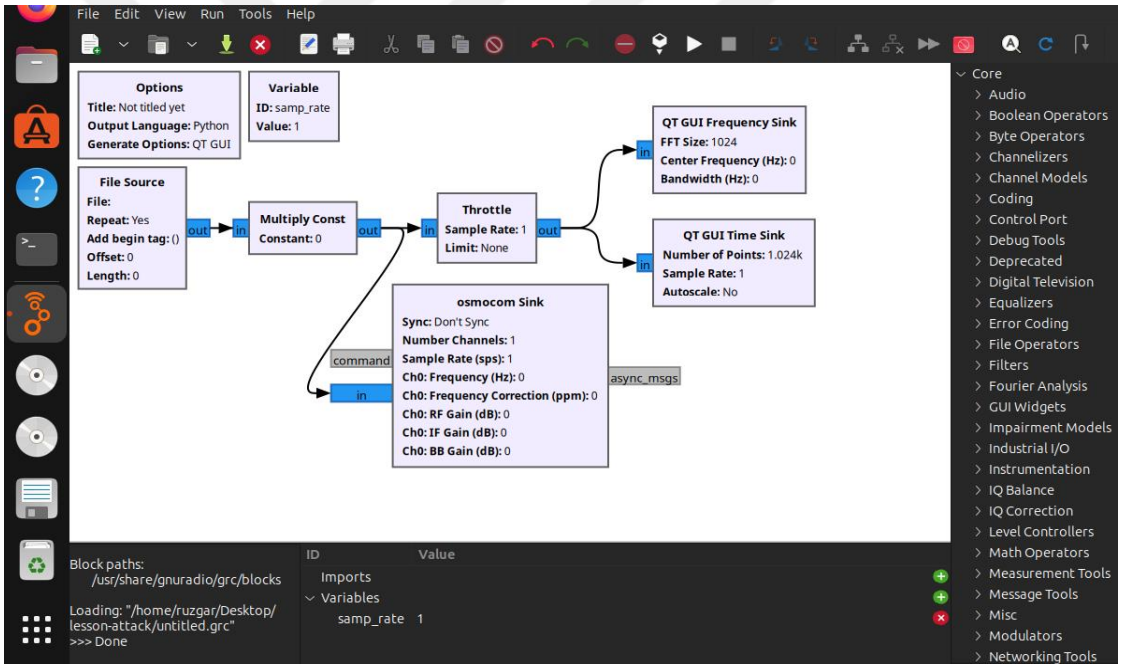
Osmocom source üzerinde ki diğer parametre Frequency Correction (ppm) frekans düzeltme olarak geçmektedir. Çevre koşulları veya donanımsal faktörlere göre frekansların yakalanmasında sapmalar olabilmektedir. Örneğin, 433 Mhz frekansta sinyal alınırken bu frekansın asıl değeri 433.04 gibi bir değere sahip olabilmektedir. Dolayısıyla, frekans düzenleme kullanılarak frekanstaki sapma düzenlenir ve 433 Mhz olarak algılar. Osmocom source üzerinde bulunan diğer parametre Dc Offset Mode(DC Ofset Modu) olmaktadır. Bu parametre hackrf one gibi yazılım tabanlı radyo frekans cihazlarının sinyal alıcı durumunda çalışırken istenmeyen sinyalleri de yakalayabilmektedir. Bu istenmeyen sinyalle gürültü kaynağı olarak sayılan DC bileşenleri denilmektedir. Dc ofset modunu çalıştırmak dc bileşeni olarak adlandırılan kaynaklarda gelecek sinyalleri filtrelemektedir. Filtrelenen sinyaller, daha doğru ve temiz olarak akış grafiğinde işlenmeye devam etmektedir. Dc ofset modu hassas sinyal işleme çalışmalarında kullanılmaktadır. Osmocom source üzerinde ki diğer parametre IQ Balance Mode (IQ denge modu) olmaktadır. Bu parametrede I(In-phase) sinyalin anlık genliğini temsil etmektedir. Q(Quadrate phase) I bileşenine göre 90 derece faz

farkına sahip olan sinyalin zaman içerisinde ki değişimi temsil etmektedir. Bu iki bileşenin birbirlerine 90 derece dik olması sinyallerin özelliklerindendir. Karmaşık sinyallerin çözümünde kullanılan bu mod, I ve Q bileşenlerini dengeleyerek sinyallerin daha doğru işlenmesini sağlamaktadır. Osmocom source üzerindeki diğer parametre Gain Mode (Kazanç modu) olmaktadır. Bu parametre, yakalanacak olan sinyalin gücünü kontrol etmektedir. Bu mod kapalı durumda olduğunda yazılım tabanlı radyo cihazları içlerinde olan varsayılan bir değer belirlemektedir. Modun açık olduğu durumlar, yapılacak olan uygulamalarının ihtiyaçlarına göre çeşitlenebilmektedir. Varsayılan olarak sabit durumda belirlenebilirken uygulamalara göre dinamik olarak da belirlenebilmesi daha uygun olabilmektedir. Osmocom source üzerindeki diğer bir parametre RF Gain (Rf kazancı) olmaktadır. Bu modun çalışma amacı, alıcı cihazda bulunan amplifikatörün kazancını ayarlayan parametredir. Sinyal gücünü artırmak veya azaltmak için kullanılan amplifikatörde daha az veya daha çok RF kazancının ayarlanması alınacak olan sinyallerin gücünüde etkilemektedir. Alıcıdaki RF kazancının düşük olması güçlü sinyalleri yakalayabilirken yüksek olmasıda daha düşük sinyalleri yakalayabilmektedir. Ancak, alıcıdaki RF kazancının yüksek olması gürültüyü artırmaktadır. Dolayısıyla, RF kazancının uygulama alanları gürültü oluşturma sebebiyle kısıtlı uygulamalarda kullanılmaktadır. Osmocom source bulunan diğer parametre IF Gain(Ara kazanç) olmaktadır. Alıcı devresi içerisinde bulunan ara frekansı kontrol etmektedir. RF kazancı yakaladığı frekansları işleyerek ara frekans olarak dönüştürür. Ara kazanç modu ise gelen bu ara frekansın sinyal gücünü ayarlayan amplifikatörün kazancını kontrol etmektedir. RF kazancı ile aynı prensipte çalışmaktadır. Yüksek ara kazançla daha düşük frekanslı sinyallerin alınmasını sağlarken, daha düşük ara kazanç yüksek frekanslı sinyallerin alınmasını sağlar. Ancak bu durumda RF kazancı gibi yüksek ara kazançta gürültü oluşturmaktadır. Dolayısıyla, alıcı içerisinde ara kazancın kontrolü hassas olarak ayarlanmalıdır. Osmocom source üzerindeki bir diğer parametre BB Gain(Bant genişliği kazancı) (dB) olmaktadır. Alıcı sistemlerinde geniş bant sinyallerinin işlenmesi için kullanılan amplifikatörün kazancını kontrol etmek için kullanılmaktadır. IF veya farklı frekans aşamasından gelen sinyalleri dijital olarak işlemektedir. IF kazanç modu ve RF kazanç moduyla aynı prensipte çalışmaktadır. Daha yüksek bant genişliği kazancı daha düşük sinyalleri işleyebilmektedir. Ancak daha fazla gürültü oluşmasına sebep olmaktadır.

Bu çalışma kapsamında kullanılacak olan osmocom source üzerinde ki en

önemli üç parametre RF kazancı, If kazancı ve BB kazancı modları olmaktadır. Dolayısıyla özet olarak, RF kazancı, alınan sinyalin gücünü kontrol edip işleyerek ara sinyallere dönüştürür. IF kazancı, ara frekansa dönüşen sinyalin gücünü kontrol etmektedir. BB kazancı ise işlenen dijital sinyallerin gücünü kontrol etmektedir. Akış grafiğinde diğer bir blok QT GUI Frequency Sink olmaktadır. Bu blok, akış grafiğinde kendisine gönderilen sinyallerin frekans spektrumunu görselleştirmek için kullanılır. Böylelikle akış grafiğini çalışmasıyla belirtilen frekanslarda ve parametrelerde bir frekans olduğu anlık olarak izlenebilir. Ayrıca, izlenen bu frekansın gücüde QT GUI Frequency Sink bloğu ile görülebilmektedir. Akış grafiğinde diğer bir blok File Sink (Dosyalama) bloğudur. Akış grafiğinde yakalanan sinyaller bu blok aracılığıyla belirtilen klasör yolunda dosyalanmaktadır.

5.2. Araç ve Kumanda Haberleşmesinde Yakalanan Sinyali İşleme



Şekil 5.2 Yakalanan sinyali iletme akış diyagramı

Şekil 5.2'de görülen akış grafiğinde, yakalanan sinyalin tekrarlanıp alıcı sisteme gönderilmesi amaçlanmaktadır. Bir önceki sinyal yakalamak için kullanılan akış grafiğine ek olarak, blok diyagramları kullanılmaktadır. Akış grafiğinde File Source bloğu, yakalanan sinyalin akış grafiğinde işlenmesi için çağırmaktadır. Multiply Const bloğu, sinyali sabit bir katsayıyla çarpmak için kullanılmaktadır. Sinyal gücünün bir

katsayıyla çarpılmasının amacı, sinyalin gücünü artırmak veya azaltmak olmaktadır. Uygulama alanlarına göre sinyalin bir katsayıyla çarpılması veya bölünmesi durumu ölçeklendirme özelliği görmektedir. Akış grafiğindeki throttle bloğu işlem hızının kontrol edilmesini sağlamaktadır. İşlem hızının kontrolünün sağlanması sinyali daha dengeli ve doğru bir şekilde iletilmesidir. Akış grafiğinde kullanılan her blok arasında veri akışı oluşmaktadır. Bu veri akışı belirli hızda gerçekleşmektedir. Ancak bloklar arasında oluşabilen işlem hızı uyumsuzluğu, sistemin çalışma performansını kötü etkileyebilmektedir. Dolayısıyla, sinyallerin işlenmesinde ve gücünde olumsuz sonuçlara yol açmaktadır. Sonuç olarak throttle bloğu, akış grafiği içerisinde ki işlem hızından sorumludur. Akış grafiğinde bulunan osmocom sink bloğu akış grafiğinde iletiminde kullanılmaktadır. Osmocom sourcenin çalışma prensibine benzer çalışmaktadır. Yazılım tanımlı radyo frekans cihazlarıyla iletişim kurmaktadır. İçerisinde tanımlanan parametrelerce yazılım tanımlı radyo frekans cihazlarını sinyal verici olarak çalışmasını belirtmektedir. Böylelikle osmocom sink tarafından belirtilen parametrelerce sinyal gönderimi sağlanmaktadır. Gönderilen bu sinyal akış grafiğinde bulunan File Source bloğundan gelmektedir. Akış grafiğinde ki QT GUI Time Sink grafiği işlenen sinyalin zaman içerisinde ki değişimini göstermektedir. Zaman grafiği olarak da tanımlanan bir grafik oluşturmaktadır. Bu grafiğe örnek olarak bir ses sinyalinin işlendiği göz önüne alınırsa, frekansların ani olarak desibellerinin veya yüksekliklerinin değiştiği gözlemlenebilmektedir.

ALTINCI BÖLÜM

6.1. Mevcut Araç Anahtar Yapısına Sinyal Saldırısı

Günümüz araçlarda kullanılan araç ve anahtar arasındaki haberleşme yapısı bu bölümde oluşturulmuştur. Oluşturulan sisteme sinyal saldırısı yapılmıştır. Mevcut sistemdeki saldırı başarılı olmuştur. Aynı işlemler geliştirilen sistemler üzerinde de gerçekleştirilmiştir.

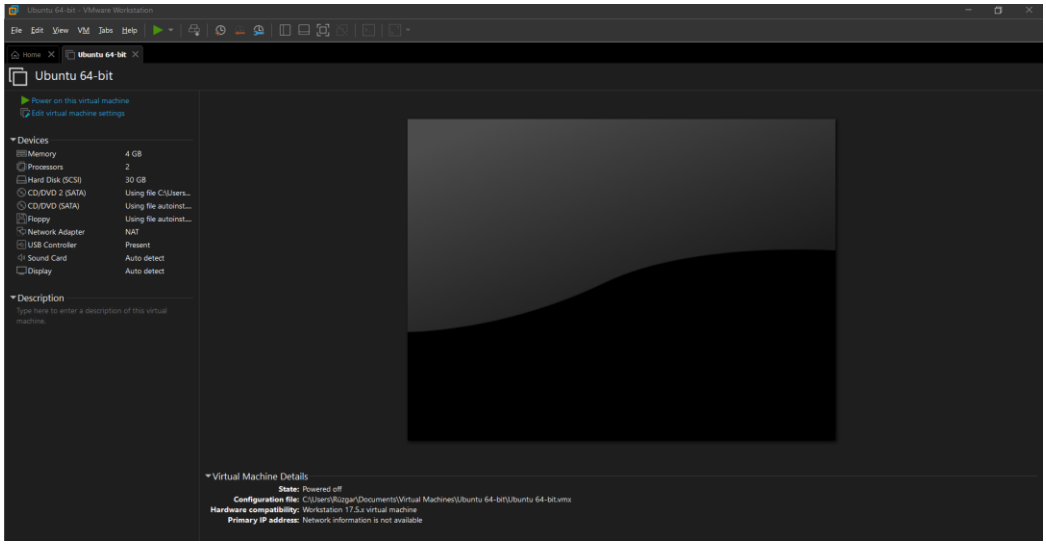
6.1.1. Kumandadan Gönderilen Kapı Açma Sinyalini Yakalamak

Sinyal saldırısı başlamadan önce aracın kapıları kapalı ve kilitli durumda olmaktadır. Aracın durumu şekil 6.1 de gösterilmektedir.



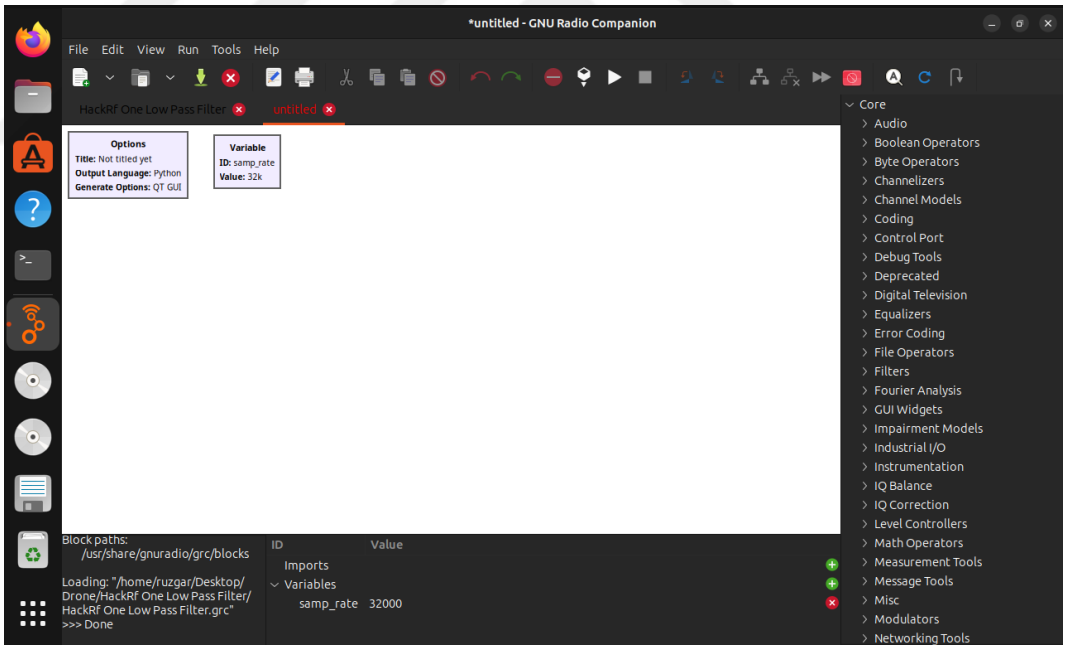
Şekil 6.1 Saldırıdan önce araç durumu

Bu çalışmada frekans saldırı için sanal işletim sistemi kullanılmıştır. Vmware (Virtual machine ware) aracılığıyla ubuntu sanal işletim sistemi kurulmuştur.

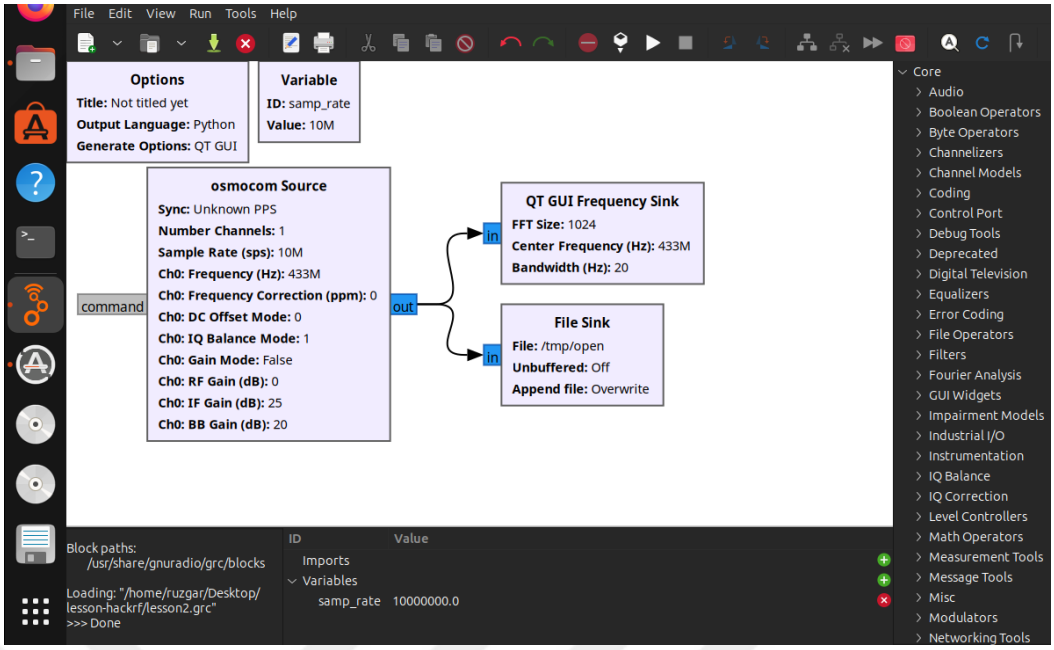


Şekil 6.2 Sanal işletim sistemi – Ubuntu

Ubuntu sanal işletim sistemi kurulumu ve güncellemeleri tamamlandıktan sonra gnuradio kurulumu yapılmıştır.

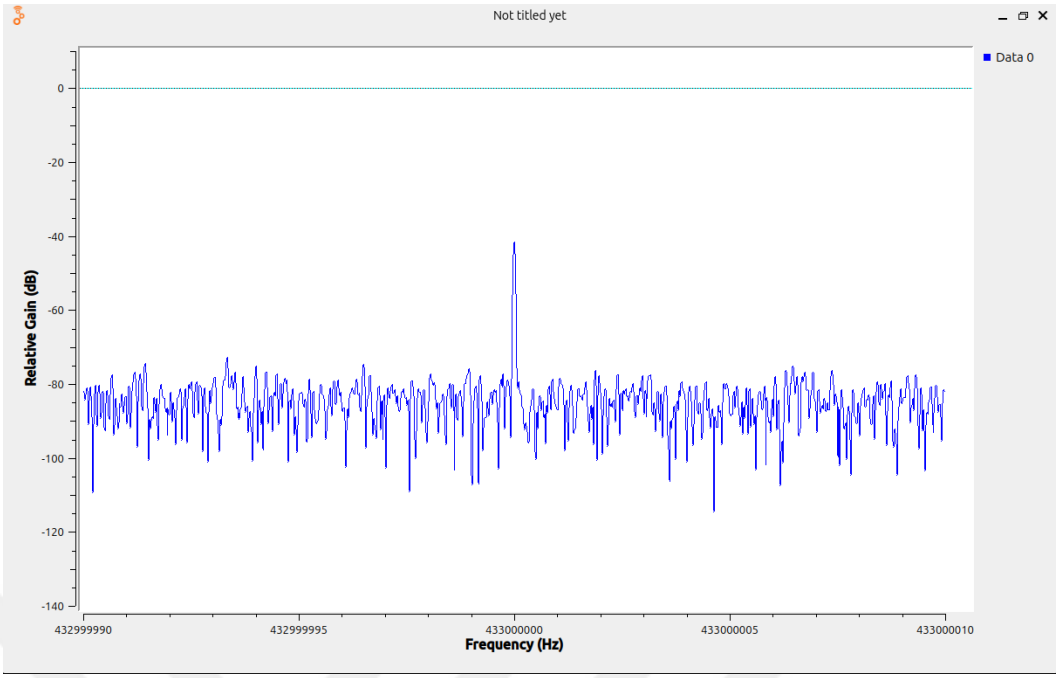


Şekil 6.3 Gnu radio açılış arayüzü



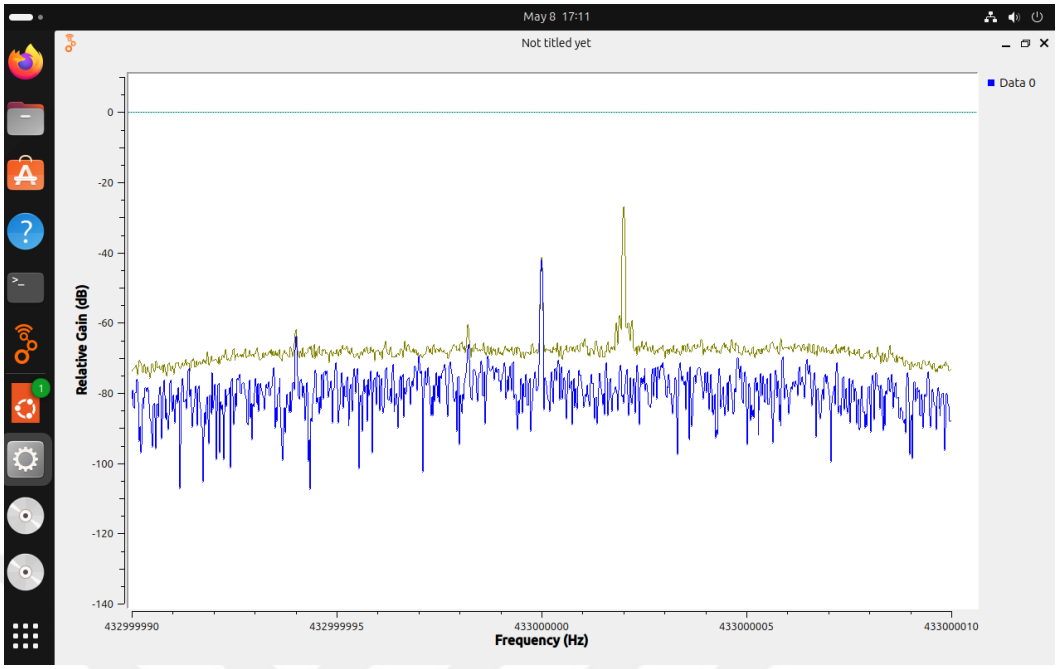
Şekil 6.2 Gnu radioda sinyal yakalamada kullanılan bloklar

Saldırı için osmocom source bloğu kullanılmıştır. Osmocom source bloğunda 433 Mhz frekans olarak ayarlanmıştır. Aracın kapı kilit sisteminde 433 Mhz frekansta çalışan alıcı verici donanım mevcuttur. Dolayısıyla, saldırı frekansı 433 Mhz olarak belirlenmiştir. Saldırının parametrelerine bakılarak dc ofset modu ile gain modu bu saldırı için ayarlanmamıştır. RF kazanç modunun gürültü yaratmaması açısından 0 olarak ayarlanmıştır. IF Gain modu ve BB gain modu sinyallerin doğru işlenmesi açısından minimum boyutlarda tutularak arttırılması veya azaltılması planlanmıştır. Bundan dolayı, IF Gain modu 25 dB ve BB Gain modu ise 20 dB olarak ayarlanmıştır. Osmocom source bloğundan gelen sinyalleri QT GUI Frequency Sink bloğu ve File Sink bloğuna eş zamanlı olarak iletilmektedir. QT GUI Frequency Sink bloğunda yakalanan sinyaller görselleştirilmektedir. Sistem çalıştırılarak sinyal yakalama saldırısı başlamıştır.



Şekil 6.5 Sinyal gösterimi

Şekil 6.5 de gösterilen grafikte sinyal yakalamak için saldırı başlangıcından sonra hangi aralıklarda ve parametrelerde olduğu gösterilmektedir. Orta kısımda bulunan yüksek genliğe sahip olan sinyal çubuğu, osmocom source bloğunda belirtilen frekans değeridir. Belirtilen frekans değeri bu grafik için orta nokta olmaktadır. Yakalanacak olan sinyal 433 Mhz frekansında çalıştığı için orta nokta civarlarında ani değişimler olacaktır.

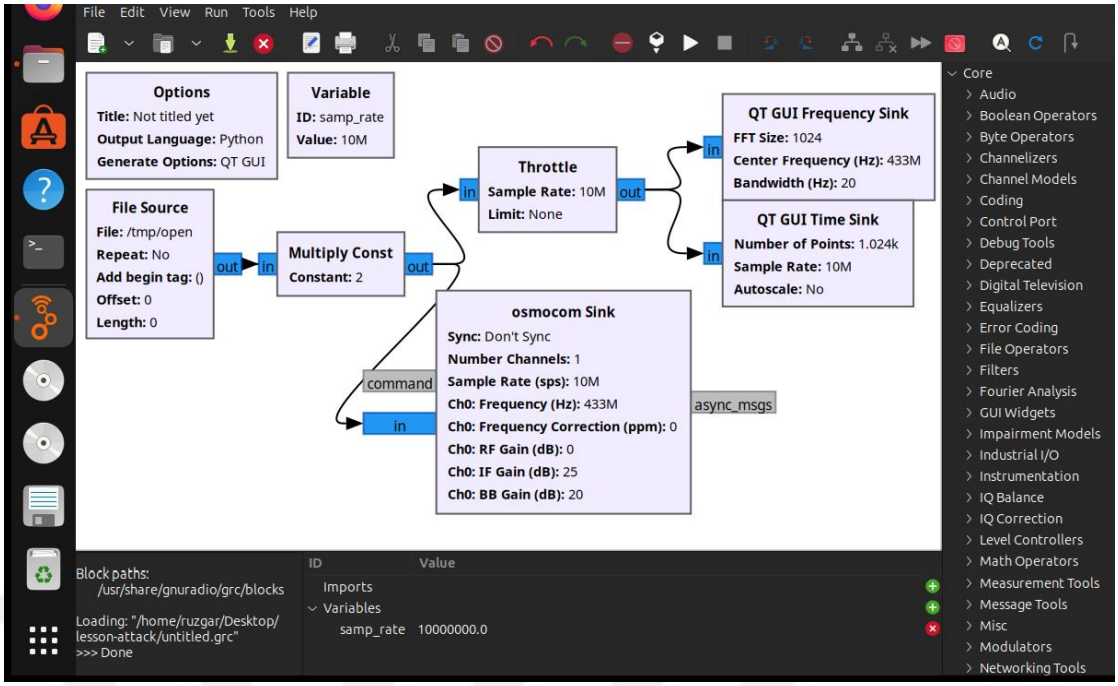


Şekil 6.3 Yakalanan sinyal gösterimi

Aracın kapısının açılması için butona basılmıştır. Araç anahtarı içerisindeki sistemin göndermiş olduğu sinyal, araç içerisinde bulunan alıcı sisteme iletilmiş ve kapı açılmıştır. Bu esnada gnu radio üzerinden yapılan akış grafiği çalışmaktadır. Çalışan akış grafiğinde osmocom source hackrf one cihazını alıcı işlevine getirmiştir. Böylelikle aracın kapısının açılması için gönderilen sinyal, hackrf one tarafından yakalanmıştır. Şekil 6.6'da görülen sarı çizgiler en yüksek desibelde ve genlikte yakalanan sinyalleri göstermektedir. Dolayısıyla butona basıldığında aracın kapılarının açılmasını sağlayan sinyalin özellikleri şekil 6.6'da görülen sarı çizgilerin sınırlarıdır. Yakalanan bu sinyal File Sink bloğu kullanılarak open adlı klasöre kayıt edilmiştir.

6.1.2. Yakalanan Sinyali Alıcıya İletmek

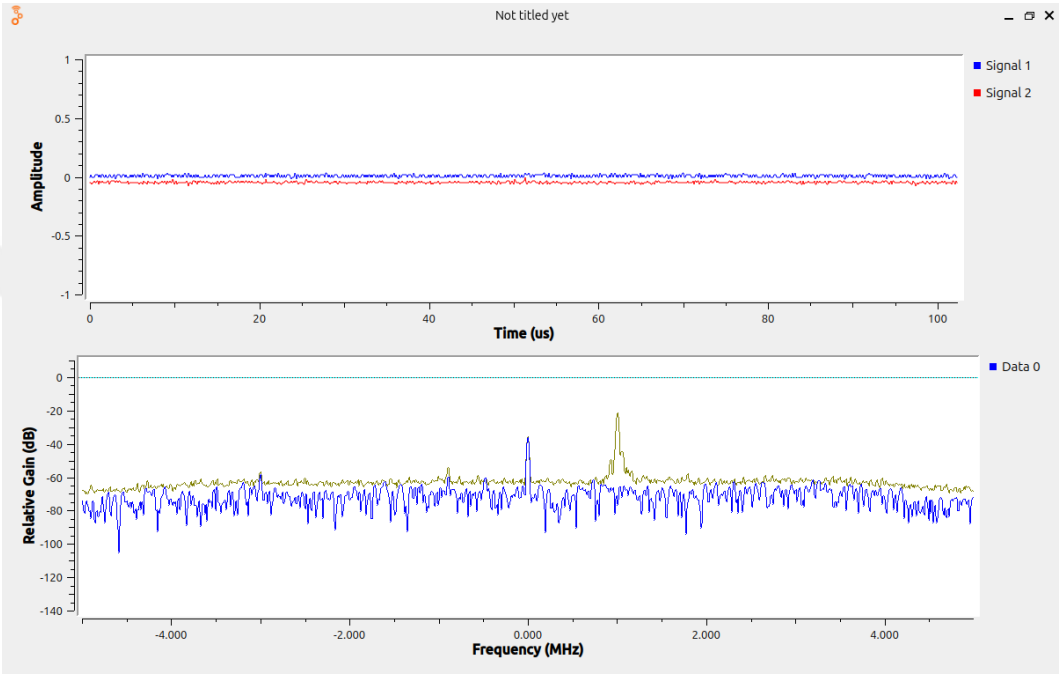
Bir önceki akış grafiğinde sinyal kopyalanmış ve open adlı klasöre kayıt edilmiştir.



Şekil 6.7 Yakalanan sinyali alıcıya ileten akış diyagramı

Şekil 6.7'de bulunan akış diyagramı ile yakalanan sinyalin alıcı sisteme iletilmesi amaçlanmaktadır. Akış grafiğinde olan File Source bloğunda repeat bölümü no yapılarak saldırının sürekli olarak tekrar etmesi engellenmiştir. File Source bloğuna şekil 6.7'de ki akış grafiği kullanılarak yakalanan sinyalin bulunduğu dosya yolu yazılmıştır. Böylelikle yakalanan sinyal şekil 6.7'de ki akış grafiğinde işlenmek üzere çağırılmıştır. Multiply Const bloğu sinyalin işlenmesiyle oluşabilecek kayıpları oluşabilmesi ihtimaline karşı akış grafiğinde kullanılmıştır. Bundan dolayı 2 olarak belirlenmiştir. Gelen sinyal 2 farklı bloğa gönderilmektedir. Bu bloklardan biri osmocom sink bloğuna iletilmiştir. Osmocom sink bloğunda ki parametreler osmocom source bloğunda sinyalin yakalandığı parametrelerle aynı olmalıdır. Dolayısıyla parametrelerin girişi değişime uğramadan yapılmıştır. Sinyalin iletildiği diğer blok ise throttle bloğudur. Throttle ile sinyalin saldırı yapıldığı esnada görselleştirilmesi için işlem hızı arttırılmaktadır. Dolayısıyla işlem hızının akış grafiğiyle eş zamanlı olması için 10 milyon örnekleme hızı olarak ayarlanmıştır. QT GUI Frequency Sink bloğu kullanılarak saldırı yapılan sinyalin görselleştirilen çizgisel grafiği görülmektedir. Sinyal 433 Mhz frekansta olduğu için merkez frekans 433 Mhz olarak yazılmıştır. QT GUI Time Sink bloğu kullanılarak ise saldırının zamanlaması görülmektedir. Sinyalin kopyalanması için akış grafiğinde belirtilen parametreler ile saldırı gerçekleştirecek

olan akış grafiğinde ki parametrelerin aynı olması büyük önem taşımaktadır. Çünkü farklı parametrelere sahip olunduğunda, alıcı devre üzerine gönderilen sinyali tanımlayamayacaktır. Dolayısıyla, bu durumda her ne kadar sinyal gönderimi gerçekleşirse bile alıcı sistem gelen sinyali işleyemeyecektir. Akış grafiğinde tüm parametreler kontrol edildikten sonra akış grafiği başlatılmıştır. Hackrf one cihazı bu durumda sinyal verici konumuna geçmiştir.



Şekil 6.8 Yakalanan sinyali iletirken oluşan grafik görüntüsü

Şekil 6.8 de sinyallerin akış grafiğinde belirtilen parametreler doğrultusunda sinyallerin görselleştirilmesi görülmektedir. Üst kısımda bulunan grafiğin QT GUI Frequency Sink bloğundan gelen sinyalleri göstermektedir. Üst kısımda ki grafikte yakalanan sinyallerin kayıt edilirken ne kadar fazla yükseklikte ve desibelde olduğu görülmektedir. Alt kısımda bulunan grafik ise sinyalin zamanlamasını göstermektedir. Saldırı için sinyal gönderilmiştir. Araç üzerindeki alıcı sistem hackrf one cihazından gelen sinyali tanımlamış ve işleyerek aracın kapılarını çalıştırmıştır.



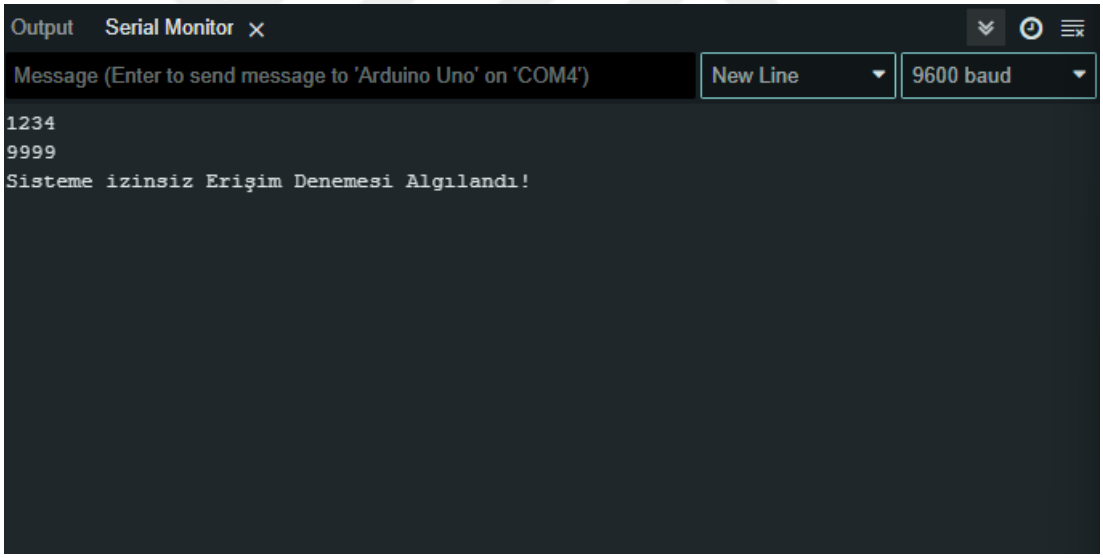
Şekil 6.9 Araç saldırı sonrası durumu

Sonuç olarak doğru frekansta doğru parametrelerin belirtilmesiyle birlikte sinyal saldırısı başarılı olmuştur. Dolayısıyla, günümüzde araçların ve anahtarlarının haberleşme yapılarına bakılarak bu türde yapılan saldırılarla araçlara dışardan erişim sağlanabilmektedir. Sürücü istemi dışında oluşan bu dışarıdan erişim araç hırsızlıklarının artmasına sebep olmaktadır. Ayrıca bu duruma ek olarak araçların fabrika anahtarlarından ziyade farklı bir anahtar ile araç kapılarını açılabilmektedir. Bu anahtar, aslında araç ile bağlantısı olmayan sahte bir anahtar olarak da nitelenebilir. Ancak sahte anahtarında çalışma yapısı sinyalin yakalanmasıyla aynı olmaktadır. Yani araç ile anahtar arasında iletilen sinyal sahte anahtar üzerinden herhangi bir araç kullanmadan kopyalanabilmektedir. Sinyalin kopyalanmasıyla birlikte sahte anahtar, fabrikadan çıkan orijinal anahtar görevini görmektedir. Sonuç olarak, yapılan her sinyal saldırısı aynı yöntemle uygulanmaktadır. Gerek yazılım tabanlı radyo frekans cihazı kullanılsın gerek ise sahte anahtar kullanılarak orijinal anahtarın sinyali kopyalansın saldırı yöntemi değişmemektedir. Dolayısıyla, bu duruma çözüm olması açısından sistemin içerisinde yapılacak mekaniksel veya daha uzun işlem süresine

sahip olacak olan şifrelendirme, yetkilendirme vb. durumlar kesin çözüm olmayabilmektedir. Dolayısıyla bu çalışma kapsamında çözüm olarak, gönderilen sinyalin yalnızca alıcı ve verici arasında tanımlanması gelen sinyalin kontrolünü sağlayan bir algoritma geliştirilmiştir.

6.2. Geliştirilen Araç Anahtar Yapısına Sinyal Saldırısı

Geliştirilen algoritma ile yapılan sinyal saldırısı başarısızlıkla sonuçlanmıştır. Bölüm 6.1 de yapılan işlemler tekrarlanmıştır. İşlemlerin tekrarlanmasıyla içerisinde şifre bulunan sinyal yakalanmıştır. Sinyalin yakalanmasıyla gnu radio içerisine kayıt edilmektedir. Bölüm 6.2 de yapılan işlemlerin aynısı burada ki saldırıda da yapılmıştır. Yakalanan sinyaller hackrf one cihazı ile iletilmeye başlanmıştır. Ancak araç üzerindeki alıcı sistemde bu sinyalin daha öncesinden algılandığı saptanmıştır. Sistemin sinyali tanımasıyla birlikte bu durumu bir sızma girişimi olarak algılamıştır. Dolayısıyla araç kapılarını açma veya kapatma işlemini gerçekleştirmemiştir.



Şekil 6.10 Geliştirilen sistemin izinsiz giriş algılaması

YEDİNCİ BÖLÜM

Çalışma kapsamında incelenen radyo dalgaları, bir çok alanda kullanılmaktadır. Bu alanlardaki kullanımları benzerlik gösteren cihazlar üzerinde ise güvenlik açığı bulunmaktadır.

7.1. Askeri

Bu çalışma kapsamında geliştirilen algoritma, radyo frekansı kullanılarak kablosuz haberleşme yapısına sahip sistemlere yönelik olmaktadır. Uygulanan sinyal saldırısı ise radyo dalgalarının yakalanıp tekrar iletilmesiyle sistemlere saldırı yapmasını mümkün kılmaktadır. Üretilen prototip araç üzerinde günümüz araçların radyo dalgaları kullanarak iletişim yapan araç ve anahtar yapısı tasarlanmış ve incelenmiştir. Sinyal saldırısı yapılarak siber saldırı başarılı olmuştur. Bu sinyal saldırısı, oluşturulan sisteme benzerlik gösteren tüm sistemlerde uygulanması mümkündür. Ayrıca, farklı alanlarda veya sistemlerde uygulanması ise farklı ve değişebilir şiddette riskler içermektedir.

Askeri alanlarda radyo dalgaları kullanılarak iletişim kurulmasını sağlayan telsizler bulunmaktadır. Bu telsizler, mesafelerine veya farklı özeliklerine göre birbirinden farklılık gösterebilmektedir. Örneğin, APCO - 25 model telsizin mesafesi TETRA model telsizden daha uzun olmaktadır (Şahin, 2015). Ancak genel olarak kullanılan iletişim yapısı radyo dalgaları ile olmaktadır. Ayrıca çalışma şekillerine göre de birbirlerinden farklılık gösterebilmektedirler. Şahin, buna örnek olarak APCO – 25 model telsiz yarı dubleks olarak çalıştığını ve bu çalışma yapısı sinyalin sadece algılanması veya iletilmesi şeklinde olduğunu belirtmiştir. Alıcı verici işlemi şeklinde olan haberleşme yapısına yapılan sinyal yakalama saldırısında telsizin algılanacağı sinyal algılanabilir. Telsizlerin kullandığı bu sinyaller, sesin iletimi olarak kullanılmaktadır. Saldırı sonucu yakalanan sinyalin işlenmesiyle bu ses dinlenebilir. Dolayısıyla askeri alanda ki gizliliğin önemli ölçüde olduğu bilindiğinden dolayı telsizlerin haberleşmesinin güvenliliğinin alınması gerekmektedir. Aksi takdirde önemli ölçüde gizliliğe sahip olması gereken bu veri akışının ele geçirilmesiyle veriler çalınabilmektedir.

Askeri alanlarda kullanılan en önemli sistemlerden olan radar sistemleri de radyo dalgaları yapısını kullanmaktadır. 1900'lı yıllarda ilk çalışmaları başlanmıştır.

Çalışmalarda radyo dalgaların iletilmesi ve iletimi algılayan sistem üzerinde de gelen radyo dalgaların değerlendirilmesiyle radar sistemlerinin ilk olarak çalışma yapıları oluşturulmuştur. Daha sonrasında teknolojiyi geliştirerek uzun alanlar boyunca bu işlemin yapılmasıyla bölgenin görüntülenmesi amaçlanmıştır (Yusufoğlu, 2013). Radarlar özelliklerine ve veri akış hızlarına bağlı olarak, birçok türde bulunabilirler. Ancak çalışma yapılarında radyo dalgaları kullanılmaktadır (Kale, 2010). Bir bölge üzerinde görüntüleme amaçlı olarak gönderilen sinyalin, radar içerisinde işlenmesiyle görüntüleme yapılmaktadır. Aynı şekilde bu gönderilen sinyale yapılacak olan sinyal saldırısında sinyalin yakalanması mümkündür. Yakalanan sinyal üzerinde işleme yapılması ile de sinyalin içerdiği gizli verilere erişilebilmektedir. Askeri alanda bu bilgilerin ele geçirilmesi hayati öneme sahip olmaktadır. Dolayısıyla, radar sistemlerinin kullandığı radyo dalgalarının güvenliği sağlamak büyük önem teşkil etmektedir.

Askeri alanda kullanılan siber fiziksel sistemlerden olan SİHA'lar (Silahlı İnsansız Hava Aracı), radyo dalgalarıyla haberleşme yapısına sahip en tehlikeli sistemlerdendir. Çünkü üzerinde çeşidine göre değişebilen silahlar bulunmaktadır. Bomba, makineli silahlar vb. bu silah çeşitlerindendir. Bu silahların ateşlenme mekanizmaları, SİHA'ların geometri yapılarında bulundukları konuma göre değişmektedir (Güçlü, 2020). Örneğin, bombalama amaçlı olan SİHA'larda tetikleme mekanizması çalıştırılarak bomba bırakılırken, makineli silah amaçlı kullanılanlar farklı şekilde tetiklenebilir. Tetiklenme mekanizması uzaktan kontrol edilebilmektedir. Bu durumda kullanılan haberleşme yapısı radyo dalgaları ile yapılmaktadır. Bu haberleşme yapısına uygulanacak olan sinyal saldırısında ateşleme mekanizmasının çalışmasını sağlayacak sinyal yakalanabilmektedir. Yakalanan sinyal tekrardan SİHA'ya iletilerek ateşlemenin başlatılabilir. Saldırının başarıyla sonuçlanmasıyla beklenmedik yerde veya zamanda ateşlenen silah sistemleri kötü durumlarla sonuçlanabilir. Dolayısıyla haberleşme yapısının güvenlik önleminin alınması hayati önem taşımaktadır.

7.2. Sağlık

Hastane kullanılan cihazların çalışma yapıları insanlar üzerinde kullanıldığı için hayati önem taşımaktadır. Hastaların iyileşmesi, takip edilmesi vb. durumlar için birçok cihaz sağlık alanında kullanılmaktadır. Çünkü hastaların iyileşme süreçlerinde yaşadığı

durumlara göre takip edilmesi gerekebilir. Dolayısıyla doktorların hastalarda oluşan bu parametreleri izleyebilmesi için radyo dalgalarını kullanarak veri alışverişi sağlayan haberleşme sistemi geliştirilmiştir. Hastanın tedavi sürecinde fizyolojik özelliklerini izleyebilmek için tasarlanan sistem, doktoru bilgilendirmektedir. Sistemde hasta üzerinde takılı olan cihaz ile parametrelerin ölçüp işlendikten sonra iletilmesini sağlamaktadır. Sistemin diğer cihaz ise doktorun hastayı takip edebilmek için görebileceği alıcı cihazıdır. Bu sistemde hastanın nabız vb. durumlarında oluşan değişmeler verici içerisinde işlenerek sinyale dönüştürülür. Alıcı tarafından algılanan sinyal ile hastanın durumunu gözlemleyebilmektedir. Radyo dalgalarını kullanan bu sisteme yapılacak olan sinyal saldırısı ile hastanın bilgilerinin iletildiği sinyal yakalanabilir. Yakalanan sinyal ile gizlilik bilgiler ele geçirilebilmektedir (Özparlak, Koçoğlu, 2009).

7.3. Taşımacılık

Firmaların ticari işlemlerinin hareketliliğini veya diğer kurumların taşımak istedikleri ürünlerin takibini kolaylaştırması için radyo dalgaları kullanan sistemler geliştirilmiştir. Bu sistemler sayesinde herhangi bir ürünün ilk üretim aşamasından dağıtımına kadar tüm süreci takip edebilmektedirler. Böylelikle herhangi bir ürün için nerede daha çok ihtiyaç olduğunu tespit edilebilmektedir. İçerisinde sinyali sorgulayıcı, sonrasında sinyali içerisinde işlemesi için denetleyici donanım içermektedir. Ayrıca bu sistemlere ek olarak, ürünler hakkında bilgi içeren etiketler bulunmaktadır (Yüksel, Odabaşı, 2009). Sorgulayıcı etikete komut göndermektedir. Komutu alan etiket, bilgileri iletmek için radyo dalgaları yaymaktadır. Radyo dalgalarını yakalayan sorgulayıcı, denetleyiciye iletmektedir. Etiketin radyo dalgalarını yayarken yapılacak olan sinyal saldırısı ile o sinyaller yakalanabilmektedir. Yakalanan sinyaller işlendikten sonra ürün hakkında ki tüm bilgiler öğrenilebilmektedir. Bu tür sistemlere ek olarak, taşımacılık alanında bu şekilde kullanılan uygulamaların alternatifleri bulunmaktadır. Otomatik ürün tanıma veya izleme, veri yönetimi, veri analizi vb. alternatifler bulunmaktadır (Yüksel, Zaim, 2009).

Bu sistemlere ek olarak radyo frekanslarının haberleşme yapılarının en yoğun olarak kullandığı bir alan ise denizcilik alanı olmaktadır. Denizlerin güvenliği için gemilerin

takip edilmesi önem arz etmektedir. Örneğin gemilerin okyanuslarda mahsur kalması durumunda yerlerinin bilinmesi yardım gelmesini kolaylaştırabilir. Ayrıca ülkelerin sınırlarının ihlal edilmemesinden dolayı gemilerin takip edilmesi önem arz etmektedir. Gemilerin ülkelerin sınırları çevresinde geçiş yapması esnasında takip edilmektedir. Buna ek olarak gemilerde bulunan etiketlerin okunmasıyla gemiler hakkında bilgi sahibi olunabilmektedir. Tüm bu işlemler radyo dalgaları kullanılarak yapılmaktadır. Dolayısıyla alıcı verici durumunda olan bu işlemlere yapılacak olan sinyal saldırılarında bilgiler ele geçirilebilmektedir (Bayrak, Yılmaz, Atik, 2019).

SEKİZİNCİ BÖLÜM

Çalışmanın sonucunda analizlerin ve incelemelerin yapılmasıyla bulgular oluşmuş ve bu bulgulara öneriler verilmiştir.

8.1. Sonuçlar

Bu çalışma kapsamında amaçlanan, otonom olarak çalışan bir aracın radyo dalgaları kullanarak çalışan sistemlerin güvenlik açıklarını saptamaktır. Amaçlar doğrultusunda otonom çalışan sistemlerin yapısı incelenmiştir. Araçlarda bulunan kapı kilit sistemi, uzaktan kontrol veya haberleşme sistemi gibi otonom olarak haberleşen sistemlerin radyo dalgalarına yapılacak saldırılar incelenmiştir. İncelemeler sonucunda radyo dalgalarının siber boyutlarda sinyal kopyalama ve sinyal iletimi saldırıları yapılarak sistemler erişim sağlanmıştır. Bu yapıları kullanan cihazların, radyo frekanslarıyla haberleşmesinde, güvenlik açıkları bulunabilmektedir. Güvenlik açıklarının sömürülmesiyle kullanılan alanlara göre kötü sonuçlar ortaya çıkmaktadır. Askeri, sağlık, taşımacılık, haberleşme, lojistik vb. birçok alanda radyo frekansı yapısını kullanan cihazlar bulunmaktadır. Bu cihazların güvenlik önlemlerinin alınması gün geçtikçe önemli hale gelmektedir.

Çalışma kapsamında, bu yapılara özgü olarak bir şifreleme saldırısı yapılmıştır. İlk aşamada haberleşme sistemlerinin yapısı incelenmiş ve prototip olarak aracın anahtarla olan yapısı kurulmuştur. Bu aşamada radyo dalgalarıyla haberleşen yapı, günümüz araçlarda kullanılan yapıda olmaktadır. Çalışmanın sonraki aşamasında bu radyo sinyallerinin kopyalanması amaçlanmıştır. Kopyalama işlemlerinin yapılabilmesi için sinyalin iyi tanımlanması gerekmektedir. Dolayısıyla, kopyalama esnasında kullanılan uygulamalarda parametre ayarları yapılmıştır. Bu ayarlar doğrultusunda anahtarın araca gönderdiği komutlar yakalanmıştır. Son aşama olarak araca tekrar iletildiğinde kapı açılmıştır. Sistem saldırısı başarı ile gerçekleşmiştir. Bu duruma çözüm olarak basit şekilde çalışan bu sinyal alıcı verici algoritması için geliştirilen sistem ile sinyalleri birbirinden farklı olarak tanımlanmıştır. Şifreleme algoritmasını geliştirilmesiyle sistem sinyali algıladığında herhangi bir eylem gerçekleştirememektedir.

8.2. Sınırlılıklar

Donanım ve Yazılım Kısıtlamaları: Tezde kullanılan HackRF One ve Gnu Radio gibi araçlar, belirli frekans aralıkları ve işlem kapasiteleri ile sınırlıdır. Bu kısıtlamalar, tezin kapsadığı siber güvenlik senaryolarının gerçek dünya uygulamalarında doğrudan replike edilmesini sınırlayabilir.

Kapsamın Darlığı: Araştırma, özellikle radyo frekans saldırılarına odaklanmıştır. Ancak, otonom araç sistemlerini tehdit edebilecek diğer siber saldırı vektörleri (örneğin, ağ güvenlik zafiyetleri veya yazılım hataları) tez kapsamında detaylandırılmamıştır.

Deneysel Validasyon: Tezde önerilen çözümlerin etkinliği, kontrol edilen laboratuvar ortamında test edilmiştir. Gerçek dünya koşulları altında, özellikle değişken çevresel faktörler ve farklı saldırı senaryoları göz önüne alındığında, bu çözümlerin performansı farklılık gösterebilir.

Ölçeklenebilirlik: Şifreleme ve sinyal işleme tekniklerinin ölçeklenebilirliği, tezde ele alınmamıştır. Büyük ölçekli otonom araç filolarında bu tekniklerin uygulanabilirliği ve yönetimi, ek araştırma gerektirebilir.

Güvenlik Güncellemeleri ve Bakım: Tezde, güvenlik çözümlerinin sürekli güncellenmesi ve bakımı gerektiği üzerinde durulmamıştır. Otonom araçlar için güvenlik güncellemelerinin dağıtımı ve yönetimi, siber güvenlik risklerini yönetmede kritik bir rol oynar.

Etkileşimli ve Bağlı Sistemlerin Kompleksitesi: Otonom araçlar, geniş bir bağlantılı cihaz ekosistemi içinde çalışır. Bu bağlamda, diğer araçlar veya altyapı ile etkileşimler, güvenlik açısından yeni zorluklar ortaya koyabilir. Tezde bu tür etkileşimlerin potansiyel güvenlik etkileri ele alınmamıştır.

Bu sınırlılıklar, tezin sonuçlarının uygulanabilirliği ve genelleştirilmesi üzerinde önemli etkilere sahip olabilir. Ancak, bu sınırlılıklar aynı zamanda gelecekteki araştırmalar için potansiyel alanlar olarak da görülebilir. Bu çalışmanın bulguları, otonom araçların güvenliğini artırmaya yönelik devam eden çabalar için değerli bir temel oluşturmaktadır.

8.3. Öneriler

Radyo dalgalarını kullanan cihazların teknik özelliklerinin belirlenmesiyle radyo dalgalarına şifreleme yapılabilir.

Sistemlerin kullandığı frekans ve parametreler özgün olabilir.

Yapılan çalışma kapsamında radyo sinyalleri üzerine tanımlama çalışmaları ile alınabilecek önlemler arttırılabilir.

Askeri alanda kullanılan teçhizatlar veya sistemlerin haberleşme yapıları ülkelerin güvenliği için önem arz etmektedir. Dolayısıyla askeri alanlara özgün haberleşme yapıları olabilir. Bu yapıların şifrelenme çalışmaları büyük bir önemle gizli tutulmalıdır. Yalnızca ülkelerin vatandaşları içerisinde bu yapıların öğretilmesi ve geliştirilmesi yapılabilecek çözümler arasında olmaktadır.

Günlük hayatta insanların sık kullandığı cep telefonları, bilgisayarlar, buzdolabı, mikrodalga vb. teknoloji aletlerin radyo frekanslarıyla haberleşme yapısı kullanan türleri bulunmaktadır. Bu cihazlar üzerinde kullanıcılara eğitim verilmelidir. Bu durumun sonucu olarak kullanıcı, cihazların veya sistemlerin güvenliğini kendi şartlarında alabilmeyi öğrenmiş olacaktır.

Sağlık alanında kullanılan cihazlar ise insanlar üzerinde işlem görmektedir. Bir kişinin veya kurumun bilgisini çalmak için yapılan saldırılar olmaktadır. Ayrıca sistem çalıştığı esnada bir saldırı yapılarak hatalı çalışmasını veya sistemin eğer varsa oluşturabileceği tehlikeleri (yangın vb.) tetikleyebilir. Dolayısıyla bunun için sistemler belirli kişilerce kullanılıp bu kişilere eğitim verilmelidir. Cihazlar üzerinde ki haberleşme yapıları ise önemli bilgiler içerebileceği için şifrelenme yöntemi uygulanmalıdır.

Gelecek çalışmalar, otonom araç sistemlerinin güvenliğini artırmak adına yapay zeka (AI) teknolojilerinin daha etkin kullanımını içermelidir. Özellikle, yapay zeka tabanlı saldırı tespit sistemleri, araçların algıladığı veriler üzerinde gerçekleştirilen False Data Injection (FDI) saldırılarını tespit edebilmek için büyük potansiyel taşımaktadır. FDI saldırıları, sensor verilerine kasıtlı olarak yanlış veya yanıltıcı bilgilerin enjekte edilmesiyle gerçekleşir, bu da otonom araçların karar verme süreçlerini ciddi şekilde bozabilir. Yapay zeka, bu tür saldırıların karakteristik örüntülerini öğrenerek, normal ve anormal veri arasındaki farkları belirleyebilir. Gelecekteki araştırmalar, çeşitli

yapay zeka modellerini (örneğin, derin öğrenme, makine öğrenmesi) kullanarak, gerçek zamanlı veri akışı içerisinde anomali ve saldırı tespiti yapma kapasitesini geliştirmeyi hedeflemelidir. Bu sayede, otonom araçların güvenlik seviyeleri artırılabilir ve bu araçların güvenilirliği konusunda kamuoyunun endişeleri azaltılabilir. Bu tür sistemlerin geliştirilmesi, aynı zamanda siber güvenlik stratejilerinin daha kapsamlı ve dinamik bir şekilde evrimleşmesine olanak tanıyacak ve otomotiv endüstrisinde yapay zekanın rolünü daha da belirginleştirecektir.

KAYNAKÇA

Akçay, M., Canbaz, M., & Diş, M. Ö. (2022). Akıllı Konut Uygulaması. Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi, 3(1), 1-5.

Ardatürk, A. Ş. (2022). Mekân temsilinde yeni bir açılım; otonom araçlar. The Journal of Academic Social Science Studies.

author unknown. (2010). Otomotiv sektör raporu : 2009. MÜSİAD.(kitap)

Baki, S., & Tutkun, N. (2021). Otomotiv haberleşmesinde denetleyici alan ağı için hibrit bir saldırı savuşturma uygulaması. Anadolu Bil Meslek Yüksekokulu Dergisi, 16(61), 51-72.

Bakioğlu, G., & Atahan, A. (2021). Otonom Araçların Benimsenmesi ve Güvenlik Algılarının İncelenmesi. Avrupa Bilim ve Teknoloji Dergisi, (32), 633-639.

Bayrak, F., Yılmaz, Ö. D., & Atik, O. (2019). Radyo Frekansı İle Tanımlama Teknolojisinin Deniz Turizminde Kullanımı. Dokuz Eylül Üniversitesi Denizcilik Fakültesi Dergisi, 11, 107-136.

Bedir, A. (2002). Türkiye'de otomotiv sanayii gelişme perspektifi (Vol. 2660). DPT.

Bilban, M. (2020). Otonom araç üzerinde artırılmış gerçeklik uygulaması (Doctoral dissertation, Necmettin Erbakan University (Turkey)).

Boyaci, A. Gömülü sistemler için mikro kernel işletim sistemi tasarımı (Master's thesis, Fen Bilimleri Enstitüsü).

Coşkun, A. R. (2003). Mekatronik Sistem Elemanlarının Incelenmesi Ve Bir PLC Kontrollü Sistem Uygulaması (Doctoral dissertation, Marmara Universitesi (Turkey)).

Demirkesen, A. (2012). Mekatronik bir sistemin modellenmesi, benzetimi, gerçeklenmesi ve gerçek zamanlı denetimi (Doctoral dissertation, Bursa Uludag University (Turkey)).

Docteur, J. (2023). Endüstriyel devrimler : Modern dünyanın doğuşu. 50Minutes.com.(kitap)

Doğru, Z. Döngüde donanımsal benzetim ve gerçek zamanlı gömülü sistemler (Master's thesis, Fen Bilimleri Enstitüsü).

Gökozan, H., & Taştan, M. (2018). Akıllı taşıtlar ve kontrol sistemleri. Mesleki Bilimler Dergisi (MBD), 7(2), 58-62.

Ghintab, S. S., & Hassan, M. Y. (2024). PID-like IT2FLC-Based Autonomous Vehicle Control in Urban Areas. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-024-09104-4 .

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

Güçlü, R. Mini Siha Konsept Tasarimi ve Analizi.

Güleryüz, H. 3D Yazıcı ve Robotik Kodlama Uygulamalarının Öğretmen Adaylarının 21. Yüzyıl Öğrenen Becerileri, STEM Farkındalık ve Stem Öğretmen Özyeterliğine Etkisi.

Günay, M., Gündüz, S., Yılmaz, H., Yaşar, N., & Kaçar, R. (2020). PLA esaslı numunelerde çekme dayanımı için 3D baskı işlem parametrelerinin optimizasyonu. Politeknik Dergisi, 23(1), 73-79.

Gürtaş, S. (2020). Otonom araç sürüş destek sistemleri ve yapay zeka uygulamaları (Doctoral dissertation, Bursa Uludag University (Turkey)).

Hakverdi, F. (2021). Akıllı Şehirlerde Engelsiz Akıllı Ulaşım (Doctoral dissertation, Necmettin Erbakan University (Turkey)).

Haritha, H., Seethal, C. R., & Gandhiraj, R. (2017, January). Realization of Kalman filter in GNU radio. In 2017 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

Hussain, G., Khan, W. A., Ashraf, H. A., Ahmad, H., Ahmed, H., Imran, A., ... & Abbas, G. (2019). Design and development of a lightweight SLS 3D printer with a controlled heating mechanism: Part A. International Journal of Lightweight Materials and Manufacture, 2(4), 373-378.

Kale, A. (2010). Yazılım tanımlı radar (Master's thesis, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü).

Kara, İ. (2009). CAN haberleşme protokolünün incelenmesi ve bir sıcaklık kontrol sistemine uygulanması (Master's thesis, Fen Bilimleri Enstitüsü).

Koçak, Ç., & Kırbaş, İ. (2016). Arduino tabanlı prototip akıllı ev sistemi tasarımı. Akademik Bilişim, 3.

Kun, K. (2016). Reconstruction and development of a 3D printer using FDM technology. Procedia Engineering, 149, 203-211.

Li, D., Zhang, H., Cheng, J. et al. Improving efficiency of DNN-based relocalization module for autonomous driving with server-side computing. J Cloud Comp 13, 25 (2024). https://doi.org/10.1186/s13677-024-00592-1

Naiseh, M., Clark, J., Akarsu, T. et al. Trust, risk perception, and intention to use autonomous vehicles: an interdisciplinary bibliometric review. AI & Soc (2024). https://doi.org/10.1007/s00146-024-01895-2

Özparlak, T. B. S. B. L., & Koçoğlu, O. K. A. Ameliyat Sonrası Hasta Üzerinden Alınan Biyoelektrik Sinyallerin Radyo Frekans (RF) Haberleşme Sistemi ile Taşınması için Sistem Tasarımı.

Schmid, T. (2006). Gnu radio 802.15. 4 en-and decoding. unpublished document and source.

Şahin, F. (2015). Telsiz Haberleşme Standartları. İstanbul Aydın Üniversitesi Dergisi, 7(27), 15-30.

Şahinoğlu, G. (2006). Akıllı evlerde otomasyon (Doctoral dissertation, Marmara Universitesi (Turkey)).

Sivasankari, S.A., Gupta, D., Keshta, I. et al. Anonymity and security improvements in heterogeneous connected vehicle networks. Int J Data Sci Anal (2024). https://doi.org/10.1007/s41060-023-00499-1

Yılmaz, F., Arar, M. E., & Koç, E. (2013). 3D baskı ile hızlı prototip ve son ürün üretimi.

Yulu, A. (2018). Türkiyede otomotiv sanayisinin coğrafi dağılışı.

Yusufoğlu, M. H. (2013). Yapay açıklıklı radar görüntülerinde hareketli hedef tespiti (Master's thesis, Bilişim Enstitüsü).

Yüksel, M. E., & Odabaşı, Ş. D. (2009). Nesneler İzlenebilir ve Yönetilebilir mi? Çözüm: RFID. Akademik Bilişim, 11-13.

Yüksel, M. E., & Zaim, A. H. (2009). Otomatik Nesne Tanımlama, Takibi ve Yönetiminde RFID'nin Yeni Nesil Kablosuz İletişim Teknolojileri ile Birlikte Kullanımı, XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa.