T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

OTOMOTİV HABERLEŞMESİNDE DENETLEYECİ ALAN AĞI (CAN) İÇİN HİBRİT BİR SALDIRI SAVUŞTURMA UYGULAMASI

YÜKSEK LİSANS TEZİ

Serkan BAKİ

Elektrik-Elektronik Mühendisliği Anabilim Dalı
Elektrik-Elektronik Mühendisliği Programı

TEMMUZ, 2021

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

OTOMOTİV HABERLEŞMESİNDE DENETLEYECİ ALAN AĞI (CAN) İÇİN HİBRİT BİR SALDIRI SAVUŞTURMA UYGULAMASI

YÜKSEK LİSANS TEZİ

Serkan BAKİ
(Y1913.100004)

Elektrik-Elektronik Mühendisliği Anabilim Dalı
Elektrik-Elektronik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Nedim TUTKUN

TEMMUZ, 2021

ONAY FORMU

ONUR SÖZÜ

Yüksek Lisans Tezi olarak sunduğum "OTOMOTİV HABERLEŞMESİNDE DENETLEYİCİ ALAN AĞI (CAN) İÇİN HİBRİT BİR SALDIRI SAVUŞTURMA UYGULAMASI" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (05/07/2021)

Serkan BAKİ

ÖNSÖZ

Hayatım boyunca her türlü desteklerini hiçbir zaman esirgemeyen başta babam Ahmet Baki ye ve annem Zeynep Baki ye, tecrübelerini aktarmada, bu tezin yazılmasında ve araştırmalarımda, yardımlarını eksik etmeyen danışman hocam Sayın Prof. Dr. Nedim Tutkun'a sonsuz teşekkürlerimi bir borç bilirim.

Temmuz, 2021 Serkan BAKİ

OTOMOTİV HABERLEŞMESİNDE DENETLEYİCİ ALAN AĞI (CAN) İÇİN HİBRİT BİR SALDIRI SAVUŞTURMA UYGULAMASI

ÖZET

Teknoloji geliştikçe insanların yaşam kalitesinden beklentileri de her geçen gün artmaktadır. İnsanlar her alanda olduğu gibi otomotiv alanında da kaliteli yaşam sürmek istemektedir. Otomotiv teknolojisi insanların yaşam kalitesini artırmak için teknolojisini her gün geliştirmektedir. Otomotiv teknolojisi geliştikçe araç içerisinde insanların isteklerini yerine getiren birimlerin, elektronik kontrol ünitelerinin (ECU) sayısı da her geçen gün artmaktadır. Araç içerisinde insanların isteklerine cevap veren elektronik kontrol ünitelerinin, haberleşmesinde gerçek zamanlı performansı ve verimli iletişiminden dolayı yaygın olarak denetleyici alan ağı (CAN) kullanılır. Ancak CAN haberleşmesinin ağ güvenliğinin nasıl sağlanacağı tartışmaları son zamanlarda oldukça artmıştır. Araştırmalara göre kontrolü basit ve doğası gereği güvenlik açığı olan bu haberleşme ağının kontrolü otomotiv korsanları tarafından kolayca ele geçirilebilir. Araç içerisinde CAN haberleşme ağına sızan korsanlar elektronik kontrol ünitelerini uzaktan kontrol ederek sadece araca değil insan sağlığına da etkilerinin olduğu yine araştırmalarda görülmüştür. Otomotiv teknolojisi gelişirken ortaya çıkan güvenlik açıklarına karşı sessiz kalmayan araştırmacılar alınması gereken önlemleri kendi makalelerinde işlemiştir. Bu araştırmanın amacı, araç içi haberleşme ağında korsan belirleme ünitesi (KBÜ) kurularak korsan varlığı belirlenip elektronik kontrol ünitelerinin birden fazla yoldan basit şifreli haberleşmesi sağlanarak saldırıları savuşturmaktır. Bu araştırma da kullanılan hibrit yöntem hem şifreli haberleşmeyi hem de saldırı belirleme ünitesini kapsamaktadır. Yöntemin bu hibrit yapısı denemelerin sonucunda CAN haberleşmesinde hem derinlemesine güvenliği sağlarken hem de kendisine ait doğal yapısından taviz vermemesini sağlamaktadır.

Anahtar Kelimeler: Denetleyici Alan Ağı, Şifreli Haberleşme, Korsan Belirleme Ünitesi, Araçta Ağ Güvenliği, Otomotiv Saldırı Tespiti

HYBRID ATTACK AVOIDANCE APPLICATION FOR THE CONTROLLER AREA NETWORK (CAN) IN AUTOMOTIVE COMMUNICATIONS

ABSTRACT

As technology develops rapidly, people are usually expected to increase their life quality day by day, especially in automotive sector. As the automotive technology develops, the number of units, electronic control units (ECU) that fulfil the wishes of the people in the vehicle is increasing as day pass. The controller area network (CAN) is widely used due to the real-time performance and efficient communication of electronic control units that respond to the requests of the people in their vehicle. However, discussions on how to secure the network of CAN communication have increased recently. According to research, the control of this communication network, which is simple to control and vulnerable in nature, can be easily taken over by automotive hackers. It has been seen in the researches that the hackers who infiltrated the CAN communication network in the vehicle have effects not only on the vehicle but also on human health by remotely controlling the electronic control units. The researchers, who did not remain silent against the security gaps that emerged as automotive technology developed, covered the precautions that should be taken in their articles. The aim of this research is to defend the attacks by establishing a hacker detection unit (KBU) in the in-vehicle communication network and determining the presence of hacker and providing simple encrypted communication of electronic control units in multiple ways. The hybrid method used in this research includes both encrypted communication and an attack detection unit. As a result of the experiments, this hybrid structure of the method mentioned in this study provides both in-depth security in CAN communication and ensures that it does not compromise its canonical structure.

Keywords: Controller Area Network, Encrypted Communication, Hacker İdentification Unit, In Vehicle Network Security, Automotive Intrusion Detection

İÇİNDEKİLER LİSTESİ

KISALTMALAR LİSTESİ

A : Amper
AC : Alternatif Akım
AES-128 : 128 Bit Elektronik Verinin Şifrelenmesi
Bit : 1 byte'lık verinin sekizde biri
Bps : Saniye başına düşen bit sayısı
Byte : 8 bitlik veri bütünü
Bus : Veri Yolu
CAN : Denetleyici Alan Ağı
CSMA / CA : Çoklu Erişimde Hat Kontrolü / Çakışma Mümkün
DC : Doğru Akım
DoS : Hizmet Reddi
EEPROM : Silinip Programlanabilir Salt Okunur Bellek
ECU : Elektronik Kontrol Ünitesi
g : Gram
GND : Toprak Hattı
Hex : Hexadesimal Sayı
HMAC : Özet Tabanlı Mesaj Doğrulama Kodu
I2C : Inter-Integrated Circuits (Entegre Devreler Arası)
ICSP : Seri Devre Programlama
ID : Kimlik Numarası
IDE : Entegre Geliştirme Ortamı
IDS : Saldırı Tespit Sistemi
ISO : Uluslararası Standartlar Organizasyonu
ISP : Sistem İçi Programlama

KB : Kilobyte

LCD : Likit Kristal Ekran

LED : Işık Yayan Diyot

m : Metre

mm : Milimetre

mA : Miliamper

MAC : İleti Kimlik Doğrulama Kodu

Mbit : Megabit

MHz : Megahertz

ms : Milisaniye

LAN : Yerel Alan Ağı

Ohm : Direnç Birimi

OBD-II : Araç Üstü Diyagnostik

OSI : Açık Sistemler Bağlantısı

PCB : Baskılı Devre Kartı

PLC : Programlanabilir Mantıksal Denetleyici

PWM : Sinyal Genişlik Modülasyonu

RISC : İndirgenmiş Komut Kümeli Bilgisayar

RxD : Gelen Veri

s : Saniye

SD : Güvenli Sayısal Hafıza

SPI : Seri Çevresel Arayüzü

SRAM : Statik Rastgele Erişim Belleği

TFT : İnce Film Transistörü

TxD : Giden Veri

UART : Evrensel Asenkron Alıcı Verici

USB : Evrensel Seri Veri yolu

V : Volt

VCC : Güç Kaynağının + Ucu

ŞEKİLLER LİSTESİ

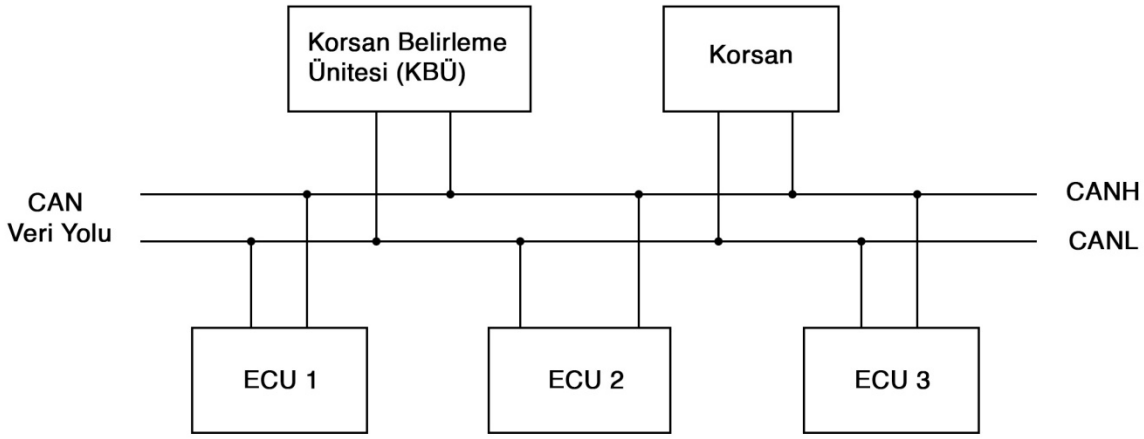
ÇİZELGELER LİSTESİ

I.GİRİŞ

Bu bölümde tezin amacı, tezin önemi ve tezin kapsamı açıklanmıştır. Ayrıca bu tez ile ilgili konular, projeler ve makaleler tartışılarak literatür taraması yapılmıştır.

A. Tezin Amacı

Bu tez çalışmasında araç içi denetleyici alan ağına (CAN) bağlı olan elektronik kontrol ünitelerini korsan saldırılara karşı korumak için hem saldırı tespit sistemi hem de elektronik kontrol üniteleri arasında ilkel şifreleme yöntemleri ile mesajlaşan hibrit bir uygulama geliştirilecektir. Bu uygulamada Şekil 1'deki gibi araç içi CAN ağını temsil eden bir veri yolu kurulacaktır. Korsan belirleme ünitesi (KBÜ) hem kendine has yöntemlerle korsan varlığını belirlerken hem de korsan ünitesinin veri yolundaki elektronik kontrol ünitelerinin mesajlarını çözmesin diye şifreli mesaj değiştirme emirleri verecektir. Kendine has basit şifreleme yöntemleri ve saldırı tespit sistemi birlikte çalışarak CAN veri yolunun güvenliği üzerinde ne gibi etkileri olacağı ve güvenlik fonksiyonlarının CAN veri yolunun gerçek zamanlı performansını hangi yönde etkileyeceği gösterilecektir.



Şekil 1 CAN veri yolunda saldırı savuşturma uygulaması

B. Tezin Önemi

Günümüzde çoğu araç içi işlevsellik, daha iyi araç performansı, yolcu güvenliği ve gelişmiş eğlence tesisleri sağlamak için birbirine bağlı elektronik kontrol üniteleri (ECU) tarafından kontrol edilmektedir. Otomotiv teknoloji şirketleri her geçen gün yeni ürettikleri araçlarına yeni bir elektronik kontrol ünitesi eklemektedir. Modern arabalar içerisinde ortalama 70 ila 100 arası elektronik kontrol ünitesi içerebilir (MILLER ve VALASEK, 2015). ECU'lar, motor kontrolü, hava yastığı açılması ve kilitlenmeyi önleyici fren sistemi gibi güvenlik açısından kritik işlevlerde içerisinde olmak üzere otomobilin birçok önemli işlevlerinin çoğunu kontrol eder. Bu yüzden güvenli bir sürüşe sahip olmak için, ECU'lar güvenilir bir iletişim ağına sahip olmalıdırlar (MUNDHENK, 2017).

Otomotiv teknolojisinde elektronik kontrol ünitelerinin haberleşmesinde yaygın olarak CAN haberleşmesi kullanılır (MILLER ve VALASEK, 2015). CAN ağı haberleşmede 2 tel kullanması kablolama gereksinimlerini ve araçların ağırlığını azaltır, bu da üreticiye daha düşük üretim maliyetleri ve tüketiciye daha düşük satın alma ve yakıt maliyeti sağlar. Elektriksel parazitlere karşı yüksek bağışıklık, kolay

kablolama, kendi kendine teşhis yeteneği ve hataları onarma gibi tanınmış avantajları CAN veri yolunu otomobil endüstrisi için uygun hale getirir (URL-2). CAN elektriksel gürültüye karşı dirençli olmasına ve güvenlik özelliklerine sahip olmasına rağmen, saldırılara karşı hala savunmasızdır. Bu haberleşme ağı otomotiv haberleşmesinde saldırılara karşı doğası gereği bazı güvenlik açıkları vardır. Örneğin veri iletiminde şifreleme ve kimlik doğrulama gibi ciddi güvenlik eksiklikleri vardır (KOSCHER ve ark., 2010). Bu güvenlik açıkları bölüm 2'de ayrıntılı olarak anlatılmıştır.

Tersine mühendislik var olan bir modelin, bir mekanizmanın ya da bir sistemin incelenerek, o yapının oluşturulması aşamaları ve mühendislik teknolojilerini keşfetmesi işlemidir. Otomotiv teknolojisinde de her geçen gün elektronik kontrol üniteleri üzerinde mühendislik teknolojileri gelişmektedir. Rakip firmalar ya da korsan kullanıcılar araçların içerisindeki elektronik kontrol ünitelerini taklit etmek, kontrol etmek ya da zarar vermek için elektronik kontrol ünitelerinin bağlı olduğu CAN ağına standart bir ECU gibi sızıp tersine mühendislik uygulayabilirler (CURRIE, 2017). Korsanlar araç içine OBD-II portundan ya da kablosuz haberleşme yoluyla sızabilirler. OBD-II portu araçlarda 1994'den beri bulunan araç içerisinde CAN ağını ve araç içi ağları da barındıran araç içi arıza tespiti sağlayan port dur (URL-6). Tersine mühendislik uygulamaları sonucunda korsanlar araç içi elektronik kontrol ünitelerinin nasıl kontrol edildiğini çözümlerler ya da elektronik kontrol ünitelerine kalıcı hasarlar verirler. Ayrıca korsanlar tersine mühendislik yerine CAN ağına yazılım katmanından hizmet reddi (DoS) saldırıları ile elektronik kontrol ünitelerine hasarlar verebilirler (MURVAY ve GROZA, 2017). Sonuç olarak CAN haberleşmesinin mevcut güvenlik açıklarından haberdar olan korsanlar CAN ağlarına tersine mühendislik uygulayarak kontrol ünitelerini çözümlerler. Bu durumda çözümlenmiş kontrol ünitelerini taklit edip piyasaya taklit edilmiş bir ürün satmak, kontrol ünitelerini farklı yollar ile kontrol edip tüketiciye tekrardan satmak ya da kontrol ünitelerine kalıcı hasarlar verme konuları akademik araştırmacılar ve

otomotiv üreticileri için gerçek bir sorun haline gelmiştir. Bu tezdeki CAN saldırı savuşturma uygulaması kullanılarak mevcut sorunlar çözülebilir.

C. Tezin Kapsamı

Yukarıdaki tezin amacı ve önemi göz önüne alındığında, bu tez gömülü sistemlerin ve CAN veri yolu teknolojisinin aşağıdaki alanlarını inceleyecektir.

- Denetleyici Alan Ağı: CAN ağının fiziksel özellikleri, CAN protokolünün elemanları, CAN ağının donanımsal elemanları, CAN ağındaki mevcut güvenlik açıkları ve bu güvenlik açıklarına karşın alınacak güvenlik önlemlerini inceleyecektir.
- Gerçek Zamanlı İşletim Sistemleri (Gömülü Sistem): CAN veri yoluna bağlanan düğümler, gerçek zamanlı performans gösteren gömülü sistemler ile CAN ağına nasıl bağlanacağı incelenecektir.
- Açık Kaynak Kodu: Hem gömülü işletim sisteminin diğer çevresel sürücülerinin hem de CAN veri yoluna gönderilen ve alınan mesajların sürücülerinin açık kaynak kodu olacaktır.
- Basit Şifreleme Yöntemleri: CAN veri yolunun gizlilik açısından güvenliğini artırmak için birden fazla basit şifreleme yöntemleri kullanılacaktır. Bu şifreleme yöntemleri mesaj içeriğini nasıl gizlediği incelenecektir. Bu basit şifrelerin CAN ağındaki gerçek zamanlı performansı nasıl etkilediği gözlemlenecektir.
- Saldırı Tespit Sistemi: CAN veri yolunun güvenliğini artırmak için saldırı tespit sistemi kurulacaktır. Bu sistemin saldırganı nasıl tespit ettiği ve şifreleme yöntemlerinin değişikliğine nasıl karar verdiği incelenecektir. Ayrıca saldırı tespit sistemi ve basit şifreleme yöntemlerinin birlikte çalışması CAN veri yolunun güvenliğini nasıl etkilediği gözlemlenecektir.

D. Literatür Araştırması

Bu alanda diğer araştırmacıların, çeşitli otomotiv ağ saldırıları, CAN ağında kullanılan çeşitli güvenlik yaklaşımları, CAN ağında denenmiş simetrik şifreleme yöntemleri ve CAN ağına kurulmuş saldırı tespit sistemleri gibi çalışmaları nasıl değerlendirdikleri incelenecektir.

1. Mevcut Saldırılar

CAN haberleşmesi, otomobillerde güvenlik açısından en yaygın kullanılan haberleşme sistemi olduğundan, bu veri yolu güvenliğindeki eksiklikler büyük bir endişe yarattığı için son on yılda araştırmanın odağı haline gelmiştir. CAN ağındaki güvenlik zayıflığını vurgulamak isteyen Hoppe ve arkadaşları aracın OBD-II portundan CAN ağına sızarak dört örnek saldırı gerçekleştirmişlerdir (HOPPE ve ark., 2011). Bu saldırıların birinci ve ikincisi elektrikli cam penceresinin ve araç içi uyarı ışıklarının DoS saldırısına maruz kalmasıdır. Üçüncüsü hava yastığı elektronik kontrol ünitesine yanlış bir veri gönderilmesidir. Son saldırı ise veri yolundan geçen mesajların elde edilmesidir.

Modern otomobiller pasif hırsızlık önleme sistemi, lastik basıncı izleme sistemi, uzaktan anahtarsız giriş, bluetooth ve radyo gibi farklı tipte kablosuz arabirimlerle donatılmışlardır. Bu kablosuz arabirimler, güvenlik duvarı olan bir ağ geçidi ECU'su aracılığıyla CAN ağı ile iletişim kurabilirler. Bazı araştırmacılar güvenlik duvarlarını aşarlar ve CAN ağına erişirler. Valasek ve Miller bu güvenlik duvarını aşarak 12 otomobil markasının 21 otomobil modeline uzaktan 3 tip saldırı gerçekleştirdiler. Bu saldırılardan ilki kablosuz arabirimden sorumlu ECU'yu tehlikeye atmaktır. İkincisi güvenlik açısından kritik ECU ile iletişim kurmak için mesajlar enjekte etmektir. Üçüncüsü ise ECU'yu kötü niyetli davranacak şekilde değiştirmektir (MILLER ve VALASEK, 2014).

Diğer birçok çalışma, araç içi ağlardaki güvenlik açıklarını ve bu güvenlik açıklarına alınan farklı güvenlik önlemlerini göstermektedir. Bu iki araştırmanın

sonunda gözlemlendiği üzere CAN ağına saldırılar araç içinden ya da kablosuz olarak gerçekleştirilebilir. Bu saldırılar araç içi önemli ünitelere zarar vererek ya da üniteleri aldatarak kullanıcının hayatının kaybolmasına sebep verebilirler. Ayrıca araştırmacılar, otomobillerdeki artan siber-fiziksel sistemlerin güvenlik açıklarını daha da artıracağına inanıyorlar. Bu yüzden otomotiv teknolojisi geliştikçe CAN haberleşmesinde veri yolu güvenliği almak daha da önemli hale gelmiştir. Bu nedenle, bu tür tehditlere karşı etkili önlemler geliştirmek acil bir konudur.

2. Mevcut Önlemler

Otomotiv güvenliği yeni bir alan olduğu için bu alanda çözümlerin sayısı ve çeşitliliği de sınırlı kalmaktadır. Bununla birlikte CAN veri yolu güvenliğini iyileştirmek için önerilen bir dizi yaklaşım vardır. Bunlar şifreleme teknikleri, hedef şaşırtma teknikleri, saldırı tespit sistemleri (IDS) ve saldırı önleme (IPS) sistemleridir (NILSSON ve LARSON, 2009).

CAN protokolünde yayın niteliği nedeniyle bir şifreleme mekanizması bulunmadığından, bir saldırgan CAN trafiğini kolayca dinleyebilir ve iletişimi anlayabilir. Ayrıca herhangi bir düğümün ağa bağlanıp mesaj gönderebileceği anlamına gelen bir kimlik doğrulama özelliği olmadığından saldırgan bir düğüm CAN ağına veri çerçevesi gönderebilir ve diğer düğümler bunu kabul edip işleyebilir. Bu tür saldırıları önlemek ve gizlilik sağlamak için, araştırmacılar yazılım ve donanım düzeylerinde farklı şifreleme yöntemleri önermektedir. Birçok araştırmacı simetrik şifreleme yöntemlerini bir arada kullanarak yeni bir şifreleme yöntemi sunmuştur. Bazı şifreleme yöntemlerinin güvenlik hizmetlerini ve ağın çalışmasında önemli rol oynayan gereksinimleri nasıl etkilediğini bu makalede görebiliyoruz (GMIDEN ve ark., 2019). Bu makalede şifreleme yöntemleri kullanılırken bazı değerlendirme ölçütleri kullanılmıştır. Bu ölçütler kimlik doğrulama, bütünlük, gizlilik, geriye dönük uyumluluk, tekrarlı saldırı direnci ve gerçek zamanlı başarıdır. Bu değerlendirme ölçütlerin sonuçları Çizelge 1'de gösterilmiştir. Çizelgedeki

ifadelerden (ok) gereksinimin karşılandığını (nok) gereksinimin karşılanmadığını ifade eder.

Çizelge 1 Tanımlanmış gereksinimlere göre şifreleme yöntemlerinin katkıları (GMIDEN ve ark., 2019)

Şifreleme Yöntemi	Kimlik Doğrulama	Bütünlük	Gizlilik	Geriye Uyumluluk	Tekrarlı Saldırı Direnci	Gerçek Zamanlı Performans
LiBrA-CAN	ok	ok	nok	nok	nok	nok
WooAuth	ok	ok	ok	nok	ok	ok
Vecure	ok	ok	nok	ok	ok	nok
CaCAN	ok	ok	nok	nok	ok	nok
VatiCAN	ok	ok	nok	ok	ok	nok
VulCAN	ok	ok	nok	ok	ok	nok

- Kimlik Doğrulama: Kimlik doğrulama, veri mesajı ve ardından bir kimlik doğrulama mesajı gönderilerek gerçekleştirilir. Kimlik doğrulama mesajı şifreleme fonksiyonu ve gizli bir anahtar içeren mesaj doğrulama kodudur. Çizelge 1'deki tüm şifreleme yöntemleri HMAC ve MAC kimlik doğrulama türü kullandığı için hepsi kimlik doğrulama ilkesini sağlar.

- Bütünlük: Bütünlük, verilerin doğruluğu ve geçerliliği olarak tanımlanır. HMAC ve MAC sadece kimlik doğrulama değil aynı zamanda veri bütünlüğünü kontrol etmek içinde kullanılır. Çizelge 1'deki tüm şifreleme yöntemleri HMAC ve MAC kimlik doğrulama türü kullandığı için hepsi bütünlük ilkesini sağlar.

- Gizlilik: Gizlilik, verilerin yalnızca yetkili kişilere sağlanması anlamına gelir. Çizelge 1'de sadece WooAuth (WOO ve ark., 2014) şifreleme yöntemi veri iletiminde AES-128 şifreleme kullandığı için gizlilik ilkesini sağlar.

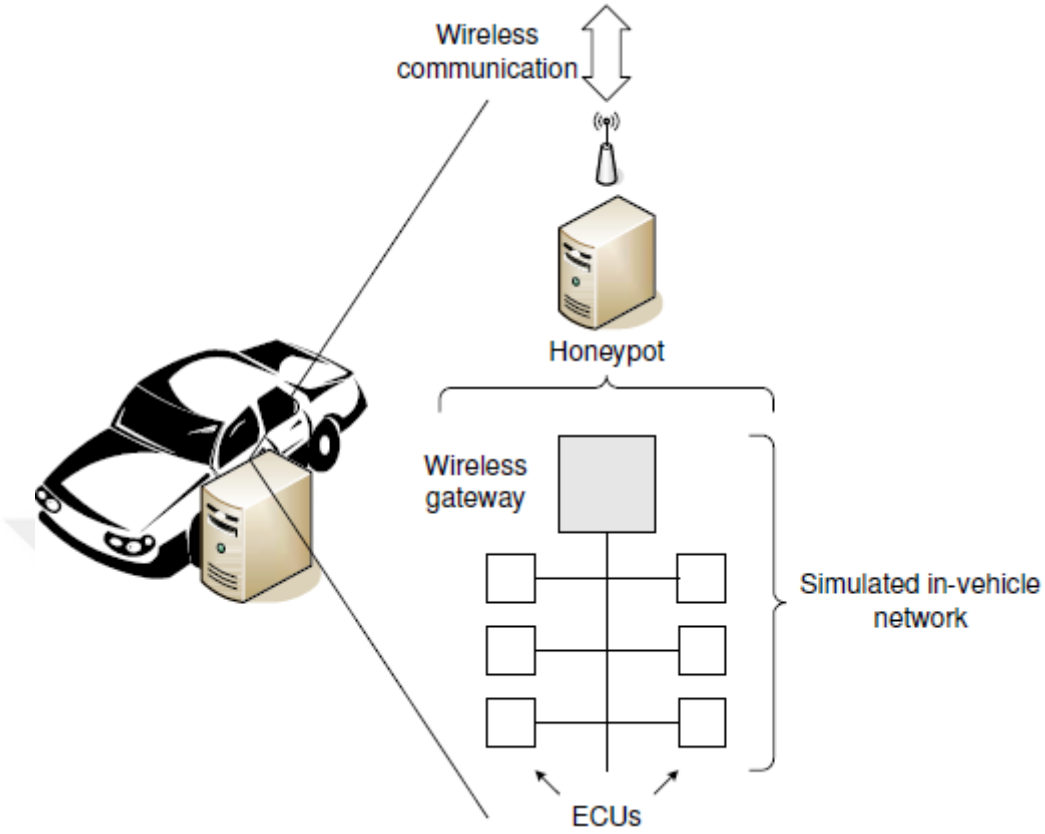
- Geriye Uyumluluk: CAN protokolünün doğal çerçeve yapısının bozulmamasıdır. Çizelge 1'deki, Vecure (WANG ve SAWHNEY, 2014) VatiCAN (NURNBERGER ve ROSSOW, 2016) ve VulCAN (BULCK ve

ark., 2017) şifreleme yöntemleri kimlik doğrulama verilerini kullanırken CAN veri çerçevelerini bozmadıkları için geriye uyumluluk ilkesini sağlarlar.

- Tekrarlı Saldırı Direnci: CAN protokolünde geçerli bir kontrol veri çerçevesinin, saldırgan tarafından yeniden iletilmesine tekrarlı saldırı denir. Buna karşı konulan dirence de tekrarlı saldırı direnci denir. Çizelge 1'de sadece LiBrA-CAN (GROZA ve ark., 2012) şifreleme yöntemi hariç hepsi tekrarlı saldırı direnci ilkesini sağlar.
- Gerçek Zamanlı Performans: CAN protokolünün veri iletişim hızı gerçek zamanlı olarak çalışır. Çizelge 1'de sadece WooAuth (WOO ve ark., 2014) şifreleme yöntemi gecikmelere sebep olmayarak gerçek zamanlı performans ilkesini sağlar.

Genel olarak Çizelge 1 incelendiğinde şifreleme yöntemlerinin CAN veri yolunun güvenliğini, kimlik doğrulama ve bütünlük ilkeleriyle artırıyor. Ama aynı çizelgede şifreleme yöntemlerinin çoğu, gizlilik ilkesinde bir şey yapamazken gerçek zamanlı uygulamalarda da gecikmelere sebebiyet veriyor. CAN protokolünde sınırlı bant genişliğini göz önüne alırsak şifreleme yöntemlerinin bir diğer kötü özelliği de kimlik doğrulama kullanarak CAN veri trafiğini iki katına çıkarmasıdır.

CAN veri yoluna yapılan saldırıların durdurulamayıp ama şaşırtıp rapor eden bir diğer teknik ise honeypotdur. Honeypot'un amacı, korsanları gerçek bir araçla etkileşime girdiklerine inandırıp onların saldırılarını üzerine çekmektir. D. Nilsson ve Larson Şekil 2'de görüldüğü gibi honeypot donanımının diğer araç içi ağlardan izole edildiği kablosuz bir ağ ile başka bir honeypot cihazına bağlanmasını önermektedir (NILSSON ve LARSON, 2009). Bu ağ araç içi ağ gibi davranan bir şaşırtma ağı olarak çalışır. Bu saya de korsanlar gerçek araç içi ağa bağlandıklarını düşünür ve saldırılarda bulunur. Sonuç olarak honeypot saldırı eğilimleri, saldırı davranışı ve saldırı teknikleri hakkında bilgi sağlayan verileri toplamak için kullanılabilir.



Şekil 2 Araç içi ağ gibi davranan kablosuz ağ geçidine sahip honeypot (NILSSON ve LARSON, 2009).

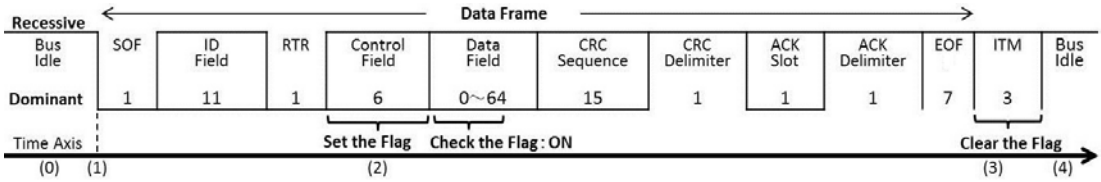
Şifreleme yöntemlerinin olumsuz özelliklerinden CAN veri yolunun gerçek zamanlı performansının düşmesi ve veri trafiğinin artması, saldırı tespit ve önleme sistemlerinin (IDS / IPS) araştırılmasına yol açar. CAN ağındaki artan mesaj sıklığı, mesaj kimliklerinin bariz şekilde kötüye kullanılması ve düşük seviyeli iletişim kalıpların kullanılması gibi anormal davranışlar saldırı tespit sistemleri ile belirlenebilir. Yine bu konuda tecrübeli olan Hoppe ve arkadaşları CAN veri yolunda korsan mesajları tespit etmek için kurdukları saldırı tespit sisteminde mesajların frekanslarına bakarak ayırt etmeyi öneriyor (HOPPE ve ark., 2009). Çizelge 2'de de görüldüğü üzere sistemlerinde belirledikleri zaman damgaları dışındaki mesajlar korsan mesajı olarak belirlenmiştir. Sonuç olarak CAN veri yolunda normal mesajların arasından bu korsan mesajları ayırarak çizelge haline getirmişlerdir.

Çizelge 2 CAN veri yoluna saldırı sırasında kaydedilen normal ve korsan mesajlar (HOPPE ve ark., 2009).

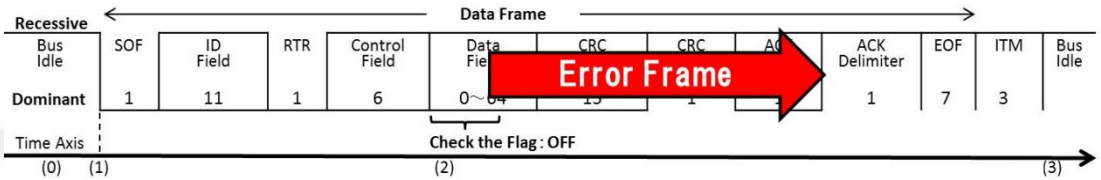
Zaman Damgası (ms)	ID (hex)	Veri (hex)	Yorum
121.038	395	8	Signal off (normal)
121.088	395	8	Signal off (normal)
121.098	395	88	Signal on (normal)
121.100	395	8	Signal off (korsan)
121.149	395	88	Signal on (normal)
121.152	395	8	Signal off (korsan)
121.198	395	88	Signal on (normal)
121.201	395	8	Signal off (korsan)
121.249	395	88	Signal on (normal)
121.252	395	8	Signal off (korsan)
121.298	395	88	Signal on (normal)
121.300	395	8	Signal off (korsan)
121.349	395	88	Signal on (normal)
121.352	395	8	Signal off (korsan)
121.398	395	88	Signal on (normal)
121.401	395	8	Signal off (korsan)
121.449	395	88	Signal on (normal)
121.452	395	8	Signal off (korsan)
121.498	395	88	Signal on (normal)
121.500	395	8	Signal off (korsan)
121.508	395	88	Signal off (normal)
121.558	395	8	Signal off (normal)

CAN veri yolu güvenliğini sağlamak için Matsumoto ve arkadaşları kendi geliştirdikleri IPS sistemini kullanmışlardır. Bu yöntem hem saldırı tespit ediyor hem da saldırıyı önlüyor (MATSUMOTO ve ark., 2012). Bu çalışma her elektronik kontrol ünitesinin ağ trafiğini izlemesini önermektedir. Matsumoto ve arkadaşları bir mesajın yetkilendirilip yetkilendirilmediğini belirlemek için CAN kimliği alanının kullanımına dayanan nispeten basit bir plan benimsemiştir. CAN denetleyicisi iletinin kimlik alanını kontrol eder ve kimliğin kendisine ait olduğunu algılar ancak iletiyi göndermediğini bilirse bir hata çerçevesi yayınlar. Yani veri yolunda iletinin kimliğine bağlı olarak olması gereken (Şekil 3) dışında bir mesaj gözlemlediğinde,

elektronik kontrol ünitesi iletilen mesajı Şekil 4‘deki gibi geçersiz kılmak için veri yoluna hemen hata mesajı gönderir.



Şekil 3 Tanımlı ECU’nun örnek veri çerçevesi (MATSUMOTO ve ark., 2012)



Şekil 4 Korsan ECU’nun örnek veri çerçevesi (MATSUMOTO ve ark., 2012)

II. DENETLEYİCİ ALAN AĞI (CAN) PROTOKOLÜ

CAN protokolü 1983 yılında otomotiv sektöründe kullanılmak üzere Robert Bosch tarafından geliştirilmeye başlanmıştır. Daha sonrasında Bosch firması tarafından 1986 yılında otomotiv topluluğuna duyurmuştur. Sonuç olarak CAN haberleşmesiyle birlikte otomobillerde merkezi ağ sistemine geçilmiştir. Intel tarafından 1987'de ilk CAN denetleyici yongası üretilmiştir. Başlangıçta yalnızca otomotiv sektöründe kullanılmaya başlanmıştır. Bu haberleşme ağı doğası gereği az yer kaplaması, güvenli olması ve yüksek hıza sahip olması gibi özelliklerinden dolayı daha sonrasında fabrika otomasyonunda, tıp elektroniğinde, tarım aletlerinde, asansör sistemlerinde, bina otomasyonlarında ve askeri uygulamalarda yaygın olarak kullanılmaya başlamıştır. CAN haberleşmesinin genel karakteristik özellikleri Çizelge 3'de gösterilmiştir (URL-10).

Çizelge 3 CAN haberleşmesi genel karakteristik (URL-10)

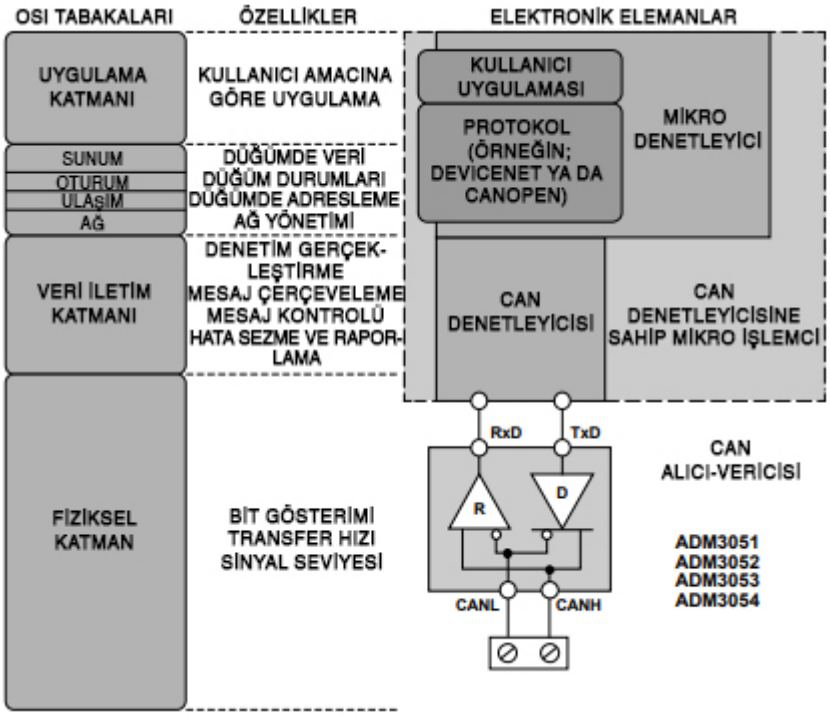
İletişim Protokolü	İletişim Standardı	İletişim Tekniği	İletim Metodu	Haberleşme Hattı	Topoloji	Kontrol Tipi	Ortam Erişim Kontrol Metodu	İletim Ortamı	Maksimum Haberleşme Hızı
Seri İletişim	ISO 11898 ve ISO 11519	Yayın	Temel Bant	LAN	Bus Topolojisi	Dağıtık Kontrol	Multi Master	Çift Tel	1 Mbit/s

A. CAN Protokol Mimarisi

CAN ağı Bosch tarafından ISO 11898 ve ISO 11519 olarak standartlaştırılmıştır. Denetleyici alan ağı (CAN), karayolu taşıtları ve diğer kontrol uygulamalarında kullanılmak üzere yaratılmıştır. Gerçek zamanlı kontrolü ve çoklu

uygulamaları destekleyen bir seri iletişim protokolüdür. Ağın genel mimarisi OSI referans modelinde hiyerarşik katmanlar şeklinde tanımlanmıştır. (Şekil 5) CAN, tasarım saydamlığı ve gerçekleme esnekliğini sağlamak için 3 katmandan oluşur (URL-9).

- Fiziksel Katman: Tipik olarak bükümlü çift kablo ile CANH ve CANL hatları üzerinden iletilen diferansiyel verileri (iki veri hattı arasındaki voltaj farkının mantıksal 1 veya 0 olması) çeviren elektriksel mantık katmanıdır. Bu katmanda bit gösterimi, transfer hızı, sinyal seviyesi ve iletim ortamı gibi görevler mevcuttur.
- Veri İletim Katmanı: ISO 11898 standardına uyan CAN denetleyicisi, veri iletim katmanı olarak değerlendirilebilir. Bu katmanda mesaj kontrolü, hata sezme ve raporlama, mesaj çerçeveleme ve denetim gerçekleştirme gibi görevler mevcuttur. Standart veridir.
- Uygulama Katmanı: CAN protokolünde yazılım ile donanım arasında bulunan katmandır. Yazılım verilerini CAN mesajlarına CAN mesajlarını da yazılım verilerine çeviren katmandır.



Şekil 5 ISO 11898 standardına göre CAN mimarisi (URL-9).

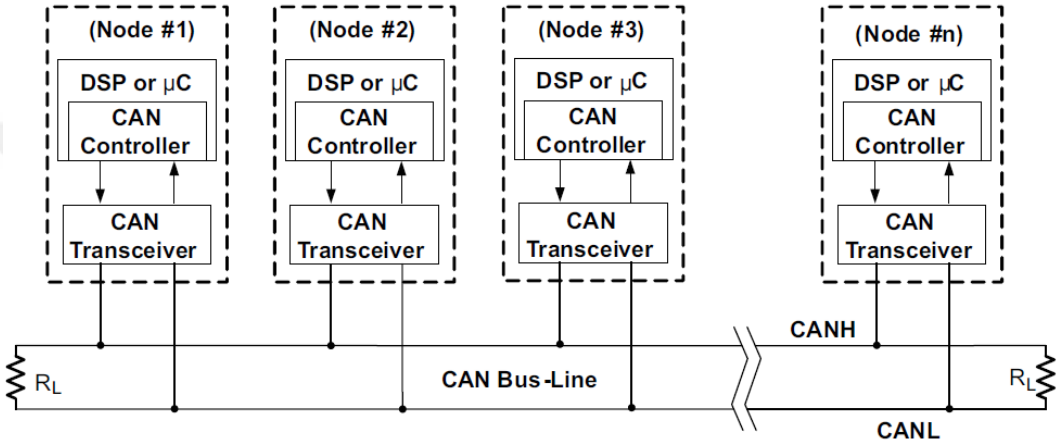
B. CAN Düğüm Yapısı ve Çalışma Mantığı

CAN, haberleşme için bükümlü çift kablonun iki kablo arasındaki voltaj farklarını kullanır. Her düğüm, voltaj farkını ayarlayarak veriyi sinyal olarak iletir ve aynı zamanda bir voltaj farkını tespit ederek veriyi alır. Veriler baskın ve çekinik sinyaller olarak ikiye ayrılır. Bunlar sırasıyla mantıksal 0 ve mantıksal 1'e karşılık gelir. Baskın, iki tel arasındaki voltaj farkının büyük olduğu durumdur. Resesif, iki tel arasındaki voltaj farkının küçük olduğu durumdur.

CAN ağında haberleşme veri yoluna bağlı olan düğümler arasında gerçekleşir. Bu düğümler bu haberleşmeyi yapabilmesi için 3 temel elemandan oluşur. Bunlar sırasıyla mikro denetleyici, CAN denetleyicisi ve CAN alıcı vericisidir (URL-5).

Şekil 6'da görüldüğü üzere ağ topolojisi tek bir çift bükümlü kablo hattından oluşur. CAN alıcı vericisi bu iki kablo arasındaki voltaj farkını değiştirir ya da voltaj

farkını tespit eder ve CAN denetleyicisine iletir. CAN denetleyicisi de bu voltaj farkını anlamlandırır mikro denetleyiciye iletir ya da mikro denetleyiciden gelen komutu CAN alıcı vericisine iletir. İletişim sırayla çift bükümlü kablo, CAN alıcı verici, CAN denetleyicisi ve mikro denetleyici arasında çift taraflı olarak sağlanır. Ayrıca ISO 11898 standardı gereği sinyal yansımalarını önlemek için hattın karakteristik empedansı 60 Ohm olması gereklidir. Bu yüzden her iki uçtaki RL dirençlerinin değeri 120 Ohm seçilir.



Şekil 6 CAN haberleşmesi örnek düğüm yapısı (URL-5)

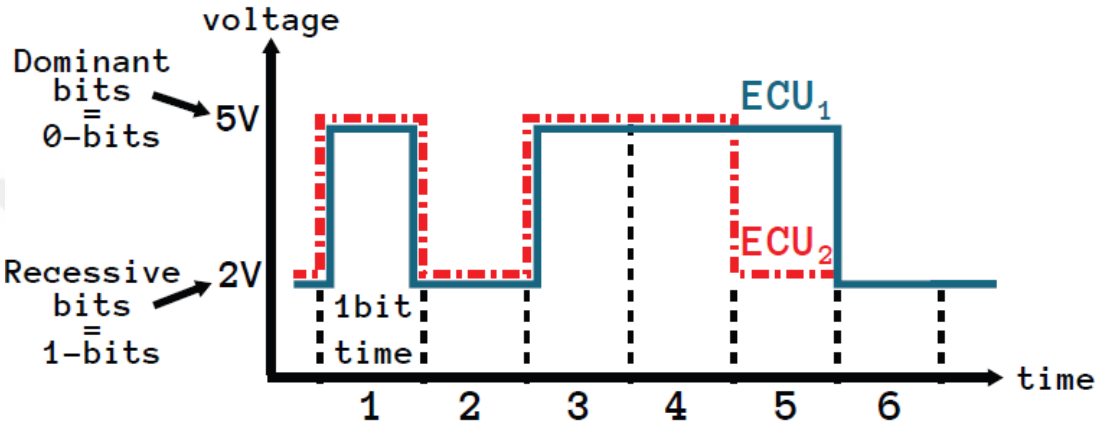
C. CAN Protokolünün Başlıca Çalışma Özellikleri

CAN haberleşme protokolünün kendine has birçok özelliği vardır. Bu özellikler haberleşmede kullanıcıya kolaylık sağlamasıyla birlikte ayrıca veri yolunda bazı güvenlik açıklarına da neden olurlar. CAN haberleşme protokolünün bazı çalışma özellikleri şunlardır:

1. Çoklu Yönetici

CAN ağına bağlı olan tüm düğümlerin veri yolu boştayken veri gönderebilme özelliğine çoklu yönetici özelliği denir. Yani CAN protokolü tarafından, düğümlerden herhangi birisi diğerlerine kıyasen önce veri gönderdiğinde verisi kesin olarak gönderileceği garanti edilir. CAN protokolü iki düğüm, veri yoluna aynı anda

veri göndermeye çalışırsa, küçük ID ye sahip verinin iletileceğini söyler. Yani CSMA / CA (çoklu erişimde hat kontrolü) mekanizmasını uygular. Bu durumda iki düğümünde veri bitleri Şekil 7'deki gibi tek tek kıyaslanır ve baskın olan önce gönderilir. Protokol gereği bitler arasında mantıksal 0 baskın iken mantıksal 1 resesiftir. Verisi iletilemeyen diğer düğüm dinleme durumuna geçer ve veri yolu boşaldığında verisini gönderir (URL-5).



Şekil 7 CAN haberleşmesinde CSMA / CA özelliğinin örnek gösterimi (BOUDGUIGA ve ark., 2016)

2. Veri Alış-Verişi

CAN ağında protokol gereği veri çerçevelerinin içinde gönderici ya da alıcı adresleri yoktur. Onun yerine veri içeriğini tanımlayan bir tanımlayıcı alan kullanılır. Alıcı düğüm bu tanımlayıcı alana bakarak verinin kendisine gelip gelmediğini anlar. Verinin kimden geldiğinin bir önemi yoktur (YAVUZ ve ark., 2018).

3. Sistem Esnekliği

CAN ağına bağlı olan düğümler herhangi bir adres gibi belirtici ID ye sahip değillerdir. Bu yüzden, kullanıcı veri yoluna başka bir düğüm ekleyip ya da çıkarmak istediğinde herhangi bir yazılım değişimine gerek duymaz. Ayrıca kullanıcı diğer düğümlerin donanımlarında da bir değişiklik yapmak zorunda kalmaz. Sonuç olarak

protokol kullanıcıya daha önceden tasarladığı sistemin kolaylıkla genişletme esnekliğine olanak sağlar (URL-2).

4. Haberleşme Hızı

CAN ağında veri yolunun uzunluğuna göre Çizelge 4'de gösterildiği gibi haberleşme hızı seçilmelidir. Aynı veri yolunda bulunan tüm düğümler aynı haberleşme hızı ile veri yoluna bağlanabilirler. Eğer düğümlerden biri farklı haberleşme hızı kullanırsa, diğer düğümlerden herhangi biri farklı haberleşme hızı kullanan düğüm için veri yoluna hata mesajı gönderir. Bu hata mesajı aynı hızı kullanan diğer düğümlere iletilmez (URL-10).

Çizelge 4 CAN haberleşme hızının mesafeye göre değişimi (URL-10)

Ağ Uzunluğu (m)	Maksimum Hız (bps)
40	1M
100	500k
200	250k
500	125k
6000	10k

5. Veri İsteği Oluşturma

CAN ağındaki herhangi bir düğüm veri almak istediğinde veri isteği çerçevesi oluşturabilir. Eğer veri isteğinde bulunduğu düğüm aktifse bu veri isteğine cevap verir (URL-2).

6. Hata Mesajı Gönderme

CAN ağına bağlı her düğüm hata belirleme özelliğine sahiptir. Hatayı belirleyen herhangi bir düğüm bunu diğer düğümlere iletebilir. Eğer bir düğüm veri gönderirken bir hata belirlerse, veri alış-verişini durdurmaya zorlayabilir ya da diğer düğümleri haberdar edebilir (URL-2).

D. CAN Protokolünün Çerçeve Tipleri

CAN ağında bir ECU'dan gelen verilerin başka bir ECU ile paylaşılması gerektiğinde, ECU'daki gömülü mikro denetleyicisi verileri CAN denetleyicisine gönderir. CAN denetleyicisi de verileri işleyerek çerçeve haline getirir ve çerçeve haline gelmiş CAN mesajlarını veri yolu üzerinden gönderir. CAN ağına bağlı tüm düğümler bütün mesajları algılayabilir. Eğer isterse CAN denetleyicisi donanımında yerel bir filtreleme yapabilir. Sonuç olarak bütün düğümler CAN denetleyicilerini kullanarak sadece ilgilendikleri mesajları kabul edebilirler. CAN ağı protokolü içerisinde 4 farklı mesaj çerçevesi tipi bulunur (URL-5).

1. Veri Çerçevesi

Veri çerçevesi CAN ağında veri iletimi için kullanılan tek çerçevedir. CAN ağında bulunan düğümler veri çerçevelerini ileterek diğer düğümlerle haberleşirler. Veri çerçevesinin standart ve genişletilmiş biçim olmak üzere iki farklı biçimi vardır. Bu veri çerçeveleri arasındaki tek fark, denetim alanlarının uzunluğudur. Veri çerçevesi, kullanıcı verisinden başka veri akışını senkronize etmek, tanımlamak ve kontrol etmek için bilgi içerir (URL-5).

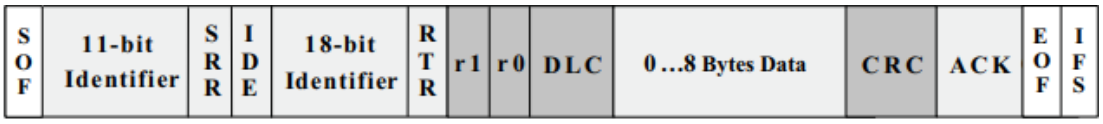
a. Standart Format Çerçevesi

Standart format olarak ta bilinen bu formatta veri yolunda 2048 adet ID ayarlanabilir. Standart format çerçevesinin tanımlayıcısı Şekil 8'de görüldüğü üzere 11 bit uzunluğunda olduğundan 2048 tür mesaj işlenebilir.

Şekil 8 CAN haberleşmesi standart format veri çerçevesi (URL-5)

b. Genişletilmiş Format Çerçevesi

Genişletilmiş format olarak ta bilinen bu formatta veri yolunda 5,3 milyon adet ID ayarlanabilir. Genişletilmiş format çerçevesinin tanımlayıcısı 29 bit uzunluğunda olduğundan 446464 tür mesaj işlenebilir. Genişletilmiş formatı standart formattan ayıran tek durum veri yolundaki ID sayısıdır. Ayrıca çerçeve alanındaki SRR ve IDE bitleri resesif (mantıksal seviye 1) ise, çerçeve genişletilmiş biçimde gönderilir. (Şekil 9)



Şekil 9 CAN haberleşmesi genişletilmiş format veri çerçevesi (URL-5)

c. Veri Çerçevesi Alanları

Şekil 8 ve Şekil 9'da gösterilen veri çerçeveleri içinde gösterilen her biri farklı uzunluklarda olan 7 alandan oluşur (URL-9).

- Çerçeve Başlangıcı (SOF): 1 bit boyutunda ve dominanttır. İsminden de anlaşılacağı üzere CAN haberleşme mesajının başlangıcını belirtir.
- Denetim Alanı: Bu alan 11 ya da 29 bitlik tanıtıcı (ID) alanı ve 1 bitlik uzak iletim isteği (RTR) alanından oluşur. Toplam 12 ya da 32 bitten oluşur. Tanıtıcı alan mesajın kimliğini belirtirken uzak iletim isteği ise istek varlığını belirtir.
- Kontrol Alanı: Bu alan 1 bit tanıtıcı uzantı alanı (IDE), 1 bitlik r0 alanı ve 4 bitlik veri uzunluk kodu (DLC) alanından oluşur. Toplam 6 bitten oluşur. Tanıtıcı uzantı alanı çerçeve format tipini belirtirken veri uzunluk kodu ise gönderilecek verinin uzunluğunu belirtir.
- Veri Alanı: Bu alan DLC değerine bağlı olarak sıfır ile sekiz bayt arasında değişen uzunluğa sahiptir. Alıcıların haberleşmede anlamlandırılması gereken alandır.
- Çevrimli Fazlalık Kontrol Alanı (CRC): Bu alan 15 bit CRC dizisi ve 1 bitlik baskın seviyeli CRC belirticiden oluşur. Bu alan başlangıç biti, denetim alanı,

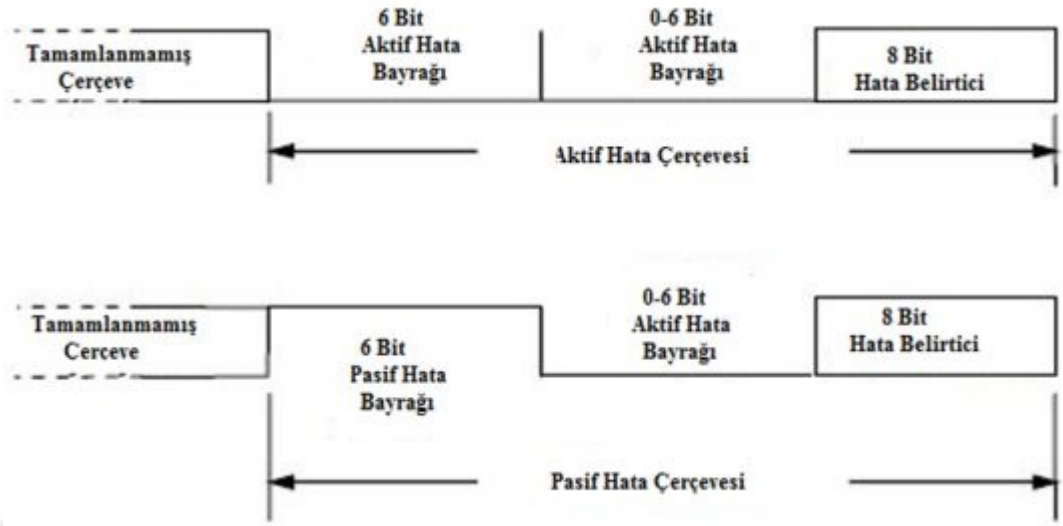
kontrol alanı, veri alanı ve CRC alanlarını bir arada hesaplayarak bir kontrol kodu oluşturur.

- Onay Alanı (ACK): Bu alan 1 bitlik ACK sıra ve 1 bitlik ACK belirtici alanından oluşur. Bu alan mesajın alınıp alınmadığını ve herhangi bir hatanın sezilip sezilmediği hakkında gönderici düğümü bilgilendirir.
- Çerçeve Sonu (EOF): Bu alan ACK alanından sonra veri ve istek çerçevelerinin tamamlandığını gösteren yedi adet resesif bit den oluşur.
- Çerçeveler Arası Boşluk (IFS): Bu alan resesif 3 bit den oluşur. Haberleşmede mesaj iletimi kontrol etmek ve eş güdümlü çalışmayı sağlamak için çerçeveler arası boşluk gereklidir. Eğer bu boşluklar olmazsa hata çerçeveleri veya aşırı yük çerçeveleri, çerçeve sonu belirtecinden hemen sonra başlayabilir. IFS den sonra veri yolu yeni bir iletime kadar boş durumdadır.

2. Hata Çerçevesi

CAN veri yolundaki düğümlerden herhangi biri mesaj gönderme veya mesaj alma sırasında CAN ağında tanımlı 5 hatadan birini tespit edip hata çerçevesi yayınlayabilir. Hata çerçevesi iki alandan oluşmaktadır. Bu alanlardan birincisi hata bayrakları ikincisi hata ayracı alanıdır. Hata bayrakları aktif ve pasif olmak üzere iki çeşittir (URL-2).

Şekil 10'da görüldüğü üzere aktif hata ile pasif hata arasında ilk 6 bitin resesif ya da baskın olması farkı vardır. Protokol gereği daha öncede söylendiği üzere bitler arasında mantıksal 0 baskın iken mantıksal 1 resesiftir. Bu yüzden aktif hata çerçevesi pasif hata çerçevesine göre baskındır. Pasif hata çerçevesi hattı meşgul etmezken aktif hata çerçevesi hattı meşgul eder ve veri iletişimini durdurur.



Şekil 10 CAN haberleşmesi aktif ve pasif hata çerçeveleri (URL-1)

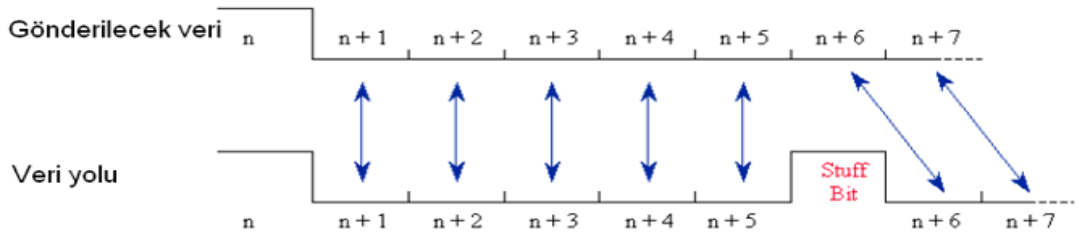
a. Tanımlı Hata Türleri

CAN protokolü, veri yolundaki tanımlı hataları algılamak için hata algılama mekanizması kullanır. CAN protokolünde beş adet hata türü vardır. Hata türlerinden 3 tanesi çerçeve düzeyinde 2 tanesi ise bit düzeyindedir (URL-8).

- Çerçeve Kontrolü: Alıcının oluşturduğu bir hata türüdür**.** CAN ağında herhangi bir düğüm verisini veri yoluna gönderdikten sonra alıcı düğüm veriyi alır ve verinin formatını kontrol eder. Yani aldığı verinin formatı olağan çerçeve yapısı ile uyumlu olup olmadığını karşılaştırır. Alınan veride eksik alan varsa veri reddedilir ve veri yoluna hata çerçevesi bırakır. Bu sistem doğru formatta veri alımını sağlar.
- CRC Kontrolü: Alıcının oluşturduğu bir hata türüdür. CAN ağında SOF bitinden CRC bitlerinin başına kadar olan bitler bir takım işlemlerden geçirilerek CRC kodu üretilir. Alıcı düğüm veriyi aldıktan sonra aldığı CRC kodu ve alınan veriden üretilen CRC kodunu karşılaştırır. Bu şekilde alınan bitlerin doğru olup olmadığı sınanır. Format kontrolünden sonra alıcının

bitleri kontrol etmesi ile formata uyan fakat hatalı mesajların önüne geçilmiş olur.

- ACK Kontrolü: Vericinin oluşturduğu bir hata türüdür. ACK bitinin anlamı alınan mesajı alıcının onaylamasıdır. Gönderici CRC bitlerini gönderdikten sonra ACK bitini resesif olarak gönderir. Alıcılardan en az bir tanesinin hattaki resesif olan ACK bitini dominant bitle ezmesi beklenir. Eğer zaman aşımı sonucu ACK biti göndericiye ulaşmamışsa ACK bitinde hata olduğu şeklinde yorumlanır. Bunun sonucu göndericide hata oluşur ve ACK onayını alana kadar aynı mesajı tekrar gönderir. Sonuç olarak gönderilip alınmayan iletinin önüne geçilir.
- Bit Kontrolü: Vericinin oluşturduğu bir hata türüdür. CAN ağında veri yolu boşaldığında düğümler mesaj göndermek için veri yolunu mesajların ID durumlarına göre ele geçirir. Her düğüm veri yoluna yazdığı biti tekrar geri okuyarak kendisinin gönderdiğinden daha önemli bir mesaj var mı diye bakar. Eğer daha önemli mesaj varsa geri çekilerek veri yolunun boş olmasını bekler. Böylece veri yolunu bir düğüm kazanmış olur ve bitleri göndermeye devam eder. Aynı zamanda gönderdiği bitleri geri okur. Eğer veri yolunu kazanan düğüm gönderdiği seviyeden farklı bir seviye okursa hata oluşturur.
- Bit İstifleme: Gönderici ile alıcı arasında saat darbeleri gönderilmez. Bunun yerine veri yolundaki CANL ve CANH hatlarındaki lojik değişimler ile eş güdümlü çalışması sağlanır. Bunun sonucu olarak aynı lojik seviyeden (dominant) 5 ten fazla bitin art arda gelmesi eş güdümlü çalışmayı bozduğu anlamına gelir ve alıcıda hataya sebebiyet verir. Bunu engellemek Şekil 11'de gösterildiği gibi gönderici aynı 5 seviyeden sonra karşı seviyeden bir bit göndererek iletişime devam eder. Bunun sonucu olarak herhangi bir düğüm herhangi bir anda hata mesajı oluşturmak istediğinde veri yoluna 6 adet dominant bit yazar ve hataya sebebiyet verir.



Şekil 3 CAN haberleşmesi bit istifleme hata türü (URL-1)

b. Hata Sınırlandırma Mekanizması

CAN protokolü fiziksel hatalara karşı dayanıklıdır. Protokol içerisindeki hata sınırlandırma mekanizması (ECM) ile hatalı düğümler veri yolu trafiğinden kaldırabilir Yani CAN donanımı oluşan hatalara göre hata durumları arasında geçiş yapabilmektedir. CAN donanımı içerisinde iki adet hata sayıcısı vardır. Bunlar gönderme hata sayacı ve alma hata sayacıdır. Herhangi bir sayaç 127 ve büyük bir değere ulaşırsa donanım pasif hata durumuna girer. Yani diğer düğümlerin hatalarını duyar fakat oluşturduğu hata hiçbir düğüm tarafından duyulmaz. Eğer gönderim hata sayısı 255 i geçerse donanım kapanır ve hattaki iletişime karışmaz ve etkilenmez. Bu mekanizmalar düğüm hatalı duruma düştüğünde art arda hata mesajları göndererek veri yolunu meşgul etmesini önlemek içindir (URL-2).

3. İstek Çerçevesi

CAN ağında bir düğüm başka bir düğümden veri isteğinde bu çerçeveyi kullanır. İstek çerçevesi ile veri çerçevesinin arasında 2 farklılık vardır. Birincisi istek çerçevelerinde RTR biti resesifken (mantıksal seviye 1) veri çerçevesinin RTR biti baskındır (mantıksal seviye 0). İkincisi istek çerçevelerinin veri alanı yokken veri çerçevesinin veri alanı vardır (URL-2).

4. Aşırı Yük Çerçevesi

Denetleyici alan ağında aşırı yük çerçevesi, Şekil 12'de gösterildiği gibi hata çerçevesine çok benzer ve bir alıcı düğüm çok meşgul olduğunda veri yoluna

gönderilir. Bu çerçeve ile alıcı düğüm bir sonraki iletimin başlamasını geciktirmek ister. Aşırı yük çerçevesi ile aktif hata çerçevesi hemen hemen aynıdır. Aşırı yük çerçevesini aktif hata çerçevesinden ayıran fark, bu çerçevenin çerçeve sonu ya da IFS alanından sonra başlamasıdır (URL-2).

Şekil 4 CAN haberleşmesi aşırı yük çerçevesi (URL-1)

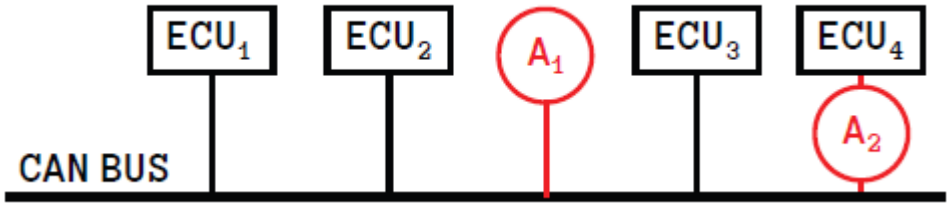
E. CAN Protokolünde Güvenlik Açıklarının Analizi

Bu bölümde CAN protokolü CIA (Gizlilik, Bütünlük ve Kullanılabilirlik) üçlüsüne göre analiz edilecektir. CIA üçlüsü, sistem güvenlik açığını değerlendirmek için basit bir güvenlik modelidir. CIA üçlüsü, herhangi bir güvenli sistemin sahip olması gereken üç temel ilkeyi analiz eder (BOZDAL ve ark., 2018). CAN haberleşme ağı her ne kadar güvenli bir ağ olsa bile yine protokol içerisinde mevcut güvenlik açıkları vardır (KOSCHER ve ark., 2010). Bu güvenlik açıkları, korsanlar tarafından kasıtlı ve akıllı bir şekilde uygulandığında zarar ve zararlara yol açabilir.

- Mesaj Alış-Veriş Doğası: Gizlilik, verilerin yalnızca yetkili kişilere sağlanması anlamına gelir. Ancak CAN veri yolunda bir düğüm tarafından gönderilen CAN mesajı, veri yoluna bağlı tüm düğümler tarafından alınır. Böylece, Şekil 13'de ki A1 veya A2 gibi bağlanan bir korsan ağ trafiğindeki veri çerçevelerini kolayca okuyabilir. Sonuç olarak CAN veri yolunda gizlilik söz konusu değildir.
- Kimlik Doğrulama Yok: CAN veri çerçevelerinin kimlik doğrulayıcı alanları yoktur. Böylece, veri yoluna Şekil 13'de ki A2 gibi bağlanan bir korsan

herhangi bir düğümün kimliğini kullanarak sahte bir mesaj gönderebilir. Sonuç olarak CAN veri yolunda kimlik doğrulama söz konusu olmadığı için yetkisiz veri iletimi mevcuttur.

- Mesaj Öncelik Doğası: Kullanılabilirlik, verilere veya ağa yetkili kullanıcı tarafından her zaman erişilebileceği anlamına gelir. Ancak CAN protokol gereği, veri yoluna aynı anda veri göndermeye çalışırsa, veri ID si yüksek olan verinin iletileceğini söyler. Böylece, Şekil 13'de ki A1 veya A2 gibi bağlanan bir korsan veri yolunu sürekli baskın bir mesaj göndererek DoS saldırılarına sebebiyet verebilir. Sonuç olarak CAN veri yolunda kullanılabilirlik söz konusu değildir.
- Döngüsel Artıklık Kontrolü (CRC): Bütünlük, verilerin doğruluğu ve geçerliliği olarak tanımlanır. Veri iletim sırasında değiştirilmemelidir. CAN protokolünde, bir mesajın değiştirilip değiştirilmediğini doğrulamak için CRC kullanır. Ancak, bir CRC saldırganın veri çerçevesini değiştirmesini engelleyemez. Sonuç olarak CAN veri yolunda bütünlük de söz konusu değildir.



Şekil 5 CAN haberleşmesinde korsan bağlantı şekilleri (BOUDGUIGA ve ark., 2016)

F. CAN Protokolünde Güvenlik Açıklarından Dolayı Oluşan Saldırılar

Yukarıda yapılan güvenlik analizine ve çıkan güvenlik açıkları göz önüne alındığında CAN ağında saldırılar gizlice dinleme, veri ekleme ve hizmet reddi (DoS) olmak üzere üç gruba ayrılır:

- Gizlice Dinleme: CAN ağını gizlice dinleme birçok saldırının başlangıç noktasıdır. CAN ağında veri mesajları arasında şifreleme eksikliği, herhangi bir düğümün veri yolu trafiğini anlamasına izin verir, böylece bir korsan CAN verilerini okuyabilir ve bilgileri toplayabilir. Gizlice dinleme pasif saldırı olarak sınıflandırılabilir, bu nedenle iletişimi bozmaz. Ancak, aktif saldırılara yol açabilir. Örneğin, Zanero ve arkadaşları bu makalede (ZANERO ve ark., 2017) CAN verilerini okudular ve saldırmayı planladıkları park sensörü düğümünün kimliğini ve verilerini belirlediler. Daha sonrasında bu düğüme bir DoS saldırısı uyguladılar.
- Veri Ekleme: Yetkisiz CAN düğümünün mevcut veri yoluna veri çerçevesi eklenmesi olarak tanımlanabilir. CAN protokolünde bir kimlik doğrulama mekanizması olmadığından, saldırgan bir düğüm ağa bağlanabilir ve istediği düğüme bir veri gönderebilir. Koscher ve arkadaşları bu araştırmada aracın OBD-II portundan CAN ağına sızdılar (KOSCHER ve ark., 2010). Daha sonrasında aracın hayati üniteleri olan gösterge panelini, fren kontrol ünitesini ve motor kontrol ünitesini çözümlediler. Yakıt seviyesini ve hız göstergesi değerlerini değiştirdiler ve gösterge panelinde yanlış veri gösterdiler. Ayrıca motoru devre dışı bırakabildiler ve devir / dakika gibi motor parametrelerini değiştirebildiler.
- Hizmet Reddi (DoS): DoS saldırıları belirli bir düğümü, düğümleri veya tüm ağı hizmet vermesini engelleyen saldırılardır. Palanca ve arkadaşları bu araştırmada ağa gizli bir düğüm ekleyerek seçici DoS saldırısı uyguladılar (ZANERO ve ark., 2017). Saldırgan düğüm, ağın tanımlı verici düğümünün veri yoluna gönderdiği bir veri çerçevesinin bitlerinin üzerine yazar ve hata çerçevesi oluşturur. CAN protokolünün hata sınırlaması nedeniyle, belirli sayıda hata oluştuktan sonra verici düğümü veri yoluna kapalı durumuna geçer ve artık kullanılamaz. Saldırı yöntemi veri yoluna bağlı herhangi bir düğümü devre dışı bırakabilir.

G. CAN Protokolünde Saldırılara Karşı Kurulan Güvenlik Mekanizması

Güvenlik mekanizması, bir saldırının gerçekleşmesini önlemek için ya da saldırının etkisini en aza indirmek için tasarlanmış önlemlerdir. Otomotiv sistemlerinin karmaşıklığı nedeniyle, tek bir mekanizmanın uygulanması bütün saldırıları engelleyemez. Bu nedenle, riskleri en aza indirmek için son güvenlik mekanizmalarının kullanılmasına dayanan 'derinlemesine savunma' stratejisi benimsenmelidir. Derinlemesine savunma saldırıları ele almak için dört yaklaşım sunar (NILSSON ve LARSON, 2009):

- Önlem: Bir saldırının gerçekleşme olasılığını engellemek için derinlemesine alınmış önlemler zinciridir. Simetrik ve asimetrik şifreleme türleri buna örnektir.
- Hedef Saptırma: Bir saldırganın bir yemle tepki verirken saldırıyı başardığına inanmasına yol açan tekniktir.
- Tespit: Bir saldırganın izinsiz giriş sonrasında veri yoluna izinsiz veri göndermesi ile sistemin normal aktivitesi arasında ayrım yapmasıdır.
- Koruma: Bir saldırganın izinsiz giriş durumu algılanıp hemen otomatik olarak tepki vererek saldırının önlenmesi tekniğidir

CAN ağında derinlemesine güvenlik sağlamak için genellikle araştırmacılar tarafından kullanılan 2 popüler konu, saldırı tespit sistemleri ve şifreleme yöntemleridir. Araştırmacılar CAN ağında bu 2 güvenlik yöntemini kullanılırken hem mevcut güvenlik açıklarını (kimlik doğrulama ve gizlilik eksikliği) çözüm getirirken hem de ağın gerçek zamanlı performansına dikkat ederler

Saldırı tespit sistemleri (IDS) CAN ağında elektronik kontrol üniteleri üzerindeki anormal veya şüpheli etkinlikleri tanımlamak için tasarlanmış sistemlerdir. CAN ağı için birçok tanımlanmış saldırı davranışları vardır. Kullanılan tespit yöntemine bağlı olarak temelde iki tip IDS tekniği vardır (GMIDEN ve ark., 2019). Bunlar senaryo yaklaşımı kullanan ve davranışsal yaklaşımı kullanan

sistemlerdir. Senaryo yaklaşımında, IDS bir saldırı senaryosu için veri tabanı kullanır. Şüpheli davranışları tespit ettiği anda bir uyarı verir. Senaryo yaklaşımı saldırıları çok hassas bir şekilde yönetmeyi mümkün kılar. Ancak senaryo veri tabanı güncellenmezse, IDS sistemi bilinmeyen saldırıları algılayamayabilir. Davranışçı yaklaşımında ise izlenecek sistemin beklenen zamanda veri alış-verişi yapmasında dayanır. Senaryo yaklaşımının aksine, bu yaklaşım saldırıları bilinmese bile tespit edebilir.

Şifreleme yöntemleri, verilerin gizli bir forma dönüştürülmesini içeren yöntemlerdir. Şifreleme yöntemleri, otomotiv sistemleri için gizlilik, bütünlük ve kimlik doğrulama için olası bir çözümdür. Şifreleme yöntemlerinde, simetrik ve asimetrik olmak üzere 2 tip anahtar kullanılır. Simetrik anahtarlar başlangıçta tüm cihazlara dağıtılırlar ve keşfedilmeleri daha kolaydır. Asimetrik anahtarlar ise daha karmaşık bir yapıya sahip olduklarından daha güvenlidir ama eklendiği gömülü sistemin işlem gücü kapasitesini etkiler buda maliyetin artmasına neden olabilir (DIFFIE ve HELLMANN, 1979). Sonuç olarak CAN veri yolunda kimlik doğrulama için sadece şifreleme yöntemleri kullanılırsa bant genişliği ve gerçek zamanlı performans gibi CAN ağının çalışmasında önemli rol oynayan özellikler kötü etkilenmiş olur. Bu nedenle, en güvenli çözüm şifreleme ve IDS den oluşan hibrit bir sistemle elde edilebilir (BOZDAL ve ark., 2018).

1. Kurulan Güvenlik Mekanizmasının Sağlaması Gereken Koşullar

Otomotiv güvenliğini sağlayan sayısız yaklaşımların ortaya koyması gerektiği koşullar vardır. Bu koşullardan bazıları şunlardır (WOLF ve ark., 2007):

- ECU içerisindeki gömülü sistem işlemcilerinin sınırlı bellek kapasiteleri ve işlem güçleri vardır. Bellek kapasitesi yüksek işlemciler de maliyeti artırabilir. Şifreleme yöntemleri ECU'lar için çok yüksek bir hesaplama yükü oluşturabilir. Maliyeti artırmamak için olabildiğince az yer kaplayan basit ama sayısı fazla şifreleme yöntemleri kullanılmalıdır.

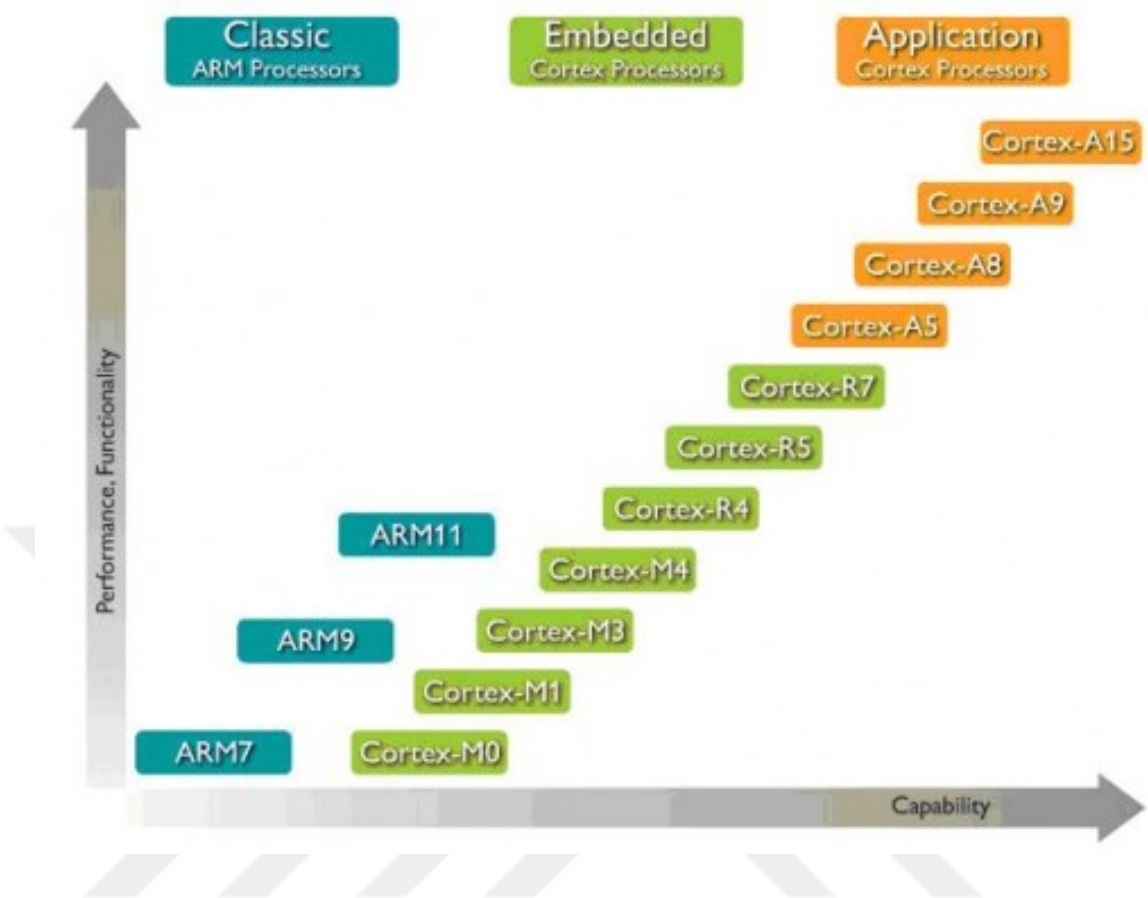
- Mevcut otomobillerin garantileri 10 veya daha fazla yıl olduğundan çözüm dayanıklı ve kalıcı olmalıdır.
- Çözümler mevcut araç içi gömülü sistemlerle uyumlu olmalı ve diğer sistemlerle meşru iletişimi engellememelidir.
- Güvenlik mekanizmaları, taşıt sistemlerinin gerçek zamanlı doğasından ödün vermemelidir, çünkü aracın yolcularının güvenliği büyük önem taşımaktadır.

III. DONANIM

CAN veri yolu ve güvenliğini araştırmak için, CAN veri yolu iletişim davranışlarının değerlendirileceği deneysel bir platform oluşturulması gerekir. Bu bölümde bu platform içerisinde yer alan CAN haberleşmesinde rol oynayan donanımlar ve devre tasarımları, CAN verilerinin gösterilmesinde rol oynayan donanım ve gömülü sistemlerle ilgili donanımlar tanıtılmakta, açıklanmakta ve kurulumları bu bölümde gösterilmektedir.

A. ARM Tabanlı Mikro Denetleyici Kartları

Mikro denetleyiciler, dışarıdan gelen bir veriyi hafızasına alan, derleyen ve sonucunda da çıktı elde eden bir çeşit bilgisayarlardır. Mikro denetleyicilerin yapısında; CPU, RAM, ROM, I/O portları, seri ve paralel portlar, sayıcılar, analog dijital çeviriciler ve çevre birimleri bulunur. ARM tabanlı mikro denetleyiciler ise ARM (Gelişmiş RISC Makineler) firması tarafından geliştirilen RISC (azaltılmış komut seti bilgisayarı) mimarisine dayanan bir CPU ailesidir. ARMv1 ile başlayıp günümüze kadar geliştirilen bu mimari 32 bitlik yapısı sayesinde 8 bitlik işlemcilere göre çok daha hızlıdır. Ayrıca düşük güç tüketimi ve yüksek performansı sayesinde günümüzde yaklaşık %75'lik oranla gömülü sistemler üzerinde en çok kullanılan işlemcilerdir (URL-12). Şekil 14'de de görüldüğü üzere ARM mimarisinin amacına uygun olarak birçok üyesi bulunmaktadır. Klasik ARM işlemciler; ARM7, ARM9 ve ARM11 iken gömülü sistemlere yönelik ARM işlemciler; Cortex-M0, Cortex-M1, Cortex-M3, Cortex-M4 dür. Ayrıca gelişmiş uygulamalar için de ARM işlemciler; Cortex-A5, Cortex-A8, Cortex-A9, Cortex-A15 serileridir.



Şekil 14 ARM mimarisinin işlemci üyeleri

1. Cortex – M Serisi Mikro denetleyiciler

ARM mimarisinin mikro denetleyici ailesinden biri olan Cortex M serisi, piyasada mevcut bulunan 8 ve 16 bitlik mikro denetleyicilere rakip olarak ortaya çıkmış 32 bitlik işlemci mimarisine sahip işlemci serisidir. Çok düşük enerji tüketimlerinin yanı sıra maliyetleri de düşüktür. Bu aileye mensup mikro denetleyiciler endüstriyel kontrol sistemlerinde, beyaz eşyalarda, medikal cihazlarda vb. alanlarda kullanılmaktadırlar. Günümüzde Cortex-M3 serisi mikro denetleyiciler daha yaygın olarak kullanılmaktadır. Bunun nedeni hem daha önce üretilmeleri hem de daha ucuz olmalarıdır. Ancak son olarak tasarlanan M4 serisine eklenen DSP(Digital Signal Process) özelliği gelecekte çok daha etkili işlerin yapılabileceğinin bir göstergesidir (URL-12).

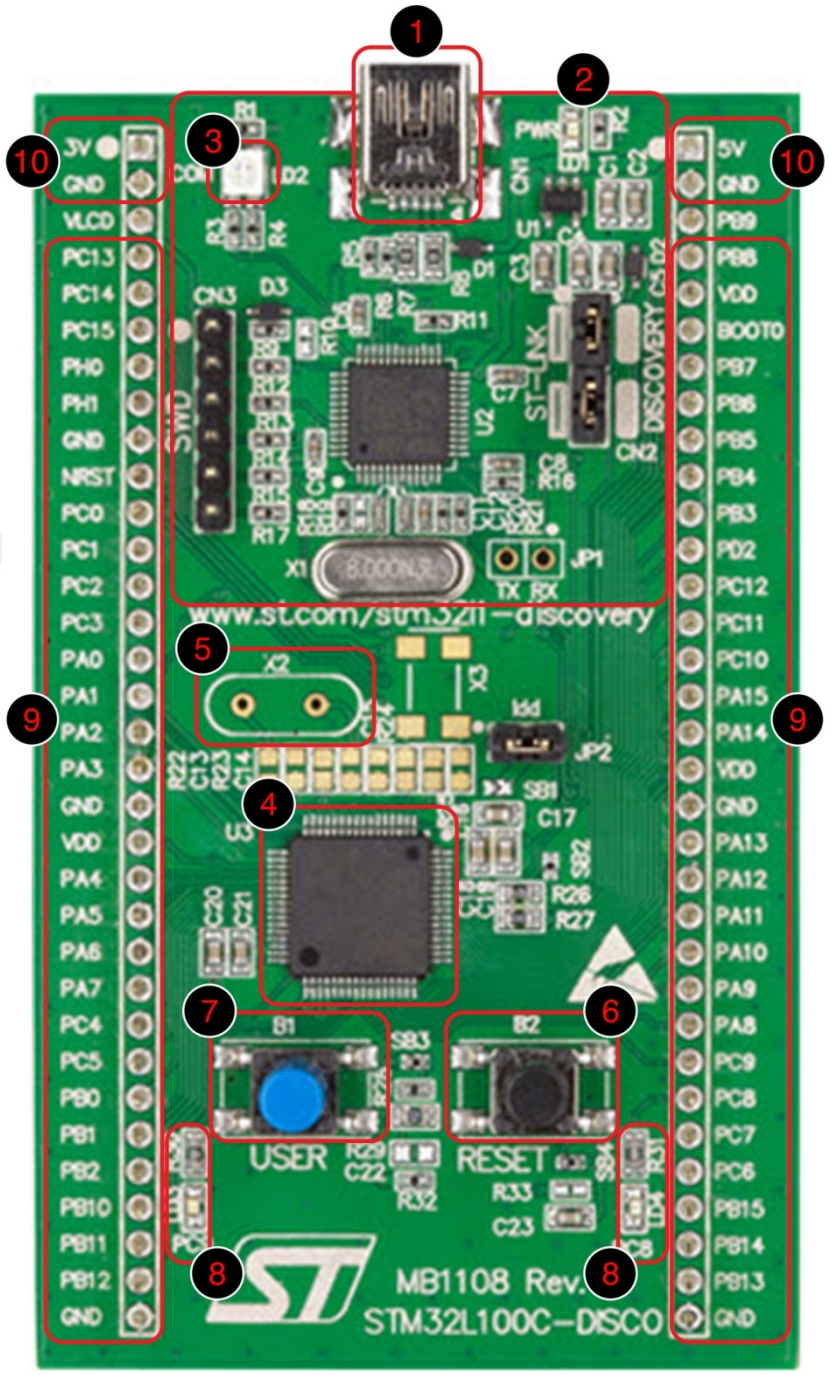
a. STM32F051R8 Mikro Denetleyici Geliştirme Kartı

STM32 mikro denetleyici platformunda birçok çeşit geliştirme kartı vardır. Bu kartların üzerinde mikro denetleyici, güç kaynağı girişi, USB bağlantısı, dijital giriş / çıkış pimleri, analog giriş pimleri, vb. ortak bileşenler bulunur. Bu kartların üzerindeki mikro denetleyiciler ST firmasının amacına uygun olarak geliştirdiği 32 bitlik mikro denetleyicilerdir. Bu mikro denetleyicilerin değişmesi kartın pim sayısını, çevresel birimlerin sayısını, çalışma hızını, bellek miktarını ve diğer teknik özelliklerini de değiştirir. STM32 mikro denetleyici kartlarının analog ve dijital girişleri sayesinde analog ve dijital veriler işlenebilir. Aynı zamanda sensörler ile üzerindeki seri haberleşme birimleri kullanılarak projeler geliştirilebilir. STM32 geliştirme kartı üzerindeki mikro denetleyici C programlama dili ile programlanır ve bu program STM32Cube IDE yardımı ile geliştirme kartına yüklenebilir (URL-11).

STM32F0 Discovery kartı, üzerinde STM32F051R8 mikro denetleyici yongasını içeren STM32 platformunun en yaygın olarak kullanılan mikro denetleyici kartlarından biridir. STM32F051R8 mikro denetleyici kartının elektriksel teknik özellikleri şunlardır:

- CPU: ARM 32-bit Cortex-M0
- Saat Hızı: 48 MHz
- Çalışma Gerilimi: 3.3 V
- Dijital Giriş/Çıkış Pimleri Sayısı: 55
- Her Giriş/Çıkış için Akım: 40 mA
- Flash Hafıza: 64 KB
- SRAM: 8 KB
- 12 Bit ADC Sayısı: 16
- 12 Bit DAC Sayısı: 1
- SPI Haberleşme Sayısı: 2

- UART Haberleşme Sayısı: 2
- I2C Haberleşme Sayısı: 2
- Timer Hat Sayısı: 11
- RTC Sayısı: 1
- DMA Kontrolcüsü Kanal Sayısı: 5
- Programlama ve Debug Hattı: SWD
- Uzunluk: 68,6 mm
- Genişlik: 53,4 mm
- Ağırlık: 25 g (URL-13).



Şekil 15 STM32F051R8 mikro denetleyici kartı

Şekil 15'deki STM32F051R8 mikro denetleyici kartının tüm bileşenleri tek tek açıklanmıştır.

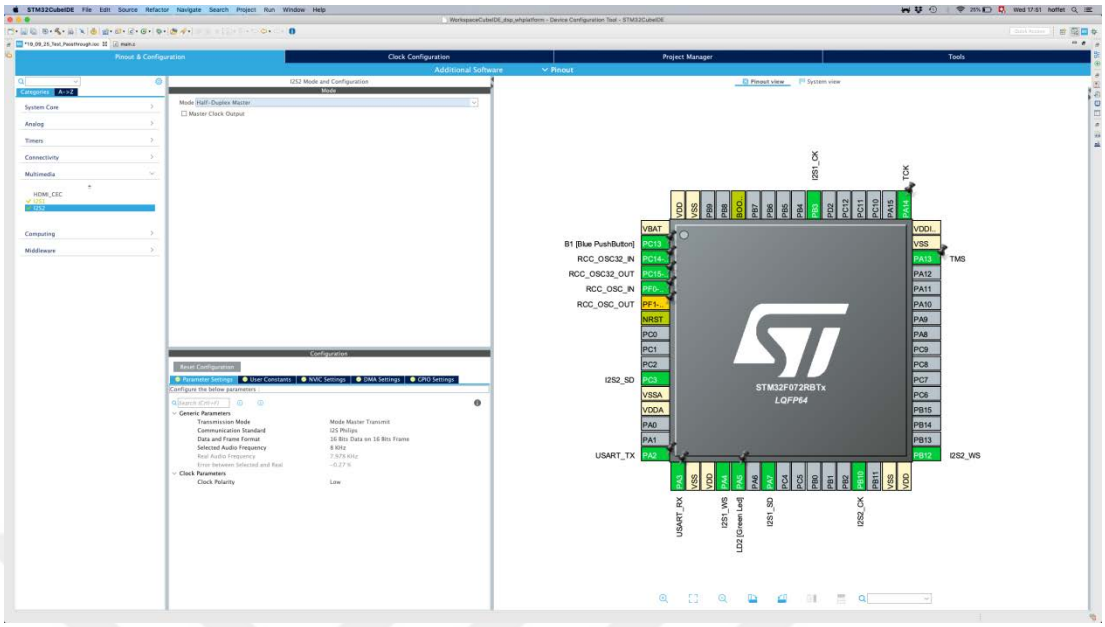
- USB Giriş Soketi: STM32F051R8 geliştirme kartına program yüklemek, debug yapmak ve çalıştırmak için kullanılan USB soketidir.
- ST Link Hattı ve SWD Pimleri: STM32F051R8 geliştirme kartını programlamak için MCU ile bilgisayar arasında USB haberleşmesini SWD seri haberleşmesine çeviren devredir. Ayrıca bu mikro denetleyiciyi dışarıdan başka bir programlayıcı ile programlamak için SWD pimleri çıkarılmıştır.
- Güç Gösterge LED'i: Geliştirme kartında gücün varlığını gösteren değişken kırmızı-yeşil LED'dir.
- Mikro Denetleyici Yongası: Geliştirme kartı üzerinde programlanabilen STM32F051R8 mikro denetleyici yongasıdır.
- Dış Osilatör: STM32F051R8 mikro denetleyicisi iç osilatörünü kullanmadığı zaman sabit bir frekans üreten elektronik bileşendir.
- Sıfırlama Butonu: STM32F051R8 mikro denetleyicisini sıfırlayan düğmedir.
- Test Butonu: STM32F051R8 mikro denetleyicisinin PA0 dijital girişine bağlı kullanıcı için ayrılmış düğmedir.
- Test LED'leri: STM32F051R8 mikro denetleyicisinin PC9 ve PC8 dijital çıkışlarına bağlı kullanıcı için ayrılmış yeşil ve mavi LED'lerdir.
- Programlanabilen Pimler: STM32F051R8 mikro denetleyicisinin programlanabilen dijital, analog ya da seri haberleşme pimleridir.
- Güç Pimleri: Diğer elektronik bileşenlere güç vermek için ve ya geliştirme kartına güç verebilmek için kullanılan pimlerdir. (3V-5V-GND)

b. STM32 Mikro Denetleyicilerini Programlama

STM32Cube IDE(Entegre Geliştirme Ortamı), çevresel yapılandırma, kod oluşturma, kod derleme ve STM32 mikro denetleyicileri ile mikro işlemcileri için hata ayıklama özelliklerine sahip gelişmiş bir C / C ++ geliştirme platformudur. Bu

platform sayesinde ST marka 32-bit gömülü sistemlere program yazılabilir. Böylece uygun elektronik devreleriyle ve mikro denetleyicilerle projeler geliştirilebilir. Geliştirme sırasında herhangi bir zamanda, kullanıcı çevre birimlerinin veya ara yazılımın başlatılmasına ve yapılandırılmasına geri dönebilir ve kullanıcı kodu üzerinde hiçbir etkisi olmadan başlatma kodunu yeniden oluşturabilir. STM32Cube IDE ayrıca, CPU çekirdek kayıtları, bellekler ve çevresel kayıtların yanı sıra canlı değişken izleme, seri kablo görüntüleyici ara yüzü veya arıza analizörü gibi standart ve gelişmiş hata ayıklama özellikleri içerir. STM32Cube IDE platformunu seçmenin birçok avantajı vardır:

- C kodlarını işlemek için derleyiciyi, kaynak kodlarını yaratmak için editörü, MCU'ları programlamak ve kontrol etmek için debug ara yüzünü ve kullanıcının gömülü sistemlere kod yazma işini kolaylaştırmak için birçok uygulamayı tek bir platform içerisinde sunar.
- Birçok mikro denetleyici sadece Windows ile sınırlı iken STM32Cube IDE Windows, Macintosh OSX ve Linux işletim sistemlerinde de çalışır.
- USB ile bilgisayara bağlandığı ve SWD seri protokol kullanılarak dubug sağladığı için kullanımı ve uygulaması da kolaydır.
- Geniş bir çevrimiçi topluluk tarafından desteklenmektedir ve birçok kaynak kodu ve eğitimi mevcuttur.
- Zengin bir C kütüphanesine sahiptir (URL-11).



Şekil 16 STM32Cube IDE genel bakış

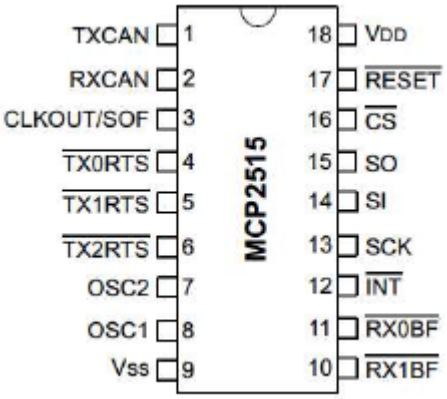
B. CAN Donanım Tasarımı

Mikro denetleyici seçimi yaptıktan sonra seçilen platformu desteklemesi amacıyla CAN veri yolu iletişiminin fiziksel, kontrolör ve yazılım düzeyinde uygun mikroçipler seçilmelidir. CAN veri yolu haberleşmesi için ST marka 32-bit mikro denetleyicileri hem donanımsal hem de yazılımsal olarak destekleyen mevcut mikroçipler aşağıda anlatılmıştır.

1. CAN Denetleyicisi

CAN haberleşmesinde mikro denetleyici ile CAN alıcı-verici donanımı arasında yer alan donanım Şekil 17'de gösterilen Microchip markasının ürettiği MCP2515 CAN denetleyicisi yongasıdır. Bu mikroçip CAN 2.0 B versiyonunu destekleyerek hem standart hem de genişletilmiş veri ve istek çerçevelerini iletme ve alma yeteneğine sahiptir. MCP2515 mikroçipi, istenmeyen iletileri filtrelemek için kullanılan iki onay maskesine ve altı onay filtresine sahip olarak mikro denetleyicilerin ek yükünü azaltır. Bu CAN denetleyicisi çevresel arabirim (SPI)

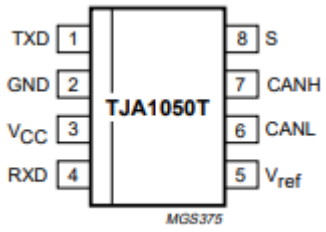
üzerinden mikro denetleyiciler ile iletişim kurar. Ayrıca çalışma gerilimi 2.7V ile 5V aralığındadır (URL-14). MCP2515 denetleyicisinin haberleşme ve çalışma gerilimi özellikleri STM32F051R8 mikro denetleyicisi ile uyumlu olduğu için seçilmiştir.



Şekil 17 MCP2515 CAN denetleyici yongası (URL-14)

2. CAN Alıcı-Vericisi

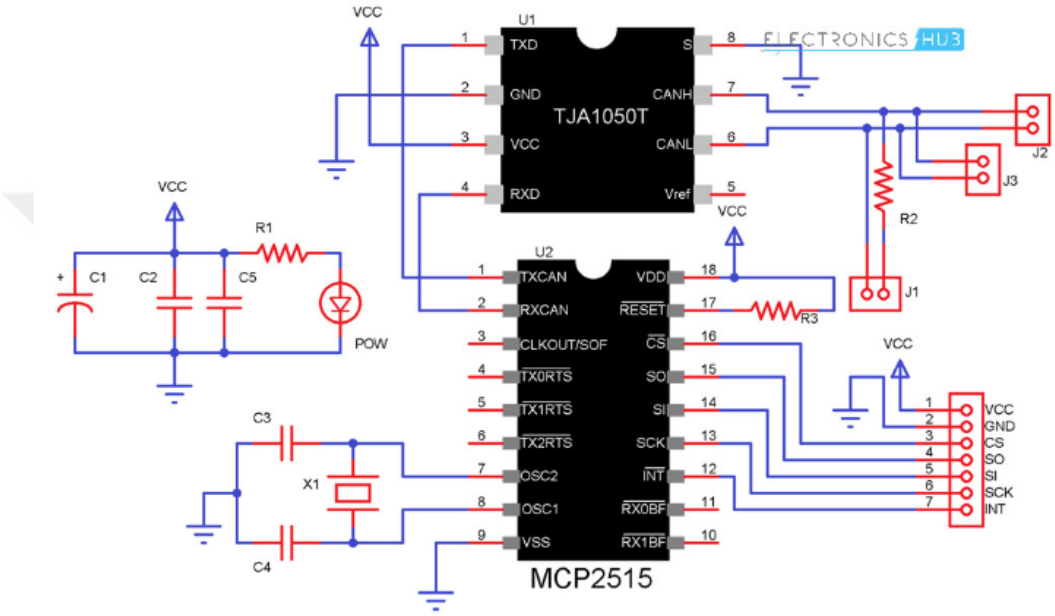
CAN haberleşmesinde CAN denetleyicisi ile CAN fiziksel veri yolu arasında köprü olan donanım ise Şekil 18'de gösterilen Nxp markasının ürettiği TJA1050 CAN alıcı-verici entegresidir. Bu CAN alıcı-vericisi tamamen ISO 11898 standartlarına uygun bir mikroçiptir. Bu mikroçip fiziksel veri yolu üzerinden aldığı diferansiyel gerilimi ikili sayı sistemine çevirir ya da CAN denetleyicisinden aldığı ikili sayı sistemini diferansiyel gerilime dönüştürür. Ayrıca çalışma gerilimi 3.3V ile 5V aralığındadır (URL-15). TJA1050 alıcı-vericisi haberleşme ve çalışma gerilimi özellikleri MCP2515 CAN denetleyicisi ile uyumlu olduğu için seçilmiştir.



Şekil 18 TJA1050 CAN alıcı-verici yongası (URL-15)

3. CAN Haberleşme Kartı

CAN veri yolu haberleşmesinde CAN haberleşme kartı yapabilmek için MCP2515 CAN denetleyici ve TJA1050 CAN alıcı-verici mikroçiplerinin referansları incelenir. Bu referanslardan çıkan sonuçlar ile Şekil 19'daki gibi bir elektriksel devre şematiği çıkarılır.

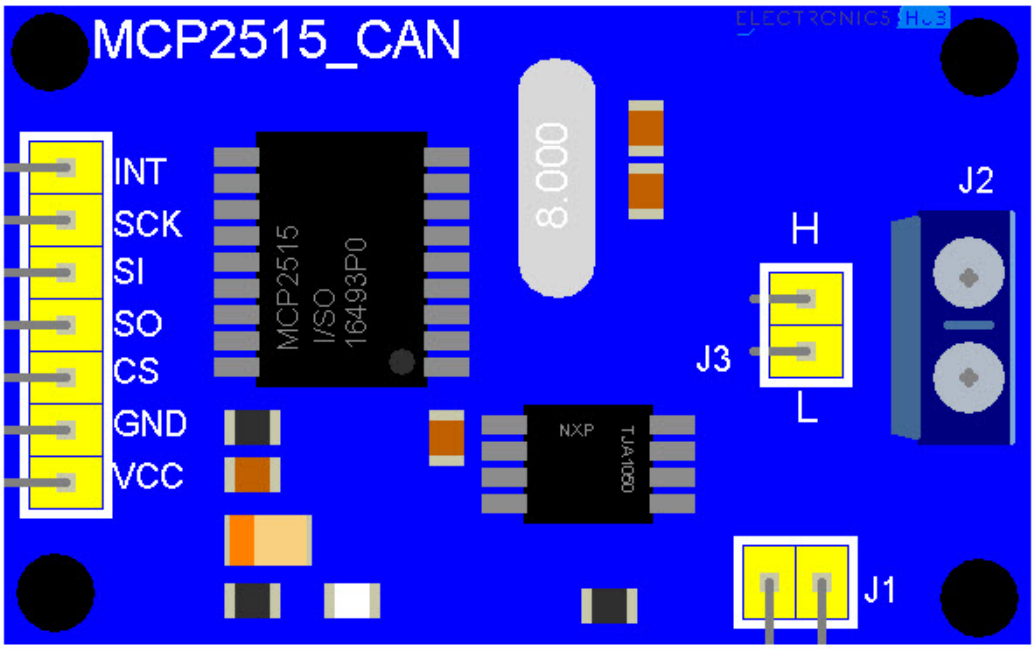


Şekil 19 CAN haberleşmesi için tasarlanan devre şematiği (URL-3)

Çizelge 5 CAN haberleşme kartı ile STM32F051R8 mikro denetleyici kartlarının SPI bağlantısı

CAN Haberleşme Kartı	STM32F051R8 Mikro Denetleyici Kartı
INT	PA1
SCK	PA5
MOSI	PA7
MISO	PA6
CS	PA4

Şekil 19'da çıkarılan bu elektriksel şematik herhangi bir elektronik kart tasarım programında çizilerek Şekil 20'deki gibi mikro denetleyici ile CAN veri yolu arasında haberleşmeyi sağlayan bir CAN haberleşme kartı elde edilebilir. TJA1050 ve MCP2515 mikroçiplerinin çalışma gerilimleri 5V olduğu için CAN haberleşme kartının da çalışma gerilimi 5V dur. Dolayısıyla SPI haberleşmesinde kullanılan SPI pimlerinin gerilim seviyesi de 5V dur. CAN haberleşme kartını SPI pimleri ile STM32F051R8 mikro denetleyici kartının SPI pimleri arasındaki bağlantı Çizelge 5'de gösterilmiştir.



Şekil 20 CAN haberleşme kartı (URL-3)

Şekil 20'de gösterilen CAN haberleşme kartı üzerinde bulunan elektronik bileşenler şunlardır:

- MCP 2515 Yongası: SPI ile haberleşen CAN denetleyici tümleşik devresidir.
- TJA 1050 Yongası: Diferansiyel gerilimleri anlamlandıran CAN alıcı-verici tümleşik devresidir.

- Kırmızı LED: CAN haberleşme kartına gerilim uygulanıp uygulanmadığını gösteren elektronik bileşendir.
- 8 MHz kristal: MCP 2515 CAN denetleyicisine sabit bir frekans üreten elektronik bileşendir.
- Diğer elektronik bileşenler: CAN veri yolu haberleşmesini sağlamak için MCP2515 ve TJA1050 yongalarının referansların da önerilen kondansatör ve dirençler.
- SPI kontrol ve güç pimleri: VCC ve GND pimleri kartın gerilim giriş pimleridir. INT, SCK, MOSI, MISO VE CS pimleri mikro denetleyiciye bağlanmak için çıkarılmış SPI pimleridir.
- CAN veri yolu bağlantı noktası (CANH ve CANL): CAN veri yoluna bağlanmak için çıkarılmış TJA 1050 CAN alıcı-vericisinin CANH ve CANL pimleri.

C. Dokunmatik Panel

Teknolojinin hızla geliştiği günümüzde hayatı kolaylaştıran yeni sistemler yeni tasarımlar insanların kullanımına sunulmaktadır. Bu teknolojik yeniliklerden bir tanesi de dokunmatik ekran kullanımıdır. Dokunmatik ekranlar 1970'li yıllarda keşfedilmiş ama son yıllarda kullanım alanı yaygınlaşmıştır (URL-4).

Kullanımının yaygınlaşmasını LCD ve grafik LCD ile mikroişlemci ve mikro denetleyici teknolojilerindeki gelişmelere borçludur. Dokunmatik ekran herhangi bir grafik LCD veya TFT LCD ekran üzerine yerleştirilmiş doğrudan ekran üzerinden giriş alabilen teknolojidir. Bu teknoloji dokunmatik ekran kalemi veya ekran yüzeyine dokunmayla kullanılabilir. Dokunmatik ekranlar basınca duyarlıdır; kullanıcı ekrandaki kelimelere ve yazılara dokunarak bilgisayarla etkileşim sağlar (AKKOYUN, 2011).

Dokunmatik ekran, birbirleriyle iletişim halinde bulunan üç sistemden meydana gelmektedir. Bunlardan bir tanesi dokunmatik ekran paneli, dokunmatik ekran panelinden gelen sinyalleri anlamlandırarak yorumlayan kontrol sistemi ve kullanıcının dokunmasıyla görüntüleri kullanıcıya aktarmada kullanılan TFT LCD'lerdir. Dokunmatik ekran paneli, üzerine kullanıcı tarafından dokunulduğunda bu dokunmanın hangi koordinatlara yapıldığı bilgisini tespit eden ve kontrol sistemine aktaran kısımdır. Kontrol sistemi ise, dokunmatik panelden gelen koordinat bilgilerini yorumlayarak sistemin hangi davranışlarda bulunması gerektiği kararına varan ünitedir. Kontrol sistemleri, mikro denetleyici, mikroişlemci ve PLC gibi sistemlerden oluşur. TFT LCD ise kontrol sisteminden gelen görüntüleri kullanıcıya sunarak, kullanıcıyı yönlendirmede kullanılır (ÇAKIR ve ark., 2007). Tasarımızda dokunmatik ekrandan gelen bilgileri anlamlı bilgilere çevirip işleyen aynı zamanda CAN hattından gelen verileri kullanıcıya göstermek için TFT LCD'ye yazdıran kontrol sistemi STM32F051R8 mikro denetleyici kartıdır.

1. Dokunmatik Panel ve Çeşitleri

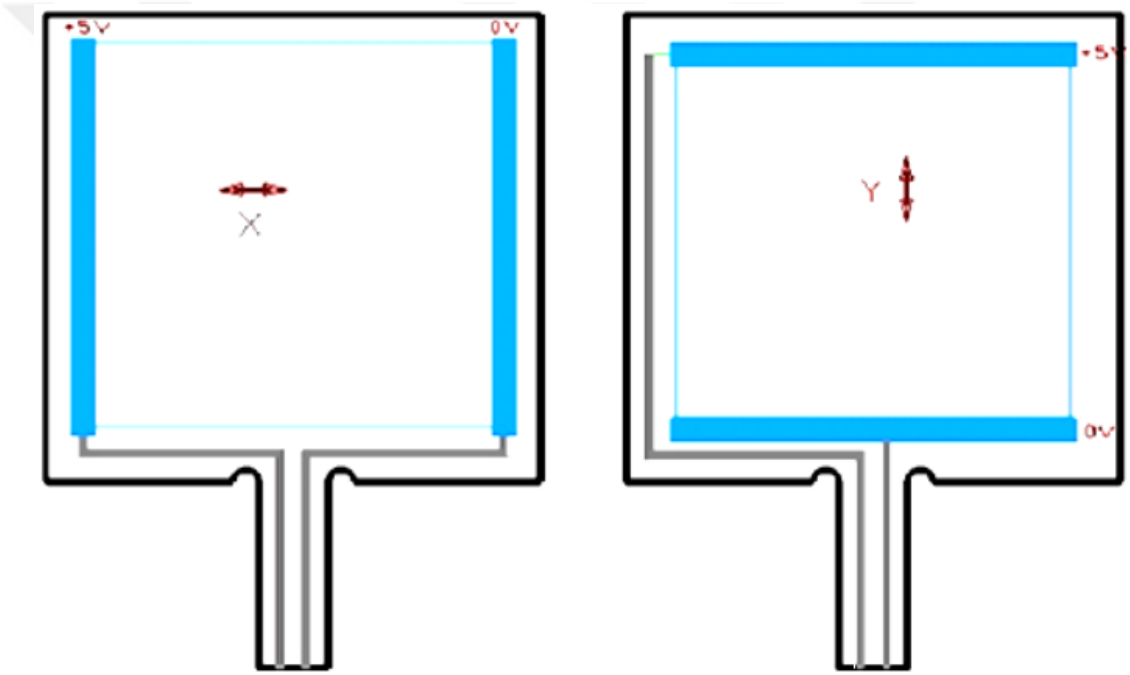
Bir dokunmatik panel görüntülenen alanın fiziksel sınırları içinde, el ya da bir cisim aracılığıyla yapılan dokunuşun basıncını ve konumunu belirler. Dokunmatik ekran üç temel (dokunma sensörü, denetleyici, sürücü)bileşenden oluşur. Bu ekranlarda en önemli bileşen dokunma algılayıcı sensördür. Bu algılayıcı sayesinde dokunuş algılanarak bir yazılım aracılığı ile bilgisayarın anlayabileceği dile çevrilmektedir. Dokunmatik paneller, yüzeyine uygulanan basıncı, farklı şekillerde yorumlayarak kendi içerisinde 3 farklı türe ayrılır (ÇAKIR ve ark., 2007).

a. Rezistif Dokunmatik Panel

Rezistif dokunmatik paneller, bir LCD ekran, elektrotlar ve aralarında hava boşluğu bulunan iki elektrik iletken katmandan oluşurlar. Bu panelin çalışma prensibi elektrik devresini kapatıp açmaya dayanır. Ekrana parmağınızla bastığınızda, üst esnek ve elektriksel olarak iletken tabaka alt elektriksel olarak

iletken tabakaya bastırılır. Bu şekilde bir elektrik devresi oluşturulur ve basıncın konumu okunabilir. Kapasitif bir ekranın aksine ekranın nasıl basıldığı önemli değil elektriksel olarak iletken iki yüzeyi birbirine bastırmak önemlidir (ALO, 2017).

Şekil 21'den anlaşılacağı üzere dokunmanın X koordinatını belirlemek için x düzleminde panelin sol tarafı 5V, sağa doğru gittikçe ise azalarak 0V'a düşmektedir. Aynı şekilde Y koordinatını belirlemek için de y düzleminde sıfıra yaklaştıkça 0V, y değeri attıkça ise 5V'a kadar artmaktadır. Buradan elde edilen gerilim değerleri ayrı ayrı analog dijital dönüşüme tabi tutularak dokunuşun hem X hem de Y düzleminde nereye yapıldığı hesaplanabilmektedir (ÇAKIR ve ark., 2007).



Şekil 21 Rezistif dokunmatik panel (ÇAKIR ve ark., 2007)

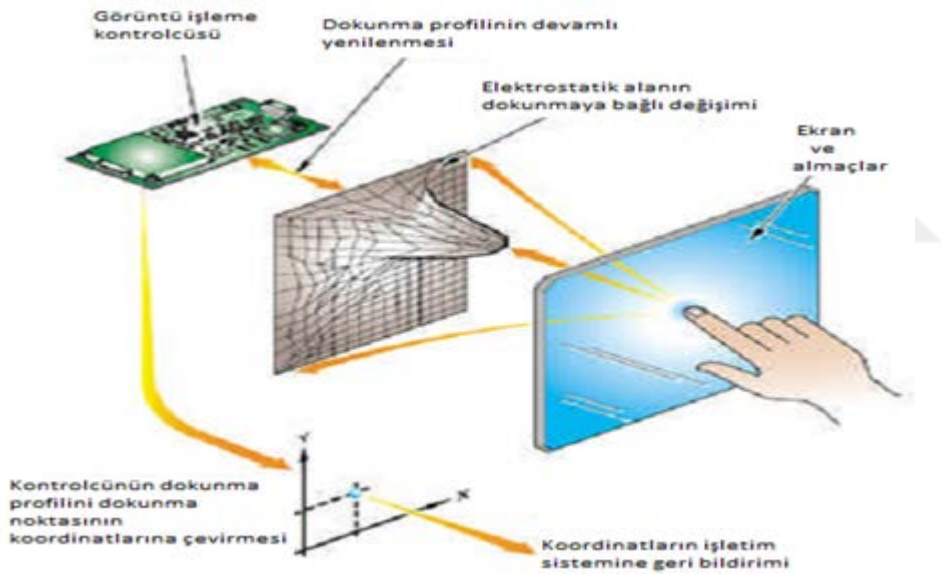
b. Kızılötesi Dokunmatik Panel

Kızılötesi ışık demetleri ekranın bir tarafından diğer tarafına gönderilir, diğer taraftaki duyargalar ışığın gelip gelmediğini sürekli kontrol ederler. Işık geliyorsa kontrol sistemine 1, gelmiyorlarsa 0 verisini gönderirler. Dokunuşla ışığın diğer tarafa geçişini engellenir, böylece duyarga kontrol sistemine 0 komutu gönderir.

Kontrol sistemi komutun geldiği duyargaya göre dokunuşun o eksendeki yerini belirler. Diğer eksende de aynı işlemler tekrarlanır, böylece iki eksende koordinatlar belirlenmiş olur. Isıya duyarlı türü de mevcuttur (ÇAKIR ve ark., 2007).

c. Kapasitif Dokunmatik Panel

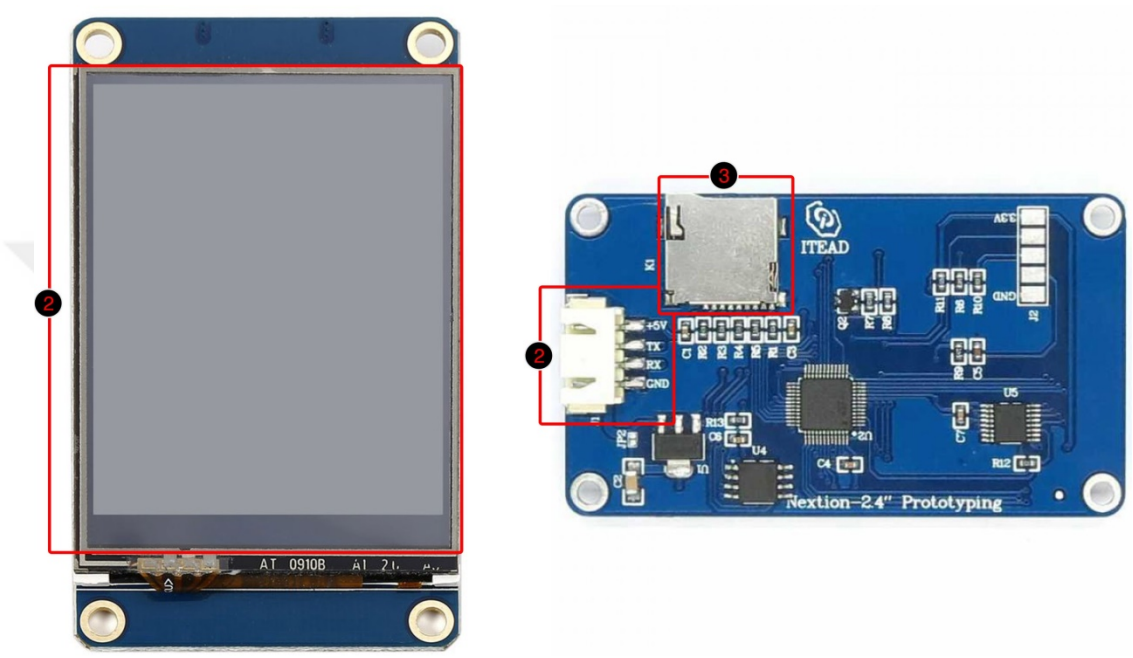
Kapasitif dokunmatik paneller, bir LCD ekran, elektrotlar, iletken bir film ve camdan oluşur. (Şekil 22) Elektriksel olarak iletken bir film, ekran boyunca düzgün bir elektrik alanı oluşturur. Parmağınız ekrana dokunduğunda, ekranın elektrik alanının dağılımı değişir. Dokunulan alan bu şekilde belirlenir. Kapasitif bir ekran için, ekrana dokunan nesnenin elektriksel olarak iletken olması (bir insan parmağı gibi) önemlidir. Kapasitif bir ekranda, ekrana hafif bir dokunuş yeterli iken resesif bir ekranda bu dokunuş daha serttir (ALO, 2017).



Şekil 22 Kapasitif dokunmatik panel (ÇAKIR ve ark., 2007)

Bu çalışmanın kontrol merkezi olan korsan belirleme ünitesinin üzerinde dokunmatik ekran kullanarak kullanıcıya, kontrol merkezi görselleştirmek istenmiştir. Ekranda görüntülenecek veriler fazla yer kaplamadığından 3,5 inç dokunmatik TFT ekran oldukça uygun ve yeterlidir. Dokunmatik ekran panelinin boyutu ve basınç hassasiyeti nedeniyle, diğer birçok projede de kullanılabilir.

Tasarımımızda kullandığımız dokunmatik panel türü ise rezistif dokunmatik paneldir. Marka olarak ise kendi editör programı sayesinde kullanıcıya tasarım kolaylığı sağlayan ayrıca USART seri haberleşme birimine sahip tüm mikro denetleyiciler tarafından kontrol edilebilen Nextion HMI dokunmatik panel seçilmiştir. (Şekil 23)



Şekil 23 NX4832T035_011 dokunmatik TFT panelin ön ve arka yüzü

Şekil 23'de gösterilen dokunmatik TFT panel aşağıdaki bileşenlerden oluşur:

- Görüntüleri kullanıcıya göstermek için TFT LCD ekran (1)
- Mikro denetleyici kartları ve güç girişi için bağlantı pimleri (2)
- Dokunmatik TFT LCD'ye program atmak ve yüksek kapasiteli görüntülerin depolanmasını sağlamak için mikro SD kart girişi (3)

NX4832T035_011 HMI dokunmatik TFT panelin teknik özellikleri şunlardır:

- Boyut: 3,5 inç
- Çözünürlük: 480x320

- Dokunmatik Panel Türü: Rezistif
- 65K RGB Ekran
- Dahili Hafıza: 16MB
- Güç Tüketimi: 5V/145mA
- İşlemci Hızı: 48 MHz
- Program atmak ve veri saklamak için mikro SD kart soketi mevcut
- Ağırlık: 38gr
- Birçok mikro denetleyicileri ile USART üzerinden kontrol edilebilir(URL-7).

Tasarımımızda kullandığımız dokunmatik TFT panelin, STM32F051R8 mikro denetleyici kartı ile bağlantısı cihazın kataloğuna göre Çizelge 6'daki gibi düzenlenmiştir. Dokunmatik TFT panel ve STM32F051R8 mikro denetleyici kartı USART seri haberleşme pimleri üzerinden haberleşirler.

Çizelge 6 NX4832T035_011 HMI dokunmatik TFT panel ile STM32F051R8 mikro denetleyici kartının bağlantısı

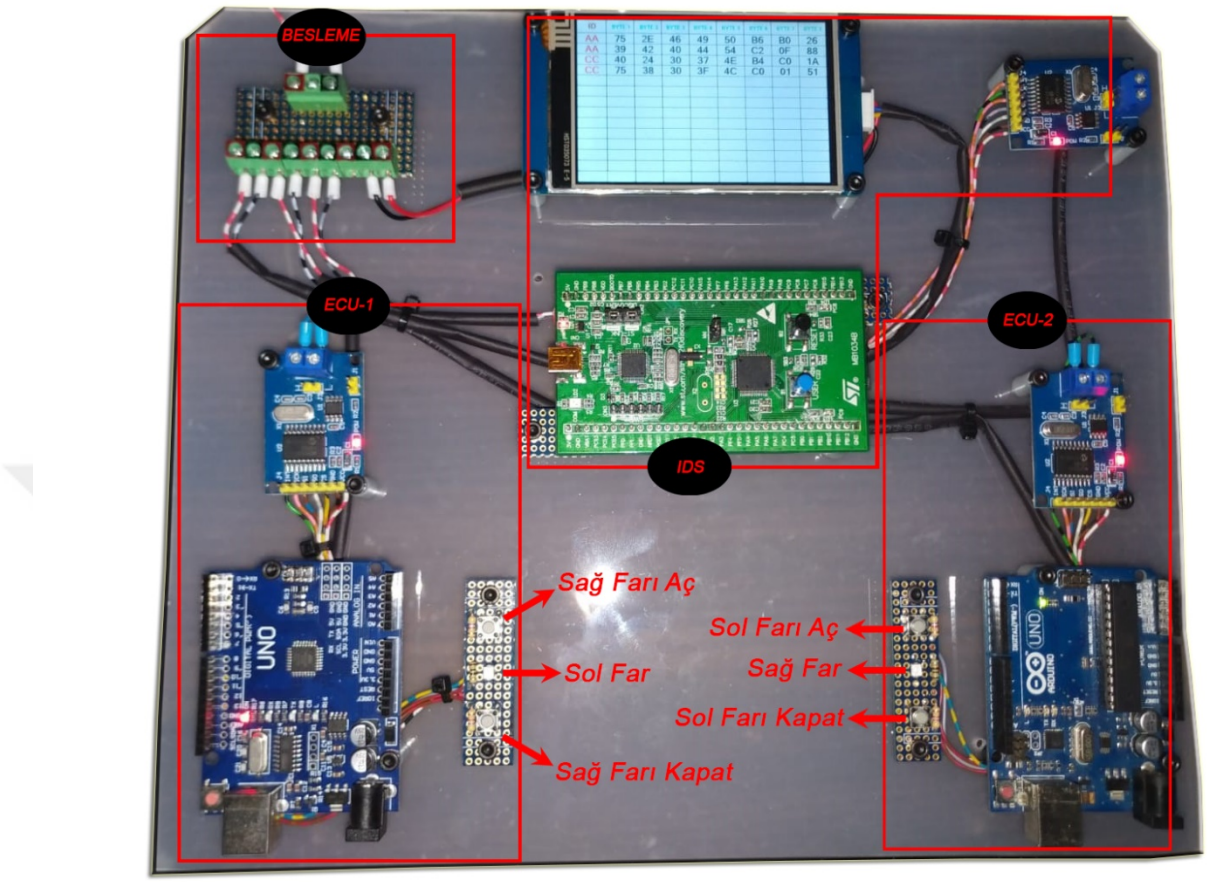
STM32F051R8 Mikro Denetleyici Kartı Pimleri	NX4832T035_011 HMI dokunmatik TFT panelin pimleri
5V	5V
PA10 (RX)	TX
PA9 (TX)	RX
GND	GND

IV. ÖNERİLEN YÖNTEM VE UYGULAMASI

Bu bölümde, üçüncü bölümde anlatılan donanımlar birleştirilerek CAN ağında hibrit saldırı savuşturma uygulaması simüle edilerek anlatılmıştır. Anlatım; Tasarım, Amaç ve Analiz olmak üzere üç bölümden oluşmaktadır.

A. Tasarım

Hibrit saldırı savuşturma uygulamasının tasarımında, donanımın fiziksel ve elektriksel bağlantıları Şekil 24'de görüldüğü gibi bir pleksi cam üzerine dizayn edilmiştir. Bu tasarım biri besleme ünitesi olmak üzere dört elektronik üniteden oluşmaktadır ve birbirlerine besleme ünitesi hariç CAN haberleşmesi ile bağlanmıştır. Şekil 24'de sağda ve solda bulunan ECU-1 ve ECU-2 üniteleri olarak adlandırılan üniteler temel olarak modern bir araba içerisinde var olan dış aydınlatma üniteleridir ve sırasıyla sağ ve sol farı temsil etmektedirler. ECU-1 ve ECU-2 üniteleri Ardunio mikro denetleyici kartı, far aç-kapa butonları, farı temsil eden LED ve CAN haberleşme kartından oluşmaktadır. ECU-1 ve ECU-2 üniteleri üzerindeki mikro denetleyici kartları far aç-kapa butonlarındaki değişimleri algılayarak CAN ağına ilgili farı aç-kapa mesajları göndermektedir. ECU-1 ve ECU-2 üniteleri arasında bu mesajlar karşılıklı olarak eğer anlamlı ise farı temsil eden sağ ve sol LED'leri açıp kapatmaktadır. Şekil 24'deki üçüncü elektronik ünite ise bu çalışmanın temel taşı olarak CAN hattına sızıp gizlice CAN ağındaki mesajları dinleyen saldırganları engelleyen korsan belirleme ünitesidir (IDS). Korsan belirleme ünitesi STM32F051R8 mikro denetleyici kartı, dokunmatik TFT LCD ve CAN haberleşme kartından oluşmaktadır. Korsan belirleme ünitesi üzerindeki dokunmatik TFT LCD aracılığı ile bağlı olduğu CAN ağındaki tüm mesajları gösterir. Ayrıca CAN ağına elektronik kontrol ünitelerini korumak için şifreli mesajlar gönderir.



Şekil 24 Hibrit saldırı savuşturma uygulamasındaki elektronik üniteler

B. Uygulamanın Amacı

Modern bir arabanın içerinde sol ve sağ farların kontrolünü sağlamak için, farlara bağlı elektronik kartlar kontrol paneline ve birbirlerine CAN ağı üzerinden mesajlar göndererek haberleşir. Şekil 24'de simüle edilen tasarımda da elektronik üniteler CAN haberleşmesi aracılığı ile birbirlerine kendi benzersiz kimlik numaraları üzerinden farları aç ve kapa mesajları göndermektedir. Bu mesajların tekrarlı olması CAN ağına sızan bir korsanın, farların kontrol mesajlarını ele geçirmesi anlamına gelir. Bu sebeple modern bir arabada bulunmayan ama bu

uygulamada var olan korsan belirleme ünitesi; elektronik ünitelerin arasındaki haberleşmenin güvenliğini sağlayarak korsanların CAN ağındaki kontrol mesajlarını ele geçirmesini engeller. Korsan belirleme ünitesi, bu güvenliği genel olarak CAN ağında korsanın varlığını belirledikten sonra ECU-1 ve ECU-2 üniteleri arasındaki tekrarlı haberleşmenin değiştirilmesini sağlayarak yapar. Bu değişikliği kriptolojik yöntem olarak CAN ağına şifreli mesajlar göndererek yapar. Bu bahsedilen kriptolojik yöntem basit bir şifreleme metodudur. Daha önceden ağda bulunan tüm elektronik kartlara, kendi kontrol haberleşmelerinde kullanmaları için ortak birden fazla anahtar teslim edilmiştir. Korsan belirleme ünitesi, CAN ağında farklı bir davranış olduğunu saptayınca ağdaki tüm elektronik kartlara kendi benzersiz kimlikleri üzerinden kontrol mesajlarını değiştirmesi için kendi zaman damgasına göre CAN ağında bulunan tüm ünitelerde var olan rastgele bir anahtar gönderir. Korsan belirleme ünitesinin ağdaki tüm kontrol komutlarının değişmesi gerektiği mesajından sonra CAN ağındaki tüm kontrol mesajları bir önceki mesajlara göre değişmiş olup tekrarsız olacaktır.

C. Uygulamanın Analizi

Hibrit saldırı savuşturma uygulamasının analizi olarak Çizelge 7 CAN veri yolundaki normal ve korsan mesajları göstermektedir. Çizelge 7'de birinci ve ikinci mesajlar incelendiğinde, ağda ve korsan belirleme ünitesinde kayıtlı kontrol paneli sağ sinyal lambasını açmak için 60 milisaniye aralıklar ile CAN ağına 0xAA benzersiz kimlik numarası üzerinden onaltılık sayı sistemine göre 8 byte'lık 18-24-2D-78-AF-88-73-F5 mesajlar göndermiştir. Bunun sonrasında Şekil 24'de gösterilen sağ farı temsil eden LED yanmıştır. Çizelge 7'de üçüncü ve dördüncü mesajlar incelendiğinde ise, CAN ağına sızmış bir korsan ünitesi birinci ve ikinci mesajları inceleyerek kayıtlı kontrol paneli gibi davranıp aynı benzersiz kimlik numarası üzerinden CAN ağına mesajlar göndermiştir. Bunun sonrasında Şekil 24'de gösterilen sağ farı temsil eden LED zaman damgasına uymadığı için yanmamıştır.

Bu süreçte CAN ağını sürekli izleyen korsan belirleme ünitesi ise gönderilen mesajların zaman damgasına göre kontrol panelinin taklit edildiğini algılayıp kontrol mesajlarının değişmesi için CAN ağına Çizelge 7'deki beşinci, altıncı ve yedinci şifreli mesajları göndermiştir. Bu şifreli mesajlar ağda kayıtlı kontrol paneli ve ECU-2 ünitesi tarafından alınıp işlendikten sonra sağ farı aç-kapa kontrol mesajları değişmiştir. Bu değişimden sonra kontrol paneli sağ farı açmak için Çizelge 7'deki sekizinci ve dokuzuncu mesajları kullanır ve bir önceki açığa çıkmış korsan tarafından taklit edilmiş kontrol mesajı ile tekrara düşmemiş olacaktır.

Çizelge 7 Hibrit saldırı savuşturma uygulamasında CAN veri yoluna saldırı anında kaydedilen normal ve korsan mesajlar

Zaman Damgası (ms)	ID (hex)	Veri (hex)	Yorum
10.060	AA	18-24-2D-78-AF-88-73-F5	Sağ Sinyal Lambası Aç (normal)
10.120	AA	18-24-2D-78-AF-88-73-F5	Sağ Sinyal Lambası Aç (normal)
10.185	AA	18-24-2D-78-AF-88-73-F5	Sağ Sinyal Lambası Aç (korsan)
10.257	AA	18-24-2D-78-AF-88-73-F5	Sağ Sinyal Lambası Aç (korsan)
10.220	AA	01-1E-15-0E-09-06-04-FF	Şifre Mesajı 1 (IDS)
10.280	AA	02-AF-77-51-38-26-19-11	Şifre Mesajı 2 (IDS)
10.340	AA	03-0B-08-55-02-06-08-06	Şifre Mesajı 3 (IDS)
10.460	AA	0F-24-2E-B6-0A-56-5F-FE	Sağ Sinyal Lambası Aç (normal)
10.520	AA	0F-24-2E-B6-0A-56-5F-FE	Sağ Sinyal Lambası Aç (normal)
11.860	CC	17-22-30-BE-9B-66-74-FE	Sol Sinyal Lambası Aç (normal)
11.920	CC	17-22-30-BE-9B-66-74-FE	Sol Sinyal Lambası Aç (normal)

12.037	CC	17-22-30-BE-9B-66-74-FE	Sol Sinyal Lambası Aç (korsan)
12.097	CC	17-22-30-BE-9B-66-74-FE	Sol Sinyal Lambası Aç (korsan)
12.320	CC	01-51-37-25-19-11-0B-08	Şifre Mesajı 1 (IDS)
12.380	CC	02-05-FF-AF-77-51-38-26	Şifre Mesajı 2 (IDS)
12.440	CC	03-19-11-03-1D-0B-13-0E	Şifre Mesajı 3 (IDS)
12.660	CC	34-30-34-3E-9B-1D-54-02	Sol Sinyal Lambası Aç (normal)
12.720	CC	34-30-34-3E-9B-1D-54-02	Sol Sinyal Lambası Aç (normal)

Genel olarak Çizelge 7 incelendiğinde korsan belirleme ünitesi, kayıtlı benzersiz kimlik numaraları üzerinden CAN ağına gönderilen mesajların zaman damgasına ve mesaj sıklığına göre incelenmektedir ve bu incelemenin sonucunda ağda bir korsan varlığı ya da yokluğu belirlenmektedir. Eğer korsan belirleme ünitesi tarafından ağa sızmış bir korsan ünitesi belirlenirse ağda kayıtlı tüm kontrol mesajlarının değişmesi için CAN ağına şifreli mesajlar gönderir. Bu şifreli mesajları CAN ağından alıp işleyen elektronik kontrol üniteleri kontrol mesajlarını değiştirir. Bu durumda CAN ağında tekrarlı kontrol mesajlarının önüne geçilerek güvenlik sağlanmış olur.

V. SONUÇ VE ÖNERİLER

Bu bölümde, hibrit saldırı savuşturma uygulamasında önerilen yöntem için sonuç ve öneriler anlatılmıştır. Anlatım; Çalışmanın Sonucu ve Öneriler olmak üzere iki bölümden oluşmaktadır.

A. Çalışmanın Sonucu

Otomotiv haberleşme ağında denetleyici alan ağı için incelenen mevcut saldırı savuşturma yöntemleri ile bu çalışmada önerilen hibrit saldırı savuşturma yöntemi, sistem güvenlik açıkları ve denetleyici alan ağının doğal yapısına göre Çizelge 8'de karşılaştırılmıştır.

Çizelge 8 Mevcut şifreleme yöntemleri ile geliştirilmiş uygulamaların hibrit saldırı savuşturma uygulaması ile karşılaştırılması

Şifreleme Yöntemi	Kimlik Doğrulama	Bütünlük	Gizlilik	Geriye Uyumluluk	Tekrarlı Saldırı Direnci	Gerçek Zamanlı Performans	Saldırı Tespit Sistemi
LiBrA-CAN	ok	ok	nok	nok	nok	nok	nok
WooAuth	ok	ok	ok	nok	ok	ok	nok
Vecure	ok	ok	nok	ok	ok	nok	nok
CaCAN	ok	ok	nok	nok	ok	nok	nok
VatiCAN	ok	ok	nok	ok	ok	nok	nok
VulCAN	ok	ok	nok	ok	ok	nok	ok
Hibrit Yöntem	nok	ok	nok	ok	ok	ok	ok

- Kimlik Doğrulama: Veri mesajından sonra kimlik doğrulama için gönderilen mesajlar CAN ağında güvenliği artırıyor ama öte yandan veri trafiğini artırarak CAN haberleşme protokolünün gerçek zamanlı performansını

etkiliyor. Otomotiv teknolojisinde CAN haberleşme ağı gerçek zamanlı performansı ve verimli iletişiminden dolayı yaygın olarak kullanıldığı için hibrit saldırı savuşturma yöntemimiz CAN haberleşme ağının gerçek zamanlı performansını etkilememek için kimlik doğrulama mesajları göndermemeyi tercih ederek kimlik doğrulama ilkesini sağlamaz.

- Bütünlük: Hibrit saldırı savuşturma uygulamamız içerisinde kullanılan basit simetrik şifreleme yöntemi kendi içerinde bir CRC'ye sahip olup verilerin doğruluğu ve geçerliliği ilkesi olan bütünlük ilkesini sağlar.

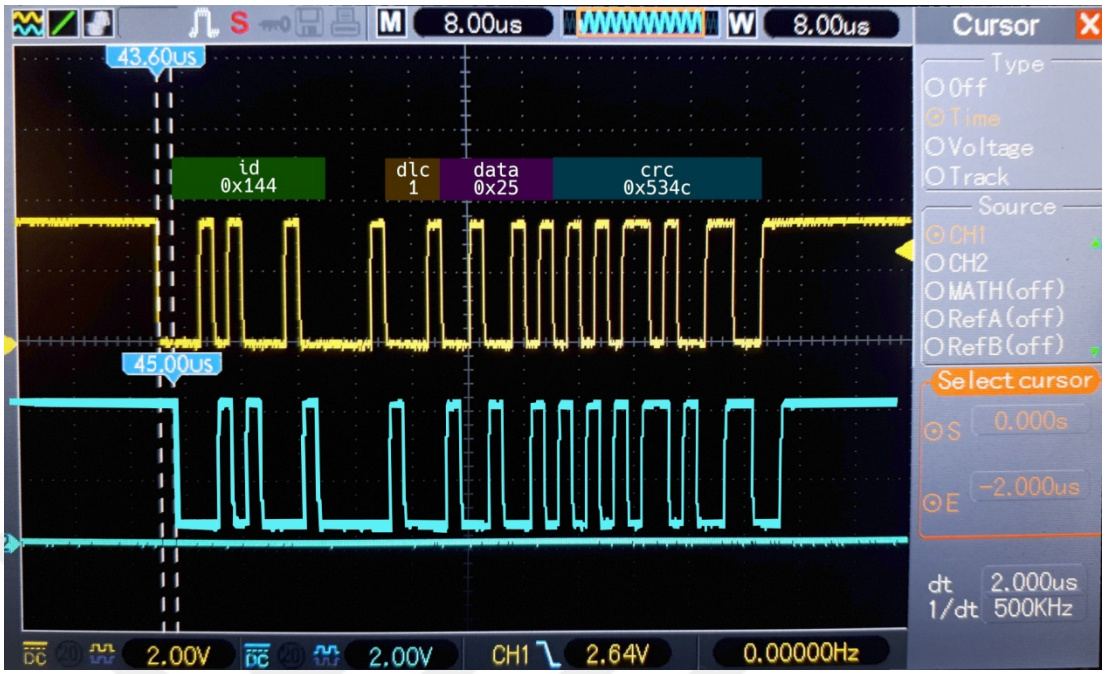
- Gizlilik: Hibrit saldırı savuşturma uygulamamız CAN ağında mevcut çerçeve yapısını bozmayıp her ağa kolay uyumluluk sağlamak için verileri yetkili kişilere değil CAN ağına göndermeyi tercih ederek gizlilik ilkesini sağlamaz.
- Geriye uyumluluk: Geriye uyumluluk mevcut CAN çerçeve yapısını bozmayarak mevcut sisteme daha hızlı adapte olmayı sağlar. Hibrit saldırı savuşturma uygulamamız gizlilik ilkesini sağlamayarak geriye uyumluluk ilkesini sağlar.
- Tekrarlı saldırı direnci: Hibrit saldırı savuşturma uygulamamızdaki ilkel simetrik şifreleme yöntemimiz belirli aralıklar ile sürekli şifrelenen anahtarı değiştirdiği için CAN ağında aynı işlem için farklı mesajlar bulunacaktır. Bu sayede saldırgan son gönderilen mesaj ile kontrolü sağlayamayacaktır.
- Gerçek zamanlı performans: CAN ağında bir görev için bir mesajdan fazlası gönderilirse CAN ağında veri trafiği artar ve CAN ağının gerçek zamanlı performansı ortadan kaybolur. Çizelge 8'de bu duruma aykırı görünen WooAuth (Woo ve ark., 2014) şifreleme yöntemi mevcut CAN çerçeve yapısını bozduğu için gerçek zamanlı performansı sağlarken geriye uyumluluğu sağlamaz. Hibrit saldırı savuşturma uygulamamız ise hem geriye uyumluluğu hem de gerçek zamanlı performans ilkelerini sağlayarak CAN

haberleşme protokolünün otomotiv teknolojisinde kullanılma sebeplerini sağlamış olur.

- Saldırı tespit sistemi: Hibrit saldırı savuşturma uygulamamızın bir diğer yöntemi olan saldırı tespit sistemi Çizelge 8'de gösterildiği üzere diğer uygulamalarda bulunmamaktadır. Saldırı tespit sistemi korsan varlığını, CAN ağına gönderilen mesajın zaman damgası ve tekrar sayısına göre algılayıp anahtar değişikliği ve raporlama aksiyonlarını yaparak diğer uygulamalardan bir adım önde olduğunu göstermektedir.

Bu çalışmada denetleyici alan ağının mevcut güvenlik açıklarını kapatmaya yönelik hibrit saldırı savuşturma yöntemi önerilirken aynı zamanda denetleyici alan ağının doğal yapısı ve pozitif yönlerinin de bozulmaması hedeflenmiştir. Denetleyici alan ağının diğer birçok haberleşmeye göre en üstün ve belirgin yanı gerçek zamanlı performansıdır. Hibrit saldırı savuşturma uygulaması da bünyesinde barındırdığı basit şifreleme yöntemi ve korsan belirleme yöntemi ile denetleyici alan ağının gerçek zamanlı performansını etkilemez.

Şekil 25'daki osiloskop görüntüsünde sarı ve mavi renkteki kare dalgalar CAN ağındaki aynı mesaja tepki veren iki ayrı elektronik kontrol ünitesinin CANH çıkışını temsil etmektedir. Sarı renk kare dalga ile cevap veren elektronik kontrol ünitesinin mikro denetleyici kartına hiçbir güvenlik yöntemi uygulanmamış iken mavi renkte cevap veren elektronik kontrol ünitesinin mikro denetleyici kartına bu çalışmada önerilen basit şifreleme algoritmaları uygulanmıştır. Osilaskop çıktısı incelendiğinde önerilen basit şifreleme algoritmalarının denetleyici alan ağı haberleşmesinin gerçek zamanlı performansını etkilemeyecek kadar az bir gecikme oluşturduğu görülmektedir. Osilaskop çıktısında görülen bu 1,4 mikro saniyelik gecikme tamamen mikro denetleyici kartının basit şifreleme algoritmalarını işleme süresi ile alakalıdır. Basit şifreleme algoritmalarının kullanıldığı elektronik kontrol ünitesinin mikro denetleyici kartı daha hızlı mikro denetleyici kartları ile değiştirildiğinde bu işlem süresinin daha da azaldığı görülecektir.



Şekil 25 Normal ve basit şifreleme algoritmalarının kullanıldığı mikro denetleyici kartlarına bağlı CAN kontrol kartlarının osilaskop görüntüsü

Bu çalışmada otomotiv içerisindeki ECU'ların birbirleri ile haberleşmesi için kullandığı CAN haberleşme protokolünü ve CAN haberleşmesinde ki mevcut güvenlik açıklarını ele aldık. Ayrıca literatür de CAN haberleşme protokolü üzerinden kablolu ya da kablosuz şekilde otomobil içerisindeki ECU'lara sızma örneklerini özetledik. Özetlenen belirli saldırılar, doğrudan aracın güvenliğini etkilemediğinden önemsiz görüldüğünü saptadık. Ancak araçlardaki elektronik kontrol üniteleri üzerindeki kablosuz haberleşme protokollerinin kullanımı artıkça kablosuz saldırıların da artacağını belirledik. İlerleyen teknoloji ile birlikte otomobil endüstrisi tamamen otonom araç teknolojisinin zirvesine ulaştığında ve her zamankinden daha fazla elektronik kontrol ünitesine ihtiyaç duyduğunda, otomobil üreticileri CAN haberleşmenin doğasında bulunan güvenlik açıklarını görmezden gelemeyeceklerini anlattık. CAN haberleşme protokolünde doğası gereği oluşan güvenlik açıklarına karşı alınması gereken tüm önlemleri derinlemesine savunma başlığı altında inceledik. Derinlemesine savunma yöntemlerinden yola çıkarak

popüler olarak kullanılan iki popüler konu olan saldırı tespit sistemleri (IDS) ve şifreleme yöntemlerini analiz ettik.

CAN veri yolunda kimlik doğrulama için sadece şifreleme yöntemleri kullanılırsa bant genişliği ve gerçek zamanlı performans gibi CAN ağının çalışmasında önemli rol oynayan özellikler kötü etkileneceğini gösterdik. Ayrıca CAN veri yolunda gizlilik ilkesini sağlama için geriye uyumluluk ilkesini bozmanın mevcut CAN ağlarında adapte sorunu ortaya çıkaracağını saptadık. Bu nedenle, CAN ağında güvenlik sağlanırken uygulanabilirlikten uzaklaşmayan çözümün, ilkel şifreleme yöntemi ve IDS den oluşan hibrit bir sistemle elde edilebileceğini anlattık.

B. Öneriler

Otomotiv teknolojisi geliştikçe, denetleyici alan ağı için güvenlik çözümleri de gelişecek ve araçlarda bu çözümler kullanılmaya devam edecektir. Öte yandan otomotiv teknolojisi geliştikçe saldırganlar güvenlik çözümleri hakkında daha fazla bilgi edinecek ve edindikleri bilgileri araçlar üzerinde siber saldırı olarak kullanmaya devam edecektir. Bu nedenle otomotiv teknolojisinin güvenli bir şekilde gelişmesi için araç içerisindeki tüm elektronik ünitelerin haberleşmesini sağlayan denetleyici alan ağındaki tüm açıklar tek tek analiz eden ve önlemler alan çalışmaların sayısı artmalıdır. Bu çalışmalar otomotiv teknolojisinde rahat bir şekilde entegre edilebilmesi adına denetleyici alan ağının doğal yapısını bozmadan devam etmelidir. Denetleyici alan ağının doğal yapısını bozmadan yapılabilecek güvenlik çalışmalarından biri basit şifreleme yöntemleridir. Gelecekteki çalışmalarda daha farklı matematiksel yöntemler kullanılarak ve denetleyici alan ağının gerçek zamanlı performansını etkilemeyen basit şifreleme yöntemleri belirlenebilir. Denetleyici alan ağının doğal yapısını bozmayan bir diğer yöntemde korsan belirleme ünitesi çalışmalarıdır. Korsan belirleme üniteleri bulunduğu ağda saldırganın varlığını ne kadar hızlı belirlerse ağdaki güvenliği o kadar hızlı kontrol altına almış olacaktır. Bu sebeple korsan belirleme ünitelerinde daha gelişmiş ve daha hızlı mikro denetleyici

kullanımı ağdaki güvenliği artıracaktır. Aynı zamanda korsan belirleme ünitesinde saldırganı belirleme yöntemlerinin sayısı arttıkça da ağdaki güvenlik artacaktır. Bu çalışmada ağdaki saldırgan varlığı belirlemek için zaman damgası ve mesaj iletim sayısı yöntemleri kullanılmıştır. Gelecekteki çalışmalarda korsanın varlığını ek olarak daha farklı senaryolar ile de belirleyerek ağdaki güvenlik artırılabilir.

Gelecekteki çalışmalarda yapay zeka yazılımlarının otomotiv teknoloji üzerindeki etkisinin artacağını düşünerek denetleyici alan ağında oluşan saldırıların nedenini bu yazılımlar ile belirlemek için korsan belirleme üniteleri saldırıların etkilerini, sayısını ve zamanlarını kaydetmelidir. Korsan belirleme ünitesi tarafından kaydedilen bu veriler kullanılarak ta denetleyici alan ağı üzerinde güvenlik önlemleri alınabilir.

VI. KAYNAKÇA

MAKALELER

AKKOYUN, F. (2011). “Fpga tabanlı dokunmatik ekranlı kullanıcı arabirim tasarlanması ve gerçekleştirilmesi”, **Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü,**

BOUDGUIGA, A. KLAUDEL, W. BOULANGER, A. ve CHIRON, P. (2016). "A Simple Intrusion Detection Method for Controller Area Network ", **2016 IEEE International Conference on Communications (ICC),**

BOZDAL, M. SAMIE, M. ve JENNIONS, J. (2018). “A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions”, **2018 International Conference on Computing, Electronics & Communications Engineering,**

BULCK, J.V. MUHLBERG, J.T. ve PIESSENS, F. (2017).“VulCAN: Efficient Component Authentication and Software Isolation for Automotive Control Networks”, **ACSAC 2017: Proceedings of the 33rd Annual Computer Security Applications Conference**

CURRIE, R. (2017). “Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering”, **The SANS Institute**

ÇAKIR, A. AKBULUT, F. T. ve ALTINTAŞ, V. (2007). “Dokunmatik Ekran”, **Süleyman Demirel Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü,**

DIFFIE, W. ve HELLMANN, M.E. (1979). “Privacy and Authentication: A Introduction to Cryptography”, **Proceedings of the IEEE**

GMIDEN, M. GMIDEN, M. H. ve TRABELSI, H. (2019). “Cryptographic and Intrusion Detection System for automotive CAN bus Survey and

contributions”, **2019 16th International Multi-Conference on Systems, Signals & Devices (SSD),**

GROZA, B. MURVAY, S. HERREWEGE, A. V. ve VARBEUWHEDE, I. (2012). “LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks”, **International Conference on Cryptology and Network Security**,

HOPPE, T. KILTZ, S. ve HITTMANN, J. (2011). “Security threats to automotive CAN networks – Practical examples and selected short-term countermeasures”, **Reliability Engineering & System Safety**

HOPPE, T. KILTZ, S. ve HITTMANN, J. (2009). "Applying Intrusion Detection to Automotive IT - Early Insights and Remaining Challenges", **Journal of Information Assurance and Security**

KOSCHER, K. CZESKIS, A. ROESNER, F. PATEL, S. KOHNO, T. CHECKOWAY, S. MCCOY, D. KANTOR, B. ANDERSON, D. SHACHAM, H. ve SAVAGE, S. (2010). “Experimental Security Analysis of a Modern Automobile”, **IEEE Symposium on Security and Privacy**

KURACHI, R. MATSUBARA, Y. TAKADA, H. ADACHI, N. MIYASHITA Y. ve HORIHATA, S. (2014). “CaCAN - Centralized authentication system in CAN (controller area network),” **in 14th Int. Conf. on Embedded Security in Cars ESCAR,**

MATSUMOTO, T. HATA, M. TANABE, M. YOSHIOKA, K. ve OISHI, K. (2012). “A Method of Preventing Unauthorized Data Transmission in Controller Area Network”, **2012 IEEE 75th Vehicular Technology Conference (VTC Spring),**

MILLER, C. ve VALASEK, C. (2015). “Remote Exploitation of an Unaltered Passenger Vehicle”, **BlackHat,** USA

MILLER, C. ve VALASEK, C. (2014). “A Survey of Remote Automotive Attack Surfaces”, **BlackHat**, USA

MUNDHENK, P. (2017). “Security for Automotive Electrical / Electronic (E/E) Architectures”, **Cuvillier Verlag,** Göttingen

MURVAY, P. S. ve GROZA, B. (2017). “Dos Attacks on Controller Area Networks by Fault Injections from the Software Layer”, **Proceedings of the 12th International Conference on Availability, Reliability and Security**,

NILSSON, D. K. ve LARSON, U. E. (2009). “A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure”, **Journal of Networks,**

NURNBERGER, S. ve ROSSOW, C. (2016). "vatiCAN -Vetted, Authenticated CAN Bus”, **International Conference on Cryptographic Hardware and Embedded Systems,**

WANG, Q. ve SAWHNEY, S. (2014). “VeCure: A Practical Security Framework to Protect the CAN Bus of Vehicles”, **2014 International Conference on the Internet of Things (IOT),**

WOLF, M. WEIMERSKIRCH, A. ve WOLLINGER, T. (2007). “State of the Art: Embedding Security in Vehicles”, **Eurasip Journal on Embedded Systems,**

WOO, S. JO, H. J. ve LEE, D. H. (2014). "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN", **IEEE Transactions On Intelligent Transportation Systems,**

YAVUZ, E. SARICA, S. S. ve ARTUÇ, E. (2018). “Kontrol Alan Ağları İçin Optimum Statik Mesaj Zamanlaması”, **Mühendislik Bilimleri ve Tasarım Dergisi,**

ZANERO, S. PALANCA, A. EVENCHICK, E. ve MAGGI F. (2017). “A Stealth, Selective, Link Layer Denial-of-Service Attack Against Automotive

Networks," **in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,**

ELEKTRONİK KAYNAKLAR

URL-1 "Enerji Yönetimi CAN Haberleşme Protokolü", https://www.tesisatmarket.com/enerji-yonetimi-can-haberlesme-protokolu, (Erişim Tarihi: 16.05.2021)

URL-2 "CAN Specification Version 2.0", http://esd.cs.ucr.edu/webres/can20.pdf, (Erişim Tarihi: 16.05.2021)

URL-3 "CAN Haberleşme Elektronik Kartı", https://www.electronicshub.org/arduino-mcp2515-can-bus-tutorial/, (Erişim Tarihi: 16.05.2021)

URL-4 T. "Dokunmatik Ekran Tarihçesi ve Çalışma Prensibi", https://www.muhendisbeyinler.net/dokunmatik-ekranin-tarihcesi-ve-calisma-prensibi/ ,(Erişim Tarihi: 16.05.2021)

URL-5 "Introduction to the Controller Area Network (CAN)",

http://www.ti.com/lit/an/sloa101b/sloa101b.pdf, (Erişim Tarihi: 16.05.2021)

URL-6 "Road vehicles, Diagnostic systems, Keyword Protocol 2000", https://www.iso.org/obp/ui/#iso:std:iso:14230:-4:ed-1:v1:en, (Erişim Tarihi: 16.05.2021)

URL-7 "NEXTION BASIC HMI DISPLAY", https://nextion.tech/basic-series-introduction/, (Erişim Tarihi: 16.05.2021)

URL-8 "LPC2000 Programlama Kılavuzu", http://www.barissamanci.net/Makale/13/lpc2000-programlama-klavuzu/, (Erişim Tarihi: 16.05.2021)

URL-9 “Control Area Network (CAN) Implementation Guide”, https://www.analog.com/media/en/technical-documentation/application-notes/AN-1123.pdf, (Erişim Tarihi: 16.05.2021)

URL-10 “CAN Bus”, https://en.wikipedia.org/wiki/CAN_bus, (Erişim Tarihi: 16.05.2021)

URL-11 “STM32Cube IDE Overview”, https://www.st.com/en/development-tools/stm32cubeide.html, (Erişim Tarihi: 16.05.2021)

URL-12 “ARM Mimarisi ve Uygulamaları” http://www.ktu.edu.tr/dosyalar/bilgisayar_a7670.pdf, (Erişim Tarihi: 16.05.2021)

URL-13 “STM32F0 DISCOVERY”, https://www.st.com/en/evaluation-tools/stm32f0discovery.html, (Erişim Tarihi: 16.05.2021)

URL-14 “Stand-Alone CAN Controller with SPI interface”, http://ww1.microchip.com/downloads/en/DeviceDoc/MCP2515-Stand-Alone-CAN-Controller-with-SPI-20001801J.pdf, (Erişim Tarihi: 16.05.2021)

URL-15 “High speed CAN transceiver“, https://www.nxp.com/docs/en/data-sheet/TJA1050.pdf, (Erişim Tarihi: 16.05.2021)

TEZLER

ALO, V. (2017). “Arduino LCD Lauatennis”, (Yayımlanmış Lisans Tezi), **Computer Science Institute, Tartu University**.

EKLER

EK-1. CD içerisinde CAN ECU1 C Kodu Programı

EK-2. CD içerisinde CAN ECU2 C Kodu Programı

EK-3. CD içerisinde CAN Korsan Belirleme Ünitesi C Kodu Programı

EK-4. CD içerisinde TFT Dokunmatik Ekran Arayüz Yazılımı

ÖZGEÇMİŞ

Ad-Soyad: Serkan Baki

ÖĞRENİM DURUMU:

Lisans: 2017, Sakarya Üniversitesi, Teknoloji Fakültesi, Elektrik/Elektronik Mühendisliği

MESLEKİ DENEYİM:

2018 DizaynVip Group

Görevi: Yazılım ve Donanım Geliştirme Mühendisi

2020 Alpplas Endüstriyel Yatırımlar A.Ş.

Görevi: Gömülü Yazılım Mühendisi

YAYINLAR:

Anadolu Bil. Meslek Yüksekokulu Dergisi

2021-Tezden Türetilen Makale

Otomotiv haberleşmesinde denetleyici alan ağı için hibrit bir saldırı savuşturma uygulaması