T.C.
MANİSA CELAL BAYAR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

ELEKTRİKLİ ARAÇLARDA SİSTEM GÜVENLİĞİNİN ARTTIRILMASI

Umut ŞENSÖZ

Danışman
Dr. Öğr. Üyesi Mustafa NİL

MANİSA–2024

Umut
ŞENSÖZ

ELEKTRİKLİ ARAÇLARDA SİSTEM GÜVENLİĞİNİN ARTTIRILMASI

2024

TAAHHÜTNAME

Bu tezin Manisa Celal Bayar Üniversitesi Lisansüstü Eğitim Enstitüsü Elektrik Elektronik Mühendisliği Ana Bilim Dalında, akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin referans gösterilerek tezde yer aldığını, tamamen kendi çalışmam olduğunu, her alıntıya kaynak gösterdiğimi, tezin yazımında akademik ve etik kurallara aykırı herhangi bir yapay zeka ve program kullanmadığımı beyan ederim.

Umut ŞENSÖZ

ÖZET

Yüksek Lisans Tezi

ELEKTRİKLİ ARAÇLARDA SİSTEM GÜVENLİĞİNİN ARTTIRILMASI

Umut ŞENSÖZ

Manisa Celal Bayar Üniversitesi
Lisansüstü Eğitim Enstitüsü
Elektrik Elektronik Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Mustafa NİL

Teknolojinin ilerlemesiyle birlikte araçlar ve otomotiv elektroniğinde bir değişim süreci yaşanmaktadır. Bu doğrultuda elektrikli araçların hayatımızdaki yeri artmış, gelişmiş elektronik cihazlar, akıllı araç özellikleri, gelişmiş sürücü destek sistemleri gibi özellikler ve cihazlar otomotiv endüstrisinde yaygın olarak kullanılmaya başlanmıştır.

Araçlarda kullanılan Elektronik Kontrol Ünitelerinin (ECU) sayıları artmakta, bu kontrol ünitelerine ek olarak çok sayıda ekran, modem, bilgi-eğlence sistemleri, gelişmiş sürücü destek sistemleri gibi elektronik bileşenler ve özellikler elektrikli araçlarda yerini almaya başlamıştır. Tüm bu özellikler ve elektronik bileşenler beraberinde birçok sensör ve ECU kullanımını gerektirmektedir. Sensörlerden gelen yüksek güvenlik seviyesindeki veriler, farklı haberleşme protokolleri üzerinden denetleyicilere taşınmakta ve denetleyiciler tarafından işlenmektedir. Bu yüksek güvenlikli veriler dışarıdan manipüle edilerek, aracın kritik özellikleri (direksiyon, gaz pedalı, fren, kilit, vb.) kontrol edilebilmektedir. Bilgi-eğlence (infotainment) ve bağlanabilirlik (connectivity) özelliklerinin gelişmiş versiyonlarının araçlarda yer alması ile birlikte araçlar dış birimler ile haberleşebilir duruma gelmiştir. Araçtan her şeye (V2X) ve ECU yazılım güncellemeleri için havadan (OTA) güncelleme gibi özellikler araçlarda kullanılmaktadır. Bulut ve internetten araca alınan veriler, araç içi ağındaki bazı ECU'lar tarafından kullanılmakta ve araçtaki bazı kritik özellikleri kontrol etmektedir. Bu durumda hem dış haberleşme hem de araç içi haberleşme güvenli bir şekilde gerçekleştirilmelidir.

Bu çalışmada, Gelişmiş Şifreleme Standartı (AES) ve Özel Veya (XOR) şifreleme yöntemlerini içeren bir şifreleme mekanizmasına ve kimlik doğrulama fonksiyonuna sahip güvenli bir araç içi haberleşme sistemi tasarlanarak elektrikli aracın sistem güvenliğinin arttırılması hedeflenmiştir. Kontrol Alan Ağı (CAN) ve Evrensel Asenkron Alıcı Verici (UART) haberleşme protokolleri kullanılarak hibrit bir sistem oluşturulmuştur. Şifreleme işlemlerinde rastgele sayılar kullanılarak şifreleme güvenliğinde artış sağlanmıştır. Tüm bu gerçekleştirilen işlemler ile araç haberleşme ağındaki kritik ve önemli verilerin dışarıdan ulaşılabilir, anlamlandırılabilir ve manipüle edilebilir olmaması amaçlanmıştır.

Anahtar Kelimeler: (Araç İçi Haberleşme, ECU, Otomotiv Siber Güvenlik, Otomotiv Elektroniği, Mesaj Şifreleme, Kimlik Doğrulama)

2024, 94 sayfa

ABSTRACT

M.Sc. Thesis

INCREASING SYSTEM SECURITY IN ELECTRIC VEHICLES

Umut ŞENSÖZ

Manisa Celal Bayar University
Graduate School of Education
Department of Electrical and Electronics Engineering

Supervisor: Asst. Prof. Dr. Mustafa NİL

With the advancement of technology, there is a change process in vehicles and automotive electronics. In this direction, the place of electric vehicles in our lives has increased, features and devices such as advanced electronic devices, smart vehicle features, advanced driver assistance systems have been widely used in the automotive industry.

The number of Electronic Control Units (ECU) used in vehicles is increasing and in addition to these control units, electronic components and features such as many screens, modems, infotainment systems and advanced driver assistance systems have begun to take their place in electric vehicles. All these features and electronic components require the use of many sensors and ECUs. High security level data coming from sensors are transferred to controllers via different communication protocols and processed by the controllers. By manipulating these highly secure data from the outside, critical features of the vehicle (steering wheel, accelerator pedal, brake, lock, etc.) can be controlled. With the introduction of advanced versions of infotainment and connectivity features in vehicles, vehicles have become able to communicate with external units. Features such as Vehicle-to-Everything (V2X) and Over-the-Air (OTA) updates for ECU software updates are used in vehicles. Data received from the cloud and the internet to the vehicle is used by some ECUs in the in-vehicle network and controls some critical features in the vehicle. In this case, both external communication and in-vehicle communication must be performed securely.

In this study, it is aimed to increase the system security of the electric vehicle by designing a secure in-vehicle communication system with an encryption mechanism that includes Advanced Encryption Standard (AES) and Exclusive Or (XOR) encryption methods and authentication function. A hybrid system was created using Controller Area Network (CAN) and Universal Asynchronous Receiver Transmitter (UART) communication protocols. An increase in encryption security has been achieved by using random numbers in encryption processes. With all these operations, it is aimed to ensure that critical and important data in the vehicle communication network cannot be accessed, interpreted and manipulated externally.

Keywords: (In-Vehicle Communication, ECU, Automotive Cyber Security, Automotive Electronics, Message Encryption, Authentication)

2024, 94 pages

ÖNSÖZ VE TEŞEKKÜR

Bu çalışmada, şifreleme ve doğrulama fonksiyonlarına sahip, güvenli bir araç içi haberleşme sistemi tasarlanarak, elektrikli aracın sistem güvenliğinin arttırılması hedeflenmiştir. Çalışmanın giriş bölümünde, çalışma motivasyonu, çalışmanın amacı, önemi ve katkısı anlatılmıştır. Genel bilgiler bölümünde, çalışma konusu hakkındaki literatür taramalarına, konu ile ilgili teorik bilgilere ve araştırmalara yer verilmiştir. Materyal ve yöntemler bölümünde, çalışmanın deneysel aşamasında kullanılan elektronik malzemeler ve kullanılan yöntemler hakkında detaylar ve bilgiler verilmiştir. Araştırma bulguları ve tartışma bölümünde, uygulama çalışmasının detayları ve çıktıları anlatılmıştır. Sonuç ve öneriler kısmında ise, çalışmadan elde edilen sonuç ve çıktılar anlatılmış, yapılabilecek gelecek çalışmalar ve geliştirmeler hakkında öneriler verilmiştir.

Çalışmamın her aşamasında bana destek olan, bilgi ve deneyimleri ile yol gösteren danışman hocam Sayın Dr. Öğr. Üyesi Mustafa NİL'e, çalışmam ve yüksek lisans eğitimim süresince verdiği fikirlerle ve önerilerle bilgi ve düşüncemi arttıran Sayın Doç. Dr. Ömer AYDIN'a, lisans eğitimim süresince aldığım kaliteli eğitimden dolayı Manisa Celal Bayar Üniversitesi Mühendislik Fakültesi Elektrik Elektronik Mühendisliği Bölümündeki sayın öğretmenlerime, her konuda beni destekleyen ve yönlendiren canım annem Bedriye ŞENSÖZ'e, şu an bir bireyi olmaktan gurur duyduğum ve zevkle yaptığım işim olan Elektrik Elektronik Mühendisliğine beni yönlendiren canım babam İsmail ŞENSÖZ'e, manevi olarak her daim yanımda olan canım kardeşim Buket ŞENSÖZ'e, teknik ve manevi olarak beni destekleyen, verdiği öneriler ile eğitim, iş ve özel hayatımda bir yol gösterici olan hayat arkadaşım Sevde GÖKCE'ye içtenlikle teşekkür ederim.

Umut ŞENSÖZ
Manisa, 2024

İÇİNDEKİLER

SİMGELER VE KISALTMALAR DİZİNİ

ABS Anti Lock Braking System (Kilitlenme Karşıtı Fren Sistemi)

ACC Adaptive Cruise Control (Uyarlanabilir Hız Kontrolü)

ADAS Advanced Driver Assistance Systems (Gelişmiş Sürücü Destek Sistemleri)

ADC Analog-to-Digital Converter (Analogtan Dijitale Dönüştürücü)

AEB Automatic Emergency Braking (Otomatik Acil Durum Frenleme)

AES Advanced Encryption Standard (Gelişmiş Şifreleme Standartı)

AFH Adaptive Frequency-Hopping (Uyarlanabilir Frekans Atlama)

A-MPDU Aggregate MAC Protocol Data Unit (Toplu MAC Protokolü Veri Birimi)

A-MSDU Aggregate MAC Service Data Unit (Toplu MAC Servis Veri Birimi)

ANV Automotive Night Vision (Otomotiv Gece Görüşü)

BLE Bluetooth Low Energy (Bluetooth Düşük Enerji)

BQB Bluetooth Qualification Process (Bluetooth Yeterlilik Süreci)

BR Basic Rate (Basit Hız)

BSD Blind Spot Detection (Kör Nokta Tespiti)

CAN Controller Area Network (Kontrol Alan Ağı)

CANFD Controller Area Network Flexible Data Rate (Kontrol Alan Ağı Esnek Veri Hızı)

CAS Collision Avoidance System (Çarpışma Önleme Sistemi)

CRC Cyclic Redundancy Check (Döngüsel Artıklık Kontrolü)

CVSD Continuously Variable Slope Delta (Sürekli Değişken Eğim Deltası)

DAC Digital-to-Analog Converter (Dijital-Analog Dönüştürücü)

DES Data Encryption Standard (Veri Şifreleme Standartı)

DLC Data Length Code (Veri Uzunluğu Kodu)

DMS Driver Monitoring System (Sürücü İzleme Sistemi)

DSRC Dedicated Short Range Communication (Özel Kısa Menzilli İletişim)

DoS Denial of Service (Hizmet Reddi)

ECU Electronic Control Unit (Elektronik Kontrol Ünitesi)

EDR Enhanced Data Rate (Gelişmiş Veri Hızı)

EOF End of Frame (Çerçeve Sonu)

ESC Electronic Stability Control (Elektronik Denge Kontrolü)

ESD Electrostatic Discharge (Elektrostatik Deşarj)

FCW Forward Collision Warning (Ön Çarpışma Uyarısı)

FOTA Firmware Over the Air (Donanım Yazılımı Hava Üzerinden)

GNSS Global Navigation Satellite Systems (Küresel Konum Belirleme Sistemi)

GPIO General-Purpose Input/Output (Genel Amaçlı Giriş/Çıkış)

GSM Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)

HBM Human-Body Model (İnsan Vücudu Modeli)

HTOL High Temperature Operating Life (Yüksek Sıcaklıkta Çalışma Ömrü)

HTSL High Temperate Storage Life (Yüksek Sıcaklıkta Depolama Ömrü)

HVAC Heating, Ventilation and Air Conditioning (Isıtma, Havalandırma ve Klima)

I2C Inter-Integrated Circuit (Entegre Devreler Arası)

I2S Integrated Inter Sound (Entegre Devreler Arası Ses)

IoT Internet of Things (Nesnelerin İnterneti)

IP Internet Protocol (İnternet Protokolü)

IPC Instrument Panel Cluster (Gösterge Paneli Kümesi)

IR Infrared (Kızılötesi)

ISO International Organization for Standardization (Uluslararası Standardizasyon Örgütü)

IVI In Vehicle Infotainment (Araç İçi Bilgi Eğlence)

Kbps Kilo Bits Per Second (Kilobit Bölü Saniye)

LCA Lane Change Assistant (Şerit Değiştirme Asistanı)

LCS Lane Centering System (Şerit Merkezleme Sistemi)

LDW Lane Departure Warning (Şeritten Ayrılma Uyarısı)

LIDAR Laser Imaging Detection and Ranging (Işın İle Tespit Etme ve Menzil Tayini)

LIN Local Interconnect Network (Yerel Ara Bağlantı Ağı)

LKA Lane Keep Assist (Şerit Koruma Yardımı)

LTE Long Term Evolution (Uzun Süreli Gelişim)

MAC Media Access Control Address (Medya Erişim Kontrolü Adresi)

Mbps Mega Bits Per Second (Megabit Bölü Saniye)

MCU Microcontroller Unit (Mikrodenetleyici Ünitesi)

MEC Multi Access Edge Computing (Çoklu Erişim Uç Bilişimi)

MHU Media Head Unit (Medya Ana Birimi)

MOST Media Oriented Systems Transport (Medya Tabanlı Sistem Taşıma)

NFC Near Field Communication (Yakın Alan İletişimi)

NZIF Near-Zero Intermediate-Frequency Technology (Sıfıra Yakın Ara Frekans Teknolojisi)

OBD On - Board Diagnostic (Yerleşik Teşhis)

OSI Open Systems Interconnection (Açık Sistem Ara Bağlantısı)

OTA Over the Air (Hava Üzerinden)

PA Park Assist (Park Yardımı)

PDC Park Distance Control (Park Mesafe Kontrolü)

PWM Pulse-Width Modulation (Darbe Genişliği Modülasyonu)

RADAR Radio Detection And Ranging (Radyo İle Tespit Etme ve Menzil Tayini)

RCTA Rear Cross Traffic Alert (Arka Çapraz Trafik Uyarısı)

REACH Registration, Evaluation, Authorisation and Restriction of Chemicals (Kimyasalların Kaydı, Değerlendirilmesi, İzni ve Kısıtlanması)

RoHS Restriction of Hazardous Substances in Electrical and Electronic Equipment (Elektrikli ve Elektronik Ekipmanlarda Tehlikeli Maddelerin Kısıtlanması)

RTR Remote Transmission Request (Uzaktan İletim Talebi)

SAE Society of Automotive Engineers (Otomotiv Mühendisleri Topluluğu)

SBC Sub Band Coding (Alt Bant Kodlaması)

SDIO Secure Digital Input Output (Güvenli Dijital Giriş Çıkışı)

SOF Start of Frame (Çerçeve Başlangıcı)

SONAR Sound Navigation and Ranging (Ses Navigasyonu ve Menzil Tayini)

SPI Serial Peripheral Interface (Seri Çevre Arayüzü)

T-BOX Telematics Box (Telematik Ünite)

TCT Temperature Cycling Test (Sıcaklık Döngüsü Testi)

TCU Telematics Control Unit (Telematik Kontrol Ünitesi)

TPMS Tire Pressure Monitoring System (Lastik Basıncı İzleme Sistemi)

TTL Transistor - Transistor Logic (Transistör – Transistör Mantığı)

UART Universal Asynchronous Receiver Transmitter (Evrensel Asenkron Alıcı Verici)

uHAST Unbiased Highly Accelerated Stress Test (Tarafsız Yüksek Hızlandırılmış Stres Testi)

USB Universal Serial Bus (Evrensel Seri Veriyolu)

UTP Unshielded Twisted Pair (Korumasız Kıvrımlı Çift)

V2C Vehicle to Cloud (Araçtan Buluta)

V2I Vehicle to Infrastructure (Araçtan Altyapıya)

V2P Vehicle to Pedestrian (Araçtan Yayaya)

V2V Vehicle to Vehicle (Araçtan Araca)

V2X Vehicle to Everything (Araçtan Her şeye)

Wi-Fi Wireless Fidelity (Kablosuz Bağlantı Alanı)

XOR Exclusive-OR (Özel Veya)

ŞEKİLLER DİZİNİ

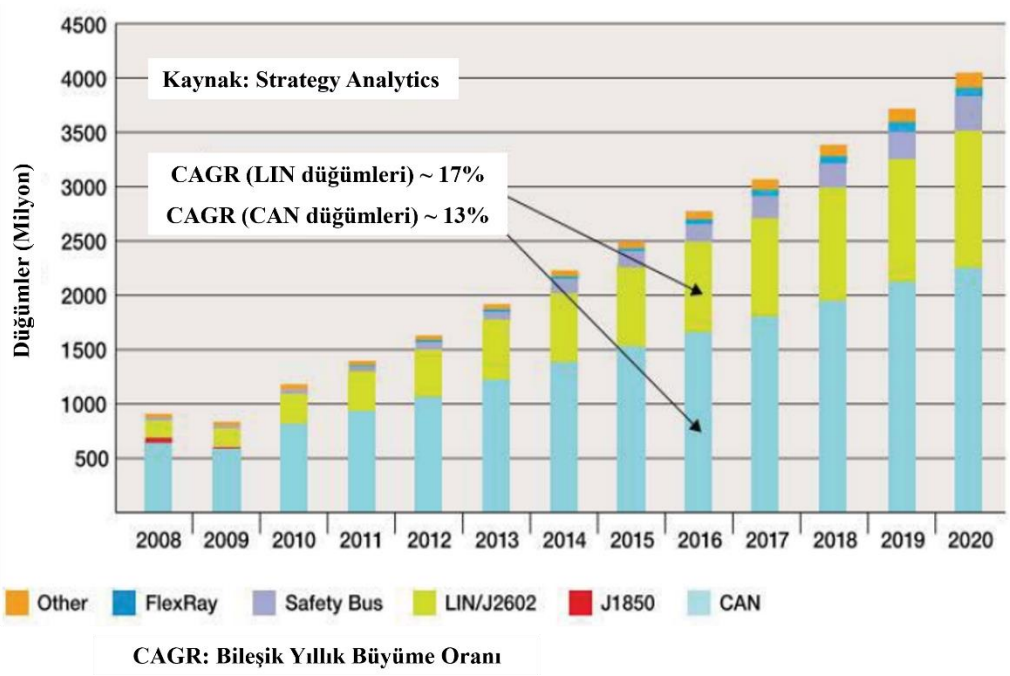
Sayfa

TABLOLAR DİZİNİ

Sayfa

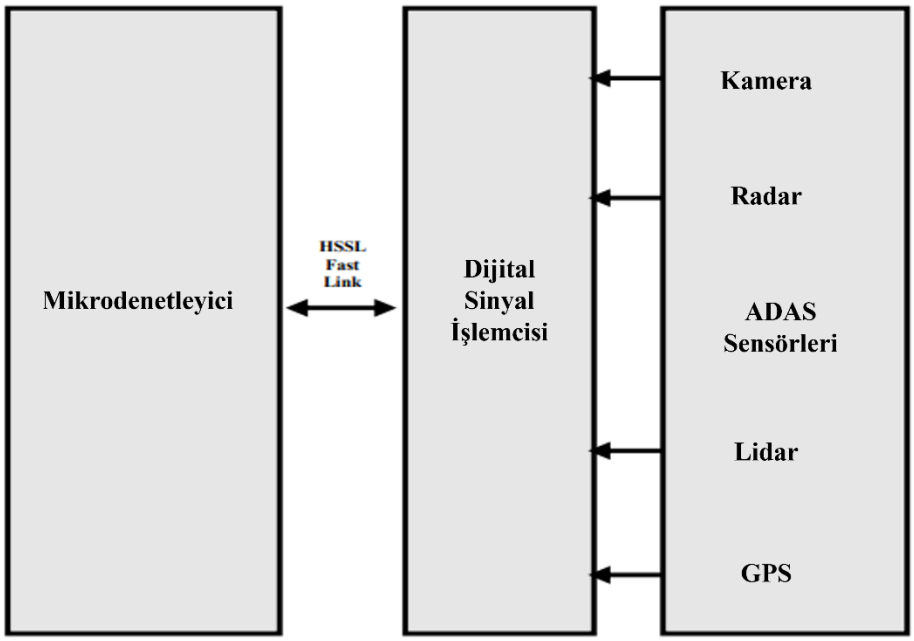
1. GİRİŞ

Teknolojinin çok hızlı büyümesi insan hayatındaki ürünlere doğrudan etki etmektedir. Hayatımızda önemli bir yeri olan ve insan hayatını oldukça kolaylaştıran otomobillerde bu etkiyi görebiliriz. Araçların teknolojik evrimine bakıldığında içten yanmalı motora sahip araçlarla birlikte diğer yakıt tipine sahip (elektrikli, hidrojen, hibrit vs.) araçlarında günlük hayatımızın birer parçası haline geldiğini artık görmekteyiz. Özellikle son yıllarda elektrikli araçlar son derece popüler ve yaygın bir hale gelmiştir. Elektrikli araçların bu kadar yaygın hale gelmesinde çevre, kullanıcı gereksinimleri ve ihtiyaçları, teknolojinin getirdiği yenilikler gibi etkenler yer almaktadır [1]. Daha derine indiğimizde araç değişimlerine daha detaylı baktığımızda mekanik bileşenlerin çok olduğu araçlardan, akıllı ve otonom, connected (bağlı) ve birbirleri ile haberleşebilen, üzerlerinde çok sayıda kontrolcü (ECU) ve elektronik bileşen (CAN ve LIN düğümleri / cihazları gibi) bulunduran arabalar artık hayatımızın bir parçası haline gelmiştir. Şekil 1.1.'de araçlardaki elektronik cihazların, CAN ve LIN haberleşme özelliklerine sahip düğümlerin (elektronik kontrol ünitesi, sensör gibi cihazlar) artışı verilmiştir [2].



Şekil 1. 1. Araçlardaki CAN / LIN ve Diğer Düğümlerin (Cihazların) Artışı

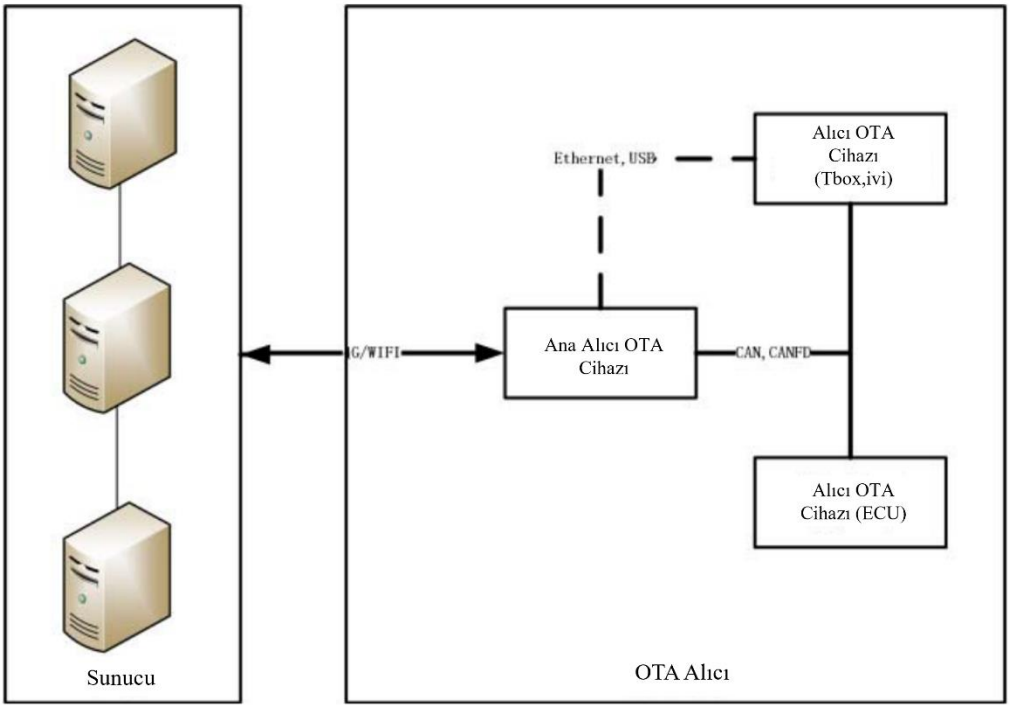
Araçlar belirli seviyelerde otonom haline gelmiş, infotainment (bilgi-eğlence) ve connectivity (bağlanabilirlik) özellikleri ile de araçlar dış dünyadaki diğer sistemler ile haberleşen ve veri gönderip alabilen akıllı cihazlara dönüşmüşlerdir [3]. Araç özellikleri kompleks bir hal aldıkça örnek olarak araçlar otonom ve akıllı hale geldikçe araçlarda kullanılması gerekli kontrolcü (elektronik kontrol ünitesi) ve sensör (RADAR, LIDAR, Kamera, Ultrasonik vs.) sayıları artmaktadır. Sensörlerden gelen gigabit hızındaki veriler elektronik kontrol üniteleri tarafından işlenmektedir. Şekil 1.2.'de otonom araçlardaki ADAS (Gelişmiş Sürücü Destek Sistemleri) blok diyagramı verilmiştir [4].



Şekil 1. 2. Otonom Araçlardaki ADAS Blok Diyagramı

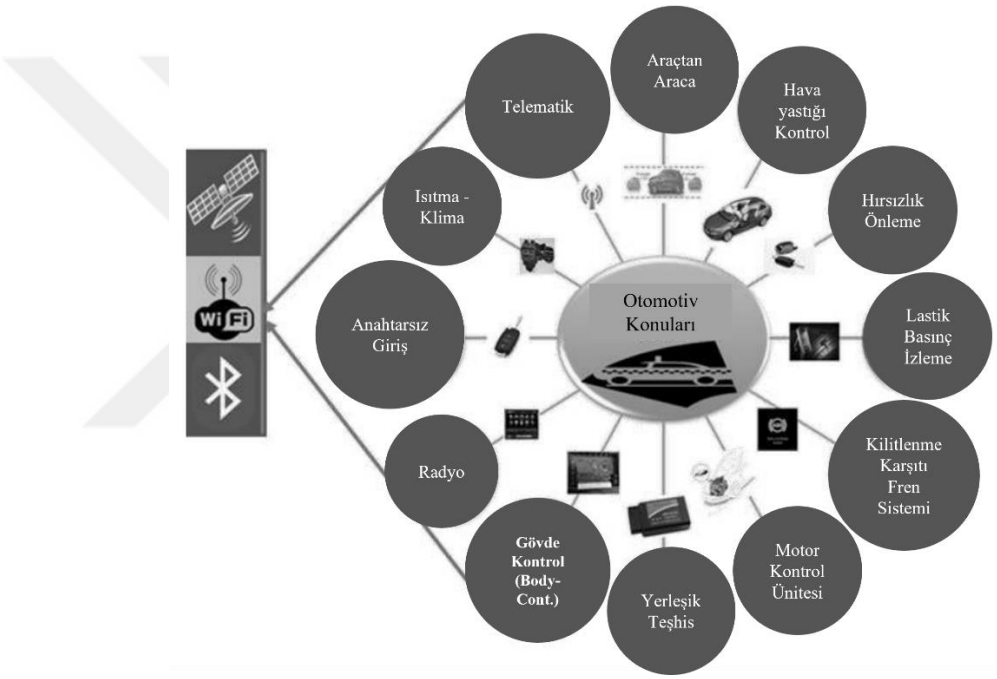
Uyarlanabilir hız sabitleyici, şerit takip sistemi, kör nokta tespiti, trafik işaret tanıma, çapraz trafik uyarısı, otomatik acil fren gibi özellikleri sağlayabilmek için aracın kritik denebilen direksiyon, gaz pedalı, fren, kilit sistemleri gibi fonksiyonları sensörlerden gelen verilere göre ECU'lar tarafından kontrol edilmektedir [5]. Sensörlerden gelen bu veriler bozulmadan, değişikliğe uğramadan ve dışarıdan ulaşılamayacak bir formda ECU'lara aktarılmalıdır.

Bilgi-eğlence ve bağlanabilirlik özellikleri ile birlikte de araçlar dış sistemler ile haberleşerek bilgi alışverişinde bulunurlar [6]. Günümüz akıllı araçlarındaki belirli elektronik kontrol üniteleri (örnek olarak TCU - Telematic Control Unit veya TBOX - Telematic Box) üzerlerinde bulundurduğu LTE veya GSM modüller sayesinde internete çıkıp, internet cihazları ile haberleşebilmektedir. Hatta araçlardaki güncellenmesi gereken bazı ünitelerin güncelleme yazılımları OTA (Over-the-Air) veya FOTA (Firmware-Over-the-Air) gibi özellikler kullanılarak Telematic Box aracılığı ile yapılabilmektedir [7]. Güncelleme paketi TBOX tarafından alınıp, gerekli ünitelere CAN veya ethernet üzerinden gönderilir, bu sayede güncellenmesi gereken ünitenin güncelleştirilme işlemi uzaktan sağlanabilmektedir. Şekil 1.3.'de tipik bir OTA güncelleme sistem mimarisi verilmiştir [7].Güncelleme paketini dış birimden alan OTA master cihaz yani TBOX, güncelleme paketini CAN / CANFD / Etherhet üzerinden aracın güncellenmesi gereken diğer ünitelerine yani OTA client cihazlara göndermektedir.



Şekil 1. 3. Tipik Bir OTA Güncelleme Sistem Mimarisi

OTA gibi araçlardaki bir çok özellik (anahtarsız giriş, radyo, telematik, hırsızlık önleyici sistemler vs.), Wi-Fi, bluetooth, GNSS, GSM, NFC gibi kablosuz haberleşme protokolleri aracılığı ile dış birimler ile etkilelim halindedir. Şekil 1.4.'de araçlardaki bazı özelliklerin kablosuz haberleşme ile etkileşim diyagramı verilmiştir [8]. Uzaktan güncelleme veya Şekil 1.4.'de görüldüğü gibi araç iç birimleri ile dış sistemler arasında birçok farklı yöntem ile farklı iletişimler bulunmaktadır. Dış birimlerden gelen bilgiler kötü niyetli olabilir. Bu birimlerden bilgi alınmadan önce dış birimler doğrulanmalıdır, doğrulama işleminden sonra araca alınan veriler şifrelenmeli ve diğer ünitelere şifreli ve güvenli bir formda iletilmelidir.



Şekil 1. 4. Kablosuz Haberleşme ile Etkileşimde Bulunan Bazı Araç Özellikleri

Akıllı şehirler ve akıllı ulaşım sistemlerinin uygulamaya geçildiği nesnelerin interneti zamanında, araçların dış birimlerle etkileşimde bulunması ve bağlı olması kaçınılmazdır [9]. Araçlar dış sistemler ile etkileşimde oldukları için bazı güvenlik riskleri oluşmaktadır [10]. Araç ve aracın iletişimde olduğu sistem dışındaki üçüncü kişiler veya sistemlerden haberleşme dinlenebilir, aradaki haberleşme bozulabilir, bağlantı koparılmaya çalışılabilir. Bu riskleri önlemek için araç ve dış sistemlerin haberleşmeleri güvenli bir şekilde gerçekleştirilmelidir ve üçüncü kişiler tarafından müdahale edilebilir, ulaşılabilir ve kontrol edilebilir olmamalıdır.

Otomotiv dünyasındaki diğer önemli bir çalışmaya baltığımızda ise karşımıza vehicle-to-everything (araçtan her şeye) kavramı ve özellikleri çıkmaktadır. Bu kavram daha da açıldığında ise, araçtan araca, araçtan altyapıya, araçtan eve, araçtan ağa, araçtan şebekeye, araçtan cihazlara gibi kavramlar ve etkileşimler görülmektedir. Araçların diğer dış birimlerle olan etkileşimi Şekil 1.5.'de verilmiştir [11].

Şekil 1. 5. Araçtan Her Şeye Etkileşim Modeli

Görüldüğü gibi akıllı, bağlı ve otonom araç özellikleri dolayısıyla, araçlar ve dış birimler / sensörler çok sayıda kablolu veya kablosuz arayüz üzerinden etkileşim halinde bulunurlar. Bu özelliklere sahip araçların çok fazla dış arayüzleri bulunur. Bu durum araçları bilgisayar korsanlarının veya üçüncü kişilerin hedefi haline getirmektedir ve otomotiv güvenliği tehditlerini hızla arttırmaktadır [12]. Kötü niyetli üçüncü kişiler tarafından bu arayüzler dinlenebilir, dinlenen mesajlar anlamlandırılabilir veya bozulabilir. Anlamlandırılan mesajlar üçüncü bir kişi tarafından kablolu veya kablosuz araca gönderilip aracın gaz, fren, direksiyon, kilit sistemi, ABS (Anti - Lock Braking System), immobilizer ve sistem güncellemeleri gibi kritik sistemleri ve fonksiyonları manipüle edilebilir veya kontrol edilebilir.

Araç içi haberleşmenin sürüş ve sürücü emniyeti açısından güvenli olması çok önemlidir. Üçüncü kişilerin araç içi haberleşme mesajlarını manipüle etmesi kötü sonuçlar doğurabilir. Örnek olarak ADAS sensörlerinden gelen bir veri dinlenip anlamlandırılır ise, elektronik kontrol ünitesine bozuk bir veri gönderilip kaza gibi kötü durumlar oluşabilir. Yine aynı şekilde güncelleme yazılım paketi, güncellenmesi gereken ECU'lara iletilirken dinlenip bozulabilir. Araçtaki bir ünitenin güncellenmemesi veya hatalı güncellenmesi kötü sonuçlar ortaya çıkarabilir.

Aracı başlatma, durdurma, direksiyon kontrolü, gaz, fren, kilit sistemi gibi fonksiyonlar ECU'lar tarafından gerçekleştirilir. İki ECU arasındaki veriyoluna sızmayı başarabilen bir kişi haberleşmeyi dinleyebilir ve verileri bozabilir. Bu durumu önlemek için veriyolunda ki mesajlar şifrelenmeli veya şifreli mesaj iletim özelliğine sahip bir veriyolu ile taşınmalıdır [13].

Araç içi haberleşmede çok sayıda mesaj elektronik kontrol üniteleri tarafından birbirlerine iletilir. Bazı CAN veriyolu mesajları son derece kritik araç güvenliği ile ilgili mesajlardır. Bu CAN mesajlarının manipüle edilebilmesi araç güvenliği açısından ciddi sonuçlar doğurabilir [14].

Araç içi iletişim ilk olarak dinlenememelidir. İki elektronik kontrol ünitesi arasındaki veya sensörlerden giden veriler dinlenebilse bile anlamlandırılabilir olmamalıdır. Araç içi ağ haberleşmesi doğrulama protokolüne sahip, şifreli ve güvenli bir yapıda olmalıdır.

Araçlar daha da otonom, connected (bağlı) ve akıllı hale geldikçe araç içi bileşenler arasındaki veya araç – dış sistemler arasındaki etkileşim daha da artacaktır. Sürücü, araç veya sistemlerin güvenliği açısından siber güvenlik araçlar için çok önemli bir unsur ve uygulanması gereken bir zorunluluk haline gelerek, akademideki ve endüstrideki yeni otomotiv elektroniği çalışmalarına temel olmaktadır [15].

1.1. Tezin Amacı

Teknolojinin gelişmesi hayatımızdaki ürünlere de yansımaktadır. Hayatımızdaki cihazlar kompleks ve yüksek fonksiyonel özellikler kazanmaya başlamıştır. Günlük hayatımızın en önemli bileşenlerinden biri olan araçlarda bu gelişimi ve durumu görebiliriz. Yakıt tipi olarak bakıldığında önemli bir değişim mevcuttur. Fosil yakıtları kullanan içten yanmalı motora sahip araçlar, batarya paketlerine sahip elektrikli araçlara dönüşmüştür. Elektrikli araçların gelecek öneminin artması araç üreticilerine yeni bir yatırım alanı oluşturmuştur. Birçok gelişmiş özellik bu araçlara eklenmeye başlanmış, araçlar akıllı, birbirleriyle ve dış sistemlerle etkileşim kurabilip haberleşen, otonom özellikli akıllı cihazlara dönüşmüşlerdir. Araçlara bu kadar özellik eklenmesi, gerekli denetleyici ve sensör gibi donanımların sayısını arttırmış, araç içi haberleşme ağındaki veri ve mesaj sayılarını çoğaltmış ve bazı riskler getirmiştir. Sistemlerin kontrolü ve emniyeti zorlaşmış, araçlar siber saldırılara açık hale gelmiştir.

Bu çalışmada, şifreleme ve doğrulama mekanizmasına sahip, güvenli ve hibrit bir araç içi haberleşme sistemi kurularak elektrikli aracın sistem güvenliğinin arttırılması hedeflenmiştir. Bu sayede, elektronik kontrol üniteleri ve sensör gibi diğer donanımlar arası haberleşmeler manipüle edilemeyecek ve aracın güvenlik kritik seviyedeki fonksiyonları dış saldırılara karşı korunacaktır.

1.2. Tezin Önemi

Bu çalışmada, şifreleme ve doğrulama mekanizmasına sahip, güvenli hibrit bir araç içi haberleşme sistemi tasarlanarak, elektrikli araçlarda bulunan kritik sistemlere yönelik saldırıların engellenmesi amaçlanmıştır. Bu sayede, aracın güvenlik seviyesi yüksek kritik sistemleri korunacak, insan hayatına doğrudan etki eden önemli sistemlerin kötü amaçlar doğrultusunda kullanımı önlenecektir. Bu çalışma, sağladığı güvenlik mekanizmaları ile sürüş ve sürücü güvenliğini arttırdığı için otomotiv siber güvenliği açısından önemlidir.

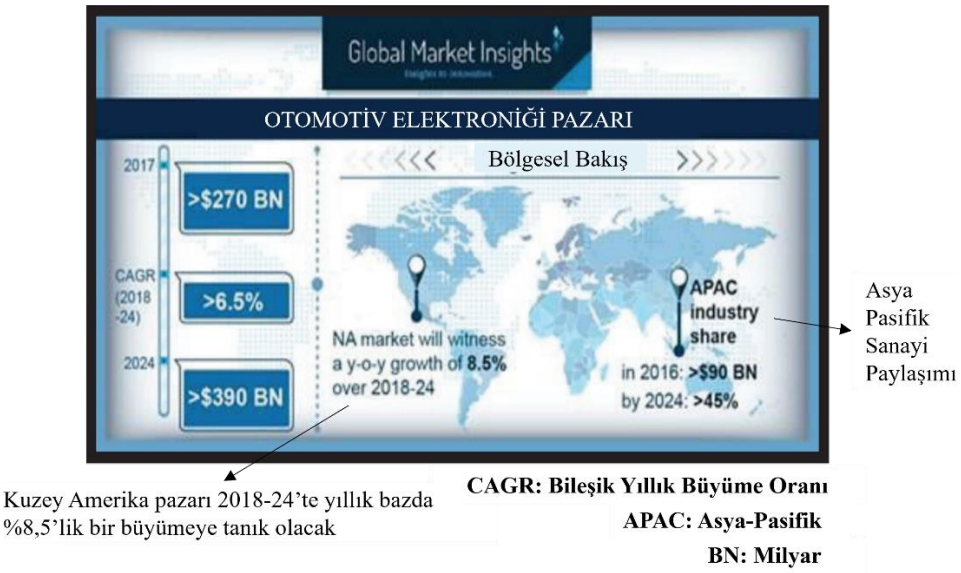
1.3. Tezin Katkısı

Bu çalışmada, araç içi haberleşme ağına yönelik yapılabilecek saldırılara karşı, şifreleme ve doğrulama fonksiyonları kullanılarak önlemler alınmıştır. Araç ağına yönelik dinleme ve anlamlandırma saldırıları için şifreli bir haberleşme sistemi tasarlanarak ve yabancı cihazlardan gelen komutlar için kimlik doğrulama fonksiyonu kullanılarak sistem güvenliği arttırılmıştır. Ayrıca hibrit bir haberleşme yaklaşımı ile, birden fazla haberleşme protokolü ve farklı iletişim hatları kullanılarak sistem güvenliğine katkı sağlanmıştır. Bu çalışma, bir araç içi haberleşme ağının ne kadar önemli ve kritik olduğunu anlatmış, ne gibi saldırılara karşı savunmasız olduğunu göstermiş ve alınabilecek önlemler ve savunma teknikleri konusunda otomotiv siber güvenlik konusuna bir katkı sunmuştur.

2. GENEL BİLGİLER

2.1. Otomotiv Elektroniği

Otomotiv dünyasındaki değişimlere ve yeniliklere bakıldığında, bu değişim ve yeniliklerin belirli alanlarda gruplandığı görülmektedir. Bu alanlara baktığımızda kuşkusuz aracın yakıt ve motor tipindeki değişimler ön plana çıkmaktadır. Geleneksel fosil yakıt kullanan araçlar, batarya paketlerine sahip elektrik enerjisini kullanan araçlara dönüşmektedir. İçten yanmalı motor kullanan araçlardan farklı tipte elektrik motoru kullanan araçlara doğru bir dönüşüm yaşanmaktadır. Malzeme teknolojileri gelişmektedir, standart plastik ve metal malzemelerden, güçlendirilmiş kompozit malzemelere geçiş yaşanmaktadır. Motor ve batarya paketlerinin yönetimleri konusunda güç elektroniği teknolojileri, otomotiv endüstrisinde çok önemli bir yere gelmiştir ve bu konudaki çalışmalar ve araştırmalar devam etmektedir. Diğer bir taraftan ise kullanıcı isterlerini karşılamak, yeni teknolojileri araçlara entegre etmek, araçları fonksiyonel akıllı cihazlar haline getirmek için araç üreticileri ve tedarikçileri çok önemli bir alan olan otomotiv elektroniği teknoloji ve fonksiyonlarına ciddi yatırımlar yapmaktadırlar. Son yıllardaki otomotiv elektroniği market değeri değişimine bakıldığında, bu alandaki değişimin önemi anlaşılmaktadır. Şekil 2.1.'de otomotiv elektroniği market değerinin son yıllardaki değişimi görünmektedir [16].



Şekil 2. 1. Otomotiv Elektroniği Market Değeri

Otomotiv elektroniğinde yaşanan gelişmeler ile araçlar günden güne yeni özellikler kazanmaktadır ve gittikçe daha akıllı ve fonksiyonel hale gelmektedir. Otomotiv elektroniğine öncülük eden, trend ve gelişmekte olan alanlar bulunmaktadır. ADAS (Gelişmiş Sürücü Destek Sistemleri), Infotainment (Bilgi-Eğlence), Connectivity (Bağlanabilirlik), V2X (Araçtan – Her şeye) gibi alanlardan gelen fonksiyonlar ve özellikler, akıllı ve teknolojik bir arabanın en kritik özelliklerini oluşturur. Tüm bu yenileşme ve yüksek teknoloji dönüşümü, elektronik bileşen ve sistemlerin araçlara entegrasyonu sayesinde olmaktadır.

2.1.1. Gelişmiş Sürücü Destek Sistemleri (ADAS)

Araçlardaki teknolojik değişim devam ettikçe insan hayatını kolaylaştıran bir çok özellik hayatımıza girmekte ve araçlardaki yerini almaktadır. Bu özelliklerden bazıları sürücünün sürüş konforunu arttırmak, gerekli yerlerde hayati önlemler almak, yaklaşan tehlike ve kazalara karşı sürücüyü uyarmak ve aracı kısmi veya tam otonom hale getirmek gibi gelişmiş fonksiyonel özelliklerdir. Bu özellikler araç hareket halinde veya park edilme durumunda iken sürücüye yardım eder ve özel durumlar için sürücü ile etkileşime girer. Bu sayede bu sistemler otomobil ve yol güvenliğini arttırır. Sensör ve kamera teknolojilerinden gelen verilerin, elektronik kontrol üniteleri tarafından yorumlanıp işlenmesi temeline dayalı bu sistemler otomotiv elektroniği altındaki temel alanlardan biridir. Araçlardaki bu özellikler gelişmiş sürücü destek sistemleri altında değerlendirilir.

Gelişmiş sürücü destek sistemlerinin araçlardaki özelliklerinin artması ve bu özelliklerinin gelişmesi, araçları otonom hale getirmektedir. Gelişmiş sürücü destek sistemleri, otomasyon miktarına ve SAE (The Society of Automotive Engineers – Otomotiv Mühendisleri Birliği) tarafından yayınlanan sınıflandırmaya göre seviye 0'dan seviye 5'e kadar altı seviyede kategorize edilir.

SAE tarafından yapılan sınıflandırmada seviye 0'dan 2'ye kadar olan seviyeler, sürücünün ana sürüş rolünü üstlendiği ve otomatik işlevlerle desteklenebilen araçları ifade ederken, seviye 3'ten 5'e kadar olan seviyeler, eğer mevcutsa, insan sürücünün daha az sorumluluğa sahip olduğu veya hiç sorumluluk taşımadığı araçlara karşılık gelir ve otomatik sürüş sistemi ana sürücüdür. Tablo 2.1.'de SAE seviye 3, 4, 5 seviyeleri ve kabiliyetleri verilmiştir [17].

Tablo 2. 1. SAE J3016 Seviye 3,4 ve 5 Otomasyon Özellikleri

<table>
<tr><th></th><th>SAE Seviye 3</th><th>SAE Seviye 4</th><th>SAE Seviye 5</th></tr>
<tr><td rowspan="2">Sürücü</td><td colspan="3">Otomatik sürüş sistemi devrede iken, aracı kullanmaz</td></tr>
<tr><td>Talep edildiğinde aracı kullanmalıdır</td><td colspan="2">Otomatik sürüş sistemi, aracı sürücünün kullanması talebinde bulunmaz</td></tr>
<tr><td>Otomatik Sürüş Sistemi</td><td colspan="2">Belirli koşullar altında aracı kullanabilir</td><td>Tüm koşullar altında aracı kullanabilir</td></tr>
</table>

Tablo 2.1.'de görüldüğü üzere, seviye 3, 4 ve 5'de otomatik sürüş sistemi devrede iken sürücü aracı kullanmamaktadır. Seviye 3 bir otomatik sürüş sisteminde, otomatik sürüş sistemi talebi durumunda sürücü arabayı kullanmalıdır. Seviye 4 ve 5 otomasyon seviyesine sahip bir otomatik sürüş sisteminde, otomatik sürüş sistemi, kontrolü verme isteğinde bulunmayacaktır. Seviye 3 ve seviye 4 otomasyon seviyesine sahip bir araçta, otomatik sürüş sistemi belirli ve limitli koşullar altında aracı kullanabilir. Seviye 5 kabiliyetine sahip bir otomatik sürüş sistemi ise tüm koşullar altında aracı kullanabilir.

Gelişmiş sürücü destek sistemleri altında değerlendirilen sistemlere baktığımızda birçok farklı durum ve sürüş için sürücüye destek olan farklı özellikler bulunmaktadır. Bu özelliklerden her biri kendine has donanımları, sensörleri ve kontrol algoritmalarını kullanmaktadır.

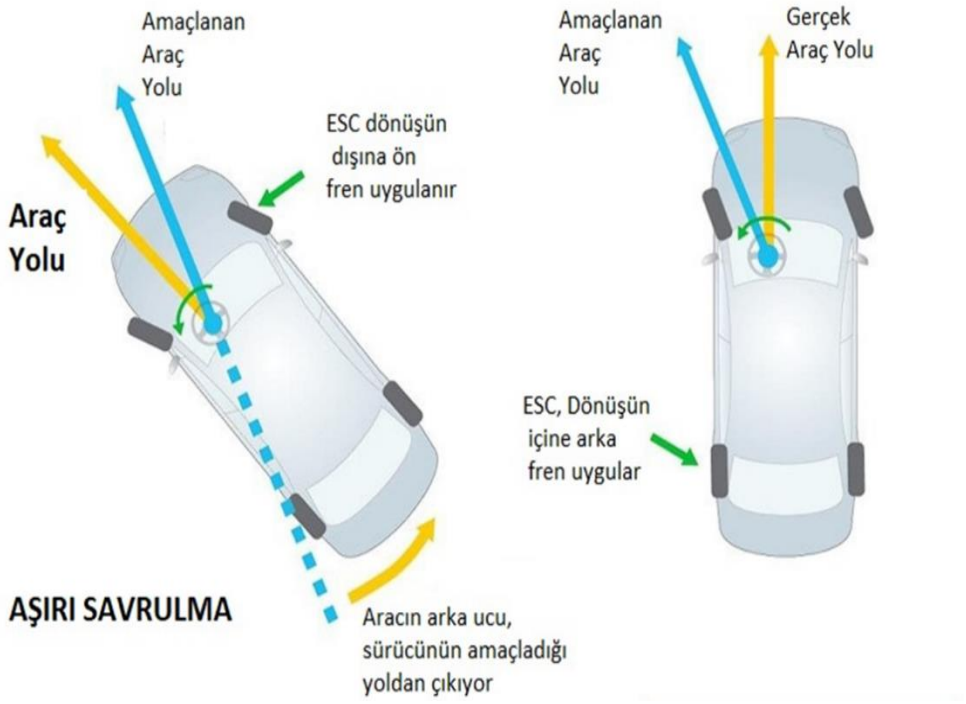
Başlıca ADAS fonksiyonları olarak ABS (Anti Lock Braking System – Kilitlenme Karşıtı Fren Sistemi), ESC (Electronic Stability Control – Elektronik Denge Kontrolü), AEB (Automatic Emergency Braking – Otomatik Acil Durum Frenleme), LCA (Lane Change Assistant – Şerit Değiştirme Asistanı), PDC (Park Distance Control – Park Mesafe Kontrolü), LDW (Lane Departure Warning – Şeritten Ayrılma Uyarısı), FCW (Forward Collision Warning – Ön Çarpışma Uyarısı), ACC (Adaptive Cruise Control – Uyarlanabilir Hız Kontrolü), LKA (Lane Keep Assist – Şerit Koruma Yardımı), PA (Park Assist – Park Yardımı), ANV (Automotive Night Vision – Otomotiv Gece Görüşü), BSD (Blind Spot Detection – Kör Nokta Tespiti), LCS (Lane Centering System – Şerit Merkezleme Sistemi), CAS (Collision Avoidance System – Çarpışma Önleme Sistemi), DMS (Driver Monitoring System – Sürücü İzleme Sistemi), RCTA (Rear Cross Traffic Alert – Arka Çapraz Trafik Uyarısı) verilebilir [18].

2.1.1.1. Kilitlenme Karşıtı Fren Sistemi (ABS)

Kilitlenme karşıtı fren sistemi, ani frenleme durumlarında dış etkiler ve ortamlar (yolun sürüş durumu, hava koşulları, aracın kendisinden doğabilecek veya araca etki eden diğer koşullardan dolayı) sebebiyle meydana gelebilen tekerlek kilitlenmesi olayını engellemek için oluşturulmuş sistemlerdir. Sürücünün güvenliğini sağlamak için geliştirilmiş sürüş güvenliği sistemlerinden biridir. Bu sistemde, tekerlek hızı ve araç hızını karşılaştırmak için sensörlerden yararlanılır. Tekerleklerde bulunan ivme ölçerler tekerlek hızını ölçer, aynı esnada ölçülen araç hızı tekerlek hızı ile istenen oranda benzer değilse kilitlenme karşıtı fren sistemi devreye girerek ilgili tekerleğin kilitlenmesini önler ve sürüş güvenliğini sağlar. Bu durumda önüne geçilmeye çalışılan risk yüksek hızlarda tekerleğin kilitlenmesi durumudur. Yüksek hızlarda kilitlenen tekerlek, aracın kayması durumunu ortaya çıkarabilir. Kilitlenme karşıtı fren sistemi, kilitlenmiş tekerleğin freni bırakıp tekrar dönmesini sağlar, bu sayede kayma olmaz ve frenleme mesafesi kısalır [19].

2.1.1.2. Elektronik Denge Kontrolü (ESC)

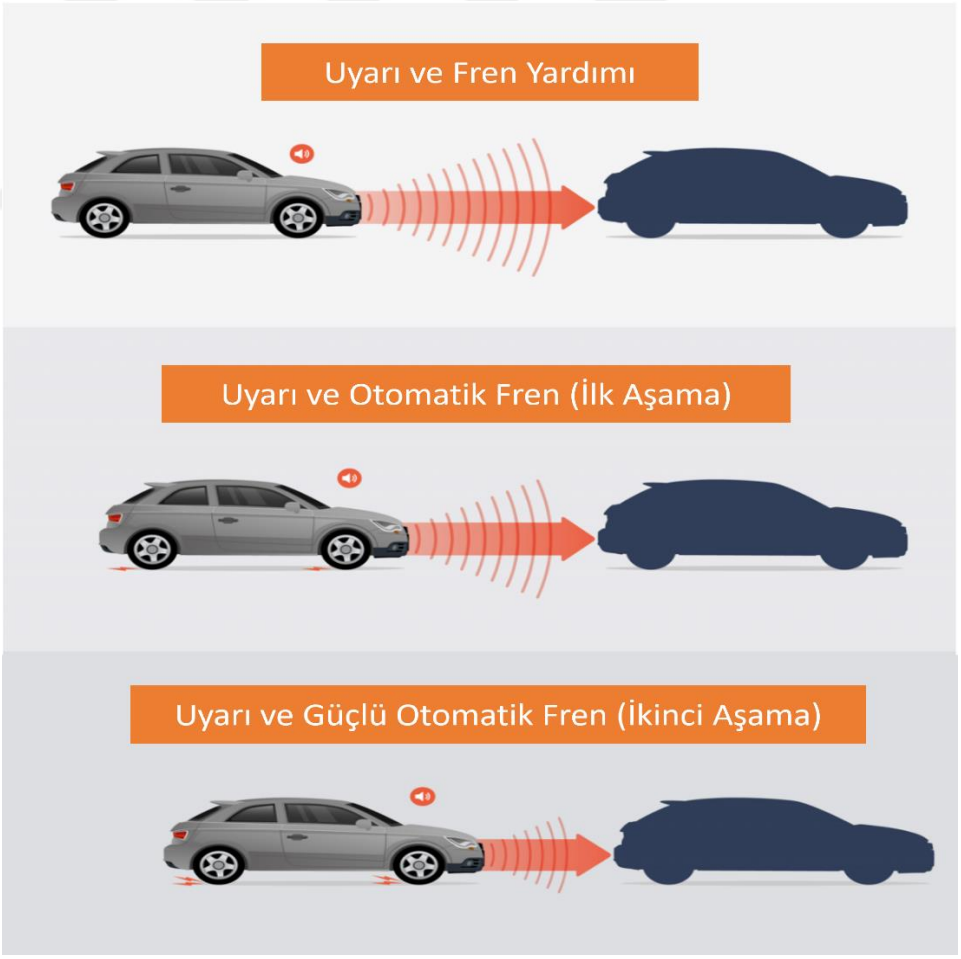
Elektronik denge kontrolü sistemi, sürücünün kontrol kaybından kaynaklı kaza ve tehlikeli durumları engellemek için geliştirilmiş sistemlerdir. Oluşabilecek savrulma, yoldan sapma, devrilme, virajı alamama gibi sürücünün kontrolünü kaybettiği durum kaynaklı kazaların oluşma riskini en aza indirmektedir. Araç virajı dönerken, hızlı manevra ve anlık fren durumlarında aracın savrulmasını önler, aşırı direksiyon veya yetersiz direksiyon sebebi ile oluşabilecek kayma durumlarında frenleri otomatik olarak etkinleştirebilir. Bu sistemin elektronik kontrol ünitesi, sistemin sensörlerinden devamlı veri alarak, sürücünün direksiyon verisi ve taşıtın asıl sürüş yönü arasında bir fark olup olmadığını anlamak için girdileri kullanıyor. Araç tekerlerinde bulunan hız sensörleri sayesinde elektronik kontrol ünitesi bazı tekerleklerin diğer tekerleklerden hızlı döndüğünü algılıyor, bu durum tekerleklerin çekiş gücünü yitirdiğini belirtiyor. Elektronik kontrol ünitesi, aracı kontrol edilebilir bir hale geri getirmek için, tekerlek hızlarına ve çekişlerine göre fren sistemini farklı fren kuvveti uygulamaya yönlendiriyor. Bu sayede, aracın savrulma durumunun önüne geçilerek, sürüş güvenliği sağlanıyor. Şekil 2.2.'de elektronik denge kontrolünün çalışma prensibi görselleştirilmiştir [20,21].



Şekil 2. 2. Elektronik Denge Kontrolü Çalışma Prensibi

2.1.1.3. Otomatik Acil Durum Frenleme (AEB)

Otomatik acil durum frenleme sistemi, yoldaki engelleri tespit ederek aracı yavaşlatmak veya bazı durumlarda ise tamamen durdurmak için otomatik fren kullanır. Bu sistem hayati durumlarda sürücünün etkisi olmadan, sürücü kontrolü dışında aracı durdurabilir. Otomatik acil durum frenleme sistemleri olası kazaları önlemek için ışık tespiti, RADAR teknolojisi veya kamera teknolojilerinin kombinasyonlarını-birleşimlerini kullanan hibrit sensör tabanlı gelişmiş sürücü destek sistemlerinden biridir. Sensörlerden gelen girdiler ile bir nesne tespit edilirse ilk önce sürücü uyarılır, belirli bir süre içerisinde sürücüden bir kontrol gerçekleşmezse, otomatik acil durum frenleme sistemi aracı durdurarak sürüş güvenliğini sağlar. Şekil 2.3.'de otomatik acil durum frenleme sisteminin, acil frenleme durumundaki çalışma aşamaları verilmiştir [22].



Şekil 2. 3. Otomatik Acil Durum Frenleme Sistemi Çalışma Aşamaları

2.1.1.4. Şerit Değiştirme Asistanı (LCA)

Şerit değiştirme asistanı, sürücülerin güvenli bir şekilde şerit değiştirmesine yardımcı olan bir teknolojidir. Sürücüler şerit değiştirirken yaklaşan arabaları bildirmek için sensör teknolojilerini kullanır. Şerit değiştirme asistanı, sürücünün göremediği kör noktadaki araçları tespit ederek şerit değiştirmelerde meydana gelebilecek tehlikeli durumları ve kazaları azaltmayı hedefler. Sistem, tehlikeli olabilicek şerit değiştirme durumu algıladığında, sürücünün önlem almasına ve güvenli şerit değişikliği yapmasına yardımcı olabilmek için sesli ve/veya görsel uyarı verir. Günümüz sürücü destek sistemlerinde 2 farklı şerit değiştirme asistanı/yardımı sistemi karşımıza çıkmaktadır. Bu sistemlerin pasif olanı direksiyon ve frenleme kontrolünü sürücüye bırakır, sesli ve/veya görsel uyarı ve algılamalar ile şerit değiştirme durumunda sürücüye yardımcı olur. Aktif olan şerit değiştirme asistanı ise hibrit sensör teknolojilerini kullanarak kendi başına şerit değiştirebilir. Direksiyon ve fren kontrolü sistemin kendisindedir [23].

2.1.1.5. Park Mesafe Kontrolü (PDC)

Park mesafe kontrolü sistemi, zorlu park durumlarında sürücüye park esnasında rehberlik ve yardım etmek için SONAR ve ultrasonik sensörleri kullanır. Günümüzde çoğu araçta karşımıza çıkan sürücü destek sistemlerinden birisidir. Park esnasında, yakın engeller için sesli ikaz vererek park manevrasında sürücüye yardımcı olur. Pasif sürücü destek sistemlerinden biridir. Park manevrasında aracı kontrol etmez. Sesli veya görsel uyarılarda bulunarak sürücünün araç kontrolünü kolaylaştırır. Aracın ön ve arka tamponlarında bulunan ultrasonik sensörler sayesinde, aracın etrafındaki cisimler algılanır ve aracın cisimlere olan mesafesi tespit edilir. Aracın cisimlere yakınlığına göre farklı tonlarda hoparlörden çıkan sesler ile sürücü yönlendirilir [24].

2.1.1.6. Şeritten Ayrılma Uyarısı (LDW)

Şeritten ayrılma uyarı sistemi, sürücünün istemeden şeritten çıkıp çıkmadığını tespit etmek için kamera teknolojilerini kullanır. Bu sistem aracın seyir halinde bulunduğu şeridi izler, sürücünün yanlışlıkla şeritten ayrıldığını anlarsa direksiyonu titreterek, sesli veya görsel uyarı vererek sürücüyü uyarır. Sistem, aracın şeritteki konumunu izlemek için ön camda bulunan kameraları kullanır. Araç şerit çizgileri içerisinde değilse veya kontrolsüz bir şekilde şeritten ayrılıyorsa sürücüyü uyarır. Sistem sadece gerekli ikazı sağladığı için düzeltici eylemi sürücünün yapması gerekir [25].

2.1.1.7. Ön Çarpışma Uyarısı (FCW)

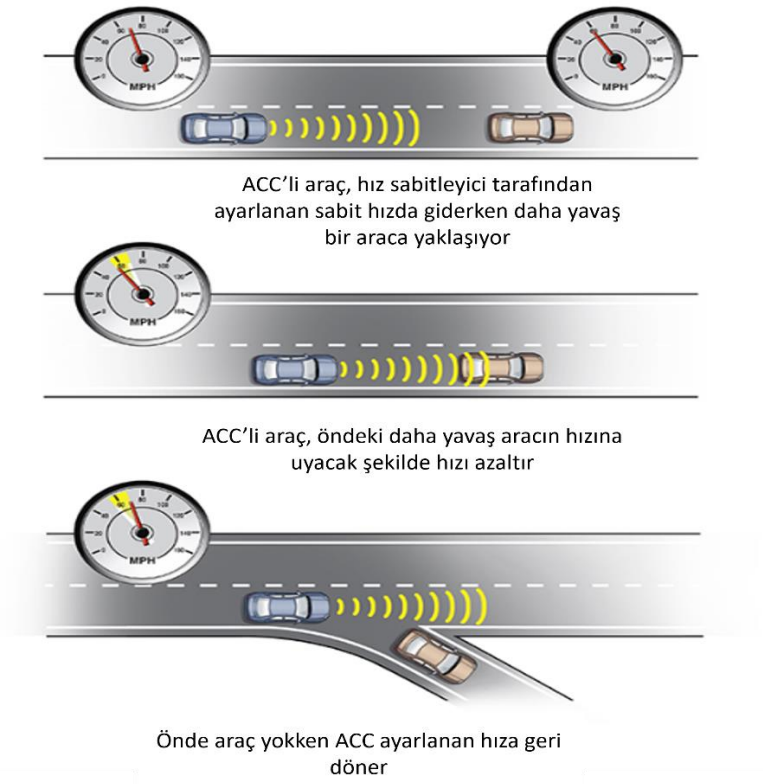
Ön çarpışma uyarı sistemleri, aracın önünde duran veya yavaş hareket eden nesne veya araçları tespit ederek sürücüyü yaklaşan bir çarpışmaya karşı uyarır. Bu sistem aracın önündeki yolu taramak için radar, lazer ve kamera gibi sensör teknolojilerini kullanır. Ön çarpışma uyarı sistemi, yaklaşmakta olan bir çarpışmayı veya tehlikeli durumu algılarsa, sesli, görsel, titreşim veya bunların bir kombinasyonunu kullanarak sürücüyü uyarır. Bazı ön çarpışma uyarı/önleme sistemleri sürücünün gerekli aksiyonu almasına yardım ederek emniyet kemerlerini sıkabilir, fren hidroliklerini ayarlayarak aracın daha hızlı durmasını sağlayabilir. Bu özellik ile birlikte eğer araçta acil fren sistemi de varsa, yaklaşan bir çarpışmaya gerekli zamanda aksiyon alınamaz ise, araç otomatik olarak fren uygulayabilir [26].

2.1.1.8. Şerit Koruma Yardımı (LKA)

Yorgunluk ve dikkatsizlik sebebiyle istemsiz bir şekilde şeritten çıkmalar yaygın kaza nedenlerinden biridir. Şerit koruma sistemi sürücünün şeritte kalmasına yardımcı olur. Şeritte kalma asistanı, gidilen şeridi izleme ve aracın şeritteki konumunu anlamak için video kamera kullanır. Aracın şerit işaretlerine olan mesafesi, belirlenmiş minimum değerin altına inerse, şerit koruma sistemi, elektrikli hidrolik direksiyonu ters yönde hareket ettirerek aracın hedef şeritte kalmasına yardımcı olur [27].

2.1.1.9. Uyarlanabilir Hız Kontrolü (ACC)

Uyarlanabilir hız kontrolü, geleneksel hız kontrolünün (cruise control) gelişmiş halidir. Cruise control sürücü tarafından set edilen hızı koruyabilir fakat, araç sürücü müdahale edene kadar hep bu hızda gider. Uyarlanabilir hız kontrolüne sahip bir araçta ise, sistem öndeki araca bulunan mesafeye ve öndeki aracın hızına göre, araç hızını otomatik olarak arttırıp azaltabilir. Öndeki araç yavaşlarsa, uyarlanabilir hız kontrolü buna uyabilir. Öndeki araç şeridinizden çıkarsa veya sizin aracınızdan daha hızlı giderse, sistem araç hızını, sürücünün ayarladığı hıza geri getirebilir. Trafik yoğunluğuna göre öndeki araç ile korunacak takip mesafesi ayarlanabilir. Sistem ayarlanan bu takip mesafesine göre araç hızını ayarlar. Araç ile öndeki araç arasındaki mesafeyi belirlemek için sensörlerden yararlanılır. Uyarlanabilir hız kontrolü sistemi 2 sensörden gelen bilgileri kullanır, birincisi önde bulunan araç ile aradaki mesafeyi ölçen mesafe sensörü, ikincisi ise aracı otomatik olarak hızlandıran ve yavaşlatan hız sensörü. Sistem hızınızı ayarlamak ve öndeki araçla aradaki mesafeyi korumak için bu girdileri kullanır. Şekil 2.4.'de uyarlanabilir hız kontrol sisteminin örnek bir çalışma durumu görselleştirilmiştir [28].



Şekil 2. 4. Örnek Bir Uyarlanabilir Hız Kontrolü Durumu

2.1.1.10. Park Yardımı (PA)

Park yardım sistemleri çeşitli özelliklerde araçlarda görülebilir. Sadece sesli uyarı ile sürücüye destek olabilir, araç etrafını tarayarak ve görüntüleyerek analiz edebilir, uygun durumlarda aracı sistemin kendisi bile park edebilir. Bu sistemler zorlu park manevralarında sürücüye yardım ederek olası kaza durumlarının önüne geçer. Gelişmiş park yardım sistemleri, 360 derecelik kamera görüşü ve tamamen otonom kendi kendine park etme gibi çeşitli özellikleri içerebilir [29].

2.1.1.11. Otomotiv Gece Görüşü (ANV)

Otomotiv gece görüş sistemleri, gece yolculuklarında araç farlarının ulaşamayacağı kişi, araç veya hayvanları tespit etmenize yardımcı olan sistemlerdir. Araç gece görüş sistemleri, öndeki nesnelerin mesafesini belirlemek için IR (Infrared – Kızılötesi) dalgalarını veya araçtaki ısıyı tespit etmek için termografik sensörleri kullanır. Gece görüş sistemleri yalnızca yoldaki araçları değil, yayaları, hayvanları ve nesneleride yakalayarak olası kazaların önlenmesine yardımcı olur. Sistemin seviyesine bağlı olarak tarama menzilleri değişebilir. Sistem 300 metrelik bir alanı tarayabilir [30].

2.1.1.12. Kör Nokta Tespiti (BSD)

Kör nokta tespit sistemleri, sürücünün araç kullanırken göremeyeceği araç ve diğer nesneleri veya yerleri sensörler sayesinde tespit eden sistemlerdir. Bu özellik, araca bir otomobil veya yaya çok yaklaştığında sürücüyü sesli veya görsel ikaz ile uyarır. Kör nokta tespit sistemleri, aracın yan noktalarını, köşelerini, sürücünün görmekte zorlanacağı yerleri izler. Bir araç kör nokta bölgesine girdiğinde sürücüyü sesli olarak uyarır. Bazı araçlarda, kör noktaya giren nesne sürücüye kameralar aracılığı ile gösterilir [31].

2.1.1.13. Şerit Merkezleme Sistemi (LCS)

Uzun yolculuklar sürücü için yorucu olabilir ve dikkat dağınıklığı yaratabilir. Şerit merkezleme sistemi, aracı sürekli olarak gittiği şeritte tutar, bu sayede de sürücü, direksiyonu kontrol görevinden kurtulur. Uzun yolculuklarda bu sistem sürücülere sürüş esnekliği tanır ve yolculuğun zorluğunu azaltır. Bu sistem aynı zamanda aracın şeritten çıkmasını engeller ve sürüş güvenliğini arttırır. Sistem, şerit işaretleri ve sınırları tespit etmek için kameraları kullanır, kameralar sayesinde aracın kendi şeridindeki konumu belirlenir. Şerit merkezleme sistemi direksiyon kontrolünü devralarak aracı devamlı olarak şeritte tutar. Bu sistem sürücü isteği ile etkinleştirilip, devre dışı bırakılabilir [32].

2.1.1.14. Çarpışma Önleme Sistemi (CAS)

Çarpışma önleme sistemleri, araç çarpışmalarını engellemek, şiddetini önlemek veya azaltmak için geliştirilmiş sistemlerdir. Sistem, yaklaşan bir çarpışma tespit ettiğinde sürücüyü sesli veya görsel olarak uyarır. Aktif çarpışma önleme sistemlerinde, sistem sürücü etkisi olmadan aracı durdurabilir veya yavaşlatabilir. Bu sistemler, araç etrafındaki diğer araçları, yayaları ve engelleri tespit etmek için kamera, radar veya lidar gibi sensörleri kullanır. Çarpışma önleme sistemi, sistem seviyesine bağlı olarak yaklaşan bir çarpışma algıladığında, sürücüyü uyarabilir veya çarpışmayı önlemek için gerekli aksiyonu alabilir [33].

2.1.1.15. Sürücü İzleme Sistemi (DMS)

Sürücü izleme sistemi, sürücünün uyanıklığını ve dikkat seviyesini izleyen, kamera ve görüntü izleme teknolojisi tabanlı bir sistemdir. Sistem sürücüyü tanır ve sürüş güvenliğini arttırmak için sürücünün dikkat düzeyini kontrol eder. Sistem, uykululuk durumu veya dikkat dağınıklığı belirtileri tespit ettiğinde sürücüyü uyarır. Bu sistem, sürücü tanıma sistemi ve göz kontrollü bazı işlevlerin seçilmesi gibi harici fonksiyonları da içerebilir. Sürücü tanıma sistemi sayesinde, her sürücüye özel tercih ve ayarların otomatik olarak geri yüklenebilmesi sağlanır [34].

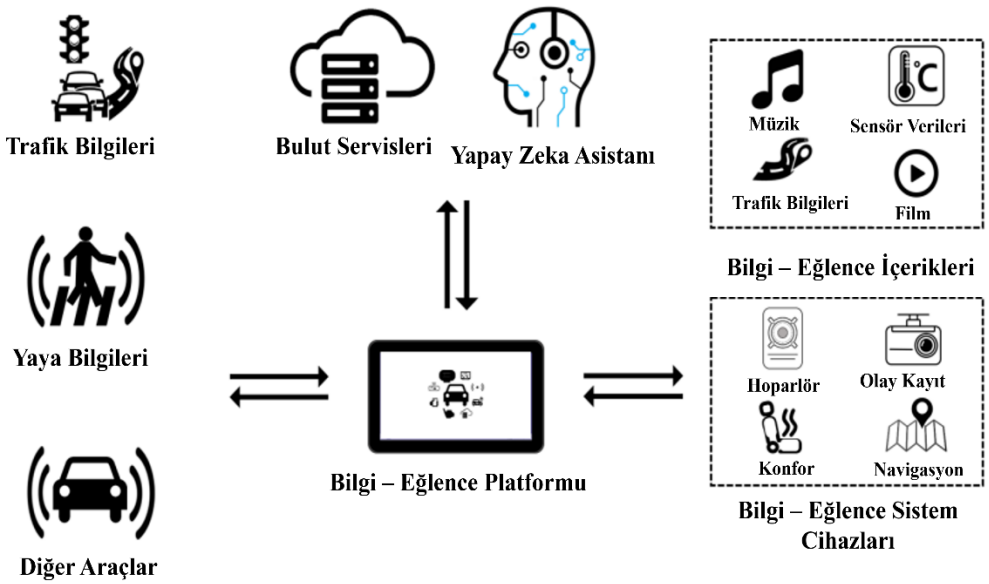
2.1.1.16. Arka Çapraz Trafik Uyarısı (RCTA)

Arka çapraz trafik uyarısı, araç park yerinden geri geri çıkarken, sağdan veya soldan yaklaşmakta olan bir aracın olup olmadığını kontrol eden, eğer herhangi bir araç yaklaşıyorsa bu durumu sürücüye bildiren uyarı tabanlı bir sistemdir. Genelde uyarı, ilgili yan ayna üzerinde sesli bir ikaz ile birlikte görünür. Araç arkasının sağ ve sol kısımlarında, herhangi bir aracın yaklaşıp yaklaşmadığını tespit etmek amacıyla, radar veya ultrasonik sensörler bulunur [35].

2.1.2. Bilgi – Eğlence (Infotainment) Sistemleri

Araçlar teknolojik olarak geliştikçe, araçların sürücü ve yolcularla görsel ve işitsel etkileşimleri gittikçe artmaktadır. Sürücüye farklı deneyim ve bilgi aktarımı sağlayan bu sistemler, otomotiv elektroniği alanındaki popüler konuların başında gelmektedir. Araç durumuna ait bilgiler, sürüşle ilgili bilgiler, aracın dış birimlerden aldığı veriler, sürücü ve yolculara bilgi-eğlence sistemlerine ait bileşen ve cihazlar yardımıyla aktarılır. Sürücü, sürüş durumuna (araç hızı, kalan yakıt, hata ve uyarılar vs.) ait bilgileri, aracın IPC (Instrument Panel Cluster – Gösterge Paneli Kümesi) üzerinden görsel ve işitsel olarak alır. Araç hızı, motor devri, yakıt durumu, gidilen kilometre gibi bilgiler sürücüye görsel olarak aktarılırken, herhangi bir arıza ve bildirim durumları sürücüye sesli bir ikaz olarak aktarılır. Sürücü araçta bulunan MHU (Media Head Unit – Medya Ana Birimi) ünitesi üzerinden müzik dinleyebilir, navigasyondan yararlanabilir, yolcular video izleyip haberleri takip edebilirler. Google ve Apple gibi şirketlerin otomotive yönelik oluşturduğu servisleri (Google Android Auto, Apple Car Play) kullanarak akıllı telefonları ile araçları bir bütün haline getirebilirler. Şirketlerin araçlara yönelik oluşturduğu yapay zeka sistemleri ve sesli asistan sistemlerini kullanarak bazı işlevlerin (ses açma – kısma, müzik açma – kapama, çağrı yanıtlama – reddetme, konfor (koltuk, ısıtma gibi) vs.) kontrollerini gerçekleştirebilirler. Bu sistemler araç ile sürücü arasındaki etkileşimleri sağlayan, sürücülere ve yolculara bilgi aktarıp (hata ve uyarılar, navigasyon, sürüş bilgileri, sensörlerden gelen bilgiler vs.) , bazı eğlence fonksiyonlarını (müzik, video, televizyon, oyun, internet vs.) sağlayan (information – entertainment) bilgi-eğlence sistemleridir [36].

Bilgi – eğlence sistemlerinin genel işlevleri, sürücülere ve yolculara aktarılan bilgiler, bilgi – eğlece içerikleri, kullanılan servisler ve cihazlar şekil 2.5.'de verilmiştir [36].



Şekil 2. 5. Bilgi - Eğlence Bileşenleri

Bilgi – eğlence sistemleri, araçlar ile sürücü – yolcular arasındaki arayüzdür. Bu sistemler belirli ana kullanım amaçları doğrultusunda sürücü ve yolculara bilgi aktarıp, servis ve eğlence hizmetleri sunmaktadır. Tablo 2.2.'de otomotiv elektroniğindeki bilgi – eğlence sistemlerinin ana amaçları ve ilgilendiği konular verilmiştir [37].

Tablo 2. 2. Bilgi - Eğlence Sistemlerinin Temel Amaçları

Numara	Bilgi – Eğlence Sistemlerinin Temel Amaç ve Konuları
1	Kişileri, mesajları, ve arama kayıtlarını içe (araç sistemine) aktarma
2	Multimedya sağlama
3	Kokpit alanının kurulması
4	Sosyal ağlara erişim
5	Bağlam (içerik) farkındalığını destekleme
6	Navigasyon sistemi sağlama

2.1.3. Bağlanabilirlik (Connectivity) Sistemleri

Araçlar daha da otonom ve akıllı hale geldikçe, araçlara uygulanması gereken fonksiyon ve özelliklerin sayısıda artmaktadır. Bağlanabilirlik özellikleri akıllı ve otonom bir araç için zorunlu sağlanması gereken özellik gruplarından bazılarıdır. Dünyadaki sanayi ve teknoloji dönüşümüne bakıldığında, IoT (Internet of Things – Nesnelerin İnterneti) dönüşümü en önde gelen teknoloji faaliyetlerinden biri olarak görülmektedir. Dünyadaki bu dönüşümün karşılığı olarak, otomotiv elektroniği alanında bağlanabilirlik sistemleri gelişmekte ve yeni nesil araçlarda yerini almaktadır. Otomotiv elektroniğindeki temel bağlanabilirlik özelliklerine bakıldığında connected vehicles (bağlantılı araçlar), V2X (Vehicle to Everything – Araçtan Her Şeye) ve OTA (Over the Air – Uzaktan) update – güncelleme fonksiyonları ön plana çıkmaktadır. Bağlantılı araçlar kavramı daha da açıldığında, aracın internete çıkması, buluta veri göndermesi, araç durumuna ait verilerin (bakım, servis ihtiyacı), sürüş durumuna ait verilerin (gidilen kilometre, ortalama hız, başlatma – durma sayısı, ani dönme, hızlanma vs.) buluta aktarılıp bir sistem tarafından incelenmesi ve raporlanması gibi işlevler ön plana gelmektedir. Bu sayede araç durumu sürekli olarak incelenebilir ve arıza, bakım zamanı gibi durumlar için ön tahminler oluşturulup sürücü uyarılabilir. Ayrıca sürüşe ait veriler, sürücü tarafından incelenip analiz edilebilir. Bağlantılı araçlar ile birlilte araçlar, kişiler ve altyapı arasındaki etkileşim ve bilgi aktarımı artacaktır [38].

2.1.3.1. Araçtan Her Şeye (V2X)

Araçlar bağlantılı hale geldikçe, araçların etkileşim kurduğu dış birimlerin de sayıları artmaktadır. Bu konsepte, araçların diğer araçlarla, altyapı ile, bulut ile, cihazlar ile, yayalar ile etkileşim kurduğu araçtan her şeye konsepti denmektedir. Araçlar bu dış birimler ile etkileşim kurarak bilgi alışverişi yaparlar. Otonom ve akıllı bir araç, dış birimler ile sağlaması gereken özellikler gereği iletişim kurmalıdır. Diğer araçlar ile konuşmalı, trafik, yol durumu ve hava durumu gibi bilgiler için altyapı ile haberleşmeli, sürüş ve araç durumuna ait verileri buluta kaydetmelidir. Ayrıca akıllı ulaşım sistemleri düşünüldüğünde, trafikteki tüm araçlar, trafik yönetiminin oluşturulması ve yol güvenliğinin sağlanması için birbirleri ile haberleşmeli ve bağlantılı olmalıdır [39].

2.1.3.1.1. Araçtan Araca (V2V)

Araçtan araca haberleşme teknolojisi, araçların birbirleri ile konuşmaları sayesinde, aracın çevresinde olup bitenleri yakalayabilen, yol koşulları ve trafik durumu hakkındaki bilgileri diğer araçlar ile paylaşabilen, araçların birbirlerine yakınlığı gibi detayların aktarıldığı, araçlar arasındaki iletişim yapısının kurulmasını sağlayan bir iletişim teknolojisidir. Araçtan araca bilgi aktarımı amacıyla gerekli hızın karşılanabilmesi için, MEC (Multi Access Edge Computing – Çoklu Erişim Uç Bilişimi) ve 5G gibi teknolojiler kullanılır ve veriler gerçek zamanlı olarak aktarılır. Bu sayede sürücüler, trafik hareketi ve durumu, hız sınırları, yol koşulları, kaza olayları gibi durumlar hakkında önceden bilgi sahibi olur [40].

2.1.3.1.2. Araçtan Altyapıya (V2I)

Araçtan altyapıya iletişim sistemi, araçları şehrin ve trafiğin altyapısına bağlayarak araçların, hız sınırları, kazalar, trafik, yol ve hava koşulları, yol ve şerit bakım çalışmaları, gerekli trafik uyarıları gibi bilgileri almasını sağlayan iletişim teknolojisidir. Bu teknoloji, araç ve sürücü güvenliğini arttırmak amacıyla kullanılabilir [40].

2.1.3.1.3. Araçtan Buluta (V2C)

Araçtan buluta teknoloji sistemi, hücresel LTE teknolojisini kullanarak araçtan buluta bir bağlantı kurabilir. Bu görevi genelde araçlarda bulunan T-BOX modülü yerine getirir. T-BOX modülü, sahip olduğu LTE fonksiyonu sayesinde, araç ağından aldığı verileri buluta göndererek, uzaktan araç teşhisi (remote diagnostic) ile arıza ve hata durumlarının tespiti, sürüş durumuna ait verilerin analizi, araç durumuna (yakıt seviyesi, pil seviyesi, menzil vs.) ait bilgilerin uzaktan kontrolü ve farklı bir IoT cihazına bağlanıp etkileşim kurma gibi fonksiyonların yapılmasını sağlar. Ayrıca OTA güncelleme paketlerini indirip, güncellenmesi gereken ünitenin yazılım veya firmware güncellemelerini gerçekleştirir. Bu sayede araç servise gitmeden veya kablolu bir donanım gerektirmeden güncellenmiş olur [40].

2.1.3.1.4. Araçtan Yayaya (V2P)

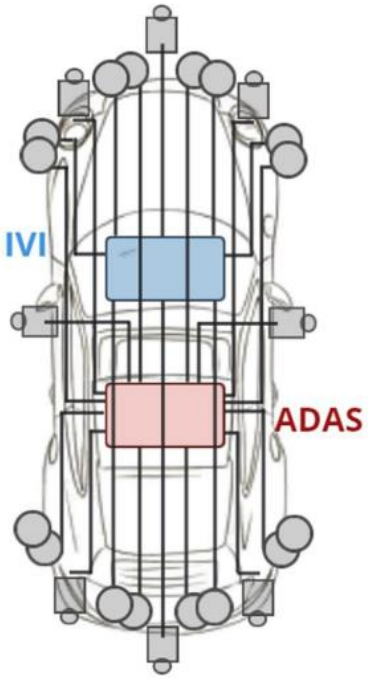
Yayalar, bisikletliler ve tekerlekli sandalye kullanan insanlar için oluşturulmuş bağlanabilirlik konsepti iletişim sistemidir. Yayalar ile araçlar arasında doğrudan iletişim kurulabilir. Yayalar, trafikte araçların yakınlarında bulunurlarsa, siyal iletimi yayalara ve araçlara sağlanır. Gelen uyarılar, sürücüleri yaklaşan yayalara karşı uyarır veya yayalara araçlar hakkında bilgi verir. Araçtan yayaya konsepti, yol güvenliğini arttırmanın yanı sıra trafik sıkışıklığını azaltmak, kaza ve çarpışmaları önlemek veya en aza indirmek gibi faydaları sağlar [41].

2.2. Araç İçi Ağ Mimarileri

Teknolojinin gelişimiyle birlikte araçlarda karşımıza çıkan özellikler yıldan yıla artmakta ve karmaşıklaşmaktadır. Gelişen ve karmaşıklığı artan özellikler, yeni ve gelişmiş donanımları ve yazılımları gerektirmektedir. Eklenen yeni özellikler ile birlikte, araçlarda kullanılan elektronik kontrol ünitesi ve sensörlerin sayıları artmaktadır. Her elektronik kontrol ünitesi ve sensör için ve elektronik kontrol ünitelerinin kendi aralarında haberleşmeleri için gerekli bir kablolama ihtiyacı oluşmaktadır. Artan elektronik kontrol üniteleri ve sensör sayıları karmaşık bir kablo demeti yığını oluşturmuştur ve bunun önüne geçmek için farklı mimari çeşitleri geçmişten günümüze düşünülmüş ve uygulanmıştır. Düşünülen mimari çeşitleri, döneminin teknolojilerini, uygulamalarını ve gereksinimlerini yansıtmaktadır. Örnek vermek gerekirse, gelişmiş sürücü destek sistemlerine ait bir fonksiyonu yöneten elektronik kontrol ünitesi, aracın ön tarafında bulunan radar sensöründen sürekli veri okuyup, veriyi işleyebilir. Aynı veri, aracın arka kısmında bulunan farklı bir elektronik kontrol ünitesi tarafından yönetilen bir fonksiyona girdi olarak da gerekebilir. Bu durumda radar sensöründen aynı anda iki elektronik kontrol ünitesine birbirinden ayrı bağlantılar yapmak hem sistemi karmaşık bir hale getirecek, kablolama maliyetini arttıracak hem de gerçek zamanlı olarak işlenmesi gereken bir veri için gecikmeye neden olacaktır. Bu nedenle, farklı araç içi ağ mimarileri ve haberleşme sistemleri geliştirilmiştir. Domain (Etki Alanı), Zonal (Bölgesel), Centralized (Merkezi) mimari çeşitleri, geleneksel karmaşık araç içi mimari sistemlerini iyileştirmek için geliştirilmiş, araç içi ağ mimari sistemleridir.

2.2.1. Etki Alanı (Domain) Araç İçi Ağ Mimarisi

Domain bazılı yönetimde, araç özellikleri ait olduğu alana göre sınıflandırılır. Örnek vermek gerekirse, araç powertrain (güç aktarma sistemleri), ADAS, IVI (In Vehicle Infotainment – Araç İçi Bilgi Eğlence), body (gövde) ve chassis (şasi) olarak beş farklı alana bölünür. Her bir etki alanının kendine ait sensörlerden gelen verileri işleyen elektronik kontrol ünitesi mevcuttur. Bu sistemde bu elektronik kontrol ünitelerine domain (etki alanı) denetleyicileri denmektedir. Ayrıca elektronik kontrol üniteleri arası bağlantıda mevcuttur, bu sayede etki alanları arası veri değişimi yapılarak diğer etki alanlarına girdi sağlanabilir. Örnek olarak ADAS alan denetleyicisinden gelen bir veri, bilgi eğlence alan kontrolcüsüne gönderilerek, multimedya ekranları üzerinden yolculara aktarılabilir. Bu sistem, aracın her yerine dağılmış, yüz adetten fazla olan elektronik kontrol ünitelerinin sayısını önemli ölçüde düşürerek, araç içi ağ karmaşıklığını azaltmıştır. Şekil 2.6.'da örnek bir domain (etki alanı) ağ mimari örneği verilmiştir [42].

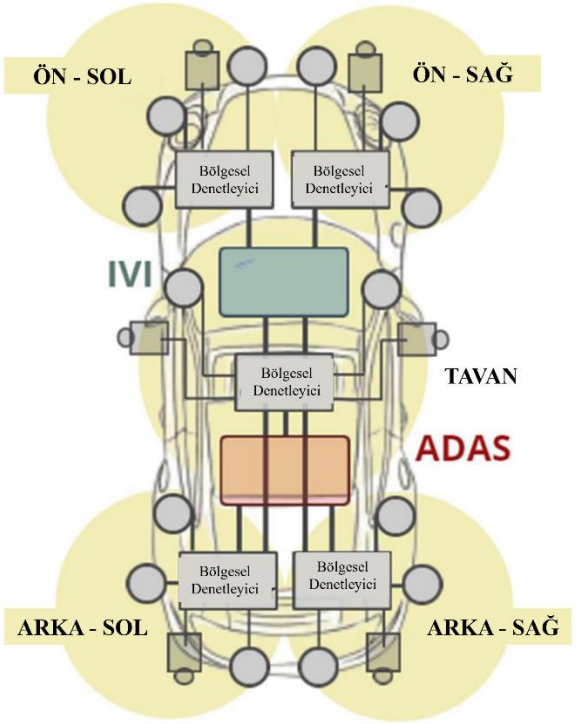


Şekil 2. 6. Domain (Etki Alanı) Ağ Mimarisi

Şekil 2.6.'da görüldüğü üzere, araçta IVI ve ADAS özelliklerine ait sensörler ve cihazlar, kendi alanlarına ait kontrolcüler üzerinde toplanmıştır. Bu mimaride her bir kontrolcü, kendi alanına ait fonksiyonları ve özellikleri yönetmektedir.

2.2.2. Bölgesel (Zonal) Araç İçi Ağ Mimarisi

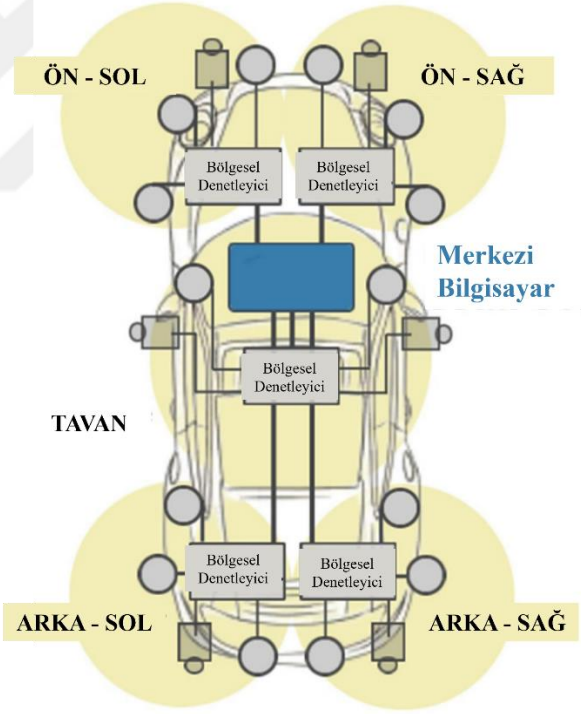
Avantajlarına rağmen etki alanı tabanlı mimari sistemi, kablolama ve kaynak çoğaltma açısından maliyetli bir çözümü temsil etmektedir. Çünkü bir sensörden gelen ham verinin, onu benzer şekilde işlemesi gerekecek farklı bir etki alanı kontrolcüsüne iletilmesini gerektirecektir. Bu tarz dezavantajların önüne geçmek için zonal (bölgesel) tabanlı araç içi ağ mimarisi geliştirilmiştir. Etki alanı tabanlı araç içi ağ mimarisi ve bölgesel tabanlı araç içi ağ mimarisi arasındaki en temel fark, sensörlerin ve aktüatörlerin doğrudan etki alanı kontrolcüsüne bağlanmayıp, bunun yerine zonal gateways (bölgesel ağ geçitlerine) bağlanmasıdır. Bu ağ geçitleri aracın ana bölgelerine yerleştirilir ve üreticiye bağlı olarak bölge tanımlamaları ve sayıları değişiklik gösterebilir. Örnek olarak araç 2 farklı bölgeye ön ve arka olacak şekilde ayrılabilir veya ön sol, ön sağ, tavan, arka sol ve arka sağ olarak daha detaylı beş farklı bölgeye de ayrılabilir. Bölgesel ağ geçitleri, sensörlerden gelen verileri bölgesel olarak işler, eğer gerekirse sonuçları diğer sistem bileşenlerine iletir. Şekil 2.7.'de ön-sol, ön-sağ, tavan, arka-sol, arka-sağ olarak 5 farklı bölgeye ayrılmış bir zonal (bölgesel) araç içi ağ mimari örneği verilmiştir. Sensör ve aktüatörlerin doğrudan bölgesel denetleyicilere bağlantılı olduğu şekilde görülmektedir [42].



Şekil 2. 7. Zonal (Bölgesel) Araç İçi Ağ Mimarisi

2.2.3. Merkezi (Centralized) Araç İçi Ağ Mimarisi

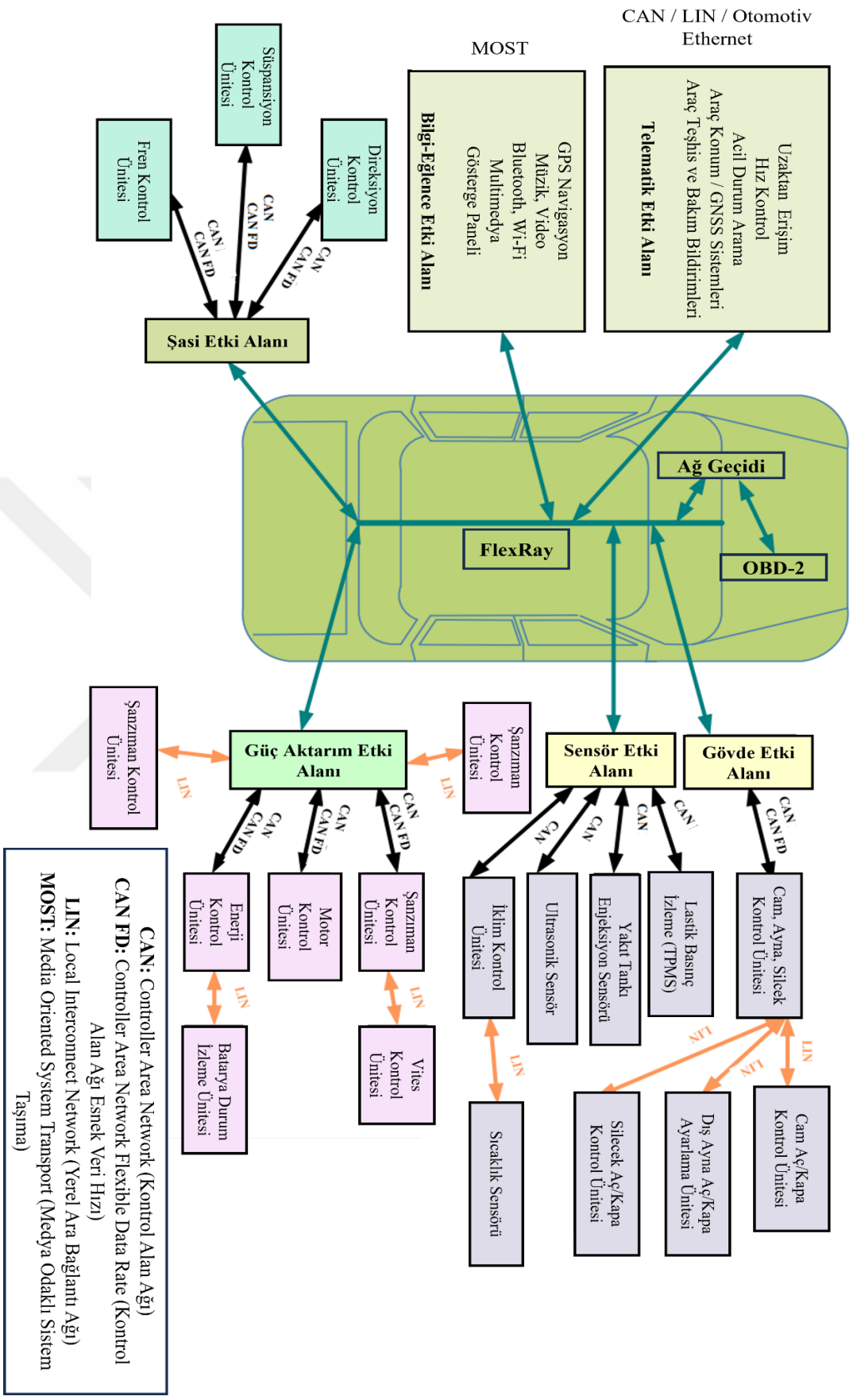
Son araştırmalar, araç fonksiyonlarını yöneten donanımları birbirinden ayırmanın gelecekte maliyetli bir çözüm olacağını göstermiştir. Fonksiyonları yöneten donanımları ayırmak yerine bu donanımları tek bir merkezi bilgisayar üzerinde birleştirmek gelecek çalışmalar için otomotiv üreticilerinin planları arasında olacaktır. Düşünülen bu sistemde, araç fonksiyonları tek bir donanımın farklı çekirdekleri üzerinden yönetilecektir. Bu durumda farklı alanlar ve fonksiyon grupları arasında kaynak ve veri paylaşımı kolaylaşacak, benzer işlevlere sahip kaynakların kopyalanması önleneceği için maliyet açısından faydalı olacaktır. Fakat tüm fonksiyonların tek bir donanım üzerinde toplanması, sağlanması gereken siber güvenlik seviyesini ve gereksinimlerini arttıracaktır. Şekil 2.8.'de örnek bir merkezi araç içi ağ mimari örneği verilmiştir [42].



Şekil 2. 8. Centralized (Merkezi) Araç İçi Ağ Mimarisi

2.3. Araç İçi Haberleşme Sistemleri

Elektronik kontrol üniteleri, sensörler, eğlence üniteleri (multimedya, ekranlar), ağ geçitleri (gateways) ve aktüatörler bir aracın ana ağ (network) bileşenlerini oluşturur. Bu bileşenler birbirleri ile haberleşirken çeşitli haberleşme sistemlerini kullanırlar. Sensörlerden gelen bilgiler, elektronik kontrol ünitelerine bu haberleşme sistemleri üzerinden aktarılır. Elektronik kontrol üniteleri arası veri iletiminde de bu haberleşme sistemlerinden yararlanılır. Aktüatörlerin kontrolünde, etki alanları (domain) arası iletişimde, araç içi bilgi – eğlence işlemlerinde, kontroller ve veri aktarımları, haberleşme sistemleri üzerinden gerçekleştirilir. Araçtaki ana bileşenler ve araç içi haberleşme sistemleri bir araya gelerek araç içi ağını oluştururlar. Günümüzdeki bir araç çeşitli domainlerden (etki alanları) oluşmaktadır. Powertrain (güç aktarma), body (gövde), chassis (şasi), infotainment (bilgi – eğlence), connectivity (bağlanabilirlik) gibi alanlar, bir aracın ana etki alanlarıdır. Her bir etki alanından sorumlu elektronik kontrol üniteleri, sensörler, ağ geçitleri ve aktüatörler bulunmaktadır. Bu bileşenler kendi aralarında bir haberleşme ağını ve bir sistemi temsil ederler. Şekil 2.9.'da genel bir araç içi ağ mimarisi verilmiştir. Aşağıdaki şekilde araç içi etki alanları ve kullanılan haberleşme protokolleri birlikte verilmiştir. Verilen mimaride, genel bir araç içerisindeki ana etki alanları görülmektedir. Bu etki alanlarının sağladığı fonksiyonlar ve etki alanları ile birlikte kullanılan haberleşme protokolleri verilmiştir. Resimde verilen etki alanı – protokol eşleştirmeleri sabit değildir. Her etki alanında birden fazla haberleşme protokolü kullanılabilir. Kullanılan haberleşme protokolleri araç özelliklerine, ihtiyaçlarına ve aracın sağladığı fonksiyonlara göre şekillenmektedir. Örneğin ADAS sensörlerinden gelen yüksek hızdaki verileri elektronik kontrol ünitelerine iletmek için, yüksek hızlarda veri aktarımını destekleyebilen bir protokol seçilmelidir. Veya cam kontrolü, koltuk ayarı, sıcaklık sensörü gibi temel fonksiyonlar için pahalı ve karmaşık sistemler yerine, basit ve ucuz bir çözüm sunan haberleşme protokollerinden birisi seçilebilir. Aşağıda verilen şekilde görüldüğü üzere bir araçta birden fazla haberleşme protokolü bulunur ve kullanılır. Bu konudaki ana seçim kriteri, sistem gereksinimleri, sistemin yapısı ve sağladığı fonksiyonlardır [43].



Şekil 2. 9. Araç İçi Ağ Mimarisi ve Haberleşme Protokolleri

Araçlarda kullanılan haberleşme protokollerine bakıldığında, sistem ihtiyaçlarına ve yapısına göre çeşitli ana protokoller kullanılmaktadır. Araç içi haberleşme sistemlerinde kullanılan ana protokollere bakıldığında, CAN (Controller Area Network – Kontrol Alan Ağı), LIN (Local Interconnect Network – Yerel Ara Bağlantı Ağı), MOST (Media Oriented Systems Transport – Medya Tabanlı Sistem Taşıma), FlexRay, Otomotiv Ethernet gibi haberleşme protokolleri öne çıkmaktadır. Tablo 2.3.'de araçlarda kullanılan ana araç içi haberleşme protokollerinin çeşitli kategoriler bakımından sınıflandırılması verilmiştir.

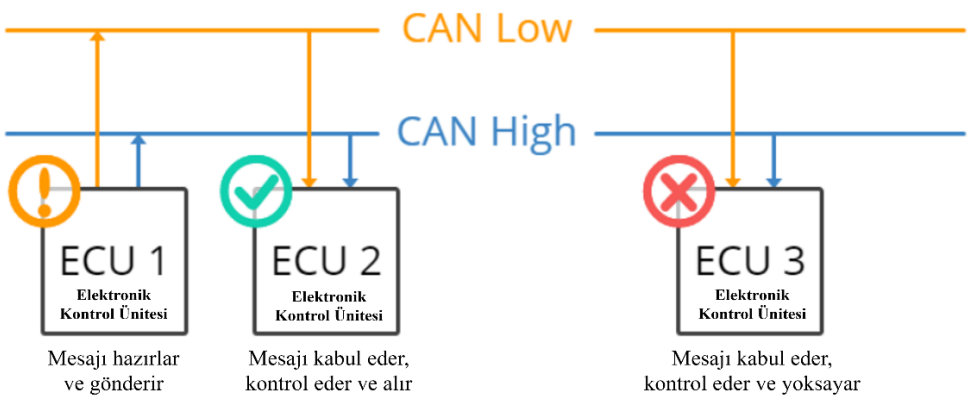
Tablo 2. 3. Araç İçi Haberleşme Protokollerinin Sınıflandırılması

Araç İçi Ağ Haberleşme Protokolleri	**CAN**	**LIN**	**FlexRay**	**MOST**	**Otomotiv Ethernet**
Etki Alanı (Domain)	Güç Aktarım, Gövde Kontrol	Basit Uygulamalar	Gelişmiş Şasi Kontrol	Bilgi – Eğlence Uygulamaları	Yüksek Bant Genişliği Uygulamaları
Bant Genişliği	125 Kbps – 1 Mbps	125 Kbps – 1 Mbps	10 Mbps kadar	150 Mbps kadar	100 Mbps kadar
Belirgin Özellik	Düşük Maliyet	Düşük Maliyet	Yüksek Hız	Yüksek Hız	Yüksek Hız
Dezavantajları	Düşük Bant Genişliği	Düşük Hız	Yüksek Maliyet	Yüksek Maliyet	Yüksek Maliyet
Topoloji	Yıldız, Halka, Doğrusal veri yolu	Doğrusal veri yolu	Yıldız, Doğrusal veri yolu, hibrit	Halka	Yıldız, Doğrusal veri yolu
Standart	ISO 11898	ISO 17987	ISO 17458	ISO 21806	ISO 21111
Kablolama	UTP	1-Tel Kablolama	UTP	UTP ve Optik	UTP
Desteklenen Maksimum Düğüm	30	16	22	64	Anahtar bağlantısı temelli
Mesajlaşma	Multi – Master (Çoklu Ana)	Master – Slave (Ana – Yardımcı)	Multi Master (Çoklu Ana)	Akış / Döngüsel Çerçeveler	IP temelli

2.3.1. Kontrol Alan Ağı (CAN)

Araç içi haberleşme sistemlerinde, elektronik kontrol üniteleri arası haberleşmelerde, sensörlerden gelen verilerde, genellikle CAN veriyolu haberleşme protokolü kullanılır. Bir CAN haberleşme sistemine bağlı cihazlara düğümler denilmektedir. CAN ağına bağlı her bir elektronik kontrol ünitesi bir düğümü temsil etmektedir. CAN veri paketleri, CAN veriyolunda birden fazla elektronik kontrol ünitesi arasında iletilir. CAN protokolünde broadcast (yayın) iletişim mekanizması kullanılır. CAN protokolünün basitlik, düşük ağ karmaşıklığı ve azaltılmış kablolama maliyetleri gibi çeşitli avantajları vardır [43].

CAN haberleşme sistemi, her bir elektronik kontrol ünitesinin, diğer tüm elektronik kontrol üniteleri ile karmaşık ve özel kablolama yapıları gerektirmeden haberleşmesini sağlar. Örnek olarak bir elektronik kontrol ünitesi, bir sensöre ait verileri CAN veriyolu aracılığı ile derleyip, yayınlayabilir. CAN ağına gönderilen sensör verileri, ağda bulunan diğer elektronik kontrol üniteleri tarafından kabul edilebilir, CAN ağında bulunan elektronik kontrol üniteleri, verileri kontrol eder ve alınması gerektiğine mi, yok sayılması gerektiğine mi karar verir. CAN haberleşme sistemi, donanımsal olarak 2 farklı kablodan oluşur, bu kablolardan biri CAN – high diğeri ise CAN – low kablosudur. CAN sinyalleri, 2 kablo üzerinden diğer elektronik kontrol ünitelerine aktarılır. Aşağıda verilen şekil 2.10.'da CAN protokolünün basit bir çalışma prensibi verilmiştir. Bir ECU tarafından hazırlanan veriler, tüm CAN ağına gönderilir, o veriyi kullanması veya alması gereken ECU, ağdaki CAN mesajını alır ve kullanır [44].

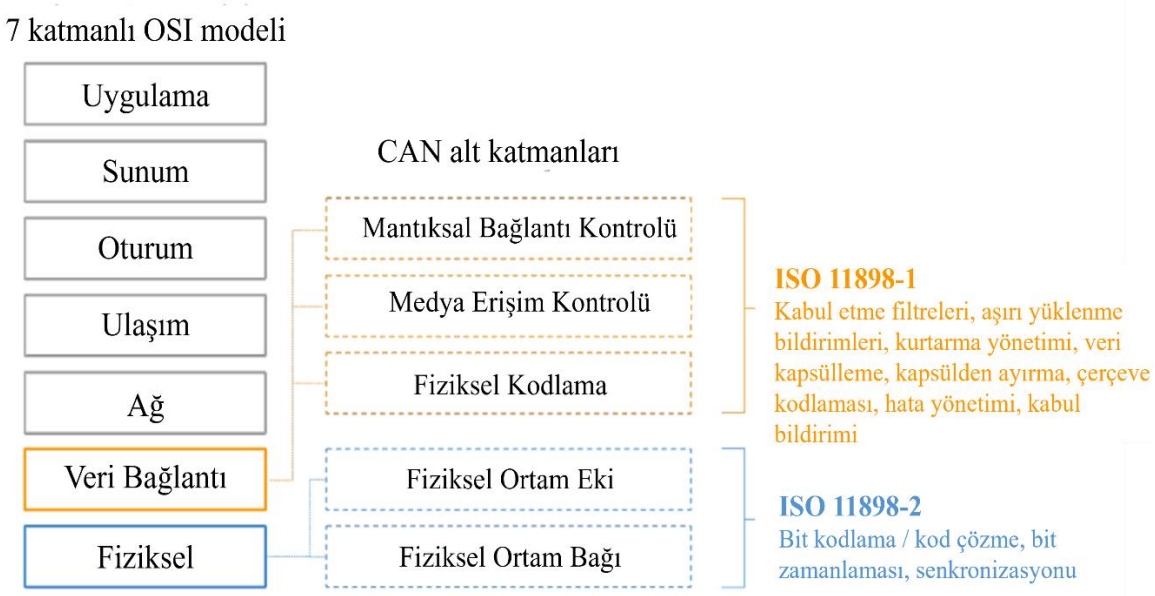


Şekil 2. 10. CAN Haberleşme Sistemi Yapısı ve Mekanizması

2.3.1.1. CAN Veriyolu Fiziksel ve Veri Bağlantı Katmanı

CAN protokolü, bir veri bağlantı katmanı ve fiziksel katmanla tanımlanır. ISO 11898-1 CAN protokolünün veri bağlantı katmanını açıklarken, ISO 11898-2 ise fiziksel katmanı açıklamaktadır. CAN protokolü, 7 katmanlı OSI (Open Systems Interconnection – Açık Sistem Ara Bağlantısı) modelinde açıklanmaktadır. Şekil 2.11.'de CAN protokolünün, OSI referans modeli katmanları verilmiştir. Fiziksel ve veri bağlantı katmanının görevleri, ilgili standarda göre açıklanmıştır [44].

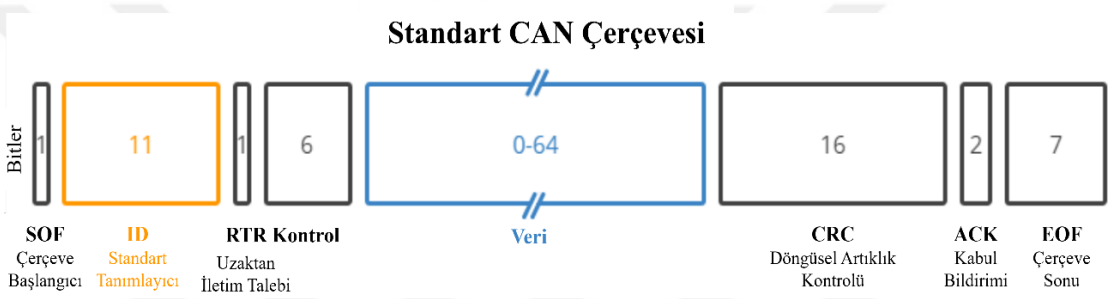
CAN veriyolu fiziksel katmanı, kablo tipleri, elektrik sinyal seviyeleri, düğüm (CAN ağına bağlı cihaz) gereksinimleri, hat ve kablo empedansı gibi teknik ifadeleri tanımlar. ISO 11898-2, CAN protokolünün baud hızı, kablo uzunluğu ve sonlandırma dirençleri gibi yapısal bilgilerini ve teknik gereksinimlerini belirler. CAN düğümleri, klasik CAN için 1 Mbit/s'ye, CAN FD için 5-8 Mbit/s'ye kadar veri hızlarına sahip iki kablolu bir yapıyı içeren veriyolu üzerinden birbirlerine bağlanmalıdır. Maksimum kablo uzunluğu 500 metre (125 kbit/s) ile 40 metre (1 Mbit/s) arasında olmalıdır. Ayrıca CAN ağındaki sinyal yansımalarını azaltmak için CAN hattının her iki ucu 120 ohm değerine sahip sonlandırma dirençleri ile sonlandırılmalıdır [44].



Şekil 2. 11. CAN Protokolü OSI Modeli Katmanları

2.3.1.2. CAN Mesaj İçeriği

CAN veriyolu haberleşmesi, CAN mesaj çerçeveleri aracılığı ile gerçekleştirilir. Bir CAN mesaj çerçevesi, farklı görevlere sahip alanlardan oluşur. Her bir alan, CAN mesajlaşması için farklı bilgileri içerir ve taşır. Klasik CAN (CAN 2.0A), haberleşmesi için standart 11 bit tanımlayıcı (Identifier) alanına sahip çerçeve kullanılırken, genellikle ağır vasıta araçlarda kullanılan, J1939 CAN protokolü (CAN 2.0B) için 29 bit tanımlayıcı alanına sahip genişletilmiş CAN çerçevesi kullanılmaktadır. Şekil 2.12.'de standart CAN mesaj çerçevesi ve çerçeve alanları verilmiştir.



Şekil 2. 12. Standart CAN Mesaj Çerçevesi ve Alanları

SOF (Start of Frame – Çerçeve Başlangıcı) Alanı : Ağdaki diğer düğümlere (cihazlara), CAN düğümünün konuşmak istediğini söyleyen baskın sıfırdır.

ID (Identifier – Tanımlayıcı) Alanı : CAN mesaj çerçevesinin tanımlayıcı alanıdır. Standart CAN yapısı için 11 bit, genişletilmiş CAN yapısı için 29 bitlik bir alana sahiptir. Daha düşük değerler daha yüksek önceliğe sahiptir.

RTR (Remote Transmission Request – Uzaktan İletim Talebi) Alanı : Uzaktan iletim talebi, bir düğümün başka bir düğüme veri gönderip göndermediğini veya başka bir düğümden veri isteyip istemediğini belirtir.

Kontrol Alanı : Standart frame (11 bit) için baskın sıfır olan tanımlayıcı uzantı bitini içerir. Ayrıca iletilecek veri baytlarının uzunluğunu (0-8 byte) belirten 4 bitlik DLC (Data Length Code - Veri Uzunluğu Kodunu) içerir.

Veri Alanı : CAN mesajının taşıdığı bilgiyi içeren yani kodlanmış CAN sinyallerinin baytlarını içerir. İlgili düğüm kodu çözülebilen CAN sinyallerini alarak gerekli bilgiyi almış olur. Bir standart CAN mesajında maksimum 8 baytlık bir veri taşınabilir. İletilen veri 8 bayttan küçük de olabilir.

CRC (Cyclic Redundancy Check – Döngüsel Artıklık Kontrolü) Alanı : Veri bütünlüğünü sağlamak ve kontrolünü yapmak için kullanılan alandır. Alınan CAN mesajının bozulup bozulmadığını anlamak için kullanılabilir. Gönderilen CAN mesajına özel üretilen bir kod taşır. CAN mesajını alan ağ düğümü, gelen mesajın düzgün olup olmadığını anlamak için bu kodu kullanır. Alınan CAN mesajı, CRC kontrolüne göre düzgün ise, alıcı düğüm gelen CAN mesajını kabul eder ve gönderici üniteye ACK (Kabul Bildirim) bilgisini gönderir. Eğer gelen CAN mesajında herhangi bir bozulma olmuş ise, mesajı alan düğüm gönderici düğüme bir hata mesajı gönderir ve mesajın tekrar gönderilmesini sağlar.

ACK (Acknowledgement – Kabul Bildirimi) Alanı : Kabul bildirim alanı, düğümün verileri doğru bir şekilde kabul edip etmediğini gösterir. CAN ağındaki önceliği bulunan düğüm, CAN mesaj çerçevesini, CAN ağına gönderir, kabul bildirim alanı bilgisini çekinik (sıfır) olarak bırakır. CAN ağındaki düğümlerden herhangi birisi CAN mesajını alır ise, CAN ağına kendi kabul bildirim bitini göndererek baskın yapar. Diğer düğüm, CAN ağının iletim kontrolünü bu düğüme bırakır. Herhangi bir düğüm kabul bildirim bilgisini ağa göndermez ise, gönderici düğüm mesajı tekrar gönderir. Belirli bir süre içerisinde, CAN ağından kabul bildirimi mesajını alamaz ise, CAN ağına hata mesaj çerçevesini göndermeye başlar.

EOF (End of Frame – Çerçeve Sonu) Alanı : CAN mesaj çerçevesinin sonunun geldiğini gösterir.

2.3.1.3. CAN Protokolünün Güvenlilik Açısından Değerlendirilmesi

CAN protokolü, güvenlik kritik uygulamalar için çok önemli bir faktör olan gerçek zamanlı performansı sağlayamamaktadır. CAN protokolü, araç içi ağ güvenlik sorunlarını çözememektedir. Kimlik doğrulama (authentication) mekanizmasının olmaması ve herhangi bir şifreleme (encryption) mekanizmasının sağlanmaması, CAN veriyolu haberleşme sisteminin ana sınırlaması ve zayıflığı olarak kabul edilir. Ek olarak, otomotiv elektroniği uygulamalarının gelişmesi ve karmaşıklaşması, aktarılması gereken veri miktarını arttırmış, yüksek hızlara ve bant genişliğine sahip sistemlerin kullanılmasını gerektirmiştir [43].

CAN protokolünün kimlik doğrulama ve şifreleme mekanizmalarını içermemesi, bu protokolü çoklu iletişim saldırılarına karşı savunmasız hale getirmektedir. Bu özellikle otomotiv elektroniğinde çok önemlidir, çünkü herhangi bir saldırı, kaza durumunu oluşturarak hayati bir tehdit oluşturabilir. CAN ağına yapılacak bir siber saldırı ile sahte bir mesaj oluşturulabilir. Bu sahte mesaj ile fren mesajı / komutu yerine, hızlan mesajı / komutu ilgili elektronik kontrol ünitesine gönderilerek kaza meydana getirilebilir. Mevcut CAN veriyolu haberleşme sisteminde bulunan elektronik kontrol üniteleri, herhangi bir veri değişikliğini, veri manipülasyonunu ve sahte veriyi tanıyamaz ve kaynağını tespit edemez. Aracın dış birimlerle herhangi bir etkileşiminin bulunmadığı veya araca yönelik herhangi bir saldırı noktasının bulunmadığı durumlarda güvenlik açısından bir sorun yoktur, fakat araçlar daha da bağlantılı ve otonom hale geldikçe, dış birimlerle olan etkileşimleri arttıkça, araçlara yönelik siber saldırı durumları ve imkanları da artmaktadır. Yapılan bir araştırmada, bir araca yönelik gerçekleştirilen siber saldırı sonucunda, saldırganın hem gaz hem de fren pedalını kontrol ettiği gözlenmiştir. Başka bir araştırma sonucunda da, araç uzaktan kumandasının güvenli olmadığı, siber saldırı için bir arayüz oluşturduğu, mekanik kilit sistemlerinin siber saldırı açısından daha güvenli olduğu ileri sürülmüştür. CAN veriyoluna yapılan siber saldırılara bakıldığında, gizlice dinlemek, mesaj değiştirme, kaynak değiştirme (message and source modification), uydurma ve yanıt saldırıları (reply attack) gibi saldırılar görülmektedir [45].

CAN veriyolu protokolünün tehditleri içinde gizlice dinleme, yanıltma ve telematik saldırı yoluyla yetkisiz erişimde yer alır. CAN veriyoluna fiziksel olarak bağlanan bir cihaz tüm ağ verilerine ve bilgilerine erişebilir ve herhangi bir çaba gerektirmeden elektronik kontrol üniteleri arasındaki iletişimi dinleyebilir. Gizlice dinlemeyi azaltmak için veriyolunda aktarılan bilgilerin güvenli bir şekilde şifrelenmesi gerekir [46].

Bir CAN mesaj çerçevesi, kaynak tanımlayıcısından değil hedef tanımlayıcısından oluşur. CAN ağında bulunan tüm cihazlar, alınan her mesajın kimlik alanını inceler ve kimliğe göre mesajın kendilerine yönelik olup olmadığını anlarlar. Kötü amaçlı bir cihaz veya bir saldırı, mesajları okumak ve hedef cihazın kimliğini (ID) bulmak için haberleşme ağını dinleyebilir. Mesajları anlayan ve yorumlayan kötü amaçlı cihaz sonrasında hedef cihazın kabul ettiği yapıya ve kimliğe göre hazırlanmış mesajlar gönderebilir. Gönderici kimlik bilgisini korumak ve verilerin gizliliğini sağlamak için CAN protokolünde kimlik doğrulama ve erişim kontrolü katmanına ihtiyaç bulunmaktadır [46].

Yakın zamanda yapılan bir çalışmada, araştırmacılar uzaktan kumanda anahtarı üzerinden harici yetkisiz erişim yapmanın mümkün olduğunu buldular. Anahtarda bulunan bellek bloğunun içeriğini çıkararak, şifreleme bloğunun kaynak kodunu tersine mühendislik yaparak ve simetrik anahtarları çıkararak bir araç üzerinde yetkisiz erişim elde etmeyi başardılar [46].

Hizmet reddi (DoS) veya hizmeti engelleme saldırıları, kaynakları veya hizmetleri erişilemez hale getirir. CAN ağında birbirleri ile haberleşen iki elektronik kontrol ünitesi bilgi aktarımında bulunurken, kötü niyetli bir cihaz CAN ağına duraklamadan rastgele mesajlar gönderebilir. Bu durum sistemin arabelleğini aşırı yükleyerek arabellek taşması durumunu oluşturabilir. Böylece CAN ağı, haberleşme için kullanılamaz hale getirilebilir [46].

2.3.2. Yerel Ara Bağlantı Ağı (LIN)

LIN protokolü, sensörleri ve aktüatörleri bağlamak için kullanılan tek kablolu bir araç içi haberleşme sistemidir. LIN haberleşmesinin güvenilirliği, CAN haberleşmesi ile kıyaslandığında daha düşük kalmaktadır. Bu nedenle, araçlardaki kritik uygulamalarda çok tercih edilmez. Ayna motoru, cam motoru, silcekler gibi karmaşık ve kritik olmayan sistemler için basit ve ucuz bir çözüm olabilir.

2.3.3. FlexRay

FlexRay protokolü, senkron ve asenkron modlarda veri gönderimi için iki paralel hat kullanır. Bu protokol, zaman açısından kritik uygulamalar ve fonksiyonlar için kullanılabilir. FlexRay haberleşme sisteminin güvenilirlik seviyesi yüksektir ve hata toleransı özelliğine sahiptir fakat bu protokol ucuz bir çözüm değildir. Bu haberleşme sistemi, sağlama toplamlarını (checksums) ve artıklık mekanizmalarını (redundancy) kullanır ve mantıksal hataları yakalayabilir.

2.3.4. Medya Tabanlı Sistem Taşıma (MOST)

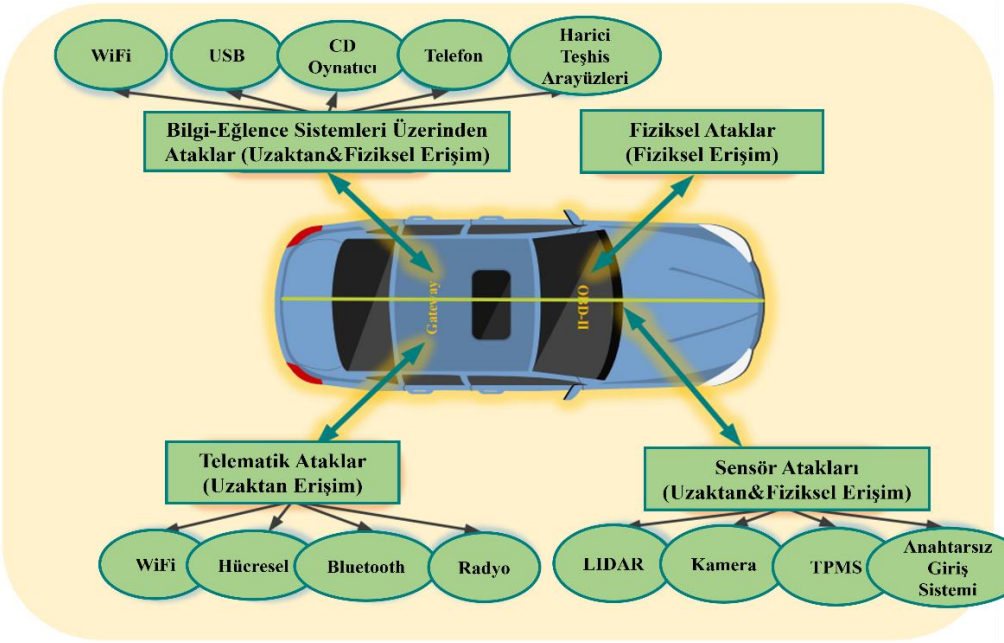
MOST protokolü veri alışverişi için, senkron ve asenkron modlardan ikisini de destekler. Bu protokol çoğunlukla GPS ve radyo uygulamalarında kullanılır. Araçlarda kullanılan bilgi – eğlence sistemlerinin gereksinimlerini karşılayabilir. Fakat artan bant genişliği gereksinimlerini karşılamada yetersiz olabilir.

2.3.5. Otomotiv Ethernet

Bu protokol araç içi haberleşme sistemlerinde bir fiziksel katman standardı olarak ele alınabilir. Farklı kapasite ve yüksek hızlara sahip olması nedeniyle, gelişmiş sürücü destek sistemleri gibi yüksek hız ve bant genişliği gerektiren gelişmiş uygulamalarda kullanılabilir. Bu protokol anahtarlamalı ağ teknolojisini desteklediği için, kablolama maliyetini düşürebilir.

2.4. Araç İçi Ağ Sistemine Yapılan Saldırıların Olası Giriş Noktalarına Göre Sınıflandırılması

Araç içi ağ sistemine saldırı yapılabilecek birçok arayüz bulunmaktadır. Bu saldırılar, kablolu veya kablosuz olarak gerçekleştirilebilir. Saldırganlar elektronik kontrol ünitelerine kolaycak erişmek için yazılım hatalarını, aracın uzaktan kumanda anahtarını, araçtan dışarıya çıkan sensör arayüzlerini ve dahasını kullanabilir. Şekil 2.13.'de araç içi ağ sistemine gerçekleştirilen saldırıların giriş noktaları ve sınıflandırması verilmiştir. Bu arayüzler, sensörler üzerinden, bilgi – eğlence sistemleri üzerinden, telematik sistemleri üzerinden veya doğrudan fiziksel olmak üzere sınıflandırılabilir. Saldırgan her bir arayüz üzerinden sistemin özelliklerine göre kablosuz veya kablolu olarak saldırabilir. Örnek olarak bilgi – eğlence sistemlerinden birine kablosuz girebilmeyi başarabilen bir saldırgan, eğer bilgi – eğlence sisteminin araç ağı ile bir arayüzü varsa, araç ağına erişebilir. Bunun dışında bir saldırgan, aracın ağına giden herhangi bir port üzerinden doğrudan saldırı gerçekleştirebilir. Bu senaryoda saldırgan ile araç arasında fiziksel bir arayüz ve erişim kurulur. Araçlarda bulunan bağlanabilirlik ve telematik özellikleri, kablosuz yapılacak bir saldırı için olası giriş noktaları olabilir. Ayrıca yeni sistemlerin araçlara entegre edilmesi ile çok fazla sayıda sensör etkileşimi gerçekleşti. Bu sensörler de aracın haberleşme ağına ulaşmak için olası giriş noktaları olabilir [43].



Şekil 2. 13. Araç İçi Ağ Sistemine Yapılan Saldırıların Arayüzleri

2.4.1. Araç Ağına Saldırı / Giriş Noktaları

Yeni nesil akıllı araçlar, otomotiv elektroniğindeki yaşanan gelişmelere bağlı olarak birçok akıllı ve işlevsel özelliğe sahiplerdir. Araçlarda yaşanan bu teknolojik gelişim, araçları siber saldırılara karşı potansiyel bir hedef haline getirmiştir. Bu yüzden otomotiv elektroniğinde siber güvenlik uygulamaları zorunlu bir boyut kazanmıştır. Araçlara yönelik saldırıları gerçekleştiren siber korsanlar, araçları hacklemek için gelişmiş yöntemler kullanmaktadır, bu yüzden araçların güvenlik mekanizmaları saldırılara karşı gerekli aksiyonları almalı ve saldırıları mümkün kılmamalıdır. Tablo 2.4.'de günümüz akıllı araçlarına yönelik gerçekleştirilebilecek saldırılara olası giriş noktaları verilmiştir [43].

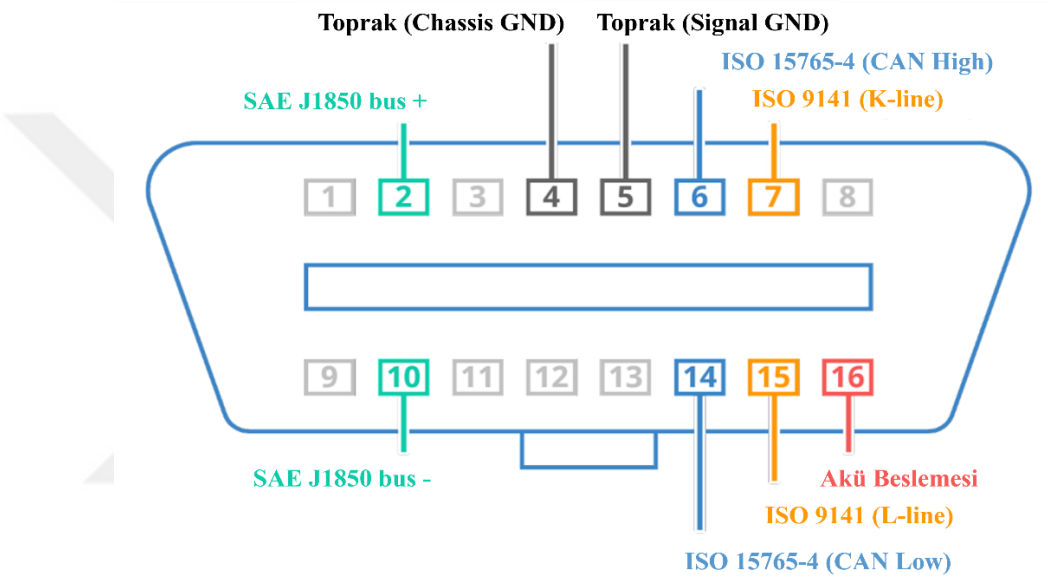
Tablo 2. 4. Akıllı Araç Ağına Giriş Noktaları

	Akıllı Araç Ağına Saldırı/Giriş Noktaları
1	OBD-2 Portu
2	USB Portu
3	Elektrikli Araç Şarj Portu
4	TPMS, LIDAR, Kamera, Anahtarsız Giriş
5	Araç Ağına Doğrudan Giriş Noktaları
6	Bluetooth
7	Wi-Fi
8	DSRC
9	Hücresel İletişim

2.4.1.1. OBD-2 Portu

OBD-2 portu, araçların teşhis / tanı, kilometre gibi bilgilerini takip etmek için kullanılır. Saldırgan bu port üzerinden aracın ağına bağlanabilir çünkü aracın ağına giden hatlara ait bağlantı noktaları bu port üzerine çıkarılmıştır. Saldırgan bu arayüz üzerinden herhangi bir CAN haberleşme cihazı kullanarak aracın teşhis / tanı bilgilerine veya araç içi ağda dolaşan diğer verilere de ulaşabilir. Bu yüzden bu port ile araç içi ağı arasına güvenli bir ağ geçidi (Secure Gateway) konulması önerilmiştir. OBD 2 portu, araç içi ağına ulaşımı kolaylaştırdığı için araçta bulunan, güvenlilik olarak en zayıf saldırı noktalarından biridir. Şekil 2.14.'de OBD 2 konnektörünün pin tanımları verilmiştir.

OBD 2 portu üzerinden 2 farklı saldırı mümkün olabilir. Bunlardan birincisi, araç içi ağına erişim saldırısı, ikincisi ise dongle (donanım kilidi) istismar saldırısıdır. İlk saldırı çeşidinde, saldırgan araç içi ağa ulaşmak için kurmak istediği kötü niyetli cihazı, OBD 2 portu üzerinden araç ağına bağlamak ister. Burada amaç, araç içi ağına fiziksel erişim elde etmektir. İkinci saldırı türünde ise saldırgan OBD 2 bağlantı noktalarına donanım kilitlerini takar. Takılan bu donanım kilitleri, uzaktan bağlantı ile saldırganlar tarafından kullanılabilir ve yönetilebilir. Bu sayede donanım kilitlerinin okuduğu veriler kaydedilip anlamlandırılabilir [43].



Şekil 2. 14. OBD-2 Portu Pin Çıkışları ve Tanımları

2.4.1.2. USB ve Şarj Bağlantı Noktaları

Araçlarda, multimedya ve bilgi – eğlence sistemlerinde şarj ve medya aktarım amaçlı kullanılan USB bağlantı noktaları, araca yönelik bir saldırı için, potansiyel güvenlik tehditleri oluşturmaktadır. Bu güvenlik tehditlerine örnek olarak elektronik kontrol ünitesinin veya multimedya denetleyicisinin yeniden programlanması, kötü amaçlı kodların yüklenmesi, işletim sistemi fonksiyonlarında yapılmak istenen kötü niyetli değişiklikler verilebilir. Buna ek olarak, USB bağlantı noktasına takılan bir flash sürücünün içindeki kötü amaçlı kod dizinleri, bilgi – eğlence ve multimedya sistemini hacklemek için kullanılabilir. Multimedya sistemi üzerinden araç ağına erişebilen saldırganlar, fren, gaz, kilit ve motor kontrol sistemleri gibi kritik sistemlere de erişebilirler [43].

Elektrikli araçlar, şarj işlemi esnasında şarj altyapısı üzerinden çeşitli kötü niyetli saldırılara karşı açık hale gelebilirler. Çünkü şarj istasyonu ve araç arasında bir etkileşim ve iletişim mekanizması kurulur. Akıllı şebekeden araca yönelik bir saldırı yapılabilir. Ayrıca elektrikli araç üzerinden akıllı şebekeye de bir saldırı gerçekleştirilebilir [43].

2.4.1.3. TPMS, LIDAR ve Anahtarsız Giriş Portları

Saldırgan, araç ağına erişmek için çeşitli yöntemler kullanabilir. Buradaki asıl konu araç ağı ile bağlantısı olan ve etkileşim kurmanın kolay olduğu bir arayüz bulmaktır. TPMS (Tire Pressure Monitoring System – Lastik Basıncı İzleme Sistemi) ve LIDAR gibi sistemler araç ağı ile bağlantılı oldukları için olası saldırı giriş noktalarıdır. Saldırgan bu cihazları, araç ağına ulaşmak için gizlice dinleyebilir. Ayrıca bu cihazlar üzerinden giden sinyalleri manipüle ederek sinyal karıştırma saldırısı gerçekleştirebilir. Anahtarsız giriş sistemine yönelik yapılan saldırıda ise saldırgan, araç uzaktan kumandasından giden radyo sinyallerini yakalamaya ve yeniden yönlendirmeye çalışır [43].

2.4.1.4. Veriyolu Ağ Portları

CAN protokolü için bir haberleşme koruma mekanizması mevcut değildir. Bu protokol bir yayınlama sistemini içerir ve ana amaç ilgili düğümün CAN mesaj çerçevesini ağ üzerinden almasıdır. CAN protokolünün yapısı gereği mesaj çerçevesi dijital imza ile güvence altına alınmaz. CAN protokolünde, kritik ve gizli veriler çalınabilir ve değiştirilebilir. Araç ağına saldırmayı amaçlayan saldırgan, her bir düğüme sahte ve rastgele CAN mesaj çerçeveleri göndererek aracın beklenmedik davranışları göstermesine ve hata durumlarına sebep olabilir.

2.4.1.5. Araç Haberleşme Portları

Yeni nesil araçların çoğunda uzaktan bağlantı için yeterli bir menzile sahip bluetooth özelliği bulunmaktadır. Cep telefonu bağlantısı, arama gerçekleştirmek, müzik için bağlantı kurmak, çağrıları yönetmek vs. gibi bir çok işlevi yerine getirmek için telematik sistemlere, multimedya ve bilgi – eğlence sistemlerine bağlantı gerçekleştirilir. Saldırganlar telefon ile araç arasında kurulan bluetooth bağlantısı üzerinden araç ile bağlantı kurabilir ve araç ağına ulaşabilir [43].

Akıllı araçların hemen hemen tamamı Wi-Fi özelliğini müşterilerine sunarlar. Wi-Fi özelliğine sahip akıllı araçlar ortak alanlarda kullanılan Wi-Fi ağları ile bağlantı kurabilirler. Ortak Wi-Fi noktalarındaki yetersiz güvenlik, güncel olmayan güvenlik sistemlerinin Wi-Fi erişim noktalarında kullanılması, bu erişim noktalarına bağlanan araçları saldırılara açık hale getirir [43].

Araçlarda kullanılan diğer haberleşme sistemlerine bakıldığında, özel kısa menzilli iletişim sistemleri de (NFC gibi) görülmektedir. Bu sistemler haberleşme için radyo frekans sinyallerini kullanır. Araçtan araca iletişim ve araçtan altyapıya iletişimi de, kısa mesafeli iletişimi destekler. Saldırgan kısa mesafeli haberleşme üzerinden araca erişim sağlayabilir ve kötü niyetli faaliyetleri gerçekleştirebilir [43].

Günümüz akıllı araçlarının neredeyse tamamı hücresel haberleşme (3G / 4G / 5G / LTE vb.) sistemlerini kullanıcılarına sağlar. Bu sayede uzun menzilli mesafeler arasıda araçla iletişim kurulabilir. Araçtan araca iletişim, araçtan altyapıya iletişim gibi teknolojiler de hücresel haberleşmeyi destekleyebilir. Hücresel ağa erişebilen bir saldırgan, karıştırma ve gizlice dinleme gibi saldırıları gerçekleştirebilir [43].

2.5. Gelişmiş Şifreleme Standardı (AES) Şifreleme

AES şifreleme algoritması (ayrıca Rijndael Algoritması olarakta bilinir), 128 bitlik blok boyutuna sahip, simertik bir blok şifreleme algoritmasıdır. Simetrik şifreleme olması, verilerin şifrelenmesi ve şifrelerinin çözülmesi için aynı anahtarın kullanılmasından kaynaklanmaktadır. AES yapısı gereği verileri 128 bitlik bloklar halinde şifreler, bu yüzden bir blok şifreleme algoritmasıdır. AES veri bloklarını şifrelerken 128, 192 ve 256 bitlik anahtarları kullanır. Şifrelenen bloklar birleştirilerek şifreli metin oluşturulur.

AES algoritmasının yapısı substitution – permutation (yer değiştirme – permütasyon) sistemine dayanır. AES şifreleme, girdilerin belirli çıktılarla yer değiştirmesi ve bit karıştırma işlemlerini içeren bağlantılı işlem zincirlerinden oluşur. AES algoritmasının her bir adımında farklı işlemler veri üzerinde uygulanır. AES algoritmasında, şifrelenecek metin arka arkaya tekrarlanan turlar sonucunda oluşur. Her bir turda veri paketi üzerinde belirli işlemler yapılır ve bir sonraki tura geçilir. Her bir tur sonucunda oluşan şifreli veri, bir sonraki tur için bir girdidir. Veri bloklarının kaç tur işlem göreceği, şifrelemede kullanılan anahtar boyutuna göre farklılık gösterebilir. Verinin işlem göreceği her bir tur, şifreleme gücünü arttırır ve şifrelenmiş metinden, orijinal düz metine dönüş sürecini zorlaştırır. Aşağıda verilen Tablo 2.5.'de AES şifrelemede kullanılan anahtar boyutu ile, verilerin işlem göreceği tur sayısı arasındaki ilişki verilmiştir [47].

Tablo 2. 5. AES Şifrelemede Anahtar Uzunluğu ile Tur Sayısı Arasındaki İlişki

Anahtar Uzunluğu (Bit)	Tur Sayısı
128	10
192	12
256	14

AES simetrik bir şifreleme türü olduğu için, şifre çözme işleminde de aynı anahtar kullanılır. Şifre çözüm işleminde, şifrelenmiş metinden geriye doğru, şifrelenirken yapılan işlemlerin tersi gerçekleştirilir. Şifre çözme işleminde farklı bir anahtar kullanılırsa, orjinal düz metin elde edilemez. Bu yüzden şifreyi çözen cihaz, şifreleme yapılırken kullanılan anahtar bilgisine sahip olmalıdır.

2.5.1. AES Algoritmasının Özellikleri

Yer Değiştirme – Permütasyon Mekanizması: AES şifreleme, DES (Data Encryption Standard – Veri Şifreleme Standartı) algoritmasındaki Feistel şifre yapısından farklı olarak, yer değiştirme – permütasyon yapısına dayalı çalışır.

Bayt Verisi: AES algoritması, şifreleme ve şifre çözme işlemlerini bit verileri yerine, bayt verileri üzerinden gerçekleştirir. Aslında şifreleme işlemine giren 128 bitlik blok, 16 bayt olarak ele alınır.

Anahtar Uzunluğu: AES şifrelemedeki gerçekleştirilecek tur sayısı, kullanılan gizli anahtarın boyutuna bağlıdır. 128 bit anahtar için 10 tur, 192 bit anahtar için 12 tur ve 256 bit anahtar boyutu için 14 tur gerçekleştirilir.

2.5.2. AES Algoritması Nasıl Çalışır

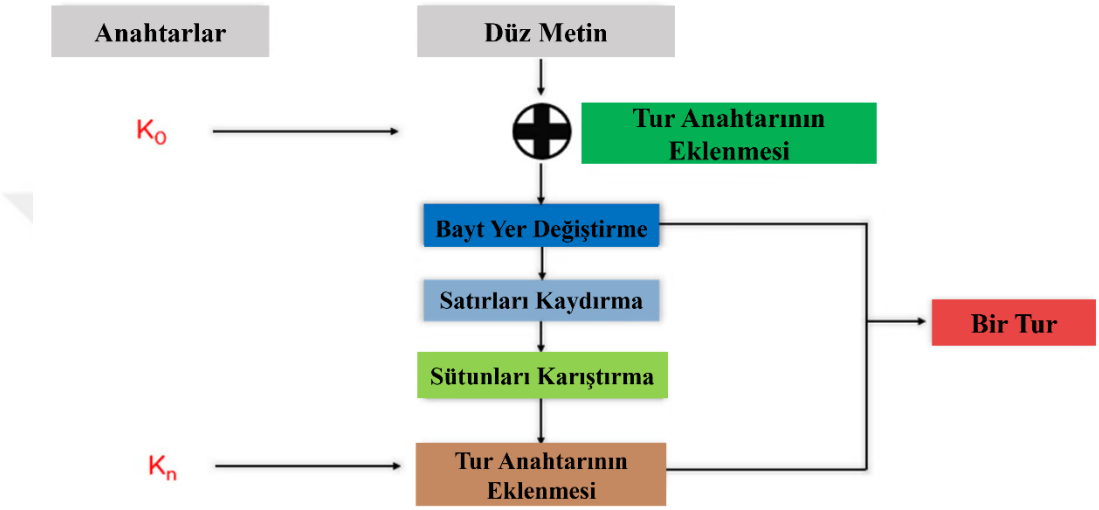
AES algoritmasında şifrelenecek olan veri bir blok halinde alınır ve bir dizi işleme tabi tutulur. AES algoritmasının en önemli çalışma karakteristiğinden birisi de, şifreleme tur sayısıdır. Yani AES tek seferlik bir şifreleme mekanizması değildir. Veriler üzerinde uygulanan işlemler, belirli bir tur sayısı kadar tekrar edilir. Turların her birinde, tura giren veri üzerine AES algoritmasının tüm işlemleri uygulanır.

AES algoritmasının nasıl çalıştığını anlamak için verilerin, AES adımları arasında nasıl aktarıldığını bilmek gerekir. AES blok şifreleme algoritması olduğu için alınan 16 baytlık blok veri 4*x*4'lük bir matriste tutulur. Yani matristeki her bir hücre 1 bayt veri tutar. Şifrelenmesi gereken düz metnin her bir baytı, AES işlemlerinden önce state (durum) adı verilen 4*x*4 bir matrisin hücrelerine aktarılır [48].

Şifrelemede kullanılacak olan anahtar başlangıçta $n + 1$ anahtara genişletilir. Burdaki n, şifreleme işleminde tekrarlanacak tur sayısıdır. 128 bitlik anahtar kullanan AES şifrelemedeki tur sayısı 10'dur. Yani oluşturulacak anahtar sayısı 10 + 1'den 11'dir [49].

2.5.2.1. AES Algoritmasında Takip Edilen İşlemler

Daha öncede bahsedildiği gibi AES şifrelemenin her bir turunda bir dizi işlem veriye uygulanarak, verinin şifrelenmesi sağlanır. Bu işlemler bütününde bir sıra vardır ve her bir sıra, her veri bloğu için takip edilmelidir. Şekil 2.15.'de AES algoritmasındaki her bir tur için gerçekleştirilen işlemler ve sırası verilmiştir.



Şekil 2. 15. AES Şifreleme Adımları

2.5.2.1.1. Tur Anahtarının Eklenmesi

Tur anahtarının eklenmesi işleminde, 4*x*4'lük 16 bayt durum matrisi ile, 4*x*4'lük 16 bayt alt anahtar (subkey), bit düzeyinde XOR işlemine tabi tutulur. Alt anahtar ise, başlangıç anahtarına yapılan anahtar genişleme işlemi ile elde edilir. Şekil 2.16'da, tur anahtarının eklenmesi işlemindeki XOR işlemi verilmiştir.

$$\begin{bmatrix} a00 & a01 & a02 & a03 \\ a10 & a11 & a12 & a13 \\ a20 & a21 & a22 & a23 \\ a30 & a31 & a32 & a33 \end{bmatrix} \oplus \begin{bmatrix} k00 & k01 & k02 & k03 \\ k10 & k11 & k12 & k13 \\ k20 & k21 & k22 & k23 \\ k30 & k31 & k32 & k33 \end{bmatrix} = \begin{bmatrix} a00 \oplus k00 & a01 \oplus k01 & a02 \oplus k02 & a03 \oplus k03 \\ a10 \oplus k10 & a11 \oplus k11 & a12 \oplus k12 & a13 \oplus k13 \\ a20 \oplus k20 & a21 \oplus k21 & a22 \oplus k22 & a23 \oplus k23 \\ a30 \oplus k30 & a31 \oplus k31 & a32 \oplus k32 & a33 \oplus k33 \end{bmatrix}$$

Şekil 2. 16. Tur Anahtarı XOR Dönüşümü

Şekil 2.16.'da verilen XOR dönüşümünde, durum matrisi ile tur anahtarı arasındaki bit seviyesindeki XOR dönüşümü görülmektedir. Durum matrisindeki her bir eleman, kendisine karşılık gelen tur anahtar elemanı ile XOR işlemine sokulmuştur. Bu dönüşüm sonucunda oluşan yeni matris, bir sonraki işleme girdi olarak verilir.

2.5.2.1.2. Bayt Yer Değiştirme

Bayt değiştirme işlemi, AES algoritması işlemlerindeki doğrusal olmayan işlemdir. Bu işlemde AES algoritması, her biri 8 bitlik bir giriş ve 8 bitlik bir çıkış olan 16 eş S kutusu (S-box) kullanır. Bayt değiştirme işleminde her bir bayt, S kutusunda karşılık gelen değer ile yer değiştirir. Şekil 2.17.'de bayt değiştirme işleminin bir temsili verilmiştir.

Şekil 2. 17. Bayt Değiştirme İşlemi

2.5.2.1.3. Satırları Kaydırma

Satır kaydırma işlemi, matrisin her satırının farklı yer değiştirme miktarlarına göre döngüsel olarak kaydırılması işlemidir.

Şekil 2. 18. Satır Kaydırma İşlemi

Şekil 2.18'de satır kaydırma dönüşümünün bir temsili verilmiştir. Şekilde görüldüğü üzere ilk satır için herhangi bir kaydırma işlemi uygulanmamıştır. Matrisin ikinci satırı üç bayt sağa, üçüncü satırı iki bayt sağa ve dördüncü satırı bir bayt sağa kaydırılmıştır. Satır kaydırma işlemi, AES algoritmasının yayılma derecesinin yükselmesini ve doğrudan algoritma güvenliğinin artmasını sağlar.

2.5.2.1.4. Sütunları Karıştırma

Sütun karıştırma dönüşümü, veri matrisinin her bir sütunu için ayrı ayrı dönüşüm gerçekleştirme işlemidir. Yeni bir matris elde etmek için, tüm sütunlar aynı sabit matris ile çarpılır. Sütun karıştırma dönüşümleri, Şekil 2.19.'da verildiği gibi matris çarpım işlemi ile temsil edilebilir.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a00 & a01 & a02 & a03 \\ a10 & a11 & a12 & a13 \\ a20 & a21 & a22 & a23 \\ a30 & a31 & a32 & a33 \end{bmatrix} = \begin{bmatrix} a'00 & a'01 & a'02 & a'03 \\ a'10 & a'11 & a'12 & a'13 \\ a'20 & a'21 & a'22 & a'23 \\ a'30 & a'31 & a'32 & a'33 \end{bmatrix}$$

Şekil 2. 19. Sütun Karıştırma Dönüşümü

3. MATERYAL VE YÖNTEMLER

3.1. Materyal

Projenin uygulama aşamasında kullanılan elektronik kartlar, entegre devre modülleri ve malzemeler bu bölümde anlatılmaktadır. Projenin uygulama çalışmasında mikrodenetleyici modülleri, CAN transceiver modülü gibi aktif bileşenler kullanılmış, direnç gibi pasif bir elemandan yararlanılmış, USB – TTL UART dönüştürücüsü ile de bazı bağlantılar gerçekleştirilmiştir.

3.1.1. Kullanılan Elektronik Malzemeler

Projede öncelikle, şifreleme işleminin yönetileceği mikrodenetleyici modülü seçilmiştir. Mikrodenetleyici modüller arasında sistem güvenliğini arttırmak için farklı haberleşme protokolleri kullanılmıştır. Kullanılan haberleşme protokollerine, uygulanan şifreleme yöntemine ve haberleşme hızlarına göre uyumlu, sistem gereksinimlerini sağlayan sistem elemanları araştırılmış ve seçilmiştir.

3.1.1.1. ESP32-WROOM-32D Mikrodenetleyici Modül

Espressif firması tarafından piyasaya sürülen bu mikrodenetleyici geliştirme kartı, özellikle IoT uygulamaları için tercih edilen, güçlü çift çekirdekli bir işlemciye sahip, sıklıkla kullanılan haberleşme protokolleri için dahili anteni ve blokları bulunan bir mikrodenetleyici modülüdür. Şekil 3.1.'de ESP32-WROOM-32D geliştirme kartının görseli verilmiştir.

Şekil 3. 1. ESP32-WROOM-32D Mikrodenetleyici Geliştirme Kartı

Özellikleri:

Projenin uygulama çalışmasında kullanılan ESP32-WROOM-32D mikrodenetleyici modül, elektrikli araçdaki elektronik kontrol ünitelerini temsil etmek için seçilmiştir. Aşağıda verilen Tablo 3.1.'de, seçilen mikrodenetleyicinin genel özellikleri verilmiştir.

Tablo 3. 1. ESP32-WROOM-32D Genel Özellikleri

Modül	**ESP32-WROOM-32D**
Çekirdek	ESP32-D0WD
SPI Flash	32 Mbits, 3.3 V
Kristal	40 MHz
Anten	Dahili PCB Anten
Boyut (mm)	18 x 25.5 x 3.1

ESP32-WROOM-32D mikrodenetleyici modül, en yaygın kullanılan haberleşme arayüzleri için dahili bloklara sahiptir, bu dahili bloklar sayesinde farklı haberleşme protokollerini bir arada kullanmak için idealdir. Üzerinde bulunan dahili anteni sayesinde, kablosuz haberleşme protokollerini kullanımı için de uygundur. Tablo 3.2.'de desteklenen kablosuz haberleşme protokolleri ve özellikleri verilmiştir.

Tablo 3. 2. ESP32-WROOM-32D Teknik Özellikleri

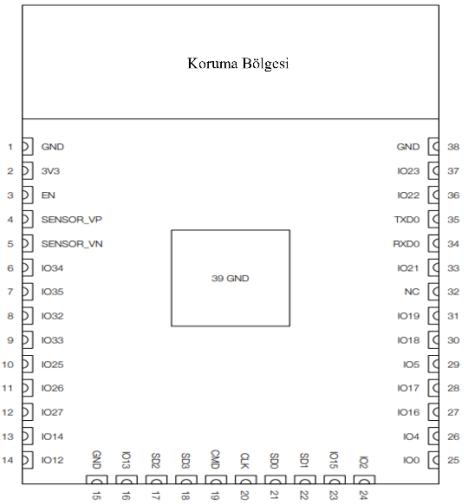
Kategoriler	**Öğe**	**Özellikler**
Sertifikasyon	Wi-Fi	Wi-Fi Alliance
	Bluetooth	BQB
	Green	REACH/RoHS
Test	Güvenilirlik	HTOL/HTSL/uHAST/TCT/ESD
Wi-Fi	Protokol	802.11 b/g/n (802.11n ~ 150 Mbps)
		A-MPDU ve A-MSDU toplama ve 0.4 μs koruma aralığı desteği
	Çalışma Kanalının Merkez Frekans Aralığı	2412 ~ 2484 MHz
Bluetooth	Protokol	Bluetooth v4.2 BR/EDR ve Bluetooth LE özelliği
	Radyo	NZIF -97 dBm hassasiyetli alıcı
		Sınıf-1,2 ve 3 gönderici
		AFH
	Ses (Audio)	CVSD ve SBC

ESP32-WROOM-32D mikrodenetleyici modül, çeşitli donanım arayüzlerine sahiptir. Aşağıda verilen Tablo 3.3.'de ESP32-WROOM-32D'nin sahip olduğu arayüzler ve çalışma gereklilikleri verilmiştir.

Tablo 3. 3. ESP32-WROOM-32D Donanım Özellikleri

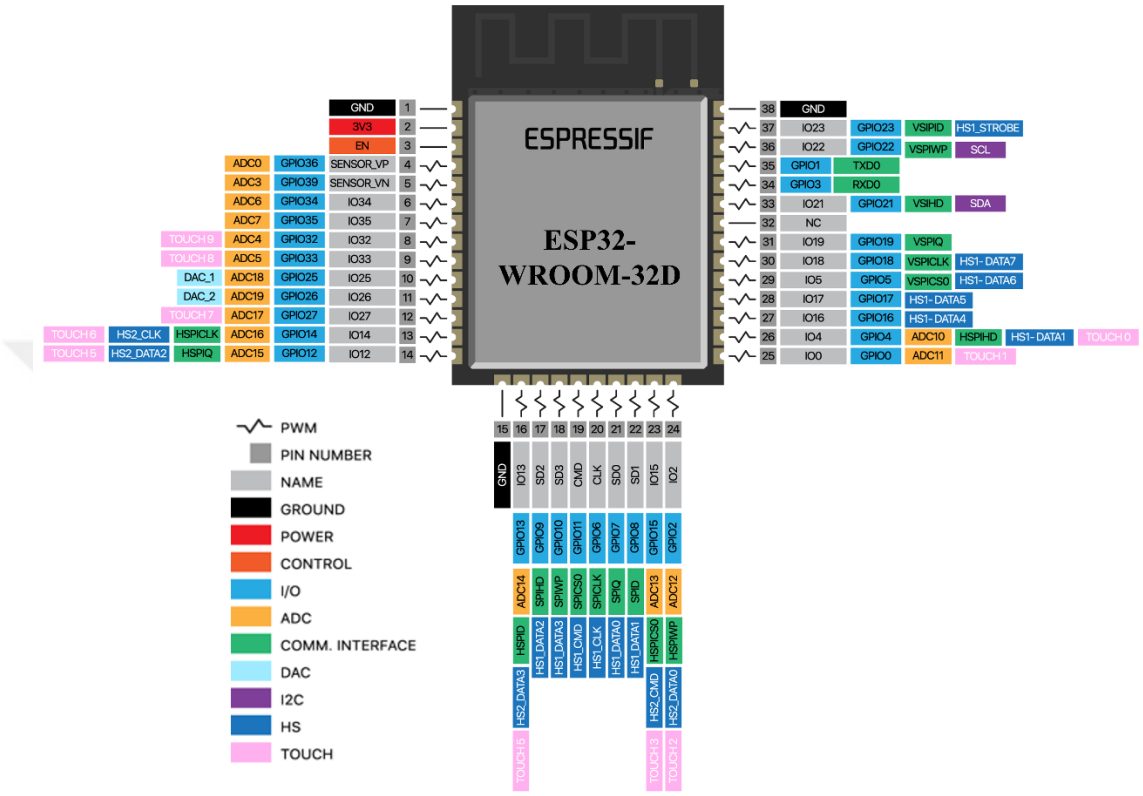
Kategori	Öğe	Özellikler
Donanım	Modül Arayüzleri	SD Kart, UART, SPI, SDIO, I2C, LED PWM, Motor PWM, I2S, IR, Darbe Sayıcı, GPIO, Kapasitif Dokunma Sensörü, ADC, DAC, ISO11898-1 Uyumlu Otomotiv Arayüzleri (CAN 2.0 Şartnamesi)
	Dahili Kristal	40 MHz
	Dahili SPI Flash	4 MB
	Çalışma Gerilimi	3 V ~ 3.6 V
	Çalışma Akımı	Ortalama 80 mA
	Güç Kaynağı Tarafından Sağlanan Minimum Akım	500 mA
	Önerilen Çalışma Ortam Sıcaklık Aralığı	-40 °C ~ +85 °C
	Nem Hassasiyeti Seviyesi	Seviye 3

Aşağıda verilen Şekil 3.2.'de, ESP32-WROOM-32D modülünün üstten bakış pin layout (düzen) bilgisi verilmiştir. Koruma Bölgesi ile belirtilen kısım, dahili antenin bulunduğu bölgeyi temsil etmektedir.



Şekil 3. 2. ESP32-WROOM-32D Pin Düzeni (Üstten Bakış)

Aşağıda verilen Şekil 3.3.'de ESP32-WROOM-32D modülünün pinleri ve pin tanımları verilmiştir. Ayrıca verilen şekilde pinler, özelliklerine göre sınıflandırılmıştır. Hangi pinin, hangi özellik (PWM, ADC, DAC, GPIO, Haberleşme vs.) için kullanılabileceği belirtilmiştir.



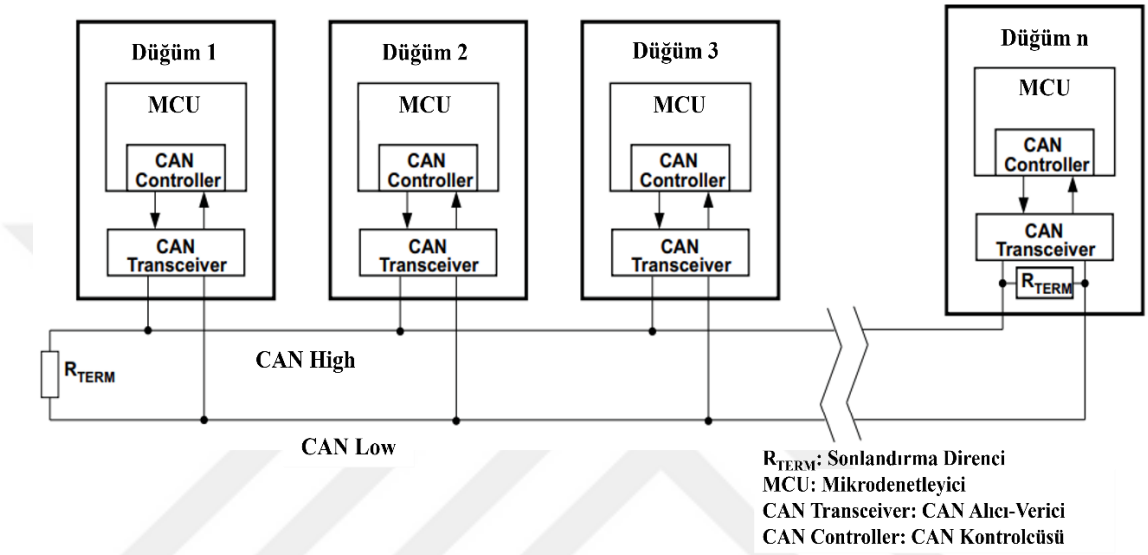
Şekil 3. 3. ESP32-WROOM-32D Pin Tanımları

3.1.1.2. SN65HVD233 CAN Alıcı-Verici (Transceiver) Entegre Devre

SN65HVD233 CAN Alıcı-Verici entegre devresi, Texas Instruments tarafından piyasaya sürülen, CAN haberleşmesinde fiziksel katman olarak kullanılan, CAN kontrolcüsü ile CAN veriyolu arasında 1 Mbps'a kadar veri alışverişi sağlayan entegre devredir.

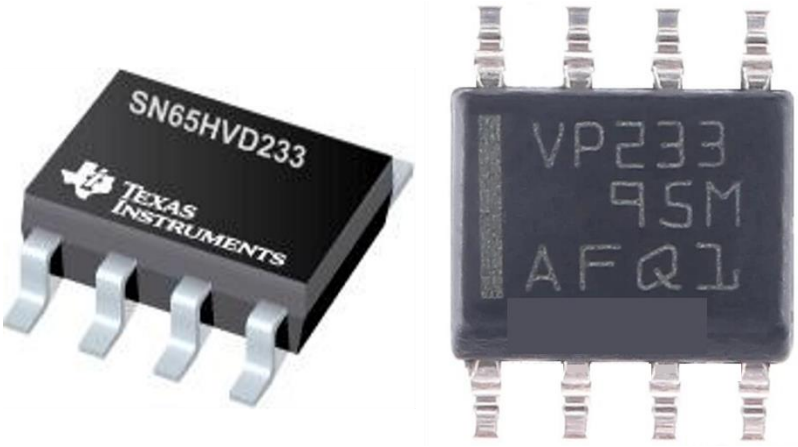
CAN fiziksel katman entegre devreleri, CAN veriyolu uygulamalarında sıklıkla görülmektedirler. Bu devreler, CAN veriyolu sinyalleri ile, CAN kontrolcüsü arasında bir hizalayıcı görevi görmektedirler. Bu devreler, CAN sinyallerini, CAN denetleyicisi için anlamlı ve çözülebilir hale getirirler. Ayrıca, CAN kontrolcüsünün CAN hattına göndereceği verileri, CAN sinyal formuna dönüştürürler.

Aşağıda verilen Şekil 3.4.'de tipik bir CAN veriyolu uygulaması gösterilmiştir. Projenin uygulama çalışmasında kullanılan SN65HVD233 entegre devresi, CAN uygulamasındaki CAN Transceiver (Alıcı-Verici) görevini yerine getirmektedir. Uygulama çalışmasında kullanılan SN65HVD233 entegre devre, ESP32-WROOM-32D mikrodenetleyici ile CAN veriyolu arasında fiziksel katman olarak çalışmaktadır.



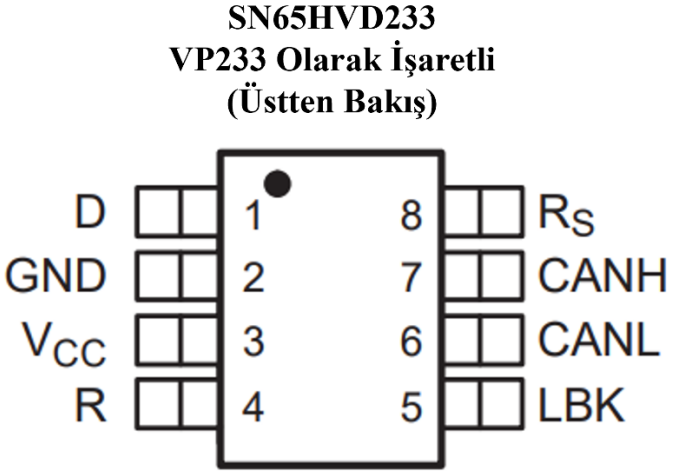
Şekil 3. 4. Tipik Bir CAN Veriyolu Uygulaması

SN65HVD233 CAN fiziksel katman entegre devresi, 4'e 4, 8 bacaklı bir entegre devredir. ISO 11898 standartına göre, CAN seri haberleşme uygulamalarında, fiziksel katman olarak çalışmaktadır. Şekil 3.5.'de temsili görseli ve gerçek hali verilmiştir.



Şekil 3. 5. SN65HVD233 CAN Fiziksel Katman Entegre Devresi

Aşağıda verilen Şekil 3.6.'da, SN65HVD233 entegresinin pinout (pin çıkışları) görseli verilmiştir. Tablo 3.4.'de, entegre pinlerinin fonksiyonları, tipi ve tanımları verilmiştir. Aşağıda verilen resim ve tabloda, entegrenin besleme pinleri (V_{cc} ve GND), CAN veriyolu pinleri (CANH ve CANL), mikrodenetleyiciye giden pinlerinin (D ve R) fonksiyonları açıklanmıştır. Ayrıca entegrenin farklı modlara geçişini kontrol eden 2 adet giriş (Input) pini de (R_s ve LBK) bulunmaktadır. Bu pinler, farklı direnç değerleri ile toprağa (pulldown) veya beslemeye (pullup) bağlanarak, entegrenin farklı modlarda (yüksek hız modu, düşük güç modu, eğim kontrol modu) çalışması sağlanır.



Şekil 3. 6. SN65HVD233 Pin Çıkışları

Tablo 3. 4. SN65HVD233 Pin Tanım Tablosu

PIN		TİP	TANIM
İSİM	NUMARA		
D	1	Giriş	CAN iletim veri girişi (baskın veriyolu durumları için düşük ve çekinik veriyolu durumları için yüksek) aynı zamanda TXD olarak da adlandırılır. (sürücü girişi)
GND	2	Toprak	Toprak bağlantısı
V_{CC}	3	Besleme	3.3 V besleme gerilimi
R	4	Çıkış	CAN alıcı veri çıkışı (baskın veriyolu durumları için düşük ve çekinik veriyolu durumları için yüksek) aynı zamanda RXD olarak da adlandırılır. (alıcı çıkışı)
LBK	5	Giriş	Geri döngü (Loopback) modu giriş pini
CANL	6	Giriş/Çıkış	Düşük seviye CAN veriyolu hattı
CANH	7	Giriş/Çıkış	Yüksek seviye CAN veriyolu hattı
R_S	8	Giriş	Mod seçim pini

Özellikleri:

- Tek 3.3 V besleme gerilimi
- Veriyolu pinleri arıza koruması (±36 V)
- Veriyolu pinleri ESD koruması (±16 kV HBM)
- ISO 11898-2 ile uyumlu
- 1 Mbps'ye kadar veri hızı
- Genişletilmiş -7 V ile 12 V ortak mod aralığı
- Yüksek giriş empedansı, 120 düğüme izin verir
- Düşük akımlı bekleme modu (200 μA) ve termal kapatma koruması
- Sorunsuz veriyolu giriş çıkışlarıyla gücü açma ve kapatma
- Düşük V_{cc} ile yüksek giriş empedansı

Uygulamalar:

- Endüstriyel otomasyon, kontrol, sensörler ve sürücü sistemleri
- Motor ve robotik kontrol
- Bina ve iklim kontrolü (HVAC)
- Backplane (arka panel) haberleşme ve kontrolü
- CANopen, SAE J1939 gibi CAN veriyolu standartları

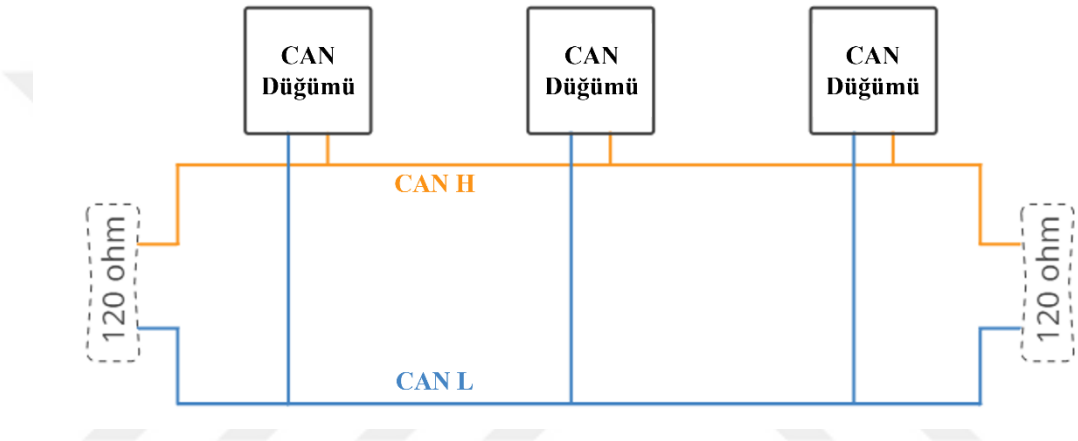
Her entegre gibi, SN65HVD233 CAN entegresininde, kendine ait elektriksel ve sıcaklık karakteristikleri bulunmaktadır. Aşağıda verilen Tablo 3.5.'de, entegrenin ilgili karakteristikleri ve değerleri verilmiştir.

Tablo 3. 5. SN65HVD233 Entegre Çalışma Karakteristikleri

	Minimum	**Maksimum**	**Birim**
V_{cc} besleme gerilimi	-0.3	7	V
CANH veya CANL veriyolu gerilimi	-36	36	V
Gerilim girişi, geçici darbe, CANH ve CANL	-100	100	V
V_i giriş gerilimi , (D, R_s, LBK)	-0.5	7	V
V_o çıkış gerilimi	-0.5	7	V
I_o alıcı çıkış akımı	-10	10	mA
T_j çalışma eklem (junction) sıcaklığı	150		°C
T_{stg} depolama sıcaklığı	125		

3.1.1.3. CAN Veriyolu Sonlandırma Direnci (R_{TERM})

Herhangi bir yüksek hızlı (ISO 11898-2) CAN veriyolunun çalışma yapısı gereği, hattın başı ve sonu, sonlandırma dirençleri kullanılarak sonlandırılır. Genellikle uygulamalarda CAN ağının her iki ucuda 120 Ohm terminal dirençleri kullanılarak sonlandırılır. Aşağıda verilen Şekil 3.7.'de tipik bir CAN veriyolu mimarisi verilmiştir. CAN hattının başı ve sonu, 120 ohm'luk sonlandırma dirençleri ile sonlandırılmıştır.



Şekil 3. 7. Tipik Bir CAN Veriyolu ve Sonlandırma Dirençleri

CAN haberleşme sisteminde, iletişim iki yönlü olduğu için, CAN veriyolu sistemlerinde terminal dirençlerine ihtiyaç duyulur. CAN hattının her iki ucundaki sonlandırma direnci, CAN sinyallerini sönümler ve CAN hattının uçlarında yansıma olmasını engeller. Bu tür yansımalar, sinyal girişimlerine ve potansiyel olarak bozulmuş sinyallere sebep olur.

Yansıma durumu, kablo uzunluğu faktörünün yanı sıra, CAN veriyolu bit hızıyla da artar. Bu yüzden, daha büyük ve karmaşık CAN ağlarına uygun sonlandırma dirençlerini eklemek son derece önemlidir.

Sonlandırma direnç seçiminde ve en az yansıma miktarında, en iyi sonuçları elde etmek için, CAN veriyolu sonlandırma direnci, ISO 11898-2 (yüksek hızlı CAN) için 120 Ohm olarak belirtilen kabloların nominal empedans değerleri ile eşleşmelidir. Bu değer, CAN veriyolu için bir standart olarak kabul edilebilir [50].

3.2. Yöntemler

Bu bölümde, projenin uygulama çalışmasında kullanılan programlar, haberleşme protokolleri, geliştirilen algoritmada kullanılan bazı yöntemlere ilişkin bilgiler ve detaylar verilecektir.

3.2.1. Kullanılan Yazılım Geliştirme Platformu

Projenin yazılım geliştirme aşamasında, birçok elektronik geliştirme kartı ile uyumlu, elektronik projelerde sıklıkla kullanılan haberleşme protokollerine ait sürücü ve kütüphanelere sahip olan Arduino IDE (Integrated Development Environment – Entegre Geliştirme Ortamı) programı kullanılmıştır. İndirmesi ve kurulumu kolay olan bu program, bazı geliştirme kartları için son derece ideal ve kullanışlıdır. Aşağıda verilen Şekil 3.8.'de, Arduino IDE programının ana sayfası ve bölümleri verilmiştir. Resimde anlatılan her bir bölüm, geliştirilen yazılıma ait işlemler, kullanılan geliştirme kartına ait ayarlar ve geliştirme kartı ile ilgili işlemler, genel dosya ayarları gibi farklı işlevlere sahiptir.

Şekil 3. 8. Arduino IDE Program Tanıtımı

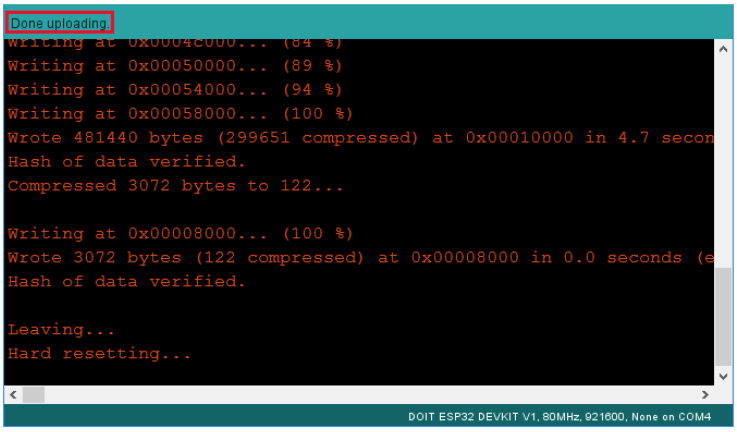
Araç çubuğu bölümünde dosya ayarları, kaydetme, geliştirme kart seçimi, program yükleme hızı seçimi, geliştirme kartı ile ilgili ayarlar, port seçimi, kütüphane yönetimi, geliştirme kartları yönetimi, sürücü ayarları, düzenleme, yardım sekmesi kullanma gibi işlemler yapılabilmektedir.

Hızlı işlem butonları ile, yazılan kodun derlenmesi, kodun geliştirme kartına yüklenmesi, dosya açma, kaydetme ve seri ekranı açma gibi işlemler yapılabilmektedir. Şekil 3.9.'da, hızlı işlem butonlarının detaylı işlevlerini anlatan görsel verilmiştir.

Şekil 3. 9. Arduino IDE Hızlı İşlem Butonları

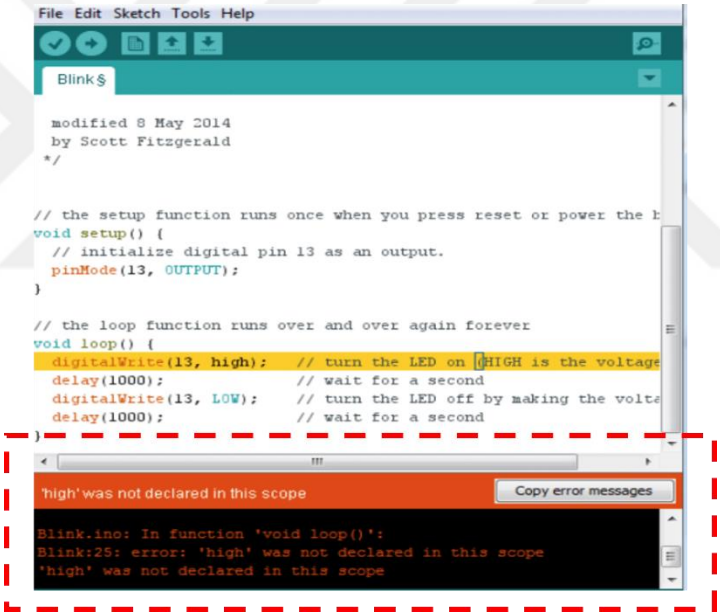
Kod düzenleme bölümü, algoritma ve yazılımın oluşturulduğu bölümdür, bu bölümde ilgili algoritma tasarlanır ve sistemin çalışması için gerekli fonksiyonlar oluşturulur. Kütüphaneler bu bölümde çağrılır, kod blokları bu bölümde yazılır. Yazılım mimarisinin oluşturulduğu ve kodların yazıldığı, programın ana bölümüdür.

Arduino IDE programının durum çubuğunda ise program, güncel kodun derlendiğini ve yüklendiğini belirtir. Eğer yükleme işlemi başarılı bir şekilde gerçekleşirse, ilgili bölümde kullanıcı, yükleme tamamlandı mesajı ile bilgilendirilir. Şekil 3.10.'da, programın durum çubuğu mesajının görseli verilmişir.



Şekil 3. 10. Arduino IDE Durum Çubuğu İşlevi

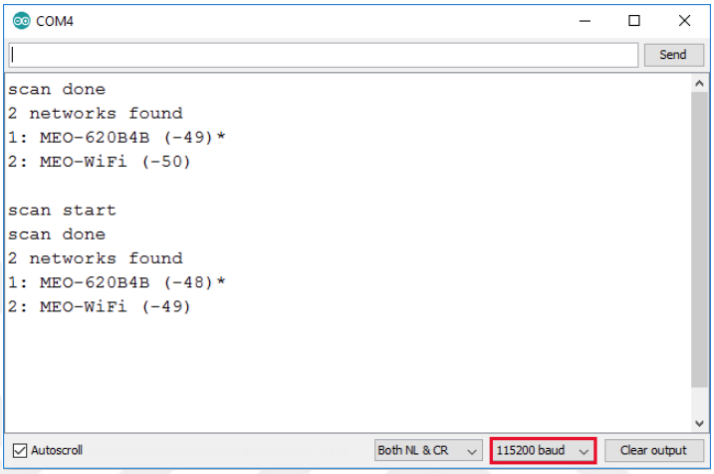
Programın konsol penceresi, geliştirme sürecinde kullanıcının sürekli kullanacağı önemli bir alandır. Kullanıcı kodu derlerken veya yüklerken herhangi bir hata alırsa, ilgili hata bu ekrandan kullanıcıya gösterilecektir. Kodun derlenme işleminde, program hatalı kod bloklarını ve satırlarını tespit edip kullanıcıyı bilgilendirebilir. Programın, geliştirme kartına yüklenmesi işleminde de herhangi bir sorun olursa, yanlış kart seçilmiş ise veya seçili kartın ayarları doğru değilse, program ilgili sorunu bu pencere üzerinden kullanıcıya gösterir. Aşağıda verilen Şekil 3.11.'de, programın derlenme aşamasında meydana gelen bir hatanın, konsol penceresi üzerinden yazılımı geliştiren kullanıcıya gösterildiği görünmektedir. Şekildeki görselde, kod bloğunda yer alan bir değişkenin, ilgili bölümde tanımlı olmadığı ve değişkenin yazılıma bildirilmediği ile ilgili bir hata mesajı görülmektedir.



Şekil 3. 11. Arduino IDE Konsol Penceresi

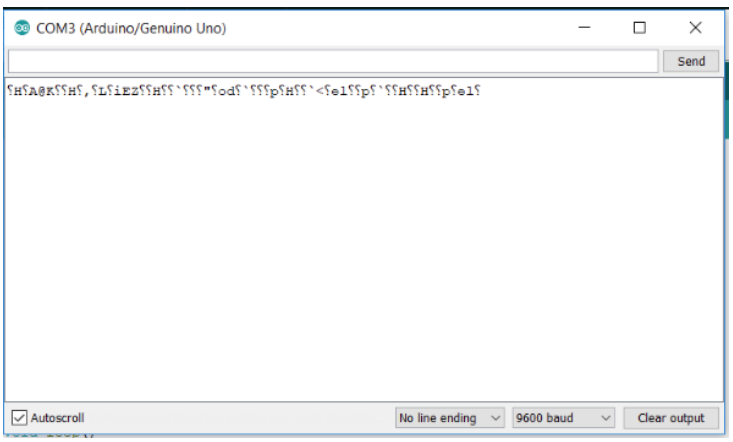
Programdaki diğer önemli bölümlerden birisi de, Şekil 3.9.'da gösterilen seri monitör penceresidir. Yazılımı geliştiren kişi, kodun ürettiği çıktıları bu pencere üzerinden takip edebilir. Bu projede, geliştirilen şifreleme algoritmasının çıktıları bu pencere üzerinden incelenmiş ve doğrulanmıştır. Yazılım geliştiricisi tasarladığı fonksiyonun girdilerini ve çıktılarını bu pencere üzerinden takip ederek, tasarladığı yazılımı doğrulayabilir. Bu pencere ayrıca hata ayıklama (debugging) işlemi içinde kullanılabilir.

Seri monitör penceresi, yazılım geliştirme süreci boyunca hem çıktıları kontrol etme ve doğrulama hem de hata ayıklama işlemleri sırasında sıklıkla kullanıldığı için, Arduino IDE programının önemli bölümlerinden birisidir. Şekil 3.12.'de, herhangi bir program için örnek seri monitör ekranı verilmiştir. Verilen resimdeki kırmızı işaretli bölüm üzerinden, seri ekranın baud rate (bit hızı) seçilebilir.



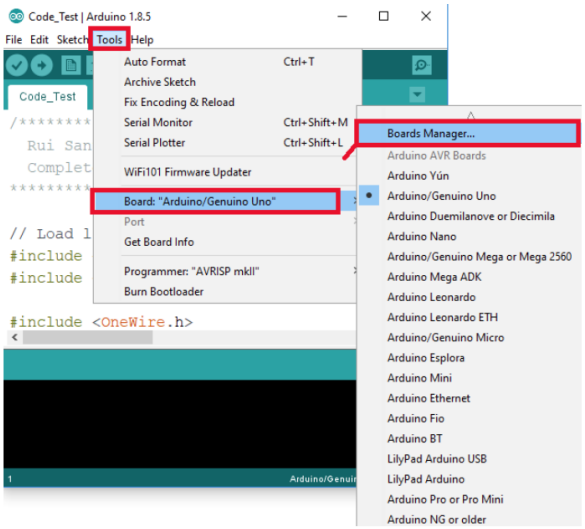
Şekil 3. 12. Arduino IDE Seri Monitör Penceresi

Seri monitör penceresinin doğru çalışması için yapılması gereken önemli bir ayar bulunmaktadır. Yazılımda, seri monitör için tanımlanmış baud rate (bit hızı) ile, pencere üzerinde seçili olan bit hızı eşleşmelidir. Aksi takdirde, görülen çıktılar bozuk ve anlamsız değerler olacaktır. Aşağıda verilen Şekil 3.13.'de, yazılımda tanımlanan seri ekran bit hızı ile seri ekran üzerinden seçilen bit hızının eşleşmemesi sonucu oluşan hatalı durum görülmektedir.



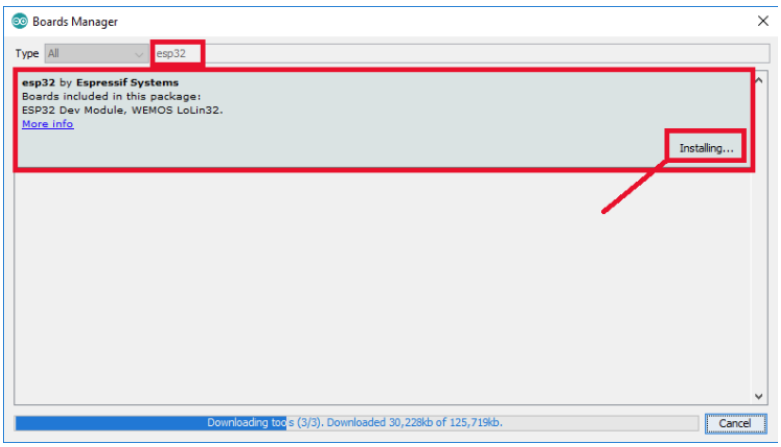
Şekil 3. 13. Yanlış Baud Rate Ayarı Seçilmiş Seri Monitör Penceresi

Projede kullanılan ESP32-WROOM-32D mikrodenetleyicisini, Arduino IDE programında kullanabilmek için bazı sürücü kurulum adımlarının tanımlanması gerekmektedir. Kurulum için gerekli adımlar yapıldıktan sonra, Arduino IDE programı, ESP32-WROOM-32D geliştirme kartını kullanabilmek, yazılım derleyebilmek ve yükleyebilmek için hazır olacaktır. Arduino IDE programının, geliştirme kartı yönetim (Boards Manager) sekmesi üzerinden, ESP32-WROOM-32D geliştirme kartına ait ayarlar ve sürücüler yüklenmelidir. Şekil 3.14.'de, Arduino IDE programında, kart yönetim bölümüne nasıl gidileceği gösterilmektedir.



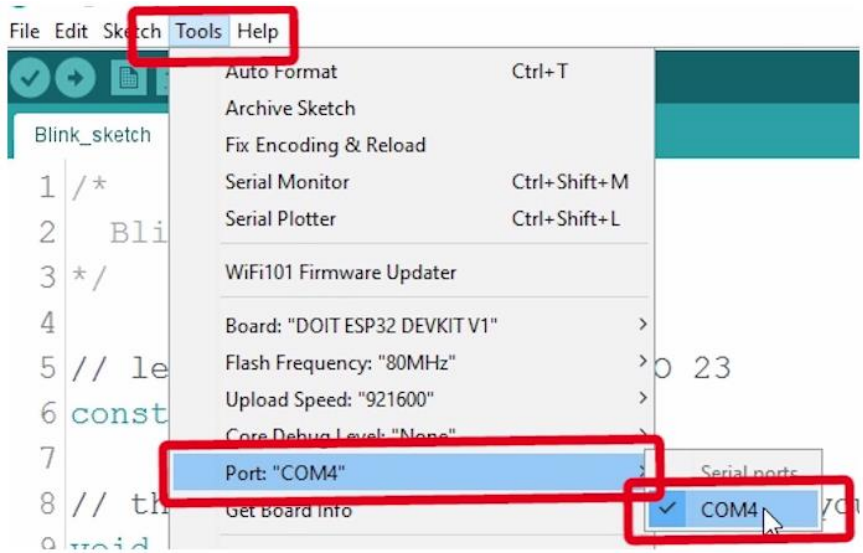
Şekil 3. 14. Arduino IDE Geliştirme Kartı Yönetim Ekranı

ESP32 geliştirme kartlarını, programda kullanabilmek için yüklenmesi gereken paket Şekil 3.15.'deki görselde verilmiştir. Bu paketin kurulum işleminden sonra ESP32 geliştirme kartları, program için tanımlı ve uyumlu olacaktır.



Şekil 3. 15. ESP32 Geliştirme Kartı Kurulum Paketi

ESP32 geliştirme kartına program atabilmek için, geliştirme kartı bilgisayarınıza mikro usb data kablosu ile bağlanmalı ve Arduino IDE programının "Araçlar" / "Tools" sekmesinin, "Port" bölümünde ilgili port seçilmelidir. Aksi takdirde, geliştirme kartına program atılamaz ve program çıktılarını takip etmek için kullanılan seri monitör ekranı kullanılamaz. Şekil 3.16.'da, geliştirme kartı için ilgili portun seçilmesi işlemi gösterilmektedir.



Şekil 3. 16. Geliştirme Kartı İçin İlgili Portun Seçimi

3.2.2. Kullanılan Haberleşme Protokolleri ve İşlemler

Projenin uygulama çalışmasında, elektrikli araçlarda sistem güvenliğinin arttırılması amacıyla, şifreleme ve doğrulama işlemlerini içeren bir haberleşme sistemi tasarlanmıştır. Çalışmanın amacı gereği, verilerin aktarımı için bazı protokoller araştırılmış ve kullanılmıştır. Tasarlanan sistem, şifreli veri aktarımını içeren bir haberleşme sistemidir. Haberleşme protokolü seçiminde projenin uygulama alanı, hedef sektör, sistem gereksinimleri gibi etmenler etkili olmuştur. Seçilen protokollerden birisi, otomotiv alanında bir çok uygulamada kullanılan, sistem gereksinimleri açısından uygun, projenin hedef sektörüne hitap eden bir protokol olmalıdır. Diğer protokol ise, sistem güvenliğini arttırmak amacıyla, ilk protokolden farklı, sistem gereksinimlerini karşılayan, kullanım alanı yaygın bir protokol olmalıdır.

Projenin uygulama alanı otomotiv olduğu için, CAN protokolü ilk akla gelen ve en öne çıkan protokoldür, bu nedenle tasarlanan sistemde kullanılan protokollerden biri CAN veriyolu haberleşme sistemidir. Otomotiv elektroniğinde oldukça yaygın bir kullanım alanına sahiptir. Bir araçtaki neredeyse her elektronik kontrol ünitesinin, aracın CAN ağı ile bir arayüzü vardır. Bu protokole ait detaylar ve özellikler önceki bölümlerde aktarılmıştır.

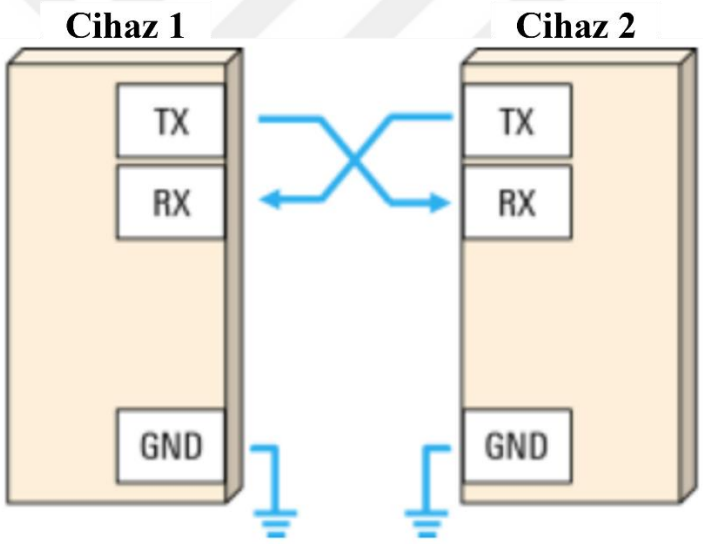
Sistemi, saldırılara karşı daha güçlü hale getirmek için karma bir hibrit sistem uygulanmış ve CAN protokolünün yanında başka bir protokol daha kullanılmıştır. Projenin uygulama çalışmasında CAN protokolünün dışında, oldukça yaygın ve kullanışlı olan UART seri haberleşme protokolü kullanılmıştır. Bu protokole ait detaylar ve özellikler aşağıdaki bölümde aktarılmıştır.

3.2.2.1. UART Haberleşme Protokolü

UART (Universal Asynchronous Receiver Transmitter - Evrensel Asenkron Alıcı Verici) iki cihaz arasında veri alışverişini sağlayan seri bir haberleşme protokolüdür. UART haberleşme mekanizması asenkron olduğu için, haberleşmede herhangi bir clock bilgisine veya sinyaline ihtiyaç duymaz. Herhangi bir clock bilgisine ihtiyaç duymadığı için asenkron haberleşme protokolleri grubunun bir üyesidir. Basit ve robust (sağlam, güvenilir) bir haberleşme protokolüdür, farklı veri bit hızlarında çalışabilir. Kullanım ve uygulama alanı oldukça yaygındır. Neredeyse tüm elektronik sensör, modül, mikrodenetleyici, sürücü cihazlarının UART arayüzü bulunmaktadır.

UART haberleşme protokolü veri taşıma hızı konusunda oldukça esnek bir protokoldür. Veri taşıma hızı oldukça çeşitli değerler ve aralıklarda olabilmektedir. Mevcut uygulamalarda genellikle 4800, 9600, 57600, 115200 ve 921600 baudrate (bit hızı) değerleri kullanılmaktadır. Bu ifade, protokolün saniyede kaç baytlık bilgi taşıyabileceğini gösterir. 9600 bit hızına sahip bir UART protokolü (Byte/saniye = 9600/8 = 1200 bayt) saniyede 1200 byte/s baytlık veri aktarımı sağlayabilir. Daha yüksek hızları destekleyen mikrodenetleyiciler ve sensör modülleri de bulunmaktadır. Bu değerin seçiminde kablo uzunluğu, sistem gereksinimleri, taşınan verinin türü ve önemi gibi kriterler etkili olmaktadır.

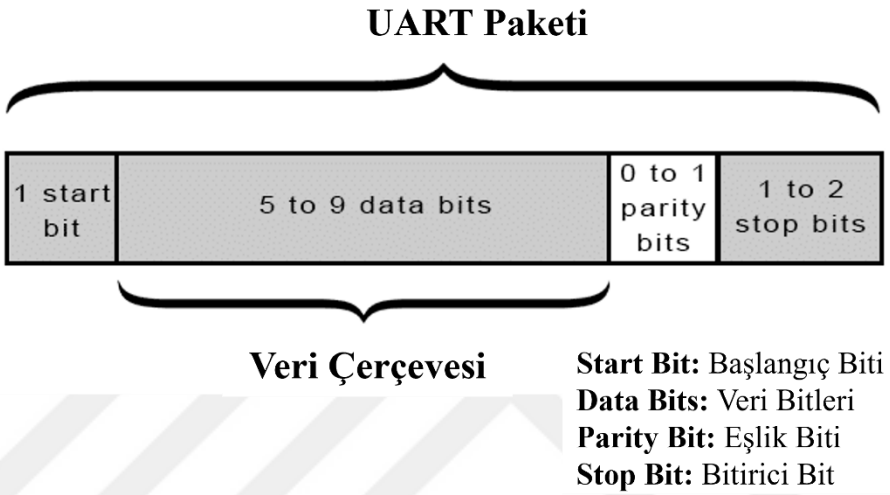
UART haberleşme protokolünün, her haberleşme protokolünün sahip olduğu gibi kendine has bir veri çerçeve yapısı, çalışma sistematiği ve bağlantı gereksinimi vardır. UART protokolünün en büyük avantajlarından birisi, gerektirdiği basit ve az bağlantı gereksinimidir. İki cihaz arasında, UART haberleşme protokolü üzerinden veri alışverişi yapabilmek için 3 adet bağlantının yapılması yeterlidir. Şekil 3.17.'de görüldüğü üzere, UART haberleşmesinde cihazlar arası 3 adet bağlantının yapılması yeterlidir. Cihazlar eşit sinyal lojik seviyeleri için aynı toprağa (GND) bağlanmalıdır. Aksi takdirde, alınan veriler bozuk veya anlamsız okunabilir. Cihaz 1'in TX (transmit - gönderme) pini, karşı cihazın RX (receive - alma) pinine takılmalı, cihaz 2'nin TX pini ise, cihaz 1'in RX pinine takılmalıdır. Cihaz 1'in TX pininden çıkan veriler, karşı cihazın RX pini üzerinden okunur. Aynı şekilde, cihaz 2'nin TX pini üzerinden çıkan veriler, cihaz 1'in RX pini üzerinden okunabilir.



Şekil 3. 17. UART Haberleşme Bağlantısı

UART haberleşme protokolü, veri alışverişi için clock sinyaline ihtiyaç duymaz fakat doğru haberleşme için bazı ön koşulları vardır. 2 farklı cihazın, UART protokolü üzerinden doğru ve uygun bir şekilde haberleşebilmesi için ilk koşul aynı lojik gerilim seviyesine sahip olmaları gerektiğidir. Sinyal referans değerleri farklı değerlerde olursa veri iletiminde bozukluklar ve kayıplar olabilir. Bu yüzden cihazların toprak bağlantıları birbirleri ile ortaklanmalıdır. İkinci önemli nokta ise, cihazların aynı baudrate (bit hızı) ayarına sahip olmaları gerektiğidir. Doğru haberleşme için iki cihazda aynı bit hızı ayarında olmalıdır.

UART haberleşmesinin de, kendisine ait bir paket yapısı ve veri çerçevesi bulunmaktadır. Haberleşmenin sistematiğini veri paketi ve veri paketinin bölümleri belirler. Bu sayede ne zaman yeni bir veri paketinin geldiğini, veri paketindeki hangi değerlerin okunması gerektiğini, veri paketinin sonlanıp sonlanmadığını, gerekli kontrol bitlerinin nasıl kontrol edilmesi gerektiğini alıcı cihaz bilir ve anlar. Bir UART paketi, başlangıç biti, veri bitleri, eşlik biti ve bitirici bit bölümlerinden oluşur. Şekil 3.18.'de, örnek bir UART veri paketinin yapısı verilmiştir.



Şekil 3. 18. UART Veri Paketi

Başlangıç Biti: UART veri iletim TX hattı, normalde veri iletiminin olmadığı zamanlarda yüksek voltaj seviyesindedir. Veri aktarımını başlatmak için gönderim yapan UART cihazı, TX iletim hattını yüksek lojik seviyeden düşük lojik seviyeye çeker. Alıcı UART cihazı, yüksek lojik seviyeden düşük lojik seviyeye olan geçişi algıladığında, UART iletiminin başladığını anlar ve gelen paketin veri çerçevesindeki bitleri, bit hızının frekansında okur.

Veri Çerçevesi: Bu bölüm, iletilmekte olan gerçek verileri içerir. Eğer pakette eşlik biti kullanılıyor ise veri çerçevesi 5 bitten 8 bit uzunluğa kadar olabilir. Eğer veri paketinde eşlik biti yoksa, veri çerçevesi uzunluğu 9 bite kadar olabilir. Çoğu durumda veriler, en az anlamlı bit önceliğinde gönderilir.

Eşlik Biti: Eşlik biti, haberleşme sırasında herhangi bir verinin değişip değişmediğinin kontrolünün yoludur. Haberleşme esnasında bitler, elektromanyetik yayılım, uygun olamayan bit hızı ayarı veya uzun mesafeli veri aktarımları ile değişebilir ve bozulabilir. Alıcı UART cihazı, gelen veri çerçevesini okuduktan sonra, 1 değerlikli bit sayısını sayar ve toplamının çift mi yoksa tek mi olduğunu kontrol eder. Eğer eşlik biti 0 (çift) ise, gelen veri paketindeki 1 değerlikli bitlerin toplamı çift sayı olmalıdır. Eğer eşlik biti 1 (tek) ise, gelen veri paketindeki 1 değerlikli bitlerin toplamı tek sayı olmalıdır. Eşlik biti ile toplamlar eşleştiğinde, UART iletimin hatasız olduğunu anlar. Fakat, eşlik biti ile toplam eşleşmediğinde, UART gelen verinin değiştiğini veya bozulduğunu anlar.

Bitirici Bit: Bu bit veri paketinin sonunun geldiğini bildirmek için kullanılır. UART, TX veri iletim hattını en az iki bitlik süre boyunca düşük lojik seviyeden, yüksek lojik seviyeye geçirir.

Aşağıda verilen Şekil 3.19.'da değerlikleri dolu olan örnek bir UART veri iletim paketi verilmiştir. Resimden görüldüğü üzere, yüksek lojik seviyeden düşük lojik seviyeye geçen başlangıç biti ile veri iletimi başlar. Sonrasında gelen bitler, bilginin taşındığı veri bitleridir. Veri bitlerinden sonra, eşlik biti gelir. Eşlik bitinin değerine göre UART verilerinin değişikliğe veya bozulmaya uğrayıp uğramadığı anlaşılır. Veri paketindeki 1 değerlikli bitlerin toplamı çift ise (verilen örnekte 4 adet 1 değerlikli bit vardır, yani toplam çift değerdir), eşlik biti 0 olmalıdır. Resimde verilen örnekte eşlik biti 0 değerliklidir. 1 değerlikli bit toplamı ve eşlik bitinin değeri eşleşmektedir. Bu sayede UART iletimin doğru gerçekleştiğini anlar. Eşlik bitinden sonra veri paketinin sonlandığını gösteren, yüksek lojik seviyede bitirici bit bulunur.

Şekil 3. 19. Örnek Bir UART Veri Paketi

3.2.2.2. Özel Veya (XOR) Operatörü

Projenin uygulama çalışmasında geliştirilen şifreleme algoritmasında, AES algoritmasına ek olarak XOR (Exclusive OR – Özel Veya) işlem yöntemi de kullanılmıştır. Düz metinler, AES algoritmasına girmeden önce üretilen bir rastgele sayı ile bitwise (bit düzeyinde) XOR işlemine sokulmuştur. Bu yöntemin kullanılması şifreleme algoritmasının daha güçlü bir sonuç elde etmesini sağlamıştır. Düz verilerin bit düzeyinde herhangi bir rastgele sayı ile özel veya işlemine sokulması sonucunda, özel veya işleminin bir çıktısı olarak şifreli bir sayı elde edilmiştir. Özel veya işlemi yapısı gereği şifreleme ve şifre çözme için oldukça uygun bir operatördür. Çünkü herhangi bir rastgele bir sayı ile özel veya işlemine sokulan bir düz metnin çıktısı, yine aynı rastgele sayı ile özel veya işlemine sokulursa, düz metnin kendisi elde edilir. Aşağıdaki bölümlerde özel veya işleminin detayları verilmiştir.

XOR operatörü, iki operanda (herhangi bir operatör tarafından kullanılan değişkenlerdir) sahip bir mantık işlemidir. Özel veya operatörü, aldığı verileri (bitleri) birbirleriyle karşılıklı olarak bit düzeyinde özel veya işlemine tutar. Genel olarak XOR operatörü, girdileri karşılıklı olarak bit düzeyinde, özel veya işlemi kurallarına göre değerlendiren ve sonuçlandıran özel bir mantık operatörüdür.

Özel veya işlemine iki operand girdiği için dört farklı durum söz konusudur. Aşağıda verilen Tablo 3.6.'da, özel veya işlemi için 4 farklı durum ve sonuçları verilmiştir.

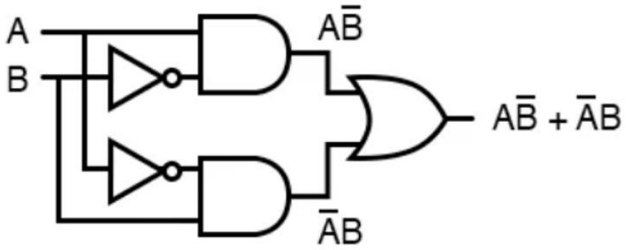
Tablo 3. 6. Özel Veya İşlemi Durumları ve Sonuçları

Operand 1	Operand 2	Sonuç
1	1	0
1	0	1
0	1	1
0	0	0

Tablo 3.6.'dan görüldüğü üzere, özel veya işleminin sonucu sadece her iki operand değeri birbirinden farklıysa 1 değerini alır. Operand değerlerinin aynı olması durumunda sonuç hep sıfır olacaktır.

Özel veya işleminin, diğer mantık kapılarını kullanarak eşleneğini elde etmek mümkündür. AND (ve), OR (veya), NOT (değili) kapı bağlantılarının kullanılması sonucunda, özel veya işlemi ile aynı sonucu veren bir lojik kapı işlemi yapılabilir. Özel veya işleminin dijital elektronikteki mantıksal kapı sembolü ve matematiksel işlem sembolü Şekil 3.20.'de verilmiştir. Ayrıca XOR işlemine karşılık gelen eşdeğer işlem de, AND, OR ve NOT kapıları kullanılarak gösterilmiştir.

Karşılık gelen işlem:

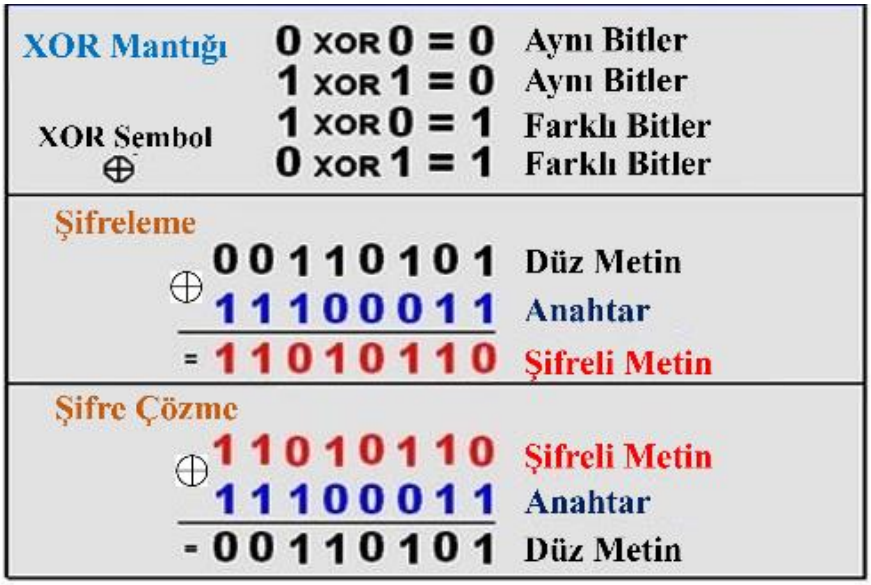


$A \oplus B = A\bar{B} + \bar{A}B$

Şekil 3. 20. XOR Operatörü ve Karşılık Gelen İşlem

XOR operatörü, şifrelemede bit düzeyinde işlem yaparak çalışır. XOR işleminin bit düzeyinde incelenmesi, operatörün şifreleme işlemlerindeki yetkinliğini ve mantığını anlamak için oldukça önemlidir. XOR işleminin şifreleme açısından en önemli özelliklerinden bir tanesi geri dönüşüm özelliğinin olmasıdır. Yani bir sayıyı, başka bir *x* sayısı ile özel veya işlemine soktuktan sonra sonucu yine aynı *x* sayısı ile özel veya işlemine tabi tutarsak, başlangıçtaki sayıyı elde ederiz. Bu özelliğinden dolayı XOR işlemi, şifreleme algoritmalarında sıklıkla kullanılmaktadır. Özellikle diğer şifreleme algoritmaları (AES, DES, vb.) ile birlikte, özel veya işleminin kullanılması, daha güçlü bir şifreleme elde edilmesini sağlar. Özel veya işleminin şifrelemedeki diğer kullanım alanları arasında, rastgele sayılarla birlikte kullanılması uygulamaları vardır. Bir rastgele sayı üretecinden (gerçek veya sözde olabilir) üretilen sayının, özel veya işleminde anahtar olarak kullanılması, yani hem şifrelemede hemde şifre çözme işleminde kullanılması, özel veya işleminin şifreleme algoritmalarındaki yaygın kullanım alanlarından birisidir.

XOR işleminin biz düzeyindeki işlem mantığı, iki sayının her bir bitinin karşılıklı olarak XOR işlemine girmesi temeline dayanmaktadır. Özel veya işlemine girecek her iki operandı, ikilik tabanda (binary form) düşünürsek, her bir bit, kendine karşılık gelen diğer sayının biti ile XOR işlemine tabi tutulur. Şekil 3.21.'de, iki sayının biz düzeyinde işlem mantığı anlatılmıştır. Burdaki ilk sayı, şifrelenmesi gereken düz metindir. İkinci sayı ise şifreleme ve şifreyi çözme işleminde kullanılacak olan anahtardır. Anahtar ile şifrelenen düz metin (plain text) sonucunda şifrelenmiş metin (cipher text) oluşur. XOR işleminin geri dönüşüm özelliği sayesinde, şifreli metin tekrardan anahtar ile özel veya işlemine girerse, düz metin elde edilir. Şekil 3.21.'de XOR işleminin bu özelliği bit düzeyinde anlatılmıştır.



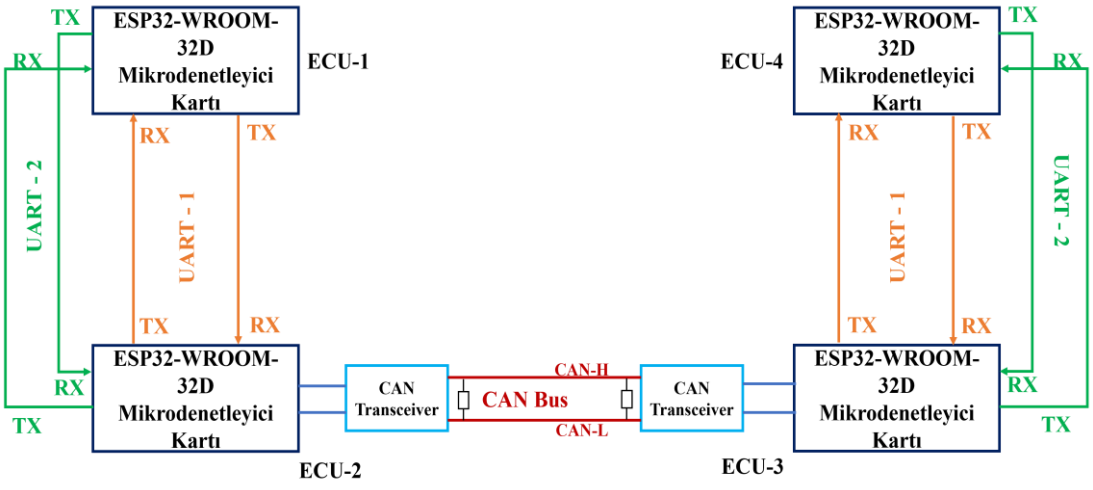
Şekil 3. 21. Bit Düzeyinde XOR İşlemi

4. ARAŞTIRMA BULGULARI VE TARTIŞMA

Araçlarda, elektronik kontrol üniteleri, sensörler, aktüatörler ve ağ geçitleri araç içi ağının elemanlarıdır. Bu elemanlar arasında sürekli olarak bir etkileşim ve haberleşme mevcuttur. Önceki bölümlerde bu elemanlar arası haberleşmenin önemi ve güvenli olması gerektiği detaylarıyla birlikte anlatılmıştır. Bu çalışmada, elektrikli araçların sistem güvenliğini arttırmak amacıyla, siber saldırılara karşı güvenli, şifreleme ve doğrulama mekanizmalarını içeren bir araç içi ağ haberleşme sistemi tasarlanmıştır. Normal bir araç içi ağ sistemini siber saldırılara karşı güvenli kılmak için bu çalışmada şifreli bir haberleşmeye sahip, hibrit bir yapı uygulanmıştır. Çalışmanın, uygulama (deneysel) aşamasında kurulan sistem ve yapı ile ilgili detaylar aşağıdaki bölümlerde anlatılmıştır.

4.1. Deneysel (Uygulama) Çalışması

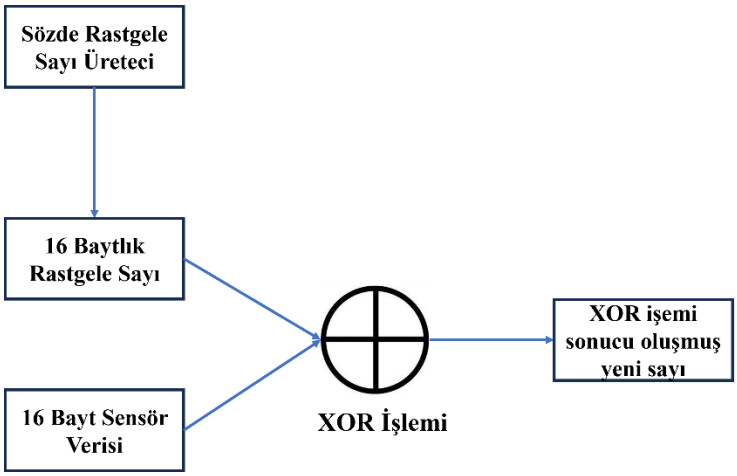
Araç içi haberleşme ağının en önemli elemanları, elektronik kontrol üniteleridir. Sensörlerden gelen verilerin işlenmesi ve yorumlanması ve araç fonksiyonlarının kontrolü elektronik kontrol üniteleri ile gerçekleştirilir. Elektronik kontrol üniteleri arası haberleşmeler önemli ve kritiktir. Bu çalışmada, elektronik kontrol ünitelerinin gerçekleştirdiği fonksiyonlar, mikrodenetleyiciler kullanılarak gerçekleştirilmiştir. Mikrodenetleyiciler arası hibrit bir haberleşme yapısı kurulmuş ve farklı protokoller kullanılmıştır. Şekil 4.1.'de, uygulama çalışmasında tasarlanan ve kurulan sistemin genel blok diyagramı verilmiştir.



Şekil 4. 1. Uygulama Çalışmasının Blok Diyagramı

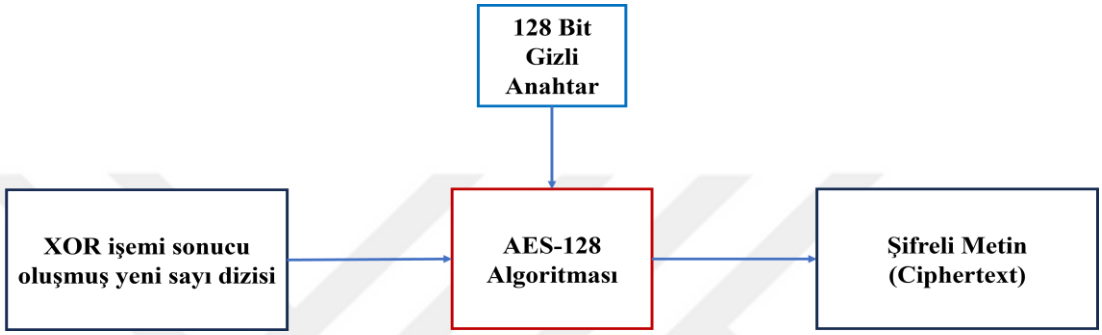
Şekil 4.1.'de görüldüğü üzere, tasarlanan ve uygulanan sistemde 4 adet mikrodenetleyici kullanılmıştır. Mikrodenetleyici olarak ESP32-WROOM-32D geliştirme kartı kullanılmıştır ve tüm mikrodenetleyiciler ortaktır. Sistemin blok diyagramında da verildiği üzere, ECU-1 ve ECU-2 arasında, 2 farklı birbirinden bağımsız UART protokolü kurulmuştur. Her bir UART hattı üzerinden 2 farklı bilgi aktarımı, ECU-1'den, ECU-2'ye yapılmaktadır. İlk mikrodenetleyici yani 1 nolu elektronik kontrol ünitesi, araç ağından aldığı herhangi bir sensör verisini 2 nolu elektronik kontrol ünitesine gönderir. Taşınan veriler kritik olabileceği için bu veriler üzerinde şifreleme işlemi gerçekleştirilmiştir. 1 nolu UART hattı, şifrelenmiş sensör verilerini taşımak için kullanılmıştır. 2 nolu UART hattında ise, sistem açısından kritik öneme sahip, rastgele üretilmiş XOR anahtarı taşınır.

ECU-1 ve ECU-2'nin nasıl bir algoritmaya sahip olduklarını açıklamak gerekirse; ECU 1'in sahip olduğu algoritma, AES şifreleme, sözde rastgele sayı üreteci ve XOR işlemlerini içerir. Şifrelenecek düz metin yani sensör verisi, AES-128 şifreleme algoritmasına girmeden önce, 16 bayt boyutunda üretilmiş bir rastgele sayı ile XOR işlemine sokulur. 16 bayttan oluşan sensör verisinin her bir baytı, 16 bayttan oluşan rastgele sayının karşılık gelen baytı ile özel veya işlemine sokulur. Sensör verisi ve rastgele sayı baytlarının karşılıklı özel veya işlemine sokulması sonucunda, her ikisinden de farklı 16 baytlık başka bir dizi oluşur. Bu dizinin elemanları, sensör verisi ile rastgele sayının özel veya işlem sonuçlarıdır. Şekil 4.2.'de, sensör verisi ile sözde rastgele sayı üretecinden üretilmiş rastgele sayının XOR işlem diyagramı verilmiştir.



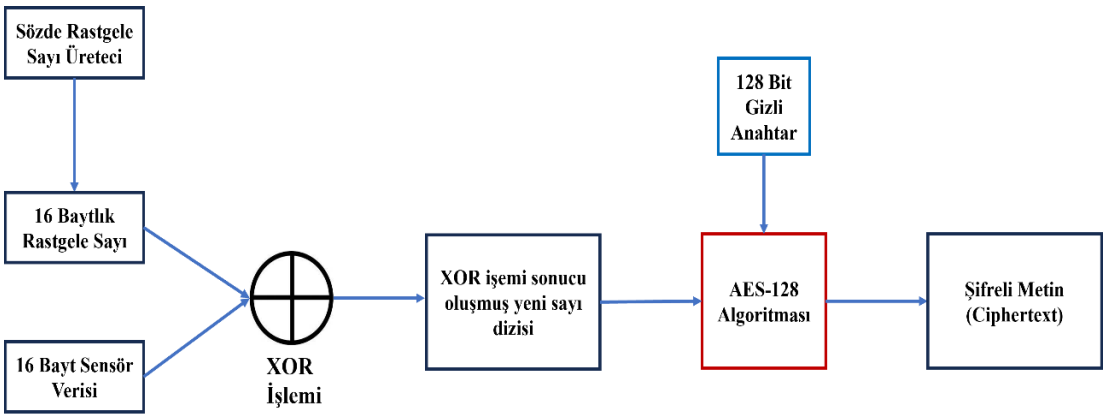
Şekil 4. 2. Sensör Verisi ile Rastgele Sayının XOR İşlemi

ECU-1'in algoritmasındaki diğer önemli bir önemli basamak ise AES şifreleme işlemidir. Sensör verisi ile rastgele sayının XOR işlemi sonucu oluşan 16 baytlık yeni sayı dizisi, AES 128 şifreleme işlemine sokulmuştur. Şifreleme algoritması AES-128 olduğu için, şifreleme işleminde 16 baytlık (128 bit boyutuna sahip) gizli anahtar kullanılmıştır. Şekil 4.3.'de, XOR işlemi sonucu oluşmuş 16 baytlık yeni sayı dizisinin, AES-128 algoritması ve gizli anahtar kullanılarak şifrelenmesi işlemi verilmiştir.



Şekil 4. 3. XOR Sonucu Oluşmuş Sayı Dizisinin AES ile Şifrelenmesi

ECU-1'de genel olarak gerçekleştirilen işlemlere bakıldığında, ilk sırada 16 bayt boyutunda bir rastgele sayı dizisi üretimi gelmektedir. Sonrasındaki önemli işlem ise üretilen bu rastgele sayı dizisi elemanları ile, sensör verisi elemanlarının özel veya işlemidir. Bu işlem sonucunda, 16 bayt boyutunda yeni bir sayı dizisi oluşur. Bir sonraki önemli adım ise, XOR işlemi sonucu oluşan yeni sayı dizisinin, AES şifreleme algoritması ile şifrelenmesidir. Bu işlem sonucunda da, 16 baytlık yeni bir şifreli sayı dizisi (ciphertext) oluşur. Şekil 4.4.'de verilen akış diyagramında, sensör verisinin genel şifrelenme basamakları verilmiştir.

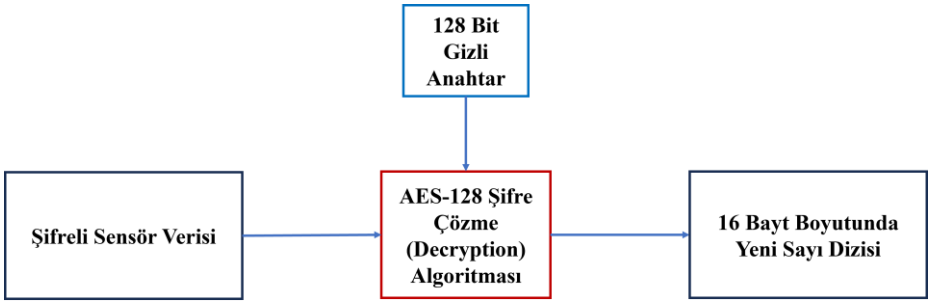


Şekil 4. 4. Sensör Verisinin Genel Şifrelenme İşlemleri

ECU-1'de gerçekleştirilen şifreleme işlemleri sırasında, üretilen rastgele sayı ile AES algoritması sonucu oluşmuş şifreli sensör verisi farklı UART hatları üzerinden, ECU-2'ye gönderilir. Böylece tasarlanan sistemdeki ilk şifreli veri alışverişi gerçekleştirilmiş olur. Farklı UART hatlarının kullanılması sayesinde, 2 yüksek öneme sahip veri, farklı hatlar üzerinden birbirinden bağımsız bir şekilde 2 numaralı ECU'ya gönderilmiştir. Farklı hatların kullanımı sistem güvenliğini arttırır çünkü sadece bir hatta saldıran saldırgan şifreyi kırmak için gerekli tüm bilgilere sahip olamaz. Şekil 4.5.'de, ECU-1 ile ECU-2 arasında bulunan UART hatları ve bu hatlar üzerinden aktarılan bilgiler verilmiştir.

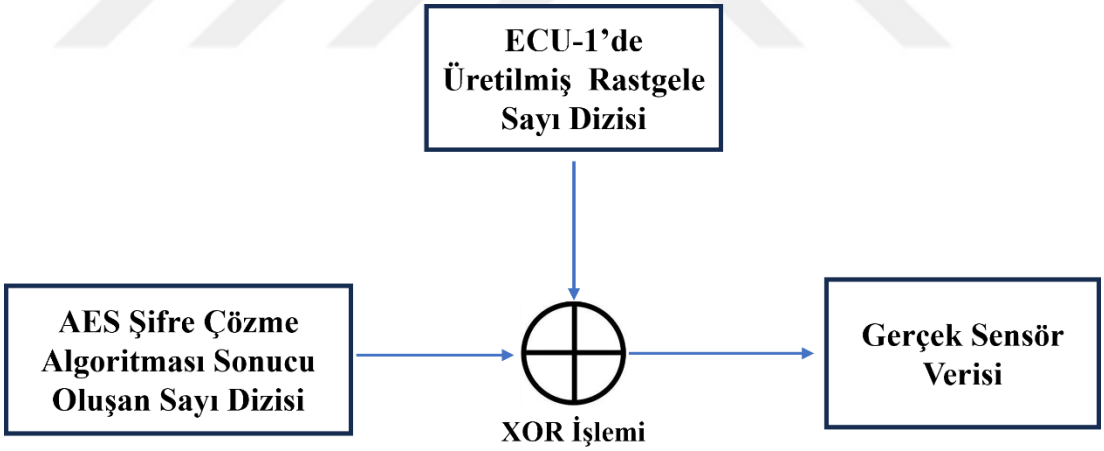
Şekil 4. 5. ECU-1'den ECU-2'ye Gönderilen Bilgiler

ECU-1'den, 2 farklı UART ile gelen şifreli sensör verisi ve ECU-1'de üretilmiş rastgele sayı, ECU-2 tarafından alınır. ECU-2 ilk olarak alınan şifreli sensör verisini, aynı gizli anahtarı ve AES-128 şifre çözme algoritmasını kullanarak çözer. Burdaki önemli nokta, şifrelemede kullanılan gizli anahtar ile, şifreyi çözme işleminde kullanılan gizli anahtarın aynı olmasıdır. Yani ECU-1 ve ECU-2 aynı AES gizli anahtarına sahip olmalıdır, aksi takdirde orjinal sensör verisine ulaşılamaz. Her iki elektronik kontrol ünitesinin kontrol algoritması da, 128 bitlik aynı gizli anahtara sahiptir. Şifreli sensör verisinin şifresi AES algoritması ile çözüldükten sonra, anlamsız bir yeni sayı dizisi elde edilir. Şekil 4.6.'da, ECU-2'de gerçekleştirilen şifre çözme işlem diyagramı verilmiştir.



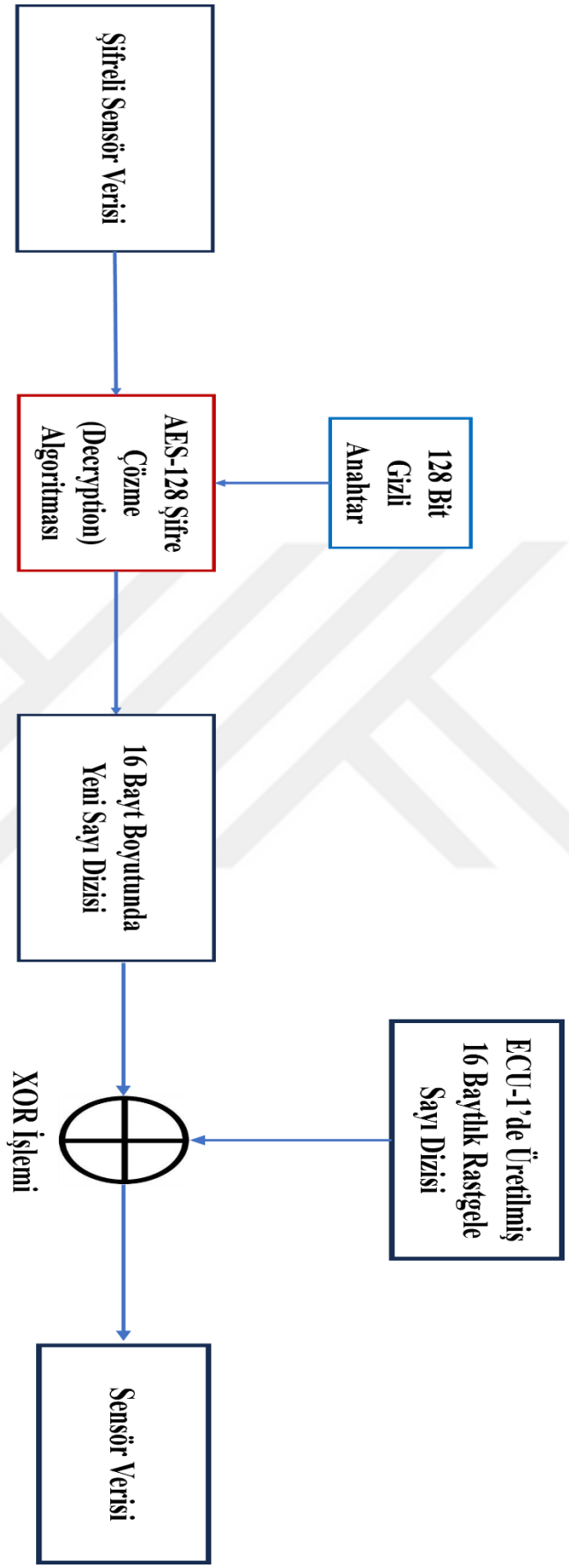
Şekil 4. 6. ECU-2'de Gerçekleştirilen Şifre Çözme İşlemi

ECU-2'de gerçekleştirilen AES şifre çözme işlemi sonucunda, 16 baytlık yeni bir sayı dizisi oluşur. Bu işlem sonucunda oluşan yeni sayı dizisi hala anlamsızdır ve doğru sensör verisi değildir. Çünkü ECU-1 kontrol algoritması içinde şifreleme işlemine giren sayı dizisi doğrudan sensör verisinin kendisi değildi. AES şifreleme işlemine giren sayı dizisi, sensör verisi ile rastgele sayı dizisinin özel veya işlemine girmesi sonucu oluşmuş sayı dizisiydi. Sensör verisine ulaşmak için, XOR işleminin geri dönüşüm özelliği kullanılır. Eğer AES şifre çözme algoritması sonucu oluşmuş sayı dizisi ile, ECU-1'de üretilen ve XOR işleminde kullanılan rastgele sayı dizisi tekrardan XOR işlemine sokulursa, sensör verisinin kendisi elde edilir. Bu yüzden, ECU-1 tarafından üretilen rastgele sayı dizisi, ECU-2 ye gönderilmiştir. ECU-2 bu rastgele sayı dizisini kullanarak orjinal sensör verisinin son ve anlamlı durumuna ulaşabilir, aksi takdirde AES şifre çözme algoritması sonucu oluşan veri anlamsızdır ve kullanılamaz. Şekil 4.7.'de, AES şifre çözme işlemi sonucunda oluşan sayı dizisi ile, ECU-1 tarafından üretilen, ECU-1'de gerçekleştirilen XOR işleminde kullanılmış ve sonrasında ECU-2'ye gönderilen aynı rastgele sayı dizisinin XOR işleminin sonucunda oluşmuş gerçek sensör verisinin XOR işlem diyagramı verilmiştir.



Şekil 4. 7. ECU-2 Algoritmasındaki XOR Geri Dönüşüm İşlemi

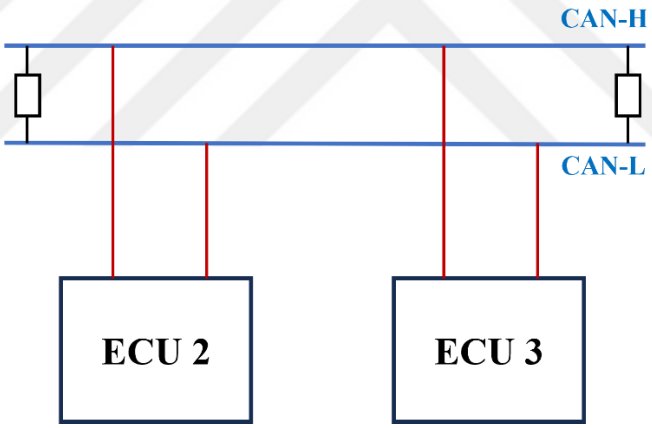
Genel olarak ECU-2'de gerçekleştirilen şifre çözme işlemleri 2 aşamalıdır. İlk aşama, 1. UART hattı üzerinden alınan şifreli sensör verisinin, AES şifre çözme algoritması ile çözülmesidir. 2. aşama, AES şifre çözme işlemi sonucu oluşan sayı dizisi ile ECU-1 tarafından gönderilen rastgele sayı dizisinin XOR işlemidir. Bu işlem sonucunda gerçek sensör verisine ulaşılır. Şekil 4.8.'de, ECU-2 kontrol algoritmasında gerçekleştirilen işlem basamakları verilmiştir.



Şekil 4. 8. ECU-2 Şifre Çözme İşlem Basamak Diyagramı

Tasarlanan sistemde, ECU-2 tarafından alınan şifreli sensör verisi, şifre çözme işlemleri tamamlandıktan sonra, CAN veriyolu üzerinden, 3 numaralı elektronik kontrol ünitesine gönderilmiştir. Tasarlanan sistemde, UART ve CAN gibi farklı haberleşme protokolleri kullanılarak, sistem güvenliğinin arttırılması amaçlanmıştır. Her haberleşme protokolünün sinyal yapısı ve çalışma mekanizması farklıdır, sisteme gerçekleştirilen herhangi bir saldırı durumunda, saldırganın birden fazla haberleşme protokolünü ve çalışma karakteristiğini hesaba katması gerekecektir.

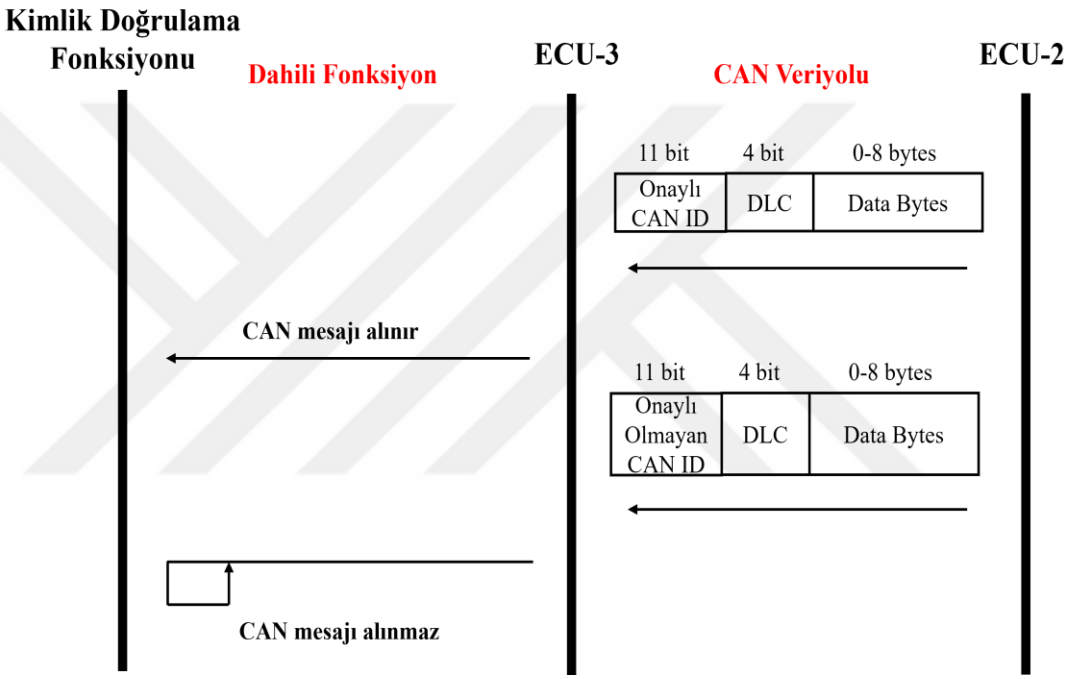
ECU-2 ile ECU-3 arasındaki haberleşme arayüzü CAN veriyoludur. Aldığı şifreli sensör verisini çözen ECU-2, bu veriyi kullandıktan sonra kurgu gereği CAN veriyolu üzerinden ECU-3'e göndermelidir. Şekil 4.9.'da verilen resimde, ECU-2 ve ECU-3'ün, sistemin CAN ağı ile olan bağlantıları görünmektedir. ECU 2'den, ECU-3'e düzenli bir şekilde veri aktarımı mevcuttur.



Şekil 4. 9. ECU-2 ile ECU-3 Arasındaki CAN Arayüzü

Tasarlanan ve gerçekleştirilen sistemde, ECU-2 ile ECU-3 arasındaki haberleşme ve sistem güvenliğini arttırmak için bir doğrulama mekanizması kurulmuştur. Geliştirilen bu sistemde, ECU-3'ün kontrol algoritması, bir ID kontrol fonksiyonuna sahiptir. ECU-3'ün kontrol yazılımında, onaylı CAN ID listesi şeklinde bir dizi bulunur. ECU-3, bu kimlik listesinin haricinde gelen hiçbir CAN mesajını değerlendirmez ve kullanmaz. Yalnızca, onaylanmış kimlik listesi içinden gelen bir CAN mesaj kimliğini kabul eder ve değerlendirir. Eğer, onaylanmamış bir CAN mesaj kimliği ile birlikte bir CAN mesajı gelirse, bilinmeyen cihaz uyarısı verir, gelen CAN mesajını görmezden gelir ve kullanmaz.

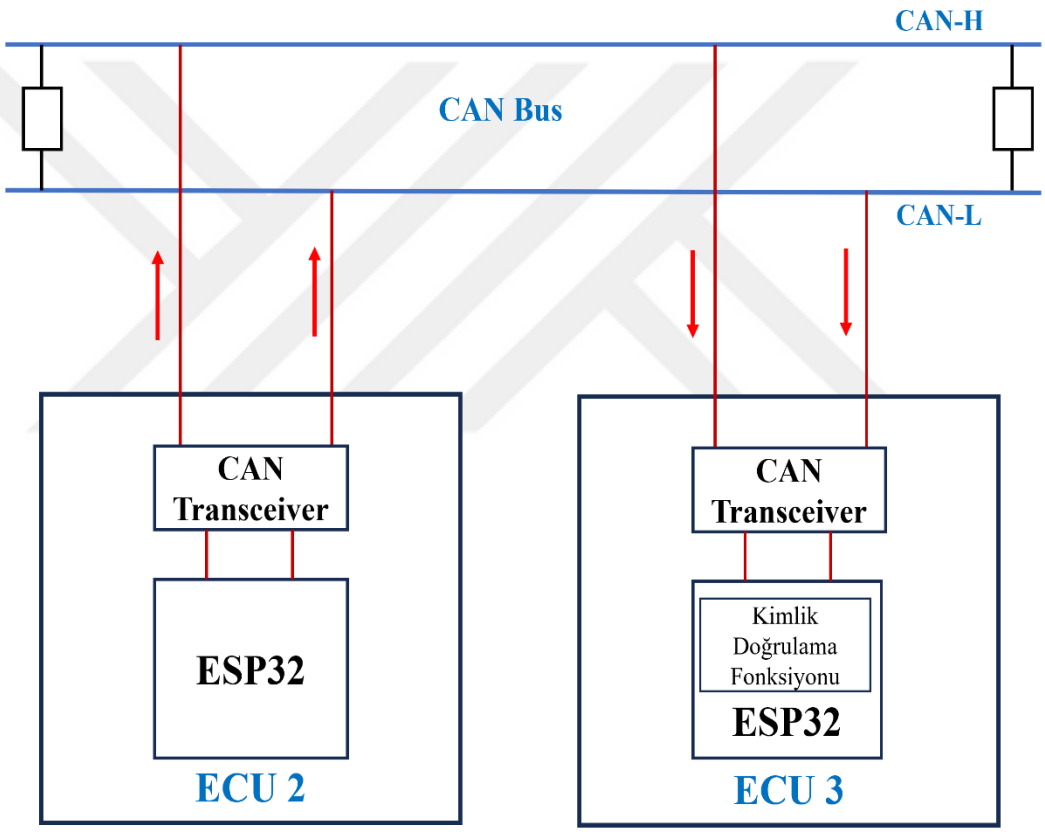
ECU-3'ün sahip olduğu kimlik doğrulama fonksiyonu tek yönlü çalışır ve doğrulama konusunda herhangi bir geri bildirim vermez. CAN veriyolu, ECU'ların yaptıkları yayınların alınması veya alınmaması esasına dayanır. CAN veriyolunun bu durumunun yapısı gereği, kimlik doğrulama fonksiyonu böyle olmalıdır. Onaylı CAN mesaj kimliği ile gelen mesajlar değerlendirilir, aksi durumdaki onaylı CAN mesaj kimliğine sahip olmayan diğer mesajlar görmezden gelinir ve değerlendirilmez. Şekil 4.10.'da, ECU-3 kimlik doğrulama fonksiyonunun farklı CAN mesajlarına göre akış şeması verilmiştir.



Şekil 4. 10. ECU-3 Kimlik Doğrulama Akış Şeması

CAN veri yolu yapısı gereği, kaba kuvvet (brute force), tekrar (replay) gibi bazı saldırılara karşı savunmasızdır. Özellikle araçların public (genel) CAN hatları için daha güçlü önlemler almak gerekir çünkü bu hatlar dışarıdan kolaylıkla ulaşılabilecek ve dinlenebilecek hatlardır. Kritik ve önemli bilgiler private (özel&gizli) CAN hatları üzerinden taşınmalıdır. Tasarlanan sistemde kurulan CAN hattı, gizli CAN ağını temsil eder. Araçlarda kullanılan çoğu elektronik kontrol ünitesinin genel CAN hatları ile de bağlantısı vardır. Kontrol yazılımlarında bu mesaj kimliklerini de barındırır. Genel CAN ağı üzerindeki bir mesaj kimliğinin, özel CAN ağına girişim sorununu engellemek için, ECU'ların doğrulanmış CAN kimliklerini bilmesi ve sadece onları değerlendirmesi sistem güvenliği açısından faydalı olur [51].

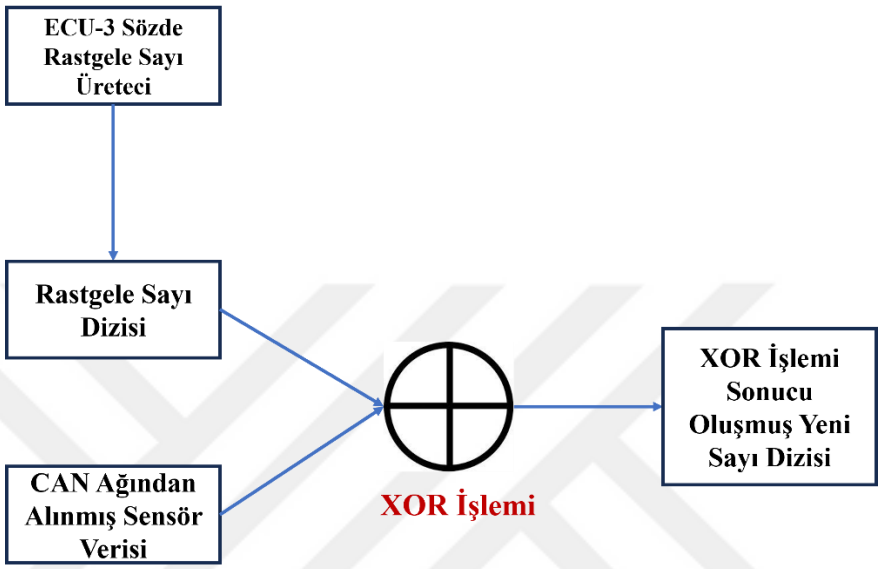
ECU-3'ün içindeki kontrol yazılımına kimlik doğrulama (authentication) fonksiyonunun eklenmesi ile sistem güvenliği seviyesinde bir artış gerçekleşmiştir. ECU-3, kendi onaylı kimlik listesi dışındaki hiçbir mesajı almayarak, yabancı mesajlara karşı kendini korur. Onaylı olmayan mesaj kimliğine sahip mesajlara karşı bir uyarı mesajı üretir. Şekil 4.11'de, ECU-2 ve ECU-3 arasındaki etkileşim gösterilmiştir. Ayrıca ESP32 geliştirme kartı ve CAN transceiver modülleri kullanılarak kurulan sistemin diyagramı da verilmiştir. Verilen diyagramda, ECU-3'ün kontrol yazılımının, kimlik doğrulama fonksiyonuna sahip olduğu da vurgulanmıştır.



Şekil 4. 11. Uygulama Çalışmasında Kurulan ECU-2 ve ECU-3 Temsili

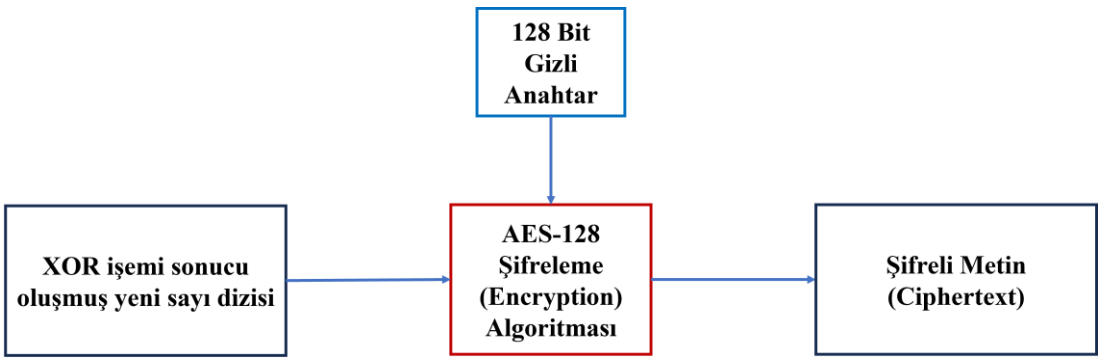
Onaylanmış kimliklerden sensör verisini alan ECU-3, bu veriyi tasarlanan sistemin son alıcısı olan ECU-4'e gönderir. CAN ağından alınan sensör verisi, ECU-4'e gönderilmeden önce şifrelenmelidir. Tekrar şifrelemedeki amaç, sistemin güvenlik düzeyini arttırmaktır. Projenin uygulama çalışmasında gerçekleştirilen tekrar şifreleme işlemleri ve farklı protokollerin kullanılması ile hibrit bir yapının oluşturulması ve sistem güvenliğinin arttırılması amaçlanmıştır.

ECU-3'ün kontrol yazılımında, rastgele sayı üretimi, XOR işlemi ve AES şifreleme algoritması bulunur. CAN ağı üzerinden alınan sensör verisi, ECU-4'e gönderilmeden önce, ECU-3 tarafından üretilen rastgele sayı ile XOR işlemine tutulur. Şekil 4.12.'de, ECU-3'ün kontrol algoritmasında bulunan, sensör verisi ile üretilen rastgele sayının özel veya işleminin diyagramı verilmiştir.



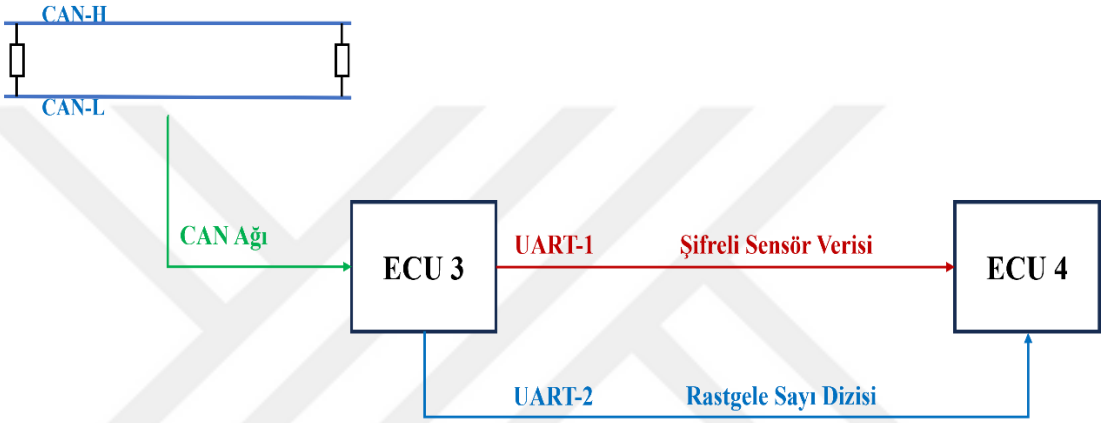
Şekil 4. 12. ECU-3 Tarafından Gerçekleştirilen XOR İşlemi

ECU-3 tarafından gerçekleştirilen XOR işlemi sonrasında oluşan yeni sayı dizisi, ECU-4'e gönderilmeden önce AES şifreleme algoritması ile şifrelenir. Şifreleme işlemi tamamlandıktan sonra oluşan yeni şifreli metin, UART protokolü üzerinden 4 numaralı elektronik kontrol ünitesine gönderilir. Şekil 4.13.'de, ECU-3 kontrol yazılımında gerçekleştirilen AES şifreleme işlem diyagramı verilmiştir. Şifreleme sonucu oluşmuş şifreli sensör verisi, ECU-4'e gönderilmek için hazırdır.



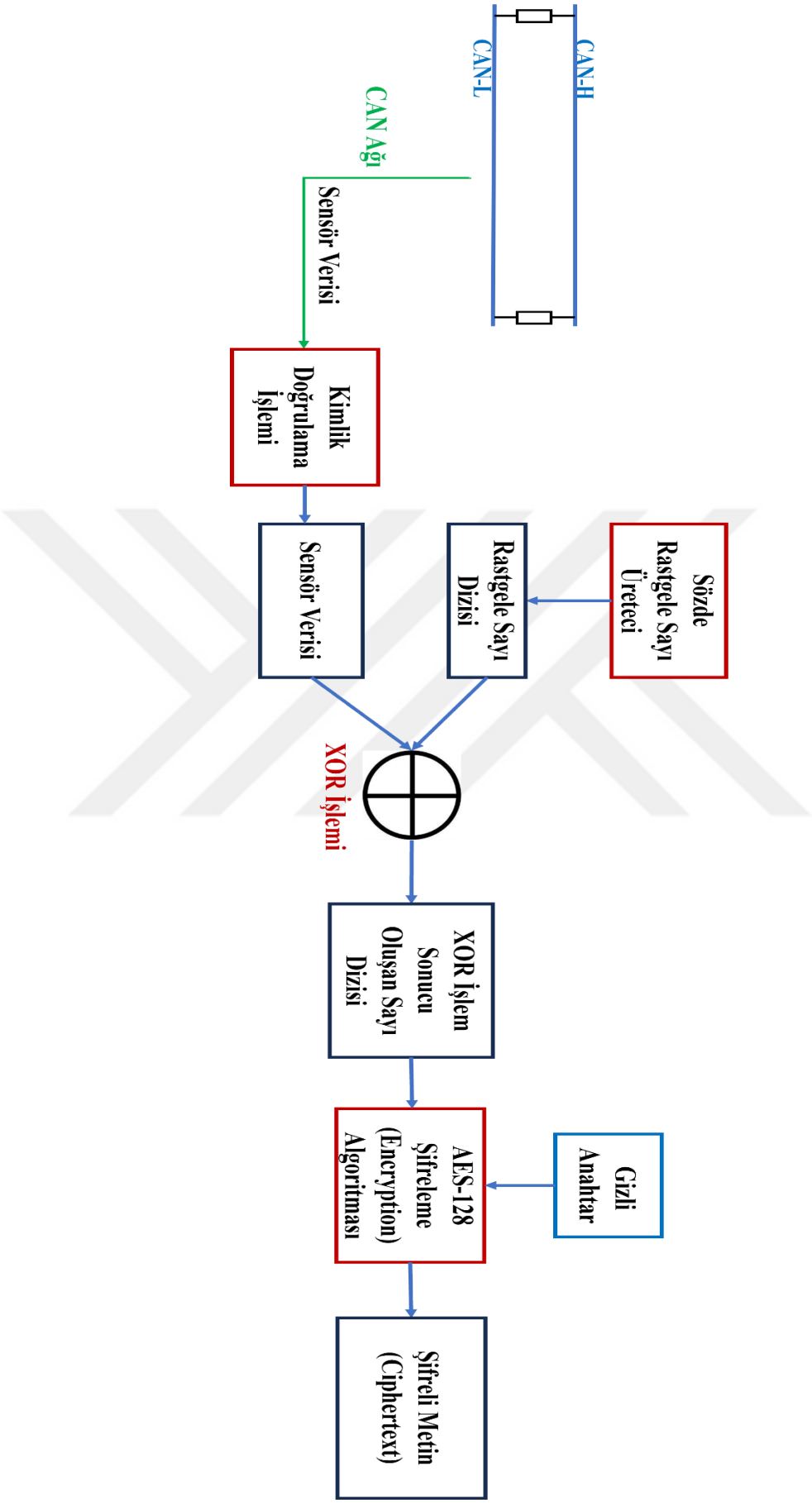
Şekil 4. 13. ECU-3 Tarafından Gerçekleştirilen AES Şifreleme İşlemi

ECU-3 kontrol yazılımında şifreleme işlemleri sırasında bazı bilgiler, ECU-4'e gönderilir. ECU-3 tarafından üretilmiş rastgele sayı, sonrasında ECU-4 tarafından kullanılacağı için, ECU-4'e gönderilir. ECU-3 ile ECU-4 arasında 2 farklı UART hattı bulunur. Bir UART hattında, şifreli sensör verisi taşınırken, diğer UART hattında, ECU-3 tarafından üretilmiş rastgele sayı taşınır. İki önemli bilginin, farklı UART hatları üzerinde taşınması ile sistem güvenliğinin arttırılması amaçlanmıştır. Şekil 4.14.'de, ECU-3 ile ECU-4 arasında bulunan UART hatları ve taşınan veri içerikleri gösterilmiştir.



Şekil 4. 14. ECU-3 ile ECU-4 Arasında Bulunan UART Hatları

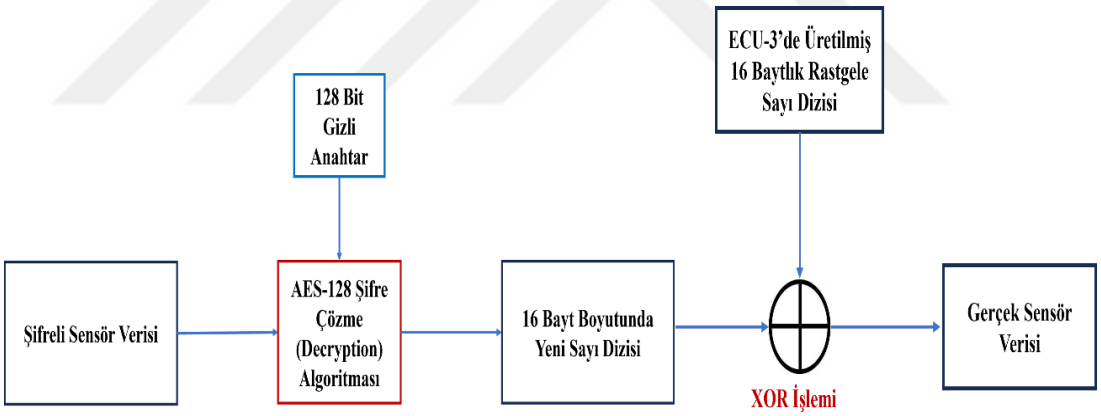
ECU-3 kontrol algoritmasını ve gerçekleştirilen işlemleri özetlemek gerekirse; ilk aşama, tasarlanan sistemin CAN ağından sensör verisinin alınmasıdır. CAN veriyolu üzerinden alınan veriler esnasında kimlik doğrulama işlemi gerçekleştirilir. Onaylı kimlik listesinde olmayan CAN kimliklerine ait mesajlar değerlendirilmez ve kullanılmaz. İkinci aşama ise, alınan sensör verisinin, üretilen rastgele sayı dizisi ile özel veya işlemine tabi tutulmasıdır. Bu işlem ile birlikte üretilen rastgele sayı, ECU-4 kontrol algoritmasında da kullanılmak üzere, ECU-4'e gönderilir. Üçüncü aşama olarak AES şifreleme işlemi verilebilir. XOR işlemi sonucu oluşmuş sayı dizisi, AES algoritması ile şifrelenir ve şifreli sensör verisine dönüştürülür. Şifreleme işlemi sonrasında, şifreli metin UART protokolü üzerinden 4 numaralı elektronik kontrol ünitesine gönderilir. ECU-3, tasarlanan sistem için önemli bir elemandır, hem CAN ağı ile, hem de UART hatları ile bağlantısı ve veri iletişimi bulunmaktadır. Şekil 4.15.'de, ECU-3 kontrol yazılımında gerçekleştirilen işlemler, bir bütün halinde verilmiştir.



Şekil 4. 15. ECU-3 Kontrol Algoritmasında Gerçekleştirilen İşlemler Bütünü

Projenin uygulama çalışmasında, sisteme entegre edilmiş son elektronik kontrol ünitesi ECU-4'tür. ECU-1'in sisteme göndermiş olduğu sensör verisi, en son ECU-4 tarafından alınır. Önceki bölümlerde anlatıldığı üzere, ECU-3'ün CAN ağından alıp şifrelediği sensör verisi, UART protokolü üzerinden, ECU-4'e gönderilir. Şifreli sensör verisi ile birlikte, farklı bir UART hattı üzerinden, ECU-3 tarafından üretilmiş rastgele sayı dizisi de, ECU-4 tarafından alınır.

Şifreli sensör verisini ve rastgele sayı dizisini alan ECU-4, ilk önce gelen şifreli sensör verisini, AES şifre çözme algoritması ve ortak gizli anahtarı kullanarak çözer. Bu işlem sonucunda oluşan yeni sayı dizisi hala şifreli durumdadır. Tam anlamıyla gerçek sensör verisine ulaşmak için, AES şifre çözme algoritmasının çıktısı olan sayı dizisi ile, ECU-3 tarafından üretilen rastgele sayı dizisi, XOR işlemine tutulmalıdır. XOR işlemi sonucu oluşan yeni sayı dizisi, sistemde elektronik kontrol üniteleri arasında aktarılan gerçek sensör verisidir. Şekil 4.16.'da, ECU-4 kontrol algoritmasında gerçekleştirilen tüm işlemlerin akış diyagramı verilmiştir.



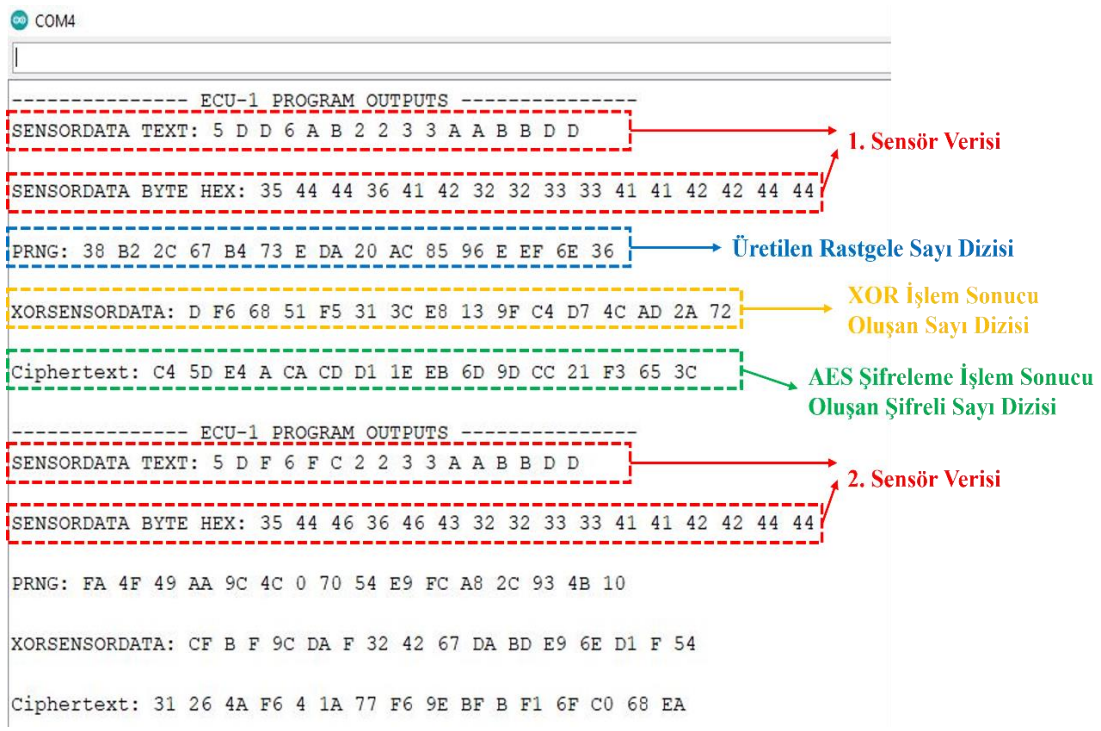
Şekil 4. 16. ECU-4 Kontrol Algoritmasında Gerçekleştirilen İşlemler

Projenin uygulama çalışmasında, tasarlanan sistemde gerçekleştirilen tüm işlemler ECU-1'in sensör verisini şifreleme işlemleri (XOR + AES şifreleme) ile başlar ve ECU-4'ün, nihai sensör verisine ulaşması ile son bulur. Tüm bu süreç boyunca, sistem güvenliğini arttırmak amacıyla, farklı şifreleme teknikleri, kimlik doğrulama kontrol işlemi, farklı haberleşme protokollerinin (UART ve CAN) kullanılması, önemli verilerin (şifreli sensör verisi ve rastgele sayılar) birbirinden ayrı hatlar üzerinden taşınması gibi birçok algoritma, teknik ve işlem, sisteme uygulanmıştır.

4.2. Uygulama Çalışması Çıktıları

Projenin uygulama çalışmasında oluşturulan kontrol ve şifreleme algoritmalarının çıktıları bu bölümde anlatılmıştır. Elektronik kontrol ünitelerini temsil eden mikrodenetleyiciler için yazılmış program çıktıları ayrı ayrı görseller ile gösterilmiştir.

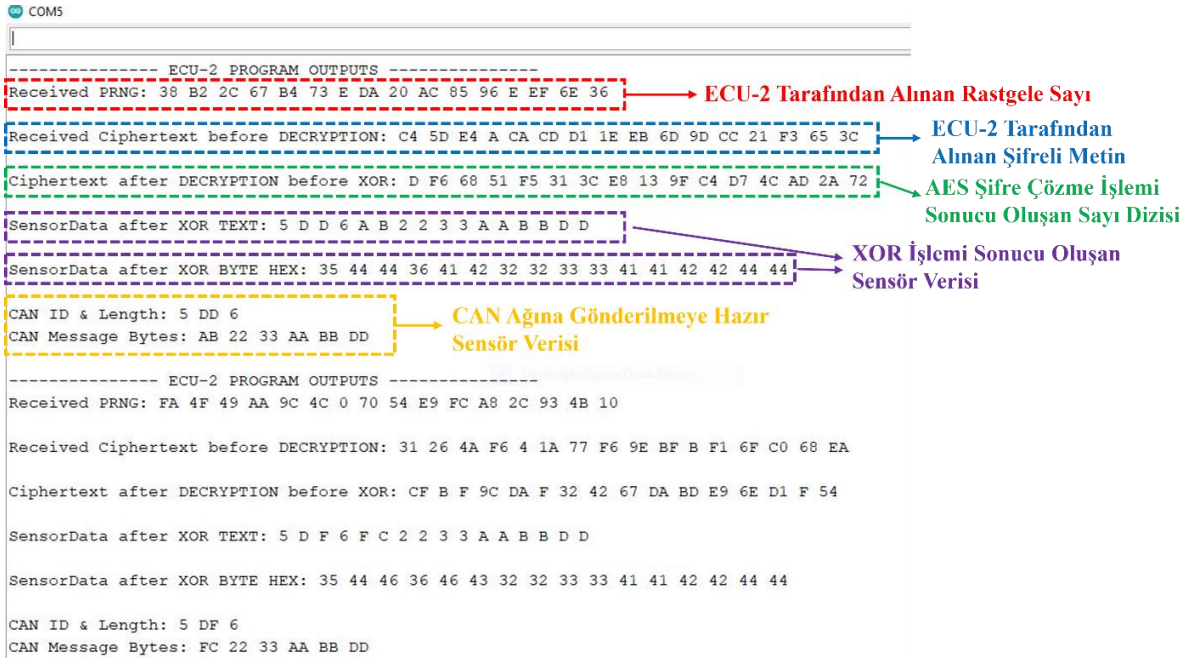
Şekil 4.17.'de, ECU-1'in sahip olduğu kontrol yazılımının çıktıları verilmiştir. ECU-1, belirli bir periyotta, 2 farklı sensör verisinden birisini şifreli olarak yayınlar. Aşağıda verilen şekilde, 2 farklı döngü için 2 farklı program çıktısı verilmiştir. Birinci döngü için kullanılan sensör verisi ile ikinci döngü için kullanılan sensör verisi farklıdır. Bunun nedeni farklı sensör verileri için, ECU-3'ün sahip olduğu kimlik doğrulama fonksiyonunu kullanmaktır. İlk döngü çıktısında kullanılan sensör verisi, ECU-3 tarafından değerlendirilir, ikinci döngü çıktısı için kullanılan sensör verisi ise, ECU-3 tarafından değerlendirilmeyecektir. ECU-1 tarafından kullanılan sensör verileri kırmızı çerçeveler ile gösterilmiştir. Verilen çıktı görselinde, ECU-1 tarafından kullanılan sensör verileri dışında, ECU-1'in ürettiği 16 baytlık rastgele sayı dizisi de mavi çerçeve ile belirtilmiştir.



Şekil 4. 17. ECU-1 Program Çıktıları

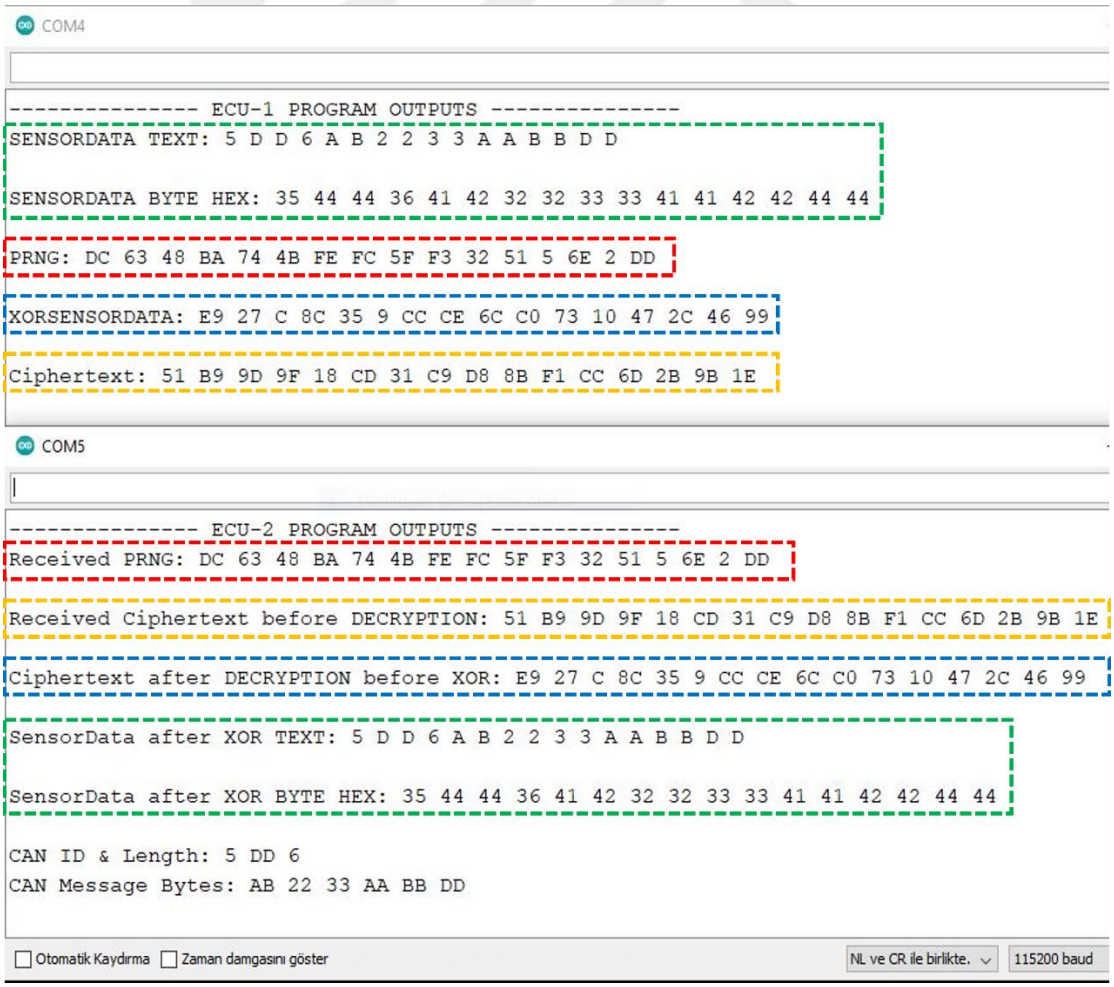
Kullanılan sensör sayı dizisinin her bir bayt değeri için, bir bayt rastgele sayı üretilmiştir, buradaki amaç daha güvenli ve çözülemez bir özel veya işlem sonucu elde etmektir. Sensör verisi ile üretilen rastgele sayının XOR işlemi sonucu oluşan yeni sayı dizisi, verilen çıktı görselinde sarı çerçeve ile belirtilmiştir. XOR işlemi sonucu oluşan sayı dizisinin, AES şifreleme algoritması ile şifrelenmesi sonucu oluşan şifreli sayı dizisi de yeşil çerçeve ile gösterilmiştir.

ECU-2'nin program çıktıları şekil 4.18.'de verilmiştir. Verilen resimde kırmızı çerçeve ile belirtilen kısım, ECU-1'de üretilen ve UART protokolü üzerinden ECU-2'ye gönderilen 16 baytlık rastgele sayı dizisidir. Verilen resimde mavi çerçeve ile gösterilen sayı dizisi ise, ECU-1 tarafından AES ile şifrelenmiş ve ECU-2'ye farklı bir UART hattı üzerinden gönderilmiş şifreli metindir. ECU-2, iki farklı UART üzerinden aldığı rastgele sayı dizisini ve şifreli metini kullanarak düz metini (gerçek sensör verisini) elde eder. ECU-2'de gerçekleşen AES şifre çözme işlemi sonucu oluşan sayı dizisi, verilen resimde yeşil çerçeve ile gösterilmiştir. ECU-2, gerçek sensör verisini elde etmek için, AES şifre çözme işlemi sonucu oluşmuş sayı dizisi ile alınan rastgele sayıyı XOR işlemine sokmalıdır. XOR işlemi sonucu oluşan veri, gerçek sensör verisidir ve resimde mor çerçeveler ile belirtilmiştir. Sonrasında ise, CAN ağına gönderilecek verinin CAN mesaj formuna dönüşümü için gerekli işlemler yapılmıştır. Sarı çerçeve ile belirtilen kısım, CAN ağına gönderilecek CAN mesaj kimliği ve veri baytlarıdır.



Şekil 4. 18. ECU-2 Program Çıktıları

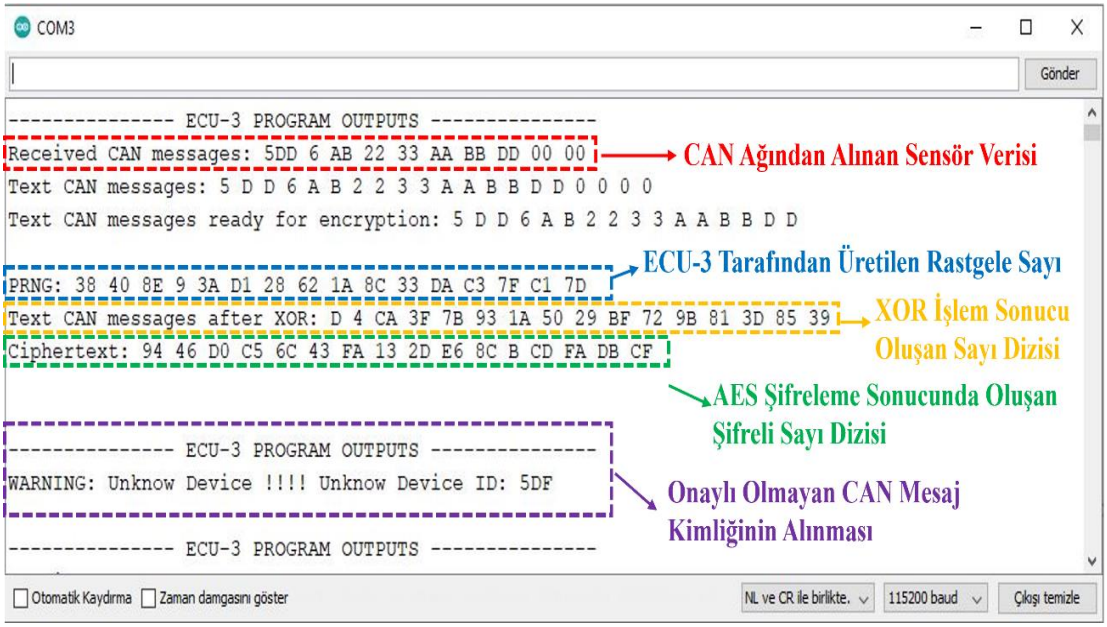
ECU-1 ve ECU-2'nin çıktılarını bir bütün olarak incelemek gerekirse aşağıda verilen şekil 4.19. referans alınabilir. Verilen resimde, aralarında ilişki bulunan çıktılar aynı renk çerçeveler içine alınmıştır. ECU-1'de üretilen rastgele sayı ile, ECU-2 tarafından alınan rastgele sayı dizisi aynı olmalıdır. Aşağıda verilen şekilde, her iki rastgele sayı dizisi de kırmızı çerçeve içine alınmıştır. ECU-1'de şifrelenmiş sensör verisi ile, ECU-2'nin aldığı şifreli veri aynı olmalıdır ve verilen resimde bu iki sayı dizisi sarı çerçeveler ile gösterilmiştir. ECU-1'de gerçekleştirilen, sensör verisi ve rastgele sayının XOR işlemi sonucu oluşmuş sayı dizisi ile (bu veri, aynı zamanda AES şifreleme işlemine giren sayı dizisidir), ECU-2'de gerçekleştirilen, şifreli metinin girdiği AES şifre çözme işlemi sonucu oluşmuş sayı dizisi aynı olmalıdır ve bu sayı dizileri verilen resimde mavi çerçeveler ile gösterilmiştir. AES şifre çözme işlemi sonucunda oluşan sayı dizisi ve alınan rastgele sayı dizisinin XOR işlemi sonucunda, XOR işleminin geri dönüşüm özelliği gereği gerçek sensör verisi elde edilir. Bu sayı dizileri de verilen resimde yeşil çerçeveler ile belirtilmiştir.



Şekil 4. 19. ECU-1 ve ECU-2 Program Çıktıları

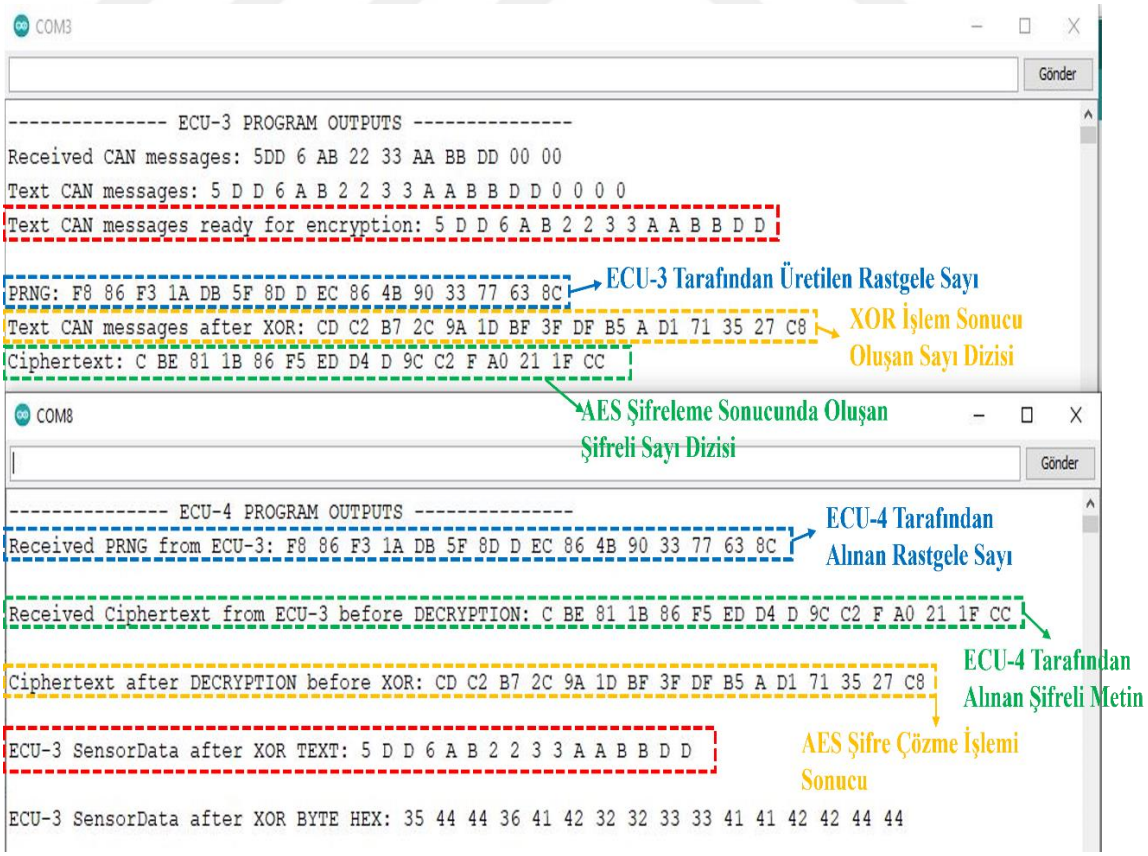
ECU-3'ün program çıktıları, aşağıda şekil 4.20.'de verilmiştir. ECU-3, ECU-2'nin CAN ağına gönderdiği sensör verisini, kimlik doğrulama koşulu ile denetler ve değerlendirip değerlendirmeyeceğine karar verir. Resimde kırmızı ile gösterilen çerçeve, ECU-3'ün CAN ağından aldığı sensör verisidir. Bu CAN mesajı, ECU-3 tarafından bilinen ve onaylı bir CAN kimliğine sahiptir. Onaylı olmayan CAN mesajı alan ECU-3, alınan CAN mesajını değerlendirmez ve cihaz kimliğini de belirterek bilinmeyen cihaz uyarısı verir. Şekil 4.20'de mor renkte gösterilen çerçevede, ECU-3'ün verdiği uyarı mesajının bir çıktısı görülmektedir.

Alınan CAN mesajı, ECU-4'e UART protokolü üzerinden şifreli olarak gönderilir. Bu yüzden ECU-3'ün kontrol yazılımında rastgele sayı üretimi, XOR işlemi ve AES şifreleme işlemi bulunur. Alınan CAN mesajı, şifreleme için uygun bir forma dönüştürüldükten sonra, üretilen rastgele sayı dizisi ile özel veya işlemine tutulur. Aşağıda verilen resimde mavi çerçeve ile belirtilen kısım, ECU-3 tarafından üretilen rastgele sayı dizisidir. Bu sayı dizisi üretildikten sonra, şifre çözme işleminde kullanılmak üzere ECU-4'e gönderilir. Resimde sarı çerçeve ile gösterilen kısım da, özel veya işlemi sonucu oluşmuş sayı dizisidir. Bu işlemden sonra, sarı çerçeve ile belirtilen sayı dizisi, AES şifreleme algoritması ile şifrelenir ve UART protokolü üzerinden ECU-4'e gönderilir. AES şifreleme işlemi sonucunda oluşmuş sayı dizisi, yeşil çerçeve ile gösterilmiştir.



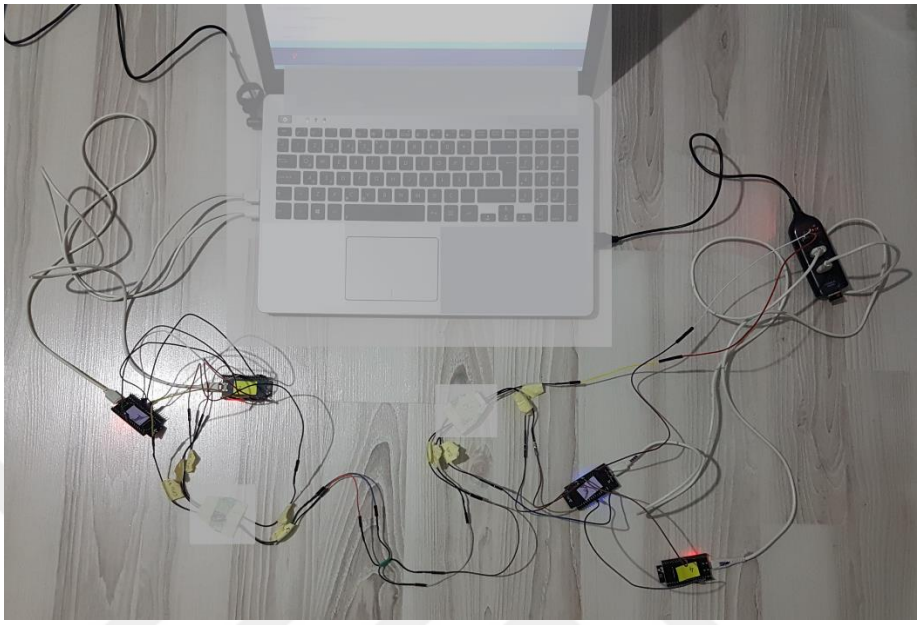
Şekil 4. 20. ECU-3 Program Çıktıları

ECU-3 ve ECU-4'ün program çıktıları, gerçek zamanlı olarak şekil 4.21.'de verilmiştir. Verilen resimde aralarında ilişki bulunan çıktılar, ECU-3 ve ECU-4 program çıktıları altında aynı çerçeve rengi ile belirtilmiştir. ECU-4 şifre çözme işlemlerine, ECU-3'ün üretip gönderdiği rastgele sayıyı almak ile başlar. ECU-4 tarafından, ilgili UART hattından alınan rastgele sayı, aşağıda verilen resimde mavi çerçeve ile gösterilmiştir. Bu işlemden sonra, ECU-4 tarafından diğer UART hattı üzerinden, ECU-3 tarafından şifrelenmiş şifreli metin alınır. ECU-4 tarafından alınan şifreli metin, aşağıda verilen resimde yeşil çerçeve ile belirtilmiştir. Şifreli metin alındıktan sonra, ECU-4 tarafından AES şifre çözme işlemi gerçekleştirilir. Bu işlem sonucu oluşan sayı dizisi verilen resimde sarı çerçeve ile gösterilmiştir. Sensör verisini elde etmek için, son şifre çözme basamağı olan rastgele sayı ile XOR işlemi yapılmalıdır. AES şifre çözme işlemi yapıldıktan sonra, bu işlem sonucu oluşan sayı dizisi ile, ECU-4 tarafından alınan rastgele sayı dizisi, XOR işlemine tabi tutulur. Bu işlem sonucunda, ECU-3 tarafından şifrelenmiş gerçek sensör verisine ulaşılır. Bu işlem sonucu oluşan sayı dizisi, ECU-4 program çıktıları bölümünde, kırmızı çerçeve ile gösterilmiştir.



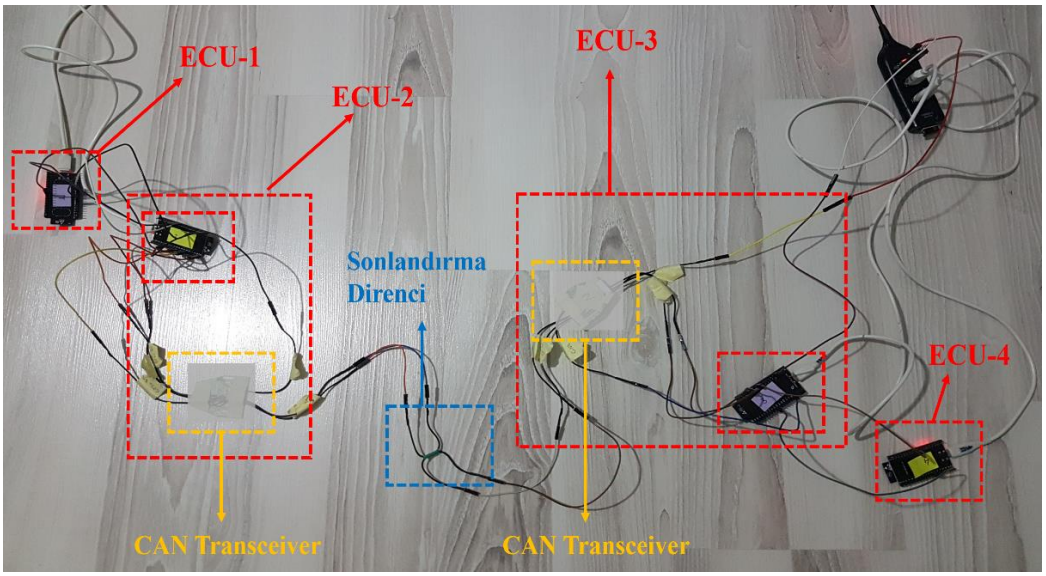
Şekil 4. 21. ECU-3 ve ECU-4 Program Çıktıları

Aşağıda verilen şekil 4.22.'de, projenin uygulama çalışmasının tüm deney ortamı verilmiştir. ECU'ların çıktıları incelenirken bilgisayar ve harici USB çoğaltıcı kullanılmıştır.



Şekil 4. 22. Uygulama Çalışması Deney Ortamı

Projenin uygulama çalışması ortamındaki elemanların detaylı belirtilmiş hali şekil 4.23.'de verilmiştir. ECU'lar için kullanılan mikrodenetleyici kartlar, CAN ağ bağlantısı için gerekli olan CAN transceiver modülleri aşağıdaki şekilde çerçeveler içinde gösterilmiştir.



Şekil 4. 23. Uygulama Çalışması Elemanları

5. SONUÇ VE ÖNERİLER

Teknolojinin otomotiv elektroniğine getirdiği yenilikler, sürücü ve sürüş konforu açısından iyileşme sağlasada, arka planda önlem alınması gereken bazı sorunlar da oluşturmaktadır. Araçların dış birimler ile olan etkileşiminin artması ve farklı fonksiyonlar için yeni eklentilere sahip olması, veri ve kontrol güvenliğinin önemini arttırmış ve otomotiv endüstrisinde siber güvenlik kavramının oluşmasına neden olmuştur.

Elektrikli araçların gelişimi ile birlikte akıllı ve otonom araç konseptleri ön plana çıkmış ve önem kazanmıştır. Bu konseptler beraberinde birçok yeniliği getirsede aynı zamanda güvenlik konusunda bazı riskler de getirmiştir. Araçlara eklenen yeni fonksiyonlar ve arayüzler, bu teknolojik cihazları siber saldırı için bir hedef haline dönüştürmüştür.

Arabanın iç haberleşme ağına sızmayı başarıp önemli mesajları anlamlandırabilen birisi, farklı saldırı yöntemleri ile aracın gaz, fren, kilit vs. önemli fonksiyonlarını kontrol edip, aracı sürücüden bağımsız bir şekilde istediği gibi yönetebilir. Bu durum, kötü niyetli bir yaklaşımla birlikte sürücü, yolcu ve toplum güvenliği açısından istenmeyen durumlar ve olumsuz sonuçlar oluşturabilir. Bu yüzden araç içi haberleşme ağı, saldırılara karşı bir güvenlik mekanizmasına sahip olmalıdır.

Bu çalışmada, elektrikli aracın sistem güvenliğini arttırmak amacıyla şifreli mesajlaşmaya sahip, hibrit bir araç içi haberleşme sistemi tasarlanmıştır. Çalışmada, araç içi haberleşme ağında bulunan ECU'ları temsil etmek için ESP32 mikrodenetleyici kartlarından ve CAN transceiver modüllerinden yararlanılmıştır. ECU'lar arası haberleşmelerde CAN ve UART gibi farklı haberleşme protokolleri kullanılarak hibrit bir yapı kurulmuştur. AES ve XOR gibi şifreleme yöntemleri kullanılarak da, ECU'lar arası haberleşmeler şifreli gerçekleştirilmiştir. Önemli veriler tek bir haberleşme hattı üzerinden aktarılmak yerine farklı haberleşme hatları kullanılarak iletilmiştir. Bu yöntem ve işlemler ile birlikte, araç içi sistem güvenliğinin arttırılması sağlanmıştır.

Araç içi haberleşme ağında bulunan önemli ve kritik verilerin haberleşmesinin şifreli olarak gerçekleştirilmesi sayesinde, verilerin üçüncü kişiler tarafından anlamlandırılmasının önüne geçilmiştir ve veri güvenliği sağlanmıştır. Verilerin anlamlandırılamaması sayesinde, aracın ana fonksiyonlarından sorumlu mesaj paketlerinin kontrol edilebilmesinin önüne geçilmiştir. Bu sayede, aracın kontrol güvenliği de sağlanmıştır.

Bu çalışmada, diğer simetrik veya asimetrik şifreleme yöntemleri de kullanılabilir ve şifreleme yöntemlerinin incelenmesi, karşılaştırılması ve verimliliği üzerinde çalışılabilir. Farklı saldırı çeşitlerinin ilgili şifreleme yöntemine uygulanması ile şifreleme yönteminin güvenliği ve sağlamlığı test edilip bir analiz raporu oluşturulabilir.

Gelecek çalışmalarda, tasarlanan bu sistemin doğruluğu ve güvenliği, sisteme uygulanacak farklı siber saldırılar ile test edilip, karşılaştırma analizleri gerçekleştirilebilir. Şifreli verinin taşındığı haberleşme hattına farklı saldırı yöntemleri uygulanarak sistemin güvenlik açısından zayıf ve güçlü noktaları analiz edilebilir. Sistemde kullanılan sözde rastgele sayı üreteçleri yerine, herhangi bir donanım kaynağından alınan örneklem ile gerçek bir rastgele sayı üreteci tasarlanıp, kullanılabilir. Tasarlanan sistemde kullanılan CAN haberleşme protokolü yerine, otomotiv elektroniğinde kullanılan diğer haberleşme protokolleri sisteme uygulanıp, verimlilik ve güvenilirlik analizleri gerçekleştirilebilir.

KAYNAKLAR

[1] Maini, C. K., Gopal, K., & Prakash, R. (2013b). Making of an ‘all reason’ electric Vehicle. 2013 World Electric Vehicle Symposium and Exhibition (EVS27). https://doi.org/10.1109/evs.2013.6915015

[2] Wang, J., Yang, D., & Lian, X. (2016). Research on electrical/electronic architecture for connected vehicles. IET International Conference on Intelligent and Connected Vehicles (ICV 2016). https://doi.org/10.1049/cp.2016.1165

[3] Zhang, H., Pan, Y., Lu, Z., Wang, J., & Liu, Z. (2021b). A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units. IEEE Access, 9, 149690–149706. https://doi.org/10.1109/access.2021.3124565

[4] Srinivasan, C., Sridhar, P., Raj, M. P., & Raj, S. (2023). Advanced Driver Assistance System (ADAS) in Autonomous Vehicles: A Complete Analysis. 2023 8th International Conference on Communication and Electronics Systems (ICCES). https://doi.org/10.1109/icces57224.2023.10192617

[5] Kaur, P., & Sobti, R. (2017). Current challenges in modelling advanced driver assistance systems: Future trends and advancements. 2017 2nd IEEE International Conference on Intelligent Transportation Engineering (ICITE). https://doi.org/10.1109/icite.2017.8056916

[6] Liu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected Vehicles: solutions and challenges. IEEE Internet of Things Journal, 1(4), 289–299. https://doi.org/10.1109/jiot.2014.2327587

[7] He, K., Wang, C., Han, Y., & Fang, X. (2020). Research on cyber security Technology and Test Method of OTA for Intelligent Connected Vehicle. 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). https://doi.org/10.1109/icbaie49996.2020.00048

[8] Singh, A. P., & Singh, M. (2018). An empirical study on automotive cyber attacks. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/wf-iot.2018.8355124

[9] Yu, M., Zhang, G., Shen, S., Ning, Y., Liu, T., & Sun, D. (2023). An Intelligent Connected Vehicles Information Security Attack Matrix Model. 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS). https://doi.org/10.1109/icpics58376.2023.10235357

[10] Boyes, H., & Lück, A. (2015). A Security-Minded Approach to Vehicle Automation, Road Infrastructure Technology, and Connectivity. 10th IET System Safety and Cyber-Security Conference 2015. https://doi.org/10.1049/cp.2015.0295

[11] Zidi, C., Sondi, P., Mitton, N., Wahl, M., & Meddahi, A. (2023). Review and perspectives on the audit of vehicle-to-everything communications. IEEE Access, 11, 81623–81645. https://doi.org/10.1109/access.2023.3301182

[12] Ju, H., Jeon, B., Kim, D., Jung, B., & Jung, K. (2019). Security Considerations for In-Vehicle Secure Communication. 2019 International Conference on Information and Communication Technology Convergence (ICTC). https://doi.org/10.1109/ictc46691.2019.8939742

[13] Ikezaki, Y., Nozaki, Y., & Yoshikawa, M. (2017b). Evaluation platform for the security of in-vehicle systems. 2017 IEEE International Meeting for Future of Electron Devices. https://doi.org/10.1109/imfedk.2017.7998034

[14] Parmar, M. R., Kumari, M., & Ramesh, S. (2020). CYBER SECURITY IN VEHICLE COMMUNICATION.2020 IEEE International Conference for Innovation in Technology (INOCON). https://doi.org/10.1109/inocon50539.2020.9298286

[15] Jiang, N., Li, H., Cao, W., Wang, Y., & Zhao, W. (2022).Research on Improvement and Experiment for Cyber Security of Automotive Electronic and Electrical Architecture. 2022 IEEE 7th International Conference on Intelligent Transportation Engineering (ICITE). https://doi.org/10.1109/icite56321.2022.10101381

[16] Ahmad, A. (2020). Automotive Semiconductor Industry - Trends, Safety and Security Challenges. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). https://doi.org/10.1109/icrito48877.2020.9197894

[17] Ramos, M. A., Correa-Jullian, C., McCullough, J., Ma, J., & Mosleh, A. (2023). Automated Driving Systems Operating as Mobility as a Service: Operational Risks and SAE J3016 Standard. 2023 Annual Reliability and Maintainability Symposium (RAMS). https://doi.org/10.1109/rams51473.2023.10088244

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

[19] ABS Fren sistemi nedir? (n.d.). https://www.otopratik.com.tr/faydali-bilgiler/arac-bakimi/abs-fren-sistemi-nedir

[20] ESC(Electronic Stability Control) Nedir? | Toyota Blog. (2021, April 19). Blog.toyota.com.tr. https://blog.toyota.com.tr/escelectronic-stability-control-nedir/

[21] Usta, C., & Usta, C. (2022, July 3). Elektronik denge Kontrolü (ESC) ne işe yarar ? | Otomakinist. Otomakinist https://www.otomakinist.com/elektronik-denge-kontrolu-esc-ne-ise-yarar/

[22] The Windscreen Company. (2022, November 28). Autonomous Emergency Braking | ADAS Guide | The Windscreen Company. https://www.thewindscreenco.co.uk/adas-guide/autonomous-emergency-braking-aeb/

[23] Lane Change Assist (LCA) | What it is and how it works. (2023, July 25). Car ADAS. https://caradas.com/lane-change-assist/

[24] What is Park Distance Control? - Private Fleet Car Broker. (2016, April 29). Private Fleet Car Broker. https://www.privatefleet.com.au/glossary/what-is-park-distance-control/

[25] The Windscreen Company. (2022b, November 28). Lane Departure Warning | ADAS Guide | The Windscreen Company. https://www.thewindscreenco.co.uk/adas-guide/lane-departure-warning/

[26] My Car Does What. (2018, April 24). Forward collision warning - My car does what. https://mycardoeswhat.org/deeper-learning/forward-collision-warning/

[27] Lane keeping assist. (n.d.). www.bosch-Mobility-Solutions.com. https://www.bosch-mobility.com/en/solutions/assistance-systems/lane-keeping-assist/

[28] My Car Does What. (2018a, April 24). Adaptive cruise control - My car does what. https://mycardoeswhat.org/deeper-learning/adaptive-cruise-control/

[29] The Windscreen Company. (2022c, November 28). Park Assist Technology | ADAS Guide | The Windscreen Company. https://www.thewindscreenco.co.uk/adas-guide/park-assist/

[30] Safelite. (n.d.). Automotive Night Vision Systems | Value of Car Night Vision | SafeLite. https://www.safelite.com/windshield-auto-glass-technology/night-vision

[31] The Windscreen Company. (2022b, November 28). Blind spot awareness | ADAS Guide | The Windscreen Company. https://www.thewindscreenco.co.uk/adas-guide/blind-spot-awareness/

[32] Lane centering assist. (n.d.). https://www.bosch-mobility.com/en/solutions/assistance-systems/lane-centering-assist/

[33] The Windscreen Company. (2022c, November 28). Collision Avoidance Systems | ADAS Guide | The Windscreen Company. https://www.thewindscreenco.co.uk/adas-guide/collision-avoidance-systems/

[34] Valeo. (2022, June 16). Driver Monitoring: a camera to monitor driver alertness | Valeo. https://www.valeo.com/en/driver-monitoring/

[35] What is a Rear Cross Traffic Alert? | Kia British Dominica. (n.d.). Kia British Dominica. https://www.kia.com/dm/discover-kia/ask/what-is-a-rear-cross-traffic-alert.html

[36] Choi, D., Jung, J., Koh, S. J., Kim, J., & Park, J. (2019). In-Vehicle Infotainment Management System in Internet-of-Things Networks. 2019 International Conference on Information Networking (ICOIN). https://doi.org/10.1109/icoin.2019.8718192

[37] Dawabsheh, A., & Owda, M. (2023). In-Vehicles Infotainment System Forensics Case Study. 2023 International Conference on Information Technology (ICIT). https://doi.org/10.1109/icit58056.2023.10225982

[38] Five automotive connectivity trends fueling the future | Jabil. (n.d.). Jabil.com. https://www.jabil.com/blog/automotive-connectivity-trends-fueling-the-future.html

[39] Otonomo. (2022, May 9). Automotive Connectivity is Driving the Future of Mobility. https://otonomo.io/blog/automotive-connectivity-future-mobility/

[40] Anđelić, T. (2023, October 26). Pushing the frontiers of Automotive industry: Five Automotive Connectivity Trends Fueling the Future - HTEC. HTEC. https://htecgroup.com/pushing-the-frontiers-of-automotive-industry-five-automotive-connectivity-trends-fueling-the-future/

[41] Sachdev, M. (2021, June 28). Defining Vehicle to Pedestrian (V2P). rgbsi. https://blog.rgbsi.com/defining-vehicle-to-pedestrian-v2p

[42] Kenjić, D., & Antić, M. (2023). Connectivity challenges in automotive solutions. IEEE Consumer Electronics Magazine, 12(5), 53–59. https://doi.org/10.1109/mce.2022.3183807

[43] Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: challenges and solutions. Sensors, 22(17), 6679. https://doi.org/10.3390/s22176679

[44] Electronics, C. (2021, November 1). CAN Bus Explained - A Simple Intro [2021]. CSS Electronics. https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial

[45] Park, C. H., Kim, Y., & Jo, J. (2021b). A Secure Communication Method for CANBus. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). https://doi.org/10.1109/ccwc51732.2021.9376166

[46] Siddiqui, A. S., Plusquellic, Y. G. J., & Saqib, F. (2017). Secure communication over CANBus. 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). https://doi.org/10.1109/mwscas.2017.8053160

[47] Su, N., Zhang, Y., & Li, M. (2019). Research on data encryption standard based on AES algorithm in Internet of Things environment. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). https://doi.org/10.1109/itnec.2019.8729488

[48] Liu, Y., Zhang, W., Peng, X., Liu, Y., Zheng, S., Wei, T., & Wang, L. (2019). Design of password encryption model based on AES algorithm. 2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT). https://doi.org/10.1109/iccasit48058.2019.8973003

[49] Jena, B. K. (2023, February 9). What is AES encryption and how does it work? Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

[50] CSS Electronics. (n.d.). Terminal resistor (120 Ohm, DB9, CAN Bus). https://www.csselectronics.com/products/terminal-resistor-can-bus

[51] Aydın, Ö. (2022). Authentication and Billing Scheme for the electric vehicles: EVABS. Uluslararası Yönetim Bilişim Sistemleri Ve Bilgisayar Bilimleri Dergisi, 6(1), 29–42. https://doi.org/10.33461/uybisbbd.1075481