T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

OTOMOTİV YERLEŞİK AĞLARI İÇİN İZİNSİZ GİRİŞ TESPİTİ

Boubacar SOW

Akıllı Ulaşım Sistemleri ve Teknolojileri Anabilim Dalı

Akıllı Ulaşım Sistemleri ve Teknolojileri Programı

AĞUSTOS 2022

T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

OTOMOTİV YERLEŞİK AĞLARI İÇİN İZİNSİZ GİRİŞ TESPİTİ

Boubacar SOW

DANIŞMAN
Dr. Öğr. Üyesi İlyas OZER

Akıllı Ulaşım Sistemleri ve Teknolojileri Anabilim Dalı

Akıllı Ulaşım Sistemleri ve Teknolojileri Programı

AĞUSTOS 2022

ONAY

Ece Sema Korkmaz tarafından hazırlanan "**Otomotiv Yerleşik Ağları İçin İzinsiz Giriş Tespiti**" adlı tez çalışması 26/8/2022 tarihinde yapılan sınavla aşağıdaki jüri tarafından oybirliği/oyçokluğu ile Bandırma Onyedi Eylül Üniversitesi Fen Bilimleri Enstitüsü Akıllı Ulaşım Sistemleri ve Teknolojileri Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Dr. Öğr. Üyesi İlyas OZER (Danışman)	_____
Prof. Dr. Mehmet TEKTAŞ (Üye)	_____
Dr. Öğr. Üyesi Hasan ŞAHİN (Üye)	_____

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …/…/…gün ve …/… sayılı kararı ile onaylanmıştır.

Doç. Abdullah YEŞİL
Enstitü Müdürü

BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ÇALIŞMASI

ETİK BEYANI

Bandırma Onyedi Eylül Üniversitesi Fen Bilimleri Enstitüsü tez yazım kılavuzuna göre hazırlamış olduğum "**Otomotiv Yerleşik Ağları İçin İzinsiz Giriş Tespiti**" adlı tezimin özgün bir çalışma olduğunu, tez hazırlanırken tüm aşamalarda bilimsel etik ilkelerine uygun davrandığımı, tez kapsamında sunulan tüm verileri bilimsel etik ilkelerine uygun elde ettiğimi, tezde faydalandığım tüm eserlere atıf yaptığımı ve kaynaklar kısmında bu eserleri gösterdiğimi beyan ederim……/……/20…

Boubacar SOW

İmza

ÖNSÖZ

Son yıllarda, otomotiv pazarı, inovasyonu zorlayan büyük rekabet ve ana pazar oyuncularının sınırlarının çizilmesi ile sürekli bir evrim geçirdi. Daha güçlü, daha verimli ve her türlü işlevi sunabilen yeni yerleşik sistemlerin entegrasyonu, giderek daha talepkar tüketicilerin ihtiyaçlarını karşılamayı mümkün kılıyor. Bu nedenle geleceğin üç ana ekseni elektrikli otomobil, bağlantılı otomobil ve otomatik otomobildir. Ancak yerleşik otomobil sistemleri, zorlu ortamlarda yolcu güvenliğini hedefleyen önemli güvenilirlik kısıtlamalarını karşılamalıdır. Bu sistemlerin çalışma güvenilirliği, gemideki insanların güvenliğini sağlamak için çok önemlidir.

Bağlantılı ve giderek daha akıllı hale gelen otomobil, gerçek bir bilgi teknoloji platformu haline geliyor ve böylece giderek daha çekici bir hedef haline geliyor. Bu tezde amacımız, otomobildeki ECU'ların çalışmasının tanımlanması ve anlaşılması ve böylece bir saldırı tespit sistemi (IDS) önermektir.

Bu tez çalışması sırasında, tez konusunun belirlenmesinden başlayarak son aşamaya kadar her konuda benden yardımlarını esirgemeyen danışman hocam Sayın Dr. Öğr. Üyesi İlyas ÖZER'e şükranlarımı sunarım.

Yüksek lisans serüvenime başlamam konusunda beni cesaretlendiren amcam Mohamed SOW'a ve bu süreçte her daim yanımda olan abim Oumar SOW'a, hayatım boyunca hep yanımda olan annem, babam teşekkür ederim.

ÖZET

YÜKSEK LİSANS TEZİ

OTOMOTİV YERLEŞİK AĞLARI İÇİN İZİNSİZ GİRİŞ TESPİTİ

Boubacar SOW

Bandırma Onyedi Eylül Üniversitesi
Fen Bilimleri Enstitüsü
Akıllı Ulaşım Sistemleri ve Teknolojileri Anabilim Dalı

Danışman: Dr. Öğr. Üyesi İlyas ÖZER
Ağustos 2022, 62 sayfa

Yerleşik otomotiv hesap makineleri veya ECU (Electronic Control Unit) araç içinde giderek artan sayıda özellikten sorumludur. Bu hesap makineleri, eylemlerini koordine etmek için iletişim veri yolları aracılığıyla veri alışverişinde bulunarak gerçek bir yerleşik ağ oluştururlar. Tarihsel olarak bu ağ kapalı bir sistem olarak kabul edilebilirlik, yerleşik bir ağa saldırı olasılığı güvenlik araştırmacıları tarafından kanıtlanmıştır. Otomobillerde birçok iletişim aracının ortaya çıkmasıyla birlikte bu ağ artık dışarıya da açık hale gelmekte ve bu alanda birçok güvenlik sorununu gündeme getirmektedir.

Bu tezde ilk olarak otomobildeki gömülü sistemlerin özelliklerini sunacağız. Ardından, modern otomobillerin yerleşik ECU'larını hedefleyebilecek farklı saldırı senaryolarını inceleyeceğiz. Daha sonra, gözlemlenen ağ trafiğine dayalı olarak yerleşik otomotiv ağları için bir saldırı tespit sistemi sunacağız. Ardından, yerleşik otomotiv ağlarını korumak için mevcut veya planlanmış çeşitli bilgisayar güvenlik mekanizmalarını sunacağız. Son olarak, bir CAN veri yoluna enjekte edilen saldırı mesajlarını öğrenmek için bir öğrenme modeli uygulayacağız.

Anahtar kelimeler: Güvenlik, Otomotiv, Saldırı Algılama, Gömülü Ağlar

ABSTRACT

M.Sc. THESIS

INTRUSION DETECTION SYSTEM FOR ON-BOARD AUTOMOTIVE NETWORKS

Boubacar SOW

Bandırma Onyedi Eylül University
Graduate School of Natural and Applied Sciences
Department of Intelligent Transportation Systems and Technologies

Supervisor: Asst. Prof. Dr. İlyas ÖZER
August 2022, 62 pages

Onboard automotive calculators or ECU (Electronic Control Unit) is responsible for a growing number of features in the vehicle. These calculators create a true on-board network by exchanging data via communication buses to coordinate their actions. While historically this network could be considered a closed system, security researchers have proved the possibility of an attack on an on-board network. With the appearance of many means of communication in automobiles, this network is now open to the outside and raises many safety problems in this area.

In this thesis, we will first present the characteristics of embedded systems in the automobile. Then we will study the different attack scenarios that can target the on-board ECU's of modern automobiles. Next, we will present an intrusion detection system for on-board automotive networks based on the observed network traffic. Then we will present the various existing or planned computer security mechanisms to protect on-board automotive networks. Finally we will implement a learning model in order to learn attack messages injected on a CAN bus.

Keywords: Security, Automotive, Intrusion Detection, Embedded Network

İÇİNDEKİLER

ŞEKİL LİSTESİ

Şekil **Sayfa**

TABLO LİSTESİ

Tablo **Sayfa**

SİMGE VE KISALTMA LİSTESİ

Simgeler	**Açıklama**
e	: Üstel Formülü
tan	: Tanjant Formülü

Kısaltmalar	**Açıklama**
ECU	: Electronic Control Unit
USB	: Universal Serial Bus
GSM	: Global System for Mobile Communications
GPS	: Global Positioning System
ASIC	: Application-Specific Integrated Circuit
OBD	: On-Board Diagnostics
V2X	: Vehicle to X
CAN	: Controller Area Network
LIN	: Local Interconnect Network
MOST	: Medya Yönelimli Sistemler Taşımacılığı
SAE	: Society for Automotive Engineers
PKES	: Passive Keyless Entry and Start
CRC	: Chain Reaction Cycles
CERT	: Computer Emergency Response Team
RFID	: Radio Frequency IDentification
TPMS	: Tire Pressure Monitoring System
IDS	: Intrusion Detection System
IPS	: Intrusion Prevention System
DMS	: Data Management System
HTM	: Hierarchical Temporal Memory
IoV	: Internet of Vehicule
RAM	: Random Access Memory
RPM	: Revolutions Per Minute
DoS	: Denial of Service
MLP	: Multi-Layer Perceptron

LSTM : Long Short-Term Memory

GRU : Gated Recurrent Unit

1. GİRİŞ

Bağlı, gittikçe daha zeki, otomobil hızlı bir değişim geçiriyor. Ancak bu gelişmenin bir dezavantajı var: gerçek bilgisayar bilimi platformu, araba giderek daha çekici bir hedef haline geliyor. Birbirleriyle bilgi alışverişinde bulunabilirler (örneğin yolun durumuna göre veya yol trafiği) veya ekosistemleriyle ve sürücünün müdahalesi olmadan dolaşıyor, modern arabalar sürüş kalitesini artıran ve yolcu güvenliğini artıran yeni özellikler sunar. Gömülü ve birbirine bağlı sistemler tarafından kontrol edilir, ancak sektör için yeni bilgisayar bilimi güvenlik sorunları ile üreticilerle karşı karşıya kalıyorlar.

Günümüzde, araçlar hem bilgi hem de eğlence sistemlerini ve en kritik işlevleri yöneten çok sayıda yerleşik bilgisayara ECU(*Electronic Control Unit,* Elektronik Kontrol Ünitesi) güvenir: enjeksiyon, frenleme, direksiyon ve, artan sayıda sürüş veya park yardımı fonksiyonları ile donatılmış araçlar için [1]. Bu tür işlevler, yerleşik bilgisayarların kullanılmasıyla mümkün kılınmıştır, ECU olarak adlandırılır, araca dağılmış bir dizi sensör ve aktüatör kullanarak bir arabanın farklı sistemlerini kontrol eden. Eylemlerini koordine edebilmek, bu ECU'lar iletişim veri yolları aracılığıyla birbirleriyle veri alışverişi yapar, bütün böylece gerçek bir yerleşik ağ oluşturur. Nihayetinde, bu mekanizmalarda yapılacak değişiklikler, insan yardımı olmadan hareket edebilen ve gerçek trafiğe girebilen tamamen otonom araçların tasarlanmasını mümkün kılacaktır. Ancak yazılıma devredilen işlevlerdeki bu artış karmaşıklığının da artmasına neden olur. Bu şekilde yerleşik sistemlerin artan karmaşıklığı, tasarımları sırasında ortaya çıkan hata riskini artırır. Bu tür arızalar, bu durumda, sonuçları aracın bütünlüğüne ve yolcularının güvenliğine ciddi şekilde zarar verebilecek arızaların nedeni olabilir [2]. Nitekim tarihsel olarak, bir arabanın araç üstü sistemleri kapalı bir sistem oluşturuyordu, yani tüm unsurların sadece birbirleriyle etkileşime girdiği ve çok özel durumlar dışında herhangi bir dış müdahaleye maruz kalmadığı (bir mekanikte geçiş), bu yerleşik bilgisayarlara karşı bilgisayar saldırısı riskini büyük ölçüde azalttı.

Ancak, otomasyona doğru evrimlerine paralel olarak, otomobiller aynı zamanda daha iletişimsel hale geldi. Artık çok yaygın olan USB anahtarları, Bluetooth, yerleşik GSM çipleri, wifi... cihazlar, aracın çeşitli yerleşik bilgisayarlarına erişmek isteyen bir bilgisayar korsanı için olası giriş noktalarıdır, güvenlik seviyesinin İnternetin ilk günlerindeki bilgisayarlara eşdeğer olduğu tahmin edilenler [1]. Dışarıyla tüm bu iletişim araçları, bir saldırgan için yerleşik ağa olabildiğince çok sayıda potansiyel giriş noktası oluşturur. Bu giriş noktalarından birinin başarılı bir şekilde izinsiz girmesi durumunda, mevcut otomobillerin ağ mimarisi, bir saldırganın kendilerine bağlı ECU'ların çalışmasını kesintiye uğratmak için iletişim veri yollarında mesajları

okuyup gönderebileceği anlamına gelir. Hedeflenen ECU'ların yeteneklerinin kapsamına ve kontrol ettikleri sistemlerin kritikliğine bağlı olarak, bu tür saldırıların sonuçları yolcular için basit bir uygunsuzluktan, aracın saldırgan tarafından geçici veya kalıcı olarak ele geçirilmesine kadar değişebilir [2]. Bir otomobil üreticisi, aracın multimedya sistemindeki bir güvenlik açığından yararlanan güvenlik araştırmacıları tarafından yapılan muhteşem bir uzaktan kumanda gösterisinin ardından Temmuz 2015'te ilgi odağı haline getirildi. Harici bir bilgisayardan, ön cam sileceklerinin kontrolünü ele geçirebildiler, radyonun sesini değiştirebildiler, frenleri uyguladılar, aynı zamanda direksiyonu çevirip motoru kapattılar [1]. Güvenlik açısından bir diğer önemli nokta: araç ve/veya sürücü ile üreticinin bilgisayar sistemi arasında bilgi alışverişine izin veren web uygulamaları. Kimlik doğrulama süreci yeterince güvenli değilse, saldırgan bir kullanıcının hesabına girebilir ve aracın kontrolünü ele geçirebilir. Bilgisayar güvenliği konusunda uzmanlaşmış mühendisler tarafından gerçekleştirilen çok sayıda test, bağlı araçların güvenlik açığını ortaya koymuştur. Büyük markaların sunduğu araçların büyük bir kısmı test edildi ve hacklendi. Güvenlik ve kimlik doğrulama konuları artık bu alandaki uzmanların yardımıyla ciddi bir şekilde ele alınmalıdır.

Bu makale aşağıdaki şekilde düzenlenmiştir. İlk bölüm, çalışmamızın bağlamının sunumuna ayrılmıştır. İlk Önce otomobillerdeki yerleşik sistemlerin özelliklerini, gelişimleriyle bağlantılı kısıtlamaları, yeniliğe yön veren mevcut eğilimleri sunuyoruz, ardından mevcut otomobillerde kullanılan ana ağ protokollerini açıklıyoruz. Sonra bu sistemlerle ilgili bilgisayar bilimi güvenliği konularını detaylandırıyor.

İkinci bölümde, bir arabanın yerleşik sistemlerini hedef alabilen farklı saldırı türlerini açıklıyoruz ve modern otomobillere karşı var olan tehditlerin çeşitliliğini vurgulamak için bu saldırıların dört eksende bir sınıflandırmasını sunuyoruz.

Üçüncü bölüm, bir saldırganın iç ağa erişim elde etmeyi başardığını ve bir veya daha fazla iletişim veri yolunda mesaj gönderebildiğini varsayarak bir saldırı tespit sisteminin sunumuna ayrılmıştır. Bir veri yoldan geçen her mesaj için, aracın durumu hakkında sahip olduğumuz bilgilere göre bunun meşru olup olmadığı.

Dördüncü bölüm, yerleşik otomotiv ağları için tasarlanmış, mevcut veya geliştirilmekte olan son teknoloji güvenlik mekanizmalarını sunar. Bu nedenle buradaki amacımız, gelecekte mümkün olduğunca kapsamlı bir savunma stratejisinin geliştirilmesini sağlamak için çok çeşitli mevcut araçları sunmak ve sınıflandırmaktır.

Beşinci Bölüm, bir enjeksiyon saldırısını gösteren bir veri tabanının analizini sunar.

2. ÇALIŞMANIN BAĞLAMI VE SORUN

Bugün elektrikli camlar, hava yastıkları, hız sabitleyici, hidrolik direksiyon... olmayan araba kullanmak zordur. Bunların hepsi, elektronik ve bilgi işlemin kavşağında yer alan mini beyinler gibi işlev gören gömülü sistem örnekleridir. Artık en yeni nesil bir araçta 100'den fazla sensör, araç tipine bağlı olarak 30 ila 80 bilgisayar ve bazen bir milyondan fazla kod satırı var (15 yıl önce bir uçakta olduğu kadar [3]). Bu bilgisayarlar, araç boyunca dağıtılan sensörleri kullanarak aracın çeşitli sistemlerini kontrol eder. Eylemlerini koordine edebilmek için ECU'ların birbirleriyle iletişim kurması ve böylece gerçek bir yerleşik ağ oluşturması gerekir. Diğer herhangi bir bilgisayar sistemi gibi, bir otomotiv ağının bir saldırganın daha sonra yararlanabileceği güvenlik açıkları içerebileceği göz ardı edilemez. Bu nedenle, modern otomobillerin bağlanabilirliği ile birlikte bu sistemlerin artan karmaşıklığı, acilen ele alınması gereken bilgisayar güvenliği sorunlarını gündeme getirmektedir.

Bu bölümde, özellikle yazılım kısmına odaklanarak ilk olarak yerleşik bilgisayarlara bakacağız. Ardından, otomobillerde kullanılan ve bu bilgisayarların birbirleriyle iletişim kurmasını sağlayan ağ mimarilerini sunuyoruz. Ardından araç içi sistemin risklerini tanımlıyoruz ve ardından otomobillerdeki araç üstü sistemlerle ilgili güvenlik konularına dikkat çekiyoruz.

2.1. OTOMOBİLLERE GÖMÜLÜ SİSTEMLER

Gömülü sistemler, belirli bir görevi yerine getirdikleri bir cihaza veya cihaza entegre edilmiş bağımsız elektronik ve bilgisayar sistemleridir. Genellikle gerçek zamanlı olarak, belirli bir zaman çerçevesi içinde doğru sonuçlar vermelidirler. Boyutları, tüketimleri ve bellekleri, toplam maliyeti azaltmak için optimize edilmiştir. Çoğu zaman, yerleşik bir sistem bilgi toplamak için sensörlerden (sıcaklık sensörleri, titreşim, ivmeölçer, GPS, vb.), bir bilgi işleme sisteminden, karar verme ve aktüatör kontrolünden (mikro denetleyici, mikroişlemciler, ASIC...) ve yazılım düzeyinde alınan kararların materyal transkripsiyonu için aktüatörler.

Otomobillerde iletişim ağlarının tanıtılması, bu nedenle verileri kolayca paylaşabilen yerleşik işlevlerin sayısındaki artışı desteklediyse, bunların araç güvenliği üzerindeki etkisi, üretim ve tüketim arasında zaten gecikmeler oluşturdukları nominal çalışma modunda baskındır. Örneğin önemli elektromanyetik bozulmalar ağlarda dolaşan çerçeveleri bozduğunda olduğu gibi, yalnızca bozulmuş durumlarda bilgi sağlar [4]. Bu nedenle, yerleşik iletişim ağlarının bir analizi, her zaman sistem güvenliği amacını dikkate almalıdır.

2.1.1. Kısıtlamalar

ECU'lar, herhangi bir yerleşik sistem gibi, çok özel ihtiyaçları karşılamak üzere tasarlanmıştır. Bir otomobil için yerleşik sistemler tasarlarken, bu nedenle aşağıdaki kısıtlamalar dikkate alınmalıdır.

2.1.1.1. Fiziksel Kısıtlamalar

Bir otomobil, istikrarlı ve homojen bir ortam oluşturmaz. Konumlarına bağlı olarak, bazı ECU'lar daha sonra, çalışmaya devam edebilmeleri gereken sıcaklık, nem veya şoklardaki büyük değişiklikler gibi fiziksel streslere maruz kalabilir.

2.1.1.2. Sınırlı Kaynaklar

Daha önce bahsedilen kısıtlamaların bir sonucu olarak, bir ECU'nun bilgi işlem gücü ve belleği, mevcut bir bilgisayara (hatta bir akıllı telefona) kıyasla genellikle çok sınırlıdır [2]. Bu nedenle gömülü yazılım, daha verimli donanım gerektirmeyecek ve dolayısıyla daha pahalı olmayacak şekilde ihtiyaç duyduğu kaynakları optimize edecek şekilde tasarlanmalıdır.

2.1.1.3. Ömür

Bir otomobilin ömrü, tipik bir bilgisayardan çok daha uzun, yaklaşık yirmi yıldır. Bu nedenle, yerleşik sistemlerin tasarımı ve izlenmesi, bu uzatılmış ömrü hesaba katmalıdır [2]. Bu nedenle, bu süre boyunca hem donanım (arızalı bir ECU değiştirebilmeniz gerekir) hem de yazılım açısından yerleşik sistemleri izleyebilmek gerekir.

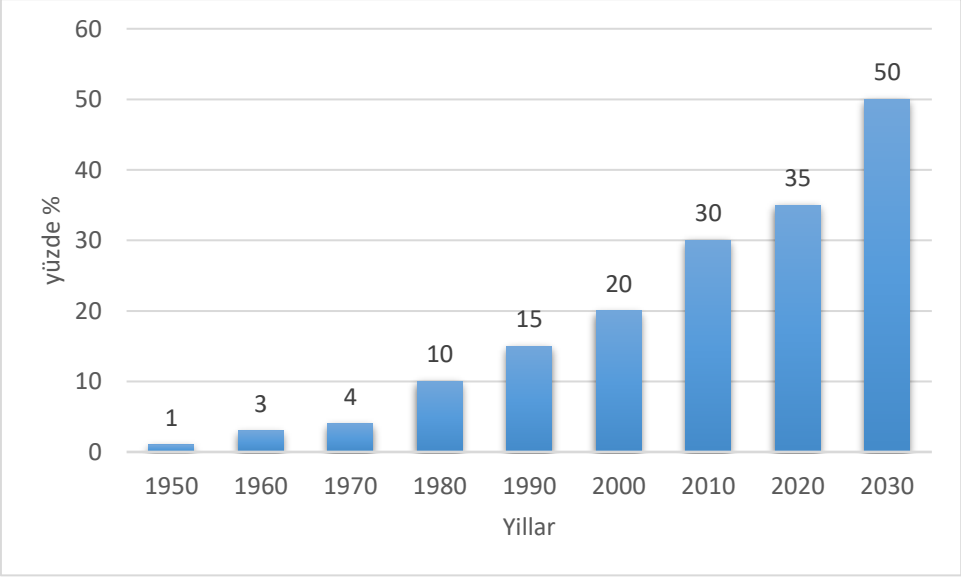
2.1.1.4. Gerçek Zamanlı

Daha önce de belirtildiği gibi, yerleşik sistemler kullanım alanlarına bağlı olarak farklı kısıtlamalara tabidir, peki, gerçek zaman, otomotiv sektöründe performans açısından, özellikle de Güvenlik açısından birincil kısıtlamalardan biridir. Geleneksel bir bilgisayarın önünde, birkaç dakikalık gecikme yalnızca kullanıcının ruh halini etkileyebilir, bir araç içi sistemde ise yalnızca birkaç saniyelik gecikme, korkunç sonuçları olan bir kazaya neden olmak için yeterlidir. Bu nedenle, aracın ve yolcularının güvenliğini garanti altına almak için belirli işlevler belirli bir süre içinde gerçekleştirilmelidir. Bu tür kısıtlamalara uyulmamasının feci sonuçlara yol açacağı durumlarda katı gerçek zamanlı sistemlerden (hard real time) bahsedeceğiz (bu, örneğin frenler gibi bir arabadaki kritik sistemler için geçerlidir). Buna karşılık, sözde yumuşak gerçek zamanlı

sistemler (*soft real time*), bu aşımları bir dereceye kadar tolere edebilir (örn. video akış hizmeti) [2].

2.1.1.5. Kalite Yönetimi

Otomotiv sektörü son derece rekabetçi bir sektördür. Üretilen büyük miktarlar arasında öne çıkmak için (2019'da 92,2 milyondan fazla ve 2020'de 77,6 milyondan fazla otomobil [5]), üreticilerin pazara düzenli olarak yeni modellerin gelmesine yol açan sürekli bir inovasyon ihtiyacı vardır. Yüksek rekabet ortamında rekabetçi kalabilmek için kalite yönetimi (*Quality Management*) politikalarının uygulanması esastır. Gerçekten de, müşteriler tarafından çok pahalı olarak kabul ediliyorsa veya ilgili geliştirme süresi ürünün piyasaya sürülmesini çok geciktiriyorsa, mümkün olan en iyi kalitede bir ürün sunmaya çalışmak yeterli değildir, böylece bir yeniliğin getirebileceği rakipler üzerindeki liderliğini kaybeder. Bu nedenle, bir otomobil tasarlarken bir üretici için zorluk, kalite, zaman ve maliyet arasındaki ideal uzlaşmayı bulmaktır. Bir otomobil tasarlama maliyetinde yerleşik elektronik sistemlerin (donanım ve yazılım) payı sürekli artıyor ve bugün üst düzey bir aracın maliyetinin %40'ını temsil ediyor [6]. Bu nedenle, bu gömülü sistemler, tasarımlarını optimize etmek için üreticiler tarafından büyük ilgi görmektedir.



Şekil 2-1: Elektronik ile karşılaştırıldığında araç fiyatı yüzdesi

2.1.2. Eğilimler

Araç içi otomotiv sistemlerindeki son yenilikler arasında iki ana eğilim ortaya çıkıyor: özerklik ve bağlanabilirlik.

2.1.2.1. Özerklik

Haziran 2020'de uluslararası bir standardın benimsenmesi, 2021'den itibaren 3. seviye otonom sürüşe izin verecek. Hâlihazırda yolda olan bir sürücü, çeşitli sürüş destek cihazlarıyla donatılmış bir aracı kullanabilir: seviye 2 menzile sahip bir araçtır (söz konusu sürüş yardımlarının mutlaka sürücü tarafından devre dışı bırakılabilmesi gerekir) [7]. Böylece güvenlik, sürüş yardımı, trafik yönetimi vb. alanlarda çeşitli kaynaklara erişebilir. Google'ın arabası, *Google car* seviye 3 menzile sahip bir araçtır. Bu aracın çatısında (fiyatı 80.000 dolar civarında) çalışması lazer teknolojisine dayanan bir sensör bulunuyor, bu sayede aracın çevresini 360 derece algılıyor [7].

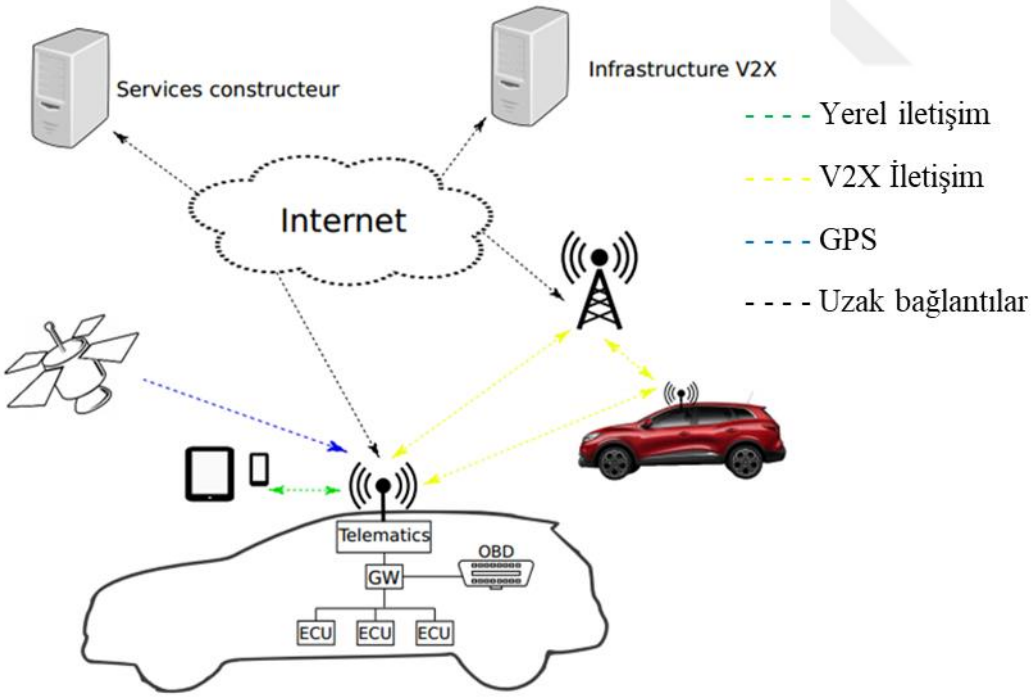
Tesla aynı zamanda Seviye 3 otonom olarak tasarlanmış araçlardır. Sistem sürüyor ve sürücü sistemi denetler ancak sürekli denetlemek zorunda değildir, sürmekten başka bir şey yapabilir, gerekirse aracın kontrolünü yeniden kazanabilmesi gerektiğinden, yine de sürüş konumunda oturmalıdır. Somut olarak, daha fazla özerkliğe yönelik bu eğilim, ECU'lar tarafından bir arabanın mekaniği üzerinde yürütülen kontrolde bir artışa dönüşüyor. ECU'lar tarafından işletilen işlevselliklerdeki bu artış, bu kontrol düzeyini uygulayabilmek için yerleşik sistemlerin karmaşıklığında bir artışa neden olur.

Şekil 2-2: Google'in otonom aracı

2.1.2.2. Bağlanabilirlik

Bağlantılı araçlar ve otomatik sürüş, kamu yol ağında hızla ortaya çıkmakta, bu nedenle yol güvenliğini artırmak, tıkanıklığı ve kirletici emisyonları azaltmak ve bireysel mobiliteye erişimi genişletmek için büyük umutlar yaratmaktadır. Böylece bir araç artık birçok ağın kesiştiği noktadadır:

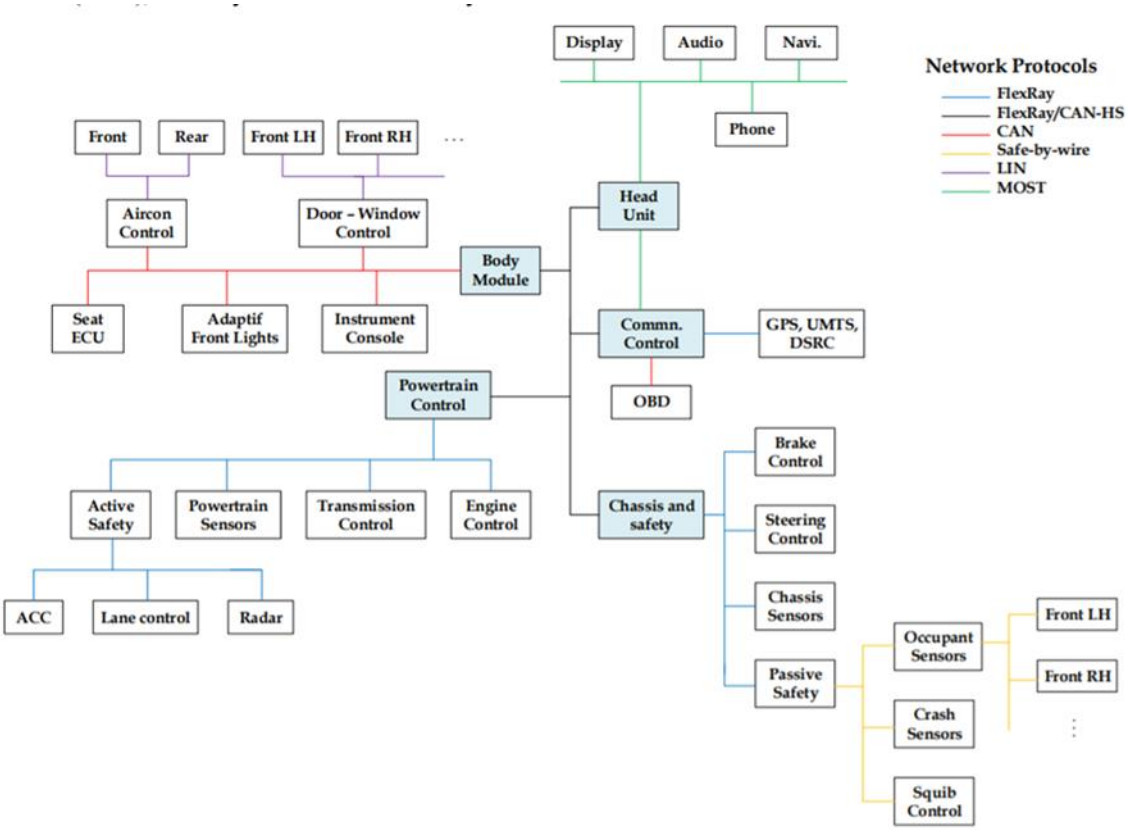
- İlk olarak, OBD (*On-Board Diagnostics*) bağlantı noktası aracılığıyla erişilebilen yerleşik bilgisayarların dâhili ağı.
- Araç aynı zamanda akıllı telefon veya tablet gibi mobil ekipmanlarla da bağlantılıdır.
- Araç, mobil ağlar (2/3/4G ve 5G) üzerinden internete bağlanabilir ve çeşitli servislere erişebilir.
- V2X iletişimi açısından iki seviye vardır:
    a. Yerel olarak, araç diğer otomobillerle iletişim kurar.
    b. Araç ayrıca, kendi başına bir ağ oluşturan inmiş bir altyapı (örneğin yol kenarında) ile de iletişim kurar.
- Son olarak araç, verileri uydu üzerinden alır (örnek: GPS).



Şekil 2-3: Modern bir brabanın farklı ağları

2.2. GÖMÜLÜ AĞ MİMARİSİ

Modern araçlar, farklı alanlarda farklı ağ protokolleri kullanır, seçim alanın işlevsel gereksinimleri, kritiklik, maliyet vb. gibi faktörler tarafından belirlenir. Birçok protokol arasında, *Local Interconnect Networks* (LIN), *Controller Area Networks* (CAN), FlexRay ve *Media Oriented Systems Transport* (MOST) günümüzde farklı üreticiler tarafından en yaygın kullanılan protokollerdir. Safe-by-wire gibi özel ağlar, hava yastıkları ve diğer aktif güvenlik sistemleri gibi güvenlik sistemleri için kullanılabilir [8].



Şekil 2-4: Modern bir aracın tipik yerleşik ağı

Araçlardaki çeşitli ağlar, öncelikle maliyet ve performans gereksinimlerine dayalı olarak gelişmiştir. SAE (*Society for Automotive Engineers*), iletişim protokollerini ağdaki hızlarına ve işlevlerine göre dört kategoriye (A'dan D'ye Sınıflar) ayırmıştır. Bu sınıflandırma aşağıdaki tabloda detaylandırılmıştır. A Sınıfı ağlar, en düşük aktarım hızlarını (10 kb/s'den az) sunar ve düşük maliyetli teknolojilere dayanır. Basit verileri düşük maliyetle, tipik olarak bir ECU ile sensörler veya aktüatörler arasında iletmek için kullanılırlar. B Sınıfı ağlar (10kb/s ile 125Kb/s arasında), güçlü gerçek zamanlı kısıtlamalar olmadığında ECU'lar arasında veri aktarımı için

tasarlanmıştır. C Sınıfı ağlar (125Kb/s'den 1Mb/s'ye kadar), gerçek zamanlı iletişim gerektiren işlevler için veri aktarımına izin verir (motor ve şasiyi kontrol eden alanlar için durum böyledir). Son olarak, D sınıfı ağlar, 1Mb / s'den daha büyük bir verime sahip tüm ağları kapsar. Bunlar günümüzde multimedya veri aktarımı için kullanılmaktadır veya X-by-wire işlevlerinde olduğu gibi çok yüksek güvenilirlik gerektirir.

Tablo 2-1: SAE'ye göre otomotiv ağlarının sınıflandırılması

	Hızı	Alan adı	Protokol
Sınıf A	Daha az 10 Kb/sn	Body Domain: alt uç	LIN
Sınıf B	10 ila 125 Kb/sn	Body Domain: Kritik olmayan ve tanılayıcı olmayan	Single-wire CAN (SWC) & CAN 2.0
Sınıf C	125 Kb/sn - 1 Mb/sn	Powertrain Domain: kritik parametreler ve gerçek zamanlı	HS-CAN
Sınıf D	1 Mbps'den büyük	Powertrain, Chassis: Zaman gerçek zor ve güvenilirlik	FlexRay
		Occupant Safety: Gerçek zamanlı ve güvenilirlik	Safe-by-wire
		Multimedya akışı ve eğlence	MOST

2.3. GÖMÜLÜ SİSTEMİN RİSKLERİ

Otomobillerdeki araç üstü sistemlerin teknolojik gelişimi, bu sistemleri kullanılamaz hale getirebilecek ancak hepsinden önemlisi tehlikeli olabilecek herhangi bir tehdide karşı giderek daha savunmasız hale getiriyor. Buna ek olarak, bazı sistemler için bir sonuç yükümlülüğü gerektiren güçlü gerçek zamanlı kısıtlama vardır. Dolayısıyla bu sistemlerin karmaşıklığı onları her türden tehdide, özellikle viral saldırılara, kötü niyetli izinsiz girişlere ve hatta sistemin başkaları tarafından tamamen kontrolüne maruz bırakır. Bu riskler, sistem verilerinin gizliliği, özgünlüğü ve kullanılabilirliği üzerinde doğrudan bir etkiye sahip olacaktır.

Ayrıca, ister donanım ister yazılım düzeyinde olsun, sistemin kendi arızasıyla doğrudan ilişkili olabilecek içeriden gelen tehditlerle de karşılaşabiliriz. Otomotiv sistemlerinin güvenliğini

garanti altına almak için ISO 26262 [9]gibi standartların oluşturulmasına rağmen, tehdidin ortaya çıkma riski devam etmektedir. Yanlış kod satırları, en iyi ihtimalle ürünün kalitesi üzerinde, en kötü ihtimalle ise ürünü kullanan kişinin doğrudan güvenliği üzerinde bir etkiye sahip olacaktır. İç veya dış riskler olsun, etkilerin çok ciddi sonuçları olabilir. Klima sistemindeki bir arızanın yansımaları, fren sistemi veya hava yastığı sistemindeki ile aynı olmayacaktır. Bu nedenle, yerleşik sistemler, esas olarak bu dört işlevsel olmayan niteliği korumak için kullanıcılarına operasyonel güvenliği garanti etmelidir [10]:

- **Güvenilirlik:** Sistemin belirli bir süre sonra hala çalışır durumda kalmasını sağlamaktır.
- **Uygunluk:** İstenilen bir hizmetin her an verilebilmesi gerçeğidir.
- **Bakım:** Hâlihazırda kullanımda olan bir sistemi geri yükleme veya iyileştirme yeteneğidir.
- **Güvenlik:** Bu nokta, öncekilerle bağlantılıdır, en önemlisidir, çünkü ciddi kazaların meydana gelmemesini sağlayan budur.

2.4. OTOMOBİLLERDE GÜVENLİK SORUNLARI

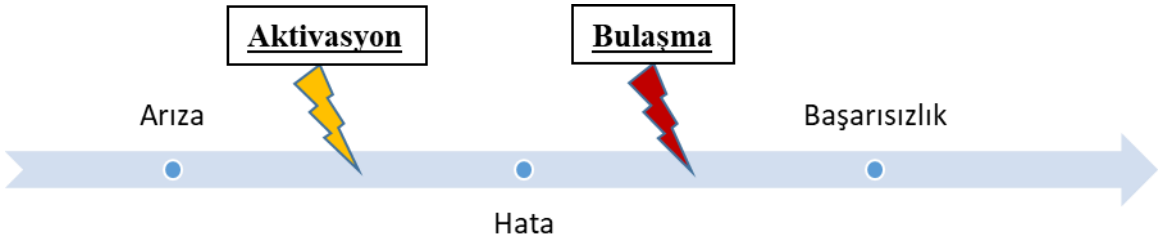
Dolayısıyla iki tür tehdidimiz var: iç tehditler ve dış tehditler.

2.4.1. İç Tehditler

İçeriden öğrenen tehditler, bir sistemin zayıf tasarımı veya sürdürülebilirliği nedeniyle oluşturabileceği tüm arızalardır. Bu nedenle, gömülü bir sistemin operasyonel güvenliğine yalnızca yazılım düzeyinde odaklanacağız.

Yazılım tasarımı, arıza durumunda ürüne benzer etki yaratma riskleri nedeniyle elektronik tasarımı kadar önemlidir. Hesap makinesinin “işleme” kısmıdır ve bu nedenle hiçbir durumda kusuru olmaması gerektiğinden hassas bir şekilde geliştirilmesi gerekir. Geliştiriciler tarafından kontrol edilmeyen birçok "bug" sunabilen programların karmaşıklığı nedeniyle bugün sistemin en kritik parçası haline geldi. Sistemdeki bir arızanın neden olduğu bir hatanın sonucu olarak bir arıza ortaya çıkabilir. Bu nedenle kusur, kullanıcı tarafından görülebilen ve sistemi kullanılamaz hale getiren bir arızanın sonucudur. Bir arıza, bu arızayı içeren işlemler çağrılıncaya kadar bir hata oluşturmaz, tersi gerçekleştiğinde arızanın aktivasyonu gerçekleşir ve dolayısıyla bir hata oluşturur. Elbette, bir bileşen diğerleriyle iletişim kurar, bilgi alışverişinde bulunur ve birinin sonucunu diğerinin işlemleri için kullanır, böylece hatalı bir bileşen, sonucunu gerektiren bir

bileşene hatalı veriler iletebilir. Bu, sistemin kirlenmesidir, çünkü tüm bileşenler, kaçınılmaz olarak arızaya neden olan hatalı verilere sahip olacaktır.



Şekil 2-5: İçeriden tehdit süreci.

Uygun programlama ortamları kullanılarak özel geliştirme yoluyla sistem tasarlanırken arızadan kaçınılabilir ve kaçınılmalıdır. Böyle bir sistemin gerçekleştirilmesi için gerçek zamanlı işletim sisteminin kullanılması esastır. Bu tür işletim sistemi nihai bir sonucu garanti etmez, ancak gerçek zamanlı davranış elde etmek için geliştirmeyi kolaylaştıran hizmetler ve araçlar sağlar [10]. Ancak, sistemin üretimi sırasında, çalıştırıldığında, kötü tasarımdan değil, ortamın parazit gibi kısıtlamalarından dolayı arızalar ortaya çıkabilir. Bu nedenle, tasarım sırasında öngörülen çoğaltma veya kontrol noktaları tekniği gibi çözümlerle sistemin yürütülmesi sırasında destekleri sağlanmalıdır. Bu çözümler, daha önce de belirtildiği gibi, karşılaşılan arıza türünün kritikliğine bağlıdır, özellikle etkilenen bileşenler güvenlikle ilgili olduğunda, bazı arızaların kullanıcı için çok ciddi sonuçları olabilir. Bazen sistem için bir hatanın olup olmadığını bilmek yeterlidir, ancak diğer durumlarda (en kritik için) başarısızlığı önlemek ve güvenilirliği garanti etmek için alternatif bir çözüm bulunmalıdır [10].

2.4.2. Dış Tehditler

Günümüzde araçlar, güçlü bir ara bağlantıya sahip gömülü sistemleri giderek daha fazla kullanıyor ve onları her türlü kötü niyetli saldırıya karşı savunmasız hale getiriyor. Wi-Fi, Bluetooth, coğrafi konum ve hatta Keyless (temassız anahtar) gibi araçlar, her türlü bilgisayar korsanlığının giriş noktalarıdır. Bununla birlikte, sisteme zarar vermek için bilgisayar korsanlığından daha az karmaşık yöntemler mevcuttur. Her biri kendi motivasyonuna sahip olan kötü niyetli kişiler bu sistemlere zarar verebilir ve bu da bu sistemlerin verilerinin gizliliğini, kullanılan ürünün performansını ve her şeyden önce kullanıcının güvenliğini zedeleyebilir.

2.4.3. Saldırı Türleri

Gömülü sistemler, en temelden en karmaşığa kadar farklı saldırı yöntemlerine sahiptir ve her birinin kendine özgü özellikleri, farklı hedeflere ulaşmayı amaçlar.

2.4.3.1. Donanım Saldırıları

Donanım saldırıları, yerleşik sistemin tüm bileşenlerini veya onunla iletişim kurması muhtemel olanları yok etmek, zarar vermek veya sabote etmek için hedefler. İki tür donanım saldırısını tanımlayabiliriz:

- **Müdahaleci:** Yani, sistemin işleyişi üzerinde güçlü bir etkiye sahip olan ve yok olmasına kadar gidebilen donanım saldırıları.
- **Müdahaleci olmayan:** Sistem üzerinde görünür bir iz bırakmayan ve işlevsel kalan saldırılarıdır.

2.4.3.2. Yazılım Saldırıları

Ana amacı, özellikle mevcut ECU'ları kullanarak, ağa kötü amaçlı kod enjekte ederek veya hatalı çerçeveler göndererek, araç ağının tamamını veya yalnızca bir kısmını kontrol altına almak olan yazılım saldırıları. Bunu yapmak için, saldırının ağına erişmek için araca bir giriş noktasıyla etkileşime girmesi gerekecek. Radyo, Wi-Fi veya OBD-II portu (araç bilgilerine erişim için bağlantı portu, teşhis aracı olarak kullanılır) gibi unsurlar olası bir saldırıya giriş noktalarını temsil edebilir. Ayrıca, tasarım gereği, CAN veri yolunun kusurlu olacağı ve sistem saldırganlarının çeşitli giriş noktalarından ağa erişme olasılığını bırakacağı belirtildi. Aslında bu iletişim yapısı, OBD-II portu üzerinden bağlanmanın basit gerçeği, verilerin net bir şekilde okunmasına izin verdiği için herhangi bir veri gizliliğini garanti etmez [10].

Uzaktan açma artık tüm yeni otomobillerde mevcut, ancak bu sistemde bir güvenlik açığı olabilir. Gönderilen sinyallerin şifrelenmesine rağmen, şifrelemeyi tespit etmek için karmaşık yöntemler mevcuttur. Keeloq şifrelemesi, anahtar tarafından yayılan sinyali kaydetmeyi ve daha sonra aracın kilidini açmak için tekrar oynatmayı içeren bir yuvarlanan kod örneğidir. Ancak bu sinyal, araca iletilmek üzere başka bir programlanabilir kutu tarafından karıştırılabilir ve engellenebilir ve böylece sahibinin bilgisi olmadan kilidi açılabilir [10]. Web tarayıcısının yüklü olduğu yeni bir araba olması durumunda, güvenlik açıkları, araçta bulunan virüsler, solucanlar veya diğer enfeksiyon türleri aracılığıyla, geleneksel bir bilgisayardaki bir web tarayıcısıyla aynı

şekilde araca maruz kalabilir. Sistem verilerine ve potansiyel olarak iletişim veri yoluna erişim sağlar.

Saldırgan bir kusurdan yararlanır yararlanmaz, tüm sistemlere erişmek ve orada en iyi veri okumasını veya en kötü kötü niyetli eylemleri kontrol altına almak için ona çok sayıda olasılık sunulur. Bu nedenle, başarılı bir saldırının sonuçları, saldırının ciddiyetine bağlı olarak değişir. Bununla birlikte, aracın marka imajı, araç sahibinin finansal yatırımı ve en ciddi durumlarda olumsuz etkiler garanti edilir: kendi hayatını tehlikeye atıyor.

3. ENTEGRE OTOMOBİL AĞLARINA SALDIRILAR

Bölümde, modern bir otomobildeki yerleşik bilgisayarları hedefleyebilecek farklı saldırı türlerini ayrıntılı olarak analiz edeceğiz. Bu nedenle, bir saldırganın eylemlerini sınıflandırmaya izin verebilecek bu tür saldırılarda yer alan tüm unsurlarla ilgileniyoruz.

3.1. BİR SALDIRININ AYRISTIRILMASI

Bir otomobil tarafından taşınan ekipmanlara yönelik saldırılar çeşitli şekillerde olabilir. Ayırt etmek önemlidir:

- Ağına girmeden aracın normal davranışını değiştirmeyi amaçlayan saldırılar, örneğin bir çarpışma önleyici radarı bozmak için bir sinyal yayarak. Bu saldırılar esas olarak araç ara yüzlerini hedef alır.
- Bilgisayar saldırıları, saldırganın gönderdiği komutların araç bilgisayarları tarafından yürütülmesi yoluyla araçtaki yerleşik ağın tamamının veya bir kısmının kontrolünün ele geçirilmesini amaçlayan, enjekte edilen kod veya iletilen kötü niyetli ağ çerçeveleri aracılığıyla.
    a. Saldırganın özel olarak yerleşik ağa erişmeye çalışmadığı, ancak yerleşik ağın bir öğesinin güvenliğinin ihlal edilmesinin ardından kurtarabileceği verilerle ilgilendiği bilgisayar saldırıları(bu nedenle aynı zamanda nihai hedeftir). Bir arabada gerçekleşen konuşmaları dinlemek için telematik sistemine yapılan bir saldırı bu kategoriye girer.
    b. Saldırganın, araç üzerindeki ağ aracılığıyla giriş noktasından aracın geri kalanıyla etkileşime girmeye çalışacağı bilgisayar saldırıları.

Araştırmamız sırasında, özellikle bilgisayar saldırılarıyla ve özellikle de yerleşik ağ üzerinden yayılan saldırılarla ilgilendik.

3.1.1. Saldırganın Hedefleri

Olası saldırı senaryolarına bakmadan önce, araç içi sisteme yönelik bir bilgisayar saldırısını motive edebilecek çıkarların neler olduğunu kendimize sormalıyız.

3.1.1.1. Hırsızlık

Belki de ilk bakışta en belirgin motivasyon hırsızlıktır. Taşıdığı elektroniğe güvenerek bir aracı (veya içindekileri) çalmak için çeşitli olasılıklar vardır. Uzaktan açma sistemine yapılan başarılı bir saldırı arabanın kilidini açabilir, hatta başlamak için artık temas gerektirmeyen araçlarda (**PKES** *Passive Keyless Entry and Start)* bile çalıştırabilir. Başka bir olasılık, ilgili ECU'lerin kontrolünü ele geçirmek için kablosuz iletişim protokolündeki bir güvenlik açığını kullanmaktır, daha sonra gizlice arabanın kilidini açmak ve immobilizer mekanizmalarını devre dışı bırakmak için kullanın veya veri yollarına talimat göndererek olası bir alarm [2]. Bu durumlarda gibi saldırganın kazancı, çalınan aracın veya içerdiği malın değeridir.

3.1.1.2. Araç Sabotajı

Bu kategori, aracın çalışmasını bozmayı amaçlayan her şeyi içerir. Bu, bir veya daha fazla ECU'nun devre dışı bırakılması veya çalışmasının değiştirilmesinden oluşur, gömülü yazılımlarını değiştirerek, kötü niyetli çerçeveler göndererek veya iletişim veri yollarında hizmet reddine neden olarak. Sonuçlar basit bir uygunsuzluktan (örneğin klimanın kesilmesi) potansiyel olarak ölümcül bir kazanın tetiklenmesine (artık tepki vermeyen frenler) kadar değişebilir. Bu durumda çok sayıda araçta meydana gelen ufak bir arıza bile üreticinin markasının imajını kalıcı olarak bozmaya yeterli olabilir.

3.1.1.3. Fikri Mülkiyet Hırsızlığı

Saldırgan hedeflenen aracın çalışması hakkında gizli bilgiler elde etmeye çalışabilir, örneğin veri yolundan geçen çerçeveleri dinleyerek ve tanımlayarak veya hatta bir ECU'nun kaynak kodunu alarak. Rakipler tarafından bu tür yöntemlerin olası kullanımının ötesinde, bu bilgiler ayrıca sahte ECU'ların üretilmesine ve ticaretine izin verebilir veya donanımdaki güvenlik açıklarını bir saldırgana ifşa edebilir.

3.1.1.4. Gizli Verilerin Çalınması

Arabalar giderek daha fazla bilgisayar ekipmanı taşıdıkça, bir saldırganın kurtarmaya çalışacağı kişisel bilgileri içerebilirler. Örneğin, telefon rehberi ve arama geçmişi listesinden, son yolculukların GPS koordinatlarından ve hatta multimedya ara yüzüne kaydedilen favori radyo frekanslarından alıntı yapabiliriz.

3.1.1.5. Araç Kapasitelerinin Modifikasyonu

Araç sahibinin aynı zamanda "saldırgan" olduğu tüm durumları bu kategoriye dâhil ediyoruz. İkincisi daha sonra kodda veya bir ECU'da bulunan verilerde yetkisiz değişiklikler yapmaya çalışacaktır. Örneğin, daha yüksek bir fiyata satmak için kilometreyi azaltmak, daha fazla güç elde etmek için motorun çalışmasını değiştirmek veya hatta yasadışı yollardan edindiği yeni programları araç bilgisayarına yüklemek isteyebilir. Saldırgan, paradan tasarruf etmek için üretici tarafından onaylananlar dışındaki ECU'ları kurmak için kimlik doğrulama mekanizmalarını atlamayı da deneyebilir.

3.1.1.6. Entelektüel Meydan Okuma

Son olarak, sadece bir aracın kontrolünü ele geçirme zorluğuyla motive olan saldırgan da dışlanmamalıdır.

3.1.2. Gömülü Ağ İle Etkileşimler

Günümüzde otomobillerde kullanılan ağlar, her şeyden önce güvenlik açısından tasarlanmıştır. Bir saldırganın ona bağlanmayı başardığını varsayarsak, şimdi ona açık olan olasılıklarla ilgileniyoruz.

3.1.2.1. ECU'ların Güvenlik Açıkları

Tasarım gereği, CAN ağı olduğu gibi birinci bölümde tanımlanan güvenlik özelliklerine izin vermez.

- **Gizlilik:** Yapısal olarak, CAN üzerinden gönderilen herhangi bir mesaj (fiziksel ve mantıksal olarak) tüm düğümlere açık bir şekilde yayınlanır. Aslında, kötü niyetli bir düğüm, bağlı olduğu veri yolunun tüm trafiğini dinleyebilir.
- **Kullanılabilirlik:** CAN'ın tahkim kuralları, bir saldırganın sürekli olarak öncelikli çerçeveler göndererek veri yolunda hizmet reddine neden olmasını kolaylaştırır, böylece diğer tüm ECU'ları iletimi durdurmaya zorlar.
- **Özgünlük:** Bir CAN çerçevesi göndericisinin tanımlanması için bir alan içermez [2]. Bu nedenle, herhangi bir düğüm, uygun mesajları göndererek aynı veri yolundaki diğerlerini kontrol edebilir.
- **Bütünlük:** Daha önce gördüğümüz gibi, CAN, bir CRC (*Chain Reaction Cycles*) sayesinde bir mesajın iletimi sırasında meydana gelen yanlışlıkla yapılan değişiklikleri

tespit etmeyi mümkün kılar. Ancak bu güvenlik açısından yeterli değildir çünkü bir saldırgan göndermek istediği çerçevelere karşılık gelen geçerli bir CRC oluşturabilmektedir [2]. Bu nedenle bir mesajın bütünlüğü garanti edilmez.

- **İnkâr etmemek:** Bir düğümün gerçekten bir mesaj gönderdiğini veya aldığını ve dolayısıyla ağdaki bir saldırının kaynağı olup olmadığını kanıtlamak mümkün değildir. Bu güvenlik özellikleri mevcut otomotiv ağları tarafından garanti edilmez (FlexRay hakkında da benzer açıklamalar yapılmıştır) [2], bir sonraki adım, bir ECU'nun veya hatta bir bütün olarak ağın kontrolünü sağlamak için bu boşluklardan yararlanmanın mümkün olup olmadığıdır.

3.1.2.2. Olası Eylemler

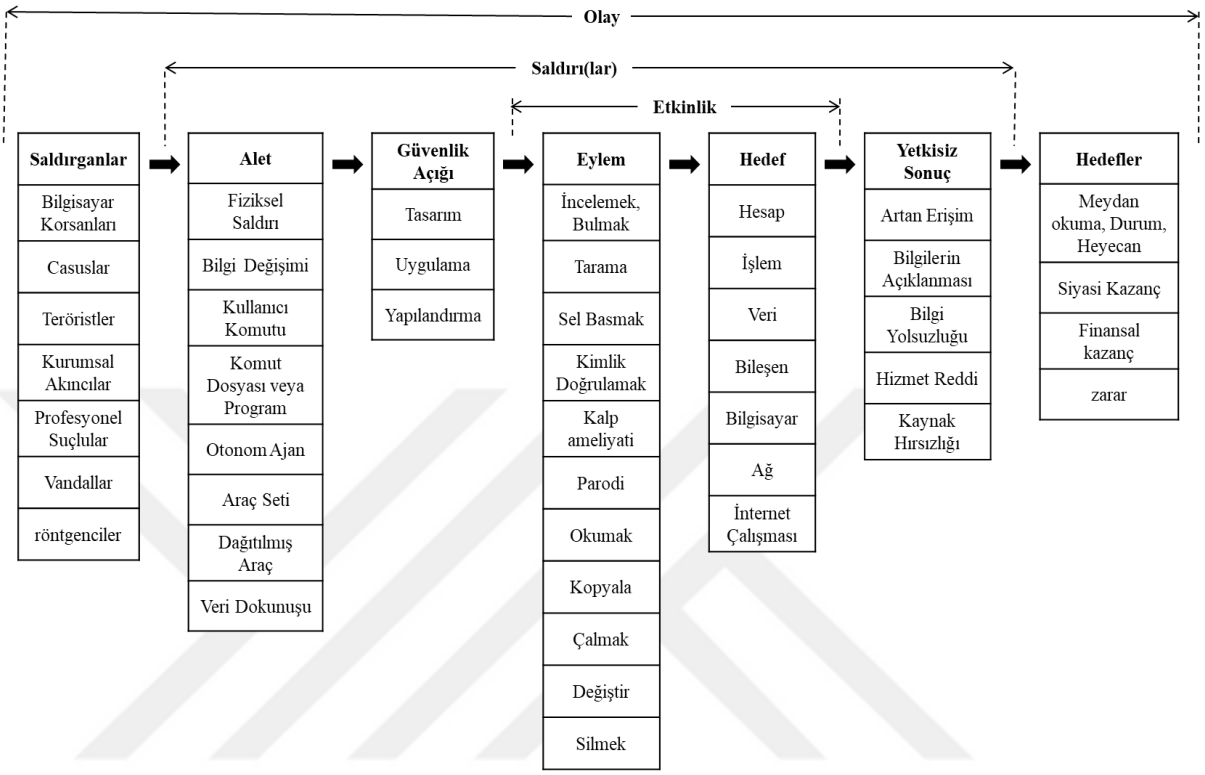
Saldırganın hedefiyle ancak bağlı olduğu ağ(lar) (kablolu veya değil) üzerinden etkileşime geçebileceğini düşünüyoruz. Güvenlik özellikleri garanti edilmezse, amaçlarına ulaşmak için gerçekleştirebileceği temel eylemler bu nedenle aşağıdaki listeye dahil edilmiştir.

- **Okuma:** Saldırganın ağ trafiğine erişimi vardır ve her çerçevenin içeriğini görebilir.
- **Kesinti:** Saldırgan, gönderilen bir mesajın alıcılarına ulaşmasını engeller. Bu nedenle herhangi bir bilgi almazlar. Hizmet reddi saldırısının amacı budur.
- **Değişiklik:** Saldırgan, yasal olarak gönderilen bir iletinin içeriğini değiştirir, böylece alıcılar yalnızca kaynak doğru bilgileri gönderdiğine inandığında değiştirilmiş sürümü alır.
- **İmalat:** Saldırgan, mesajları ya sıfırdan oluşturarak ya da daha önce gözlemlenen mesajları yeniden oynayarak ağdaki başka bir düğüm gibi davranarak kendisi gönderir.

3.1.3. Saldırıların Modellenmesi

3.1.1'de gördüğümüz gibi, bir araba ağına bilgisayar saldırıları gerçekleştirmenin birçok nedeni vardır. Bu nedenle, araç içi bilgi işlemi hedefleyen saldırganların varlığını varsaymak meşrudur. Bu motivasyonların her birine bir veya daha fazla saldırgan türü karşılık gelebilir, farklı kaynaklara sahip olan (bilgi düzeyi, araçlar, finansal kaynaklar), o zaman amaçlarına ulaşmak için çeşitli yöntemlere sahip olacaklardır. Bu parametrelerin kombinasyonları çeşitli olası saldırı senaryolarına yol açar. Otomobile uyarlanmış modeli yeniden üretiyoruz. Bu model, CERT'ler (*Computer Emergency Response Team*) tarafından olayların sınıflandırılması için kullanılan modele dayanmaktadır [11]. Bu sınıflandırma etkinlikler, saldırılar ve olaylar arasında ayrım yapar. Böylece bir etkinlik, şeklin orta kısmına karşılık gelen bir hedefe karşı bir eylemin

uygulanmasından oluşur. Bir saldırının tanımı, kullanılan araçları, yararlanılan güvenlik açıklarını ve sistemdeki bu eylemlerin sonuçlarını da dikkate alır. Son olarak, bir saldırıya karşılık gelen olay, saldırgan ve amaçları belirlenerek sınıflandırılır.



Şekil 3-1: Otomotiv ortamına uyarlanmış cert sınıflandırması

Şu anda, aşağıda göreceğimiz gibi, otomobil ağlarına yönelik birçok saldırı örneği bulmak mümkün olsa da, dolaşımdaki arabaları içeren güvenlikle ilgili çok az olay rapor edilmiştir. Şimdilik, bu nedenle, bu tür sınıflandırmaların tüm gerçek tehditleri yeterince temsil edip etmediğini çok az veriyle belirlemek zor görünüyor.

3.1.4. Bir Saldırının Sonuçları

Klasik bir sisteme yapılacak bir saldırı, elbette, onun üzerinde zararlı etkileri olacak ve bu da onun yok olmasına yol açabilecektir. Bununla birlikte, gömülü bir sistemin bozulması, yalnızca sistem üzerinde değil, özellikle sistemin ciddi kısıtlamaları nedeniyle kullanıcı üzerinde yankı uyandırabilir. Bu nedenle bir saldırı, kullanıcıları tehlikeye atmak da dâhil olmak üzere birçok olumsuz yansıma pahasına saldırganın hedefine ulaşmasıyla sona erer.

İki farklı sonuç kategorisi buluyoruz:

- **Fonksiyonel:** Bunu sistemin işlevselliği üzerindeki olumsuz etkileri açıklar, saldırganın manipüle ettiği veya zarar verdiği.
- **Yapısal:** Bunlar, sistemin ortamıyla doğrudan ilgili sonuçları temsil eder, yani araca. Bu sonuçlar saldırganın amaçlarıyla değil, ortaya çıkan yan etkilerle ilgilidir. Çevresel etkiler bu nedenle sürücüyü tehlikeye atmayı içerir.

Bu ayrımları göstermek için, kritik bir veri yolundaki ECU'ları kontrol etmek isteyen ve bunun üzerine çerçeveleri başarılı bir şekilde ileten ve böylece ağ trafiğini artıran saldırganı düşünün. Bu çerçeveler düşük bir tanımlayıcıya sahip olduğundan, tahkim kuralları veri yolundaki mesajlarına öncelik verir ve bu nedenle diğer mesajların iletimini geciktirerek kritik işlevlerin yürütülmesinde potansiyel olarak gecikmelere neden olur. Burada işlevsel sonuçlar, saldırgan tarafından gönderilen çerçevelerin neden olduğu tepkiler olacaktır. Yapısal sonuçlar, ağ tıkanıklığının geri kalan veri yolu bilgisayarları üzerindeki etkisiyle ilgilidir (düşük moda geçiş, gecikmeli tepkiler...).

3.2. FARKLI SALDIRILAR

Bu bölümde, yerleşik ağa erişimi olduğunda bir saldırgana sunulan olanaklarla ilgileniyoruz, yani ağdaki bir (veya daha fazla) düğüm üzerinde kontrolü vardır.

3.2.1. Yerel Saldırılar

Saldırıları aracın araç içi ağı üzerindeki etkisine göre kategorize ettik. İlk olarak, bir saldırganın etkileşimde bulunmak istediği ağ hakkında yeterli bilgi edinmesine izin veren yöntemleri sunuyoruz. Ardından, yerleşik ağdaki geçici saldırıları detaylandırıyoruz. Son olarak, ağdaki kalıcı saldırıyla ilgileniyoruz.

3.2.1.1. Sisteme Aşinalık

Bir saldırıdaki ilk adım, genellikle her bir çerçevenin rolünün ne olduğunu anlamak için sistem hakkında bilgi edinmek olacaktır. CAN ağı (ve diğer yaygın olarak kullanılan protokoller) veri gizliliğini garanti etmez, bir veri yoluna bağlı olmanın basit gerçeği, trafiğini net bir şekilde gözlemlemek için yeterlidir. Böylece ağın işleyişini keşfetmek için "kara kutu" saldırıları gerçekleştirilebilir. Bunu, gözlemlemek istediğiniz sistemle aynı veri yoluna bağlanarak yapılır.

Son olarak, bazı ECU'ların nasıl çalıştığını daha derinlemesine anlamak için içerdikleri kodu alıp hata ayıklayarak tersine mühendislik yapmak hala mümkündür. Araç modellerine bağlı olarak (ve dolayısıyla yerleşik ağın mimarisine bağlı olarak), trafiğin önemli bir bölümünü dinleyebilmek için OBD portu üzerinden basit bir bağlantı yeterlidir ve birçok ECU ile doğrudan etkileşime girer.

3.2.1.2. Geçici Devralma

Hedef araç hakkında yeterli bilgi edinildikten sonra, gözlemlerin ardından seçilen belirli çerçevelerin iletimi, normal olarak başka bir ECU tarafından yayınlanan talimatları göndererek veya başka koşullar altında doğrudan bilgisayarlar üzerinde hareket etmeyi mümkün kılacaktır. Literatürdeki örnekler çok sayıda ve ayrıntılı olmaya başlıyor: bazıları keşiflerinin sonuçlarını anonimleştirirken (aracın markasını açıklamayarak ve yayılan çerçevelerin bazılarını maskeleyerek) sonuçlarının potansiyel olarak kötü niyetli yeniden kullanılmasını önlemek için, diğerleri, saldırdıkları arabaların modellerini açıkça adlandırır ve çalışmalarını çoğaltmak ve sürdürmek için gerekli tüm araçları sağlar.

Bu nedenle, saldırılardan etkilenen veri yola bağlı olarak, sonuçların yolcuların güvenliği üzerinde değişken etkileri olabilir, küçük bir rahatsızlıktan (örneğin artık çalışmayan elektrikli camlar veya radyonun sesinin bloke olması) ölümcül risklere (hava yastığının kesilmesi, frenler...) kadar değişebilir. Bununla birlikte, bu siparişin en küçük olayının bile, görünüşte küçük bile olsa, yeterince tekrarlanması durumunda üreticinin marka imajına ciddi zararlar verebileceğine dikkat edilmelidir.

3.2.1.3. Kalıcı Devralma

ECU'ların ağ üzerinden bir güncelleme süreci vardır. Ayrıca, saldırgan geçtikten sonra aracı tehlikeye atarak yeniden programlanabilirler. Ayrıca, saldırgan geçtikten sonra aracı tehlikeye atacak şekilde programlanabilirler. Bununla birlikte, ECU'lar normalde yazılımlarının yeni bir sürümünün yalnızca bir sorgulama-yanıt dizisi sonucunda kimliği başarıyla doğrulanmış bir kaynaktan indirilmesini kabul edecek şekilde tasarlanmıştır [2]. Bununla birlikte, bu mekanizmanın şu anda birkaç kusuru vardır. Her şeyden önce, ECU'ların bilgi işlem gücü sınırlı olduğundan, şifreleme için kullanılan anahtar genellikle zayıftır (16 bit) ve bu nedenle saldırganın erişim elde edebilmesi için bir kaba kuvvet saldırısı tarafından keşfedilebilir, etkilenen ECU'ya genişletilir. Böylece, saldırgan kodunun bir ECU tarafından indirilmesini başarırsa, ağa kalıcı erişim elde eder ve artık araca bağlı olmadığında saldırısının devam etmesine izin verir.

Bir ECU'nun yeniden programlanması, bir saldırıyı başka bir veri yoluna yaymak için de kullanılır. Gerçekten de, mevcut ağ mimarileri, ağ geçidi ECU'ları tarafından birbirine bağlanan birkaç veri yolundan oluştuğundan, bir ağ geçidinin ele geçirilmesi, saldırganın ağın yeni bir bölümüne erişmesine izin verecektir. Bu nedenle, bir saldırgan ağa erişmeyi başarırsa, mevcut mimariler, sonunda aracın ECU'ları üzerinde tam kontrol sahibi olabileceği anlamına gelir.

Ancak, yukarıda belirtilen saldırıların, bir saldırganın aracın dâhili ağına zaten fiziksel erişim elde ettiğini ima ettiğine itiraz edilebilir. Saldırgan kendi ağına bağlanmak için araca girebildiği için zaten bir güvenlik ihlali vardı. Ayrıca bu durumda araca daha basit ve hızlı bir şekilde mekanik saldırılar gerçekleştirerek (örneğin ilgili bilgisayarlara elektronik olarak saldırmak yerine frenlerin bağlantısını keserek) zarar vermek de mümkündür.

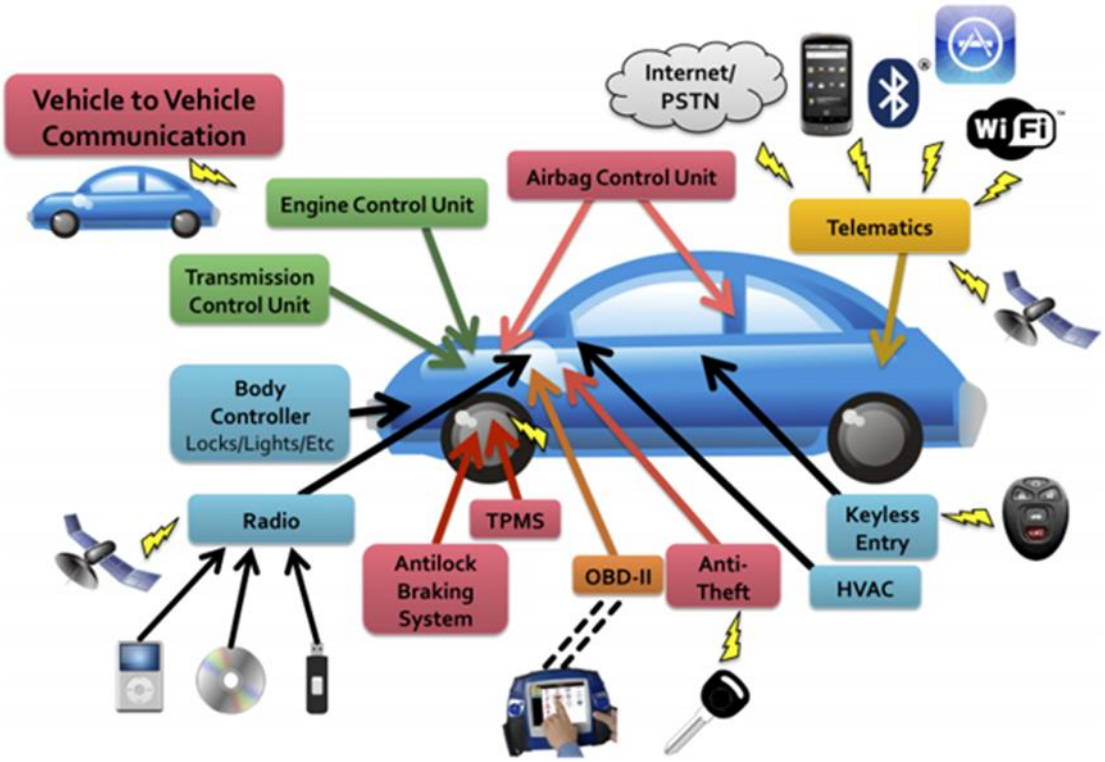
3.2.2. Uzaktan Saldırılar

Modern araçlarda bulunan birçok iletişim aracı, bu tür araçların yerleşik ağlarının artık kapalı (veya izole) olarak kabul edilemeyeceği anlamına gelir, çünkü bunlar saldırgana uzaktan bir saldırı gerçekleştirmesi için potansiyel bir ağ geçidi sağlar.

Gerçekten de, aracın birçok arayüzü, harici bir veri kaynağı ile iletişime izin vererek, bir aracın dahili ağının kontrolünü ele geçirmek için artık fiziksel erişimin gerekli olmadığını kanıtlıyor. Bu saldırılar kapsamlarına göre sınıflandırılabilir: dolaylı fiziksel erişim, kısa menzilli kablosuz erişim ve uzun menzilli kablosuz erişim. Bunları aşağıda açıklıyoruz.

3.2.2.1. Dolaylı Fiziksel Erişim

Dolaylı fiziksel erişim ile saldırının başlangıçta arabanın dışındaki bir unsuru içerdiği durumları kastediyoruz. Saldırının iç ağa ulaşmasını sağlayan bu elemanın ağa olan bağlantısıdır. Bu nedenle, saldırıyı tamamlamak için hala iç ağa fiziksel erişim gerekiyorsa, bu adım artık saldırgan tarafından değil ama bilgisi dışında üçüncü bir tarafça gerçekleştirilir. Bu tür saldırıları uzaktan saldırılar olarak görüyoruz.



Şekil 3-2: Modern bir otomobilin iç ağının kritik hedefleri

- **OBD-II:** Bu port, bir aracın kontrol ünitelerinden teşhis verilerini ve bilgilerini almak için standart hale getirilmiştir. OBD dongle ve OBD kod okuyucuları mevcuttur ve uzaktan satın alınabilir. Ancak veriler yayınlandığında CAN veri yolu, CAN veri çerçevesinin gizliliğini ve kimlik doğrulamasını sağlamaz ve kötü niyetli bir düşmanın verileri kolayca dinlemesinin veya bir saldırı başlatmasının yolunu açar. Bağlantı noktasına bağlanan ve bir bilgisayardan Wi-Fi üzerinden kontrol edilen böyle bir araç, bu nedenle saldırıya uğrayabilir [12]. Araçla aynı ağa bağlı bir bilgisayardan, ikincisi tarafından kullanılan iletişim protokollerinin uygulanmasındaki kusurları takiben bir kod enjeksiyonu gerçekleştirilebilir.
- **CD Çalar:** ECU'ların CD-ROM ile güncellenmesine karşılık gelen bir saldırı olasılığı düşük kalırsa (sürücü, önce içeriğini tanımlamaya çalışmadan sürücüsüne bilinmeyen bir CD yerleştirmelidir), ancak bu, bileşenlerin (donanım veya yazılım) kapsamlı doğrulama olmadan yeniden kullanılmasıyla ilişkili riskleri gösterir. Ancak, oynatıcı tarafından WMA dosyalarının kodunun çözülmesinde bir güvenlik açığı tespit edildi. Kapsamlı bir analiz, görünüşte normal bir ses dosyasının (ve bir bilgisayarda mükemmel bir şekilde okunabilir) oluşturulmasına izin verdi, ancak bu, bir arabellek taşmasından yararlanarak, burada oynatıldığında otomobilin multimedya sistemi tarafından CAN çerçevelerinin emisyonuna

neden oldu [2]. Bu güvenlik açığı ile bir saldırganın kötü amaçlı dosyaları çevrimiçi paylaşım ağlarında kullanıma sunarak bu multimedya sistemini kullanarak mümkün olduğu kadar çok aracı ayrım gözetmeksizin ele geçirmeye çalışacağı bir saldırı senaryosu hayal etmek oldukça mümkündür.

- **USB fişi:** Bir USB çubuğunda bulunan bozuk bir dosyaya erişen yerleşik bir multimedya oynatıcı ile CD çalarınkine benzer bir durum mümkündür. Başka bir olasılık, USB üzerinden bağlanan virüslü bir akıllı telefonla ilgili olabilir. Bu tür bir saldırı henüz belgelenmemişse, bir telefona karşı olası saldırılarla (örneğin Bluetooth üzerinden veya kötü amaçlı bir uygulamanın indirilmesini takiben) bir arabanın bağlantı ara yüzlerinin güvenliğine ilişkin emsaller bu makul varsayımı desteklemektedir.

3.2.2.2. Yakın Menzilli Saldırılar

Bu bölüm, kısa menzilli kablosuz iletişim araçlarını kullanan olası saldırıları tartışır.

- **Mobil ekipmanın kablosuz bağlantısı:** Modern araçlar, mobil ekipmanlarla bağlantı imkânı sunar. Örneğin, sürücü telefonunu Bluetooth veya Wi-Fi aracılığıyla bağlayabilir ve arabasındaki hoparlörleri eller serbest kiti olarak kullanabilir. Ancak, bu protokollerin uygulanmasında kusurlar olabilir. Bunlar, araca yakın bir terminali olan bir saldırganın bu bağlantıları yöneten modülün kontrolünü ele geçirmeye çalıştığı doğrudan saldırı senaryolarına veya ilk önce daha önce yetkilendirilmiş bir üçüncü taraf cihazı hedef alıyorsa dolaylı olarak bu ekipmanla iletişim kurmak için (örn. sürücünün akıllı telefonu olarak). Bu nedenle ilk örnek, Truva atı türünde bir mobil uygulamanın telefonun Bluetooth bağlantılarını izlediği dolaylı bir saldırıdan oluşur. Daha önce olduğu gibi, saldırı senaryosu, hedef aracın sahibinin farkında olmadan programı akıllı telefonuna indirmesini içerir. Aracın telematik sistemiyle eşleştiği tespit edildiğinde, uygulama saldırısını tetikler ve ECU'nun kontrolünü ele alır. İkinci örnek, ilk adımı otomobilin MAC adresini (Bluetooth) belirlemek ve ardından onunla eşleştirmek olan doğrudan bir saldırıdır. Ancak, arabanın, sürücünün müdahalesine gerek kalmadan eşleştirme isteklerini kabul edebildiği ortaya çıktı ve bu da, eşleştirmeyi onaylamak için araba tarafından oluşturulan şifreyi bulmak için bir kaba kuvvet saldırısına izin verdi. Unutulmamalıdır ki böyle bir saldırı için gereken süre 10 saatten fazla olabilir [2], bu da saldırganın uzun süre hedeflenen araca yakın kalabileceği anlamına gelir. Bununla birlikte, süreç çoğullanabilir, bu da saldırganın belirli bir aracı hedeflemeye çalışmaması durumunda başarı şansını artırmak için (örneğin bir park yerinde) aynı anda birden fazla arabaya saldırılmasına izin verebilir. Bu tür

saldırıların kullanılması, iletişim modülünde saklanan verilerin kurtarılmasına, geçmiş iletişimlerin dinlenmesine veya tekrar iç ağın ele geçirilmesine izin verebilir.

- **V2V iletişimi:** Bir araç ile diğer araçlar veya yol kenarındaki ekipmanlar arasındaki iletişim, ulaşım alanındaki önemli gelişmelerdir. Bu değişiklikler, örneğin yakın bir tehlike durumunda (hız sınırındaki değişiklik, kör kavşakta gelen araçlar, acil frenleme vb.) aracın sürücüyü uyarmasına ve hatta otomatik olarak tepki vermesine olanak tanır. Riskler arasında, örneğin araçlar arasındaki iletişimin casusluğunu sayabiliriz, bir araca, hedefe zarar vermek (örneğin, fren yapmamak suretiyle) veya bir fayda sağlamak (öncelikli araç gibi davranarak) için uygun olmayan bir tepkiyi tetiklemek için araca yanlış bilgi göndermek.
- **Uzaktan açma:** RFID araç immobilizerleri, modern otomobillerde neredeyse her yerde bulunur. Bu sistemler, bir anahtar veya anahtarlıkta bir RFID etiketi ve aracın direksiyon kolonunun yanında bir okuyucu içerir. Doğru anahtar (doğru RFID etiketinin varlığıyla doğrulandığı gibi) olmadığı sürece aracın çalışmasını engellerler. Ancak bugün insanlar bir kutu geliştirdiler: **RollJam.** Bir anahtardan komutları yakalayabilir ve kaydedebilir [13]. Prensip: Araç sahibi aracı kapatmak istediğinde, RollJam kutusu sinyali karıştırır ve anahtar tarafından gönderilen kodu kaydeder. Sahibi için kötü bir temas olabilir ve tekrar kapat düğmesine basar. Kutu tekrar sinyali karıştırır, yeni kodu yakalar ve kaydeder, ancak yakalanan ilk kodu araca gönderir. Bilgisayar korsanının istediği zaman kullanabileceği bir kodu vardır.
- **Keyless:** Anahtar, sürücü herhangi bir müdahalede bulunmadan bir arabayı açıp çalıştırmanızı sağlar. Arabadan uzaklaştığınızda otomatik olarak kapanır. Bunun için iki adet amplifikatör kutusu yeterlidir. Biri sahibine diğeri arabaya yakın. Sinyal birinci tarafından alındığında, sinyal kapıların açılmasını etkinleştiren ve aracın çalıştırılmasına izin veren ikinciye gönderilir. Bilgisayar korsanı, kartın veya amplifikatörün sinyalinden uzaklaşsa bile araba durmaz. Çünkü güvenlik nedeniyle, anahtar sinyali kaybolduğunda araba durmayacaktır. Kaza yapmamak için.
- **TPMS:** TPMS (Tire Pressure Monitoring System), Lastik Basıncı İzleme Sistemi anlamına gelir, lastiğin içine yerleştirilmiş ve ölçümlerini kısa menzilli bir radyo vericisi aracılığıyla yerleşik bir ağ ECU'suna gönderen bir basınç sensöründen oluşur. TPMS artık Amerika Birleşik Devletleri, Avrupa ve Japonya'da zorunludur. TPMS'yi hedef alan saldırılar, onun tarafından iletilen bilgileri 40 metreye kadar mesafelerden dinlemenin mümkün olduğunu göstermiştir [2], bu, aracın izlenmesine izin verdi, ancak alıcı ECU'ya hatalı bilgiler içeren

kötü amaçlı mesajlar göndermek de mümkün oldu. Sonuç olarak, gerçek bir tehlike olmadığında anormal lastik basıncı uyarı ışığı yandı.

3.2.2.3. Uzun Menzilli Saldırılar

Bu kategori, uzun menzilli iletişim teknolojileri aracılığıyla gerçekleştirilebilen ve böylece bir saldırganın hedef araçtan herhangi bir mesafeden erişmesine izin veren saldırılarla ilgilidir.

Genişletilmiş bağlantı için araç bir cep telefonu arayüzü ile donatılmıştır. İnternet veri işlevleri (navigasyon) için ve aynı zamanda ses için (konum tabanlı yardım servisi veya sadece telefon görüşmeleri yapmak için) kullanılır. Ayrıca, bağlı araç ortamını destekleyen uygulamalar artık Google Play ve Apple App Store gibi uygulama pazarlarında satılmaktadır, örneğin: Send To Car, UVO Smart Control ve BMW ConnectedDrive.

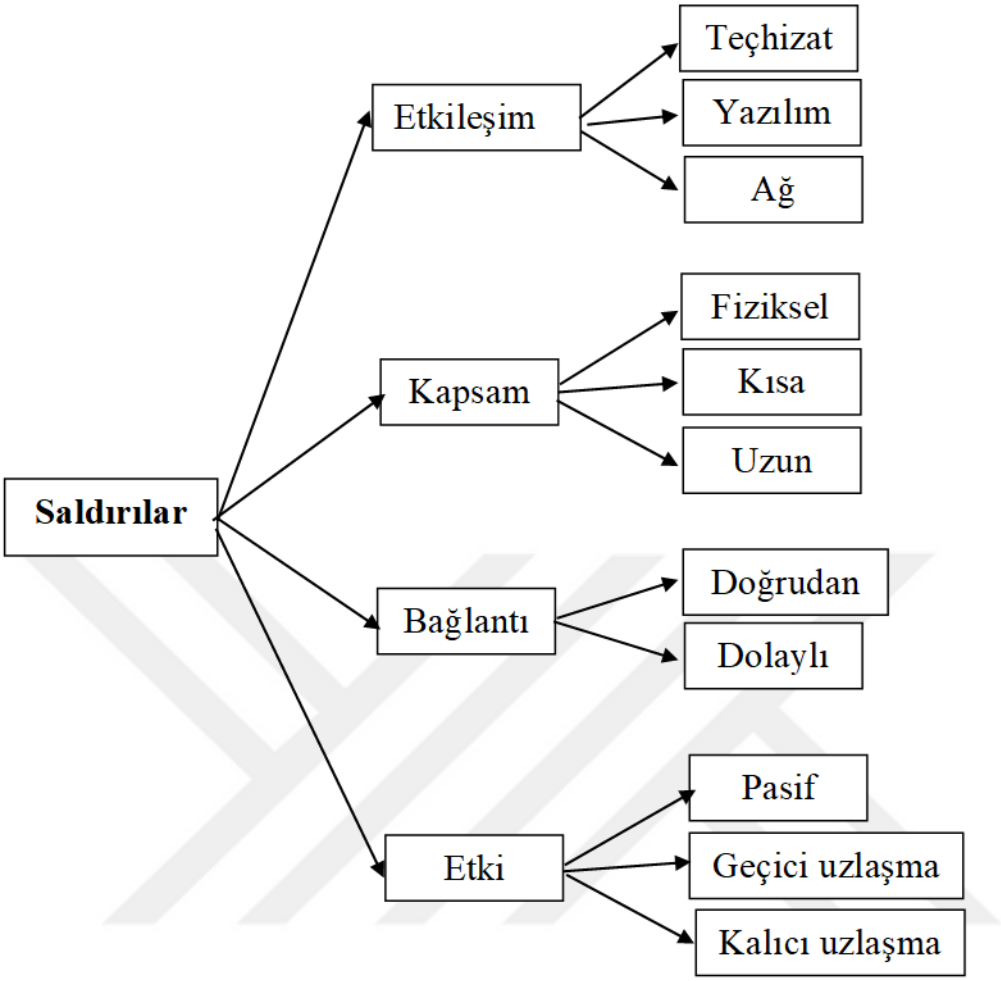
BlackHat USA 2015 bilgisayar güvenliği konferansı sırasında Charlie Miller ve Chris Valasek Jeep Chrysler saldırını sundular [14]. Mobil ağ aracılığıyla, bilgisayarlarından CAN veri yoluna ulaşabildiler. Telsizlerin, sileceklerin, şanzımanın, direksiyonun ve frenlerin kontrolünü ele geçirmeyi başardılar.

Bir aracın bir web tarayıcısını entegre etmesi durumunda, geleneksel bilgisayarları ve mobil cihazları etkileyebilecek olana benzer bir şekilde, olası güvenlik açıklarından yararlanılması tamamen mümkündür. Burada da sonuçlar yukarıda bahsedilen saldırılara benzer olabilir: tarayıcıyı barındıran modülde depolanan verilere erişim ve bağlı olduğu veri yollarına potansiyel erişim.

3.3. SALDIRILARIN SINIFLANDIRILMASI

Bu bölümde, mevcut otomobillere gömülü ağ mimarileri tasarlanırken dikkate alınması gereken olası senaryoların ve tehditlerin çeşitliliğini vurgulamaya çalışacağız. Bu sınıflandırmada, araç üstü araç sistemlerini hedef alan saldırıları kategorize etmemize izin veren dört eksen belirledik [2]: sistemle etkileşim düzeyi; kapsam; saldırının bağlantısı ve etkisi.

İlk kategori için üç olası etkileşim düzeyini ayırt ediyoruz. İlk olarak, saldırgan, donanımın kendisine karşı fiziksel saldırılar yoluyla veya sensörler tarafından alınan sinyalleri karıştırarak donanımla etkileşime girebilir. Bir saldırı, bir ECU'ya gömülü yazılıma da etki edebilir. Son olarak, bir saldırı aracın iç ağını etkileyebilir.



Şekil 3-3: Yerleşik bilgisayarları hedef alan saldırıların sınıflandırılması

İkinci kategori için, modern bir otomobilde bulunan farklı iletişim araçlarının, onu doğrudan fiziksel bağlantı yoluyla veya kısa ve uzun menzilli iletişim protokolleri aracılığıyla uzaktan gerçekleştirilen saldırılara karşı savunmasız hale getirdiğini biliyoruz.

Üçüncü kategori için, örneğin, bir saldırgan, hedeflediği araçla doğrudan veya dolaylı olarak etkileşime girebilir. İlk durumda, saldırısı yalnızca bir aracın yerleşik sistemlerine yöneliktir. İkinci durumda, saldırgan önce araçla iletişim kuracak ve bu nedenle saldırıyı sonuçlandırmak için röle görevi görecek bir cihazı hedef alır.

Son kategori için, bir saldırının etkisini üç düzeyde karakterize ediyoruz. En küçük etki pasif olarak sınıflandırılır, yani saldırı hedeflenen sistemin işleyişini etkilemez. Örneğin, bir otomobilin Bluetooth cihazıyla, içerdiği verilere erişmek için kendini tanımlamaya yönelik bir saldırı bu kategoriye girer. Bu tür saldırıları tespit etmek zor olabilir, ancak aracın bütünlüğü için büyük riskler oluşturmaz. Geçici bir uzlaşma, saldırganın yerleşik bir sistemin çalışmasını aktif

olarak bozacağı, ancak saldırı sona erdiğinde zararlı etkilerinin sona ereceği bir durumu belirtir: eğer bir saldırgan yeni bir saldırı yapmak isterse, aynısını yeniden yapmalıdır. Son olarak, kalıcı bir uzlaşma, bir saldırının yerleşik bir sistemi kalıcı olarak tehlikeye attığı durumları ifade eder. Saldırgan artık araca bağlı olmadığında bile saldırının etkileri devam eder. Bir ECU'nun yetkisiz olarak yeniden programlanması veya bir multimedya sistemine bir arka kapının takılması, kalıcı uzlaşma örnekleridir.

4. OTOMOTIV AĞLARI İÇİN GİRİŞ TESPİTİ

Bölüm 3'de gördüğümüz gibi, günümüzün otomotiv ağları saldırılara karşı savunmasızdır. Aslında, yerleşik bir ağa erişim elde eden bir saldırgan, hedeflerine ulaşmak için okuma, kesme, değiştirme veya çerçeve üretme gibi eylemler gerçekleştirebilir. Bu nedenle, saldırı tespit sistemleri gibi ağı "içeriden" izlemek için mekanizmaların yerleştirilmesi gerekli görünmektedir. Ancak, Bölüm 1'de gördüğümüz gibi, otomotiv güvenlik çözümleri, yerleşik sistemlerin tasarımıyla ilgili genel kısıtlamalara ek olarak, uyumluluk ve özerklik kısıtlamalarını da hesaba katmalıdır.

Bu bölümde, gözlemlenen ağ trafiğine dayalı olarak araç içi otomotiv ağları için bir saldırı tespit sistemi sunuyoruz.

4.1. SALDIRI HİPOTEZLERİ

Çalışmamızın bir parçası olarak, bir saldırganın dâhili ağa erişim sağlamada başarılı olduğunu varsayıyoruz. İkincisinin, dâhili ağ üzerinden erişilebilen diğer bilgisayarları bozmak veya kontrolünü ele geçirmek için araca saldırısını sürdürmek için bu erişimi kullanmaya çalışacağını varsayıyoruz. Amacımız daha sonra devam eden bir saldırıyı tespit ederek tespit etmektir. Başka bir deyişle, çalışmamız yerleşik ağdaki bir saldırıyı tespit etmeyi ve bu izinsiz girişin kökenini belirlemeyi değil, bu nedenle saldırıları ağ ile etkileşime giren ve geçici veya kalıcı bir uzlaşmaya yol açan saldırıları göz önünde bulunduruyoruz.

Bu nedenle, ağdaki dört tür şüpheli davranışı ayırt edebiliriz:

- Ağ protokolünün özelliklerine uymayan çerçeveler. Tipik olarak CAN durumunda bu, örneğin bilinmeyen bir tanımlayıcı içeren çerçeveler, yanlış boyutta bir veri alanı ile ilgilidir.
- İlgili meşru trafik sistem tarafından üretilmeye devam ederken periyodik olarak gönderilen kötü amaçlı çerçeveler. Örneğin, bir saldırgan periyodik olarak kısa huzmeli farların sönmesini komuta eden bir çerçeve gönderirken, sistem bunların açılmasını talep eden çerçeveler gönderir.
- Yasal çerçevelerin yerine gönderilen periyodik kötü amaçlı çerçeveler veya diziler. Bunlar daha sonra artık ağ üzerinde iletilmez.

- İletimi normal olarak belirli bir olay tarafından koşullandırılan, iyi biçimlendirilmiş periyodik olmayan çerçevelere karşılık gelen, zamanında iletilen kötü amaçlı çerçeveler veya diziler.

Bölüm 1'de sunulan kısıtlamaları dikkate alarak, özellikle dört hususa odaklanıyoruz: verinin kaynağı, tespit yöntemi, tespit etmek istediğimiz saldırı türleri ve tespitten sonraki davranış.

4.1.1. Veri Kaynağı

Her ECU'nun, bu ECU tarafından gönderilen veya tüketilen çerçevelerin bu kurallara uygun olup olmadığını kontrol etmekten sorumlu bir modül ile donatılması durumunda. Bazı saldırılar, tespit edilebilmesi için birkaç modül arasında işbirliği gerektirebilir. Böyle bir sistem, ECU'ların kendileri sensörlerle donatıldığından, okuma tipi saldırıları tespit edebilme avantajına sahiptir. Her ECU, çerçevelerinin ağın diğer öğeleri tarafından da iletilip iletilmediğini tespit etmelidir. Böylece, potansiyel olarak karmaşık kuralların uygulanmasını gerektirmeden üretim tipi saldırıları tespit etmek (hatta hata çerçevelerinin emisyonu yoluyla otomatik olarak karşı koymak) mümkündür [2]. Buna karşılık, güvenliği ihlal edilmiş bir ECU, yalnızca normal koşullar altında göndermesi gereken çerçeveleri gönderene kadar algılanmaz. Ayrıca, bu iki durumda, ECU'ları değiştirmek zorunda kalma durumu, uyumluluğun kaybolması anlamına gelir, bu da aslında maliyetleri artırır. Uyumluluk kısıtlamalarını en iyi şekilde karşılamak için mevcut ECU'ları değiştirmek istemiyoruz. Bu durumda, verilerin kaynağı yalnızca ağ trafiğidir. Ancak, bu artık yasadışı okuma eylemlerini tespit etmeyi mümkün kılmaz.

Ancak bunlar saldırı olarak kabul edilse ve bazen saldırganın amaçlarına ulaşması için yeterli olabilse de, aracın çalışmasında değişikliklere yol açmazlar ve bu nedenle aracın performansı üzerinde herhangi bir etkisi yoktur. Sonuç olarak, karşılığında elde edilen uyumluluk kazancından yararlanmak için işlenmemeleri tercih edilir.

4.1.2. Algılama Yöntemi

Algılama yöntemiyle ilgili olarak, araç üstü ağlara yönelik nispeten düşük sayıda belgelenmiş saldırı ile birleşen otomotiv mimarilerinin büyük çeşitliliği, bir senaryo yaklaşımını karmaşık hale getirir. Aslında çok sayıda sisteme uyarlanabilmesi için böyle bir yöntemin kolayca genellenebilir olması gerekir. Ayrıca, bu tür yaklaşımların potansiyel olarak gerektirdiği

güncellemeleri bir otomobilde yapmak, bilgisayarda olduğu kadar kolay değildir. Buna karşılık, otomobil üreticileri bu sistemlerin nasıl çalıştığı konusunda kapsamlı bilgiye sahiptir. Bir saldırı tespit sistemi tanımlamak için bu bilgiyi kullanmak, uygulanması çok daha kolay bir çözümdür. Ek olarak, yazılım tasarım süreçlerinin (örneğin AUTOSAR ile) birleştirilmesine yönelik eğilim, böyle bir prosedürün genelleştirilmesini düşünmeyi mümkün kılmaktadır [2].

4.1.3. Tespit Etmek İstediğimiz Saldırı Türleri

Yukarıda açıklanan dört tür şüpheli davranışa atıfta bulunarak. Davranışsal bir yaklaşım bağlamında, bir dizi kural sayesinde ilk iki vakayı tespit etmek kolaydır. Aslında, bu iki durum, ağ spesifikasyonlarına uyulmamasına tekabül etmektedir:

- Hatalı çerçeveleri tespit etmek için bir özellikler listesi kullanılabilir.
- Aynı şekilde, meşru trafiğe ek olarak periyodik olarak gönderilen kötü niyetli çerçeveler de oluşma sıklığı artırılarak tespit edilebilir.

Öte yandan, son iki durumda, bir saldırgan tarafından gönderilen mesajlar, spesifikasyonlara mükemmel bir şekilde uyabilir ve zaman kısıtlamalarına uyabilir. Standart trafik arasında bu tür çerçevelerin belirlenmesi, bir çerçeve tarafından sağlanan bilgileri önceden gözlemlenen verilerle karşılaştırmak için mekanizmaların kurulmasını içerir. Korelasyon mekanizmaları gibi bir mekanizmaya sahibiz. Bundan böyle bu tür mekanizmaları korelasyon mekanizmaları olarak adlandıracağız.

4.1.4. Tespitten Sonraki Davranış

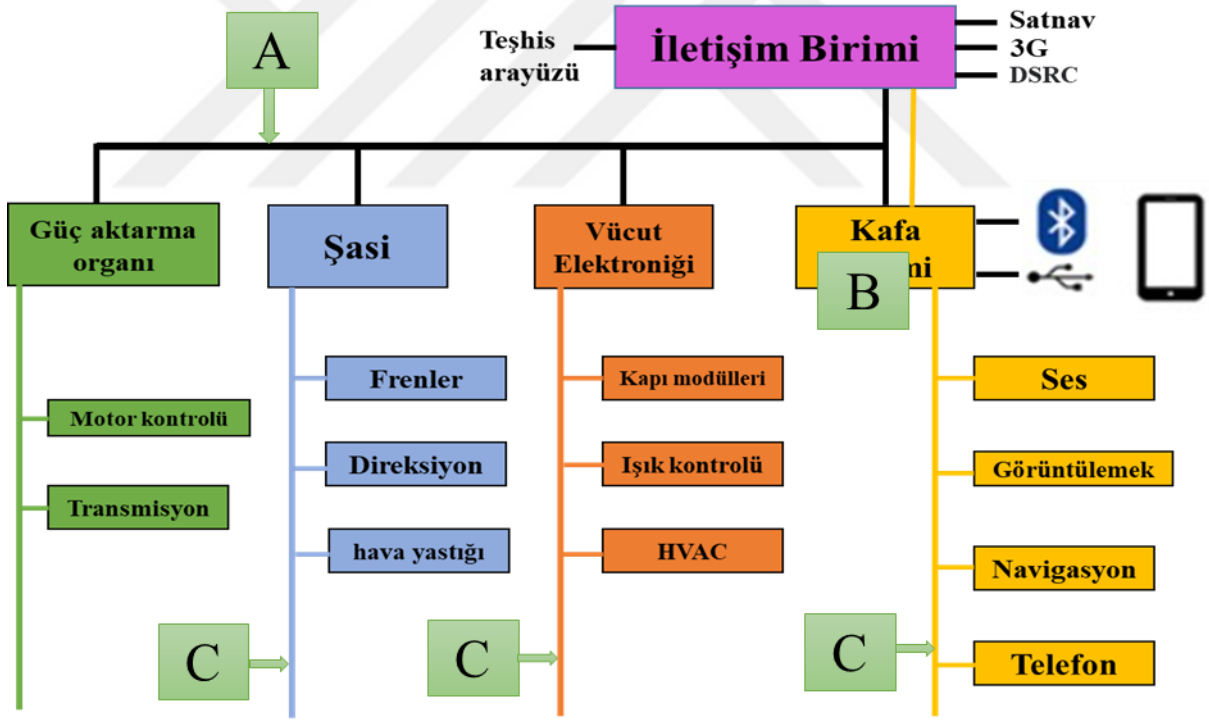
Bir saldırganın, bir arabadaki yerleşik sistemlerle etkileşim kurmak için yerleşik ağı kullanmaya çalıştığına inanıyoruz. İdeal olarak, bu nedenle, ağı izleyen bir IDS (*Intrusion Detection System*), saldırganın hedeflerine ulaşamaması için sürmekte olan bir saldırının durdurulmasına izin verebilmelidir. Ancak ağda zaten mevcut olan ECU'ları değiştirmeyen bir sistem düşündüğümüzden, tepkime araçları sınırlıdır. Böylece, tespit edilen bir saldırı durumunda, diğer çerçevelerin iletimini önlemek için veri yolunu doyurmak mümkün olabilir ve bu, ağ üzerinde birçok ECU'nun bozulmuş bir moda geçmesi sonucunu doğuracaktır, artık veri yolu aracılığıyla bilgi alamazlar. Bizim durumumuzda, burada tespit kısmına odaklanıyoruz ve bu nedenle sistemimizi tespit edilen saldırılara karşı pasif olarak görüyoruz.

4.2. ÇALIŞMA PRENSİBİ

Bu bölümde izinsiz giriş tespit sisteminin (IDS) çalışmasını anlatacağız, ardından bir veri yolu üzerinden iletildiğinde bir mesajın tutarlılığını belirlemek için bir yöntemi detaylandıracağız.

4.2.1. IDS Konumu

Genel olarak, modern bir arabanın yerleşik ağı, ağ geçidi görevi gören bir veya daha fazla ECU aracılığıyla birbirine bağlanan en az iki alt ağdan oluşur. Mümkün olduğunca fazla veri alabilmek için, IDS'mizin ağ izleme için gerekli tüm alt ağlara bağlı olması gerekir. Bu nedenle, sistemimiz bu ağ geçitlerinden birine dâhil edilebilir veya gerekli tüm veri yollarına bağlı ağın yeni bir parçası olabilir. Farklı alt ağlara yerleştirilmiş birkaç modülden oluşan dağıtılmış bir IDS sürümü de mümkündür.



Şekil 4-1: Bir otomotiv mimarisinde bir ıds'nin olası konumları

Aslında, modern bir otomobilin ağ mimarisini, örneğin EVITA projesinin referans mimarisini düşünürsek, bir IDS için olası farklı konumlar aşağıdaki gibidir:

A. Birkaç ağ geçidini birbirine bağlayan bir otobüste. Böyle bir durumda, farklı etki alanları arasındaki alışverişleri izlemeyi mümkün kılar. Öte yandan, bu, bir ağ geçidinin arkasına yerleştirilmiş alt ağlar içinde iletilen mesajlara erişim sağlamaz.
B. Zaten var olan bir ağ geçidi içinde. Burada bu, birkaç veri yolunda dolaşan mesajlara erişim sağlar. Ancak, bir ağ geçidi, bir saldırıda ana hedeftir. Bu nedenle, bir saldırı sırasında bozulmaması için bu ağ geçidi içinde IDS'nin güvenliğini sağlamaya ekstra dikkat gösterilmelidir.
C. Ağ boyunca dağıtılmış bir veya daha fazla modül. Bunlar bağımsız olarak çalışabilir veya birbirleriyle iletişim kurabilir.

4.2.2. IDS Nasıl Çalışır

"**Security by Design**" ilkesine göre, şirketler araç geliştirilir geliştirilmez bir IDS tasarlamalı ve planlamalıdır. Araç içindeki ağa ve kontrol yapısına bağlı olarak IDS farklı şekilde çalışır. Örneğin, her karmaşık kontrol cihazına donanım yazılımı, CAN Bus trafiği ve sensör verilerindeki anormallikleri tanımlayan bir sensör bileşeni takılabilir. Bu sensörler, Ağ Geçidi işlevine sahip bir merkezi kontrol ünitesinde çalışan temel IDS bileşeninde tanımlanan anormallikleri rapor eder. Merkezi araç ağ geçidinde bir yazılım modülü olarak bir IDS ile anormallikleri arayarak araç ağının iletişimini gerçek zamanlı olarak izlemek mümkündür [15]. IDS, bilinen bir hatalı davranış tespit ederse, aracı korumak için bir savunma davranışını tetikler (*Intrusion Prevention System*, IPS). Bunun, dâhili araç ağına yönelik bir siber saldırının araç fonksiyonlarını etkilemesini ve yolcu güvenliğini tehdit etmesini önlemesi gerekiyor.

4.2.2.1. Kontrol Kuralları

Daha önce gördüğümüz gibi, ağ özelliklerini karşılamayan saldırılar bir dizi kontrol kuralı aracılığıyla tespit edilebilir:

- **Bilinmeyen tanımlayıcı:** belirli bir listenin parçası olmayan bir çerçevenin tanımlayıcısı.
- **Kötü gönderme veri yolu:** Bir veri yolunda olmaması gereken bir yere bir çerçeve gönderilir.
- **Geçersiz veri alanı boyutu:** Veri alanı belirtilenle eşleşmiyor.
- **Yanlış frekans:** Periyodik bir çerçeve için, o çerçevenin iki gözlemi arasında geçen süre, spesifikasyonları karşılamalıdır.

4.2.2.2. Bir Sorun Bağlamının Tanımı

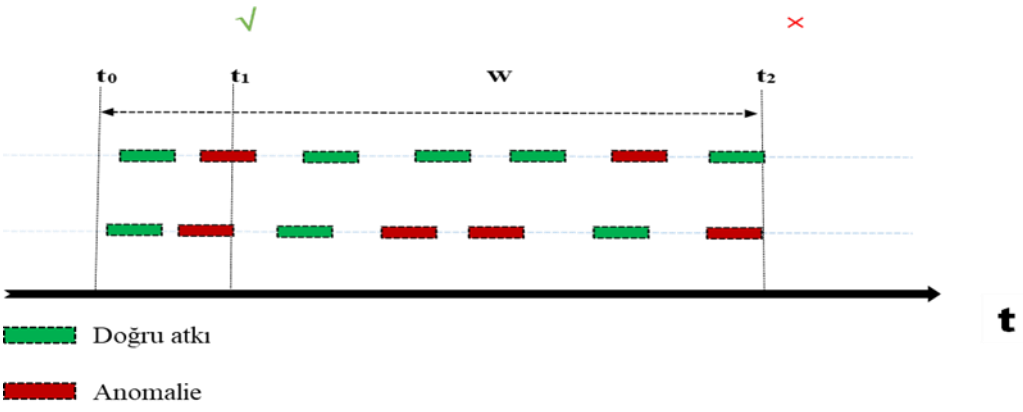
Ancak son iki kategoriye giren saldırıları tespit etmek için bu tür kontrol kuralları yetersizdir. Nitekim bu tür saldırılarda gönderilen çerçeveler potansiyel olarak yukarıda bahsedilen tüm kurallara uyacaktır. Bu gibi durumlarda, çerçevelerin iletim bağlamına dayanmak gerekir. Arabanın mevcut durumunu belirlemek için daha önce gözlemlenen mesajlardan bilgi almamız ve çapraz kontrol etmemiz gerekiyor. Algılama sistemi daha sonra bu verileri çerçevenin veya içerdiği mesajın bu şekilde tanımlanan bağlamla tutarlı olup olmadığına karar vermek için kullanır.

Böyle bir bağlamı tanımlamak için ve duruma bağlı olarak, korelasyon iki parametreye göre yapılabilir:

- **Fazlalık:** Ayrı kaynaklardan gelen benzer veriler. Örneğin, aracın hızını içeren bir mesaj fren sisteminden gelebileceği gibi uydu navigasyon sisteminden de gelebilir.
- **Tutarlılık:** Daha önce gönderilen veya dikkate alınan alt sistem tarafından tüketilen çerçevelerin geçmişi, bir sonraki hangi çerçevenin beklendiğini belirlemeyi mümkün kılar.

4.2.2.3. Uyarı Tetikleyicileri

Gerçekten de, elektromanyetik bozulmalar bir çerçevenin içeriğini değiştirebilir, bir sensör bazen bir hata yapabilir veya bir çerçevenin iletimi gecikebilir. Bu nedenle, bu tür anormalliklerin bir kerelik meydana gelmesi, mutlaka bir saldırıyı göstermez. Daha sonra, bir alarm vermeden önce bu tür anormalliklerin meydana gelme sıklığıyla ilgilenmek daha uygun hale gelir [16]. Aşağıdaki şekilde detaylandırıldığı gibi.

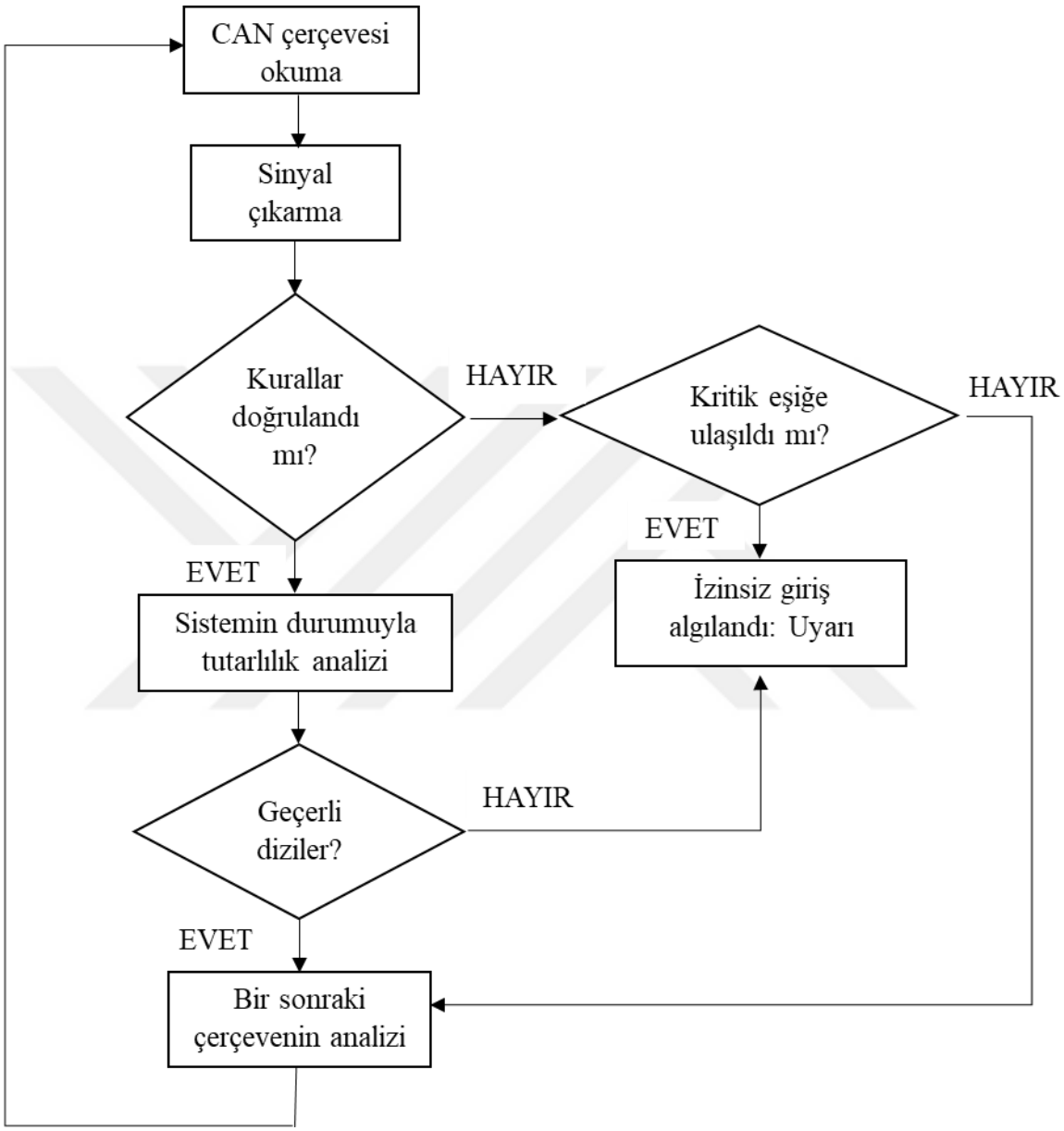


Şekil 4-2: Sürgülü pencere prensibi

Bu durumda, W boyutunda bir pencere sırasında algılanan minimum 4 anormallik için bir eşik ayarlanır. t2'den önce, kayan pencere hiçbir zaman 4 uyarı içermediğinden t1'de bir anormallik algılanmasına rağmen hiçbir uyarı yükseltilmez. Öte yandan, t2'de bu eşiğe ulaşılır ve bir uyarı

verilir. W'nin boyutu ve eşik değerleri sabit değildir. İlgili sistemler için üreticinin gereksinimlerine bağlı olacaktır.

Dolayısıyla aşağıdaki şekil bir IDS'nin genel çalışmasını özetleyebilir.



Şekil 4-3: İzinsiz giriş algılama sürecinin şeması

4.3. BİR IDS'NİN TEKNİK ZORLUKLARI

Bir IDS tasarlarken, CAN veri yolu ağ sistemi ile ilgili belirli zorluklar dikkate alınmalıdır: sınırlı kaynaklar, zamanlama gereksinimi, trafik kalıplarının davranışı, kararsız bağlantı boyutu, ağırlık ve maliyet.

- **Sınırlı kaynaklar:** Bir araçta bulunan tüm ECU'ların bellek depolama, bilgi işlem gücü ve veri aktarım hızı ile ilgili çeşitli sınırlamaları vardır (bant genişliği).
- **Gerçek zamanlı kısıtlama:** CAN paketleri, bilgisayarlardan diğer düğümlerin çalışmasına gerçek zamanlı olarak iletilir, bu nedenle paket arabelleklerinin gecikmesi ve sıraya alınması çok riskli ve kabul edilemez. Araç sensörlerinden alınan CAN paketi, aktüatörlerin gecikme olmaksızın araç işlevini yerine getirebilmesi için gerçek zamanlı olarak yönetilmelidir. Güvenlik çözümleri teklif edilirken gerçek zaman sınırlaması dikkate alınmalıdır.
- **Trafik davranışı:** Otomotiv iletişim sistemi için CAN trafik protokolü modelleri, geleneksel IP(*internet protocol*) ağlarından farklıdır [17]. Ayrıca araçlar üzerinde firmware güncellemeleri ve kablosuz tanılama yapabilmek için araç ile V2I arasında geçici bir bağlantı kurulmalıdır, bu da iletişim modelleri ve protokoller trafiği için farklı çözümler gerektirir. Bu nedenle, bir IP ağ çözümünü benimsemek mümkün değildir.
- **Kararsız Bağlantılar:** Araçlar hareket ederken hızdan bağımsız olarak internet bağlantısı olmayan bir alanda hareket edebilirler. Bu nedenle, IDS otomotiv çözümleri, üçüncü bir tarafla bağlantı kurmanın her zaman mümkün olmayabileceğinin farkında olmalıdır.
- **Boyut, Ağırlık ve Maliyet:** IDS çözümleri, ağırlık ve boyut açısından farklılık gösterebilir ve ayrıca, sonunda maliyeti etkileyecek küçük veya belki de büyük değişiklikler gerektirebilir. Örneğin, bir hat topolojisi benimseyen bir CAN veri yolu ağının kaldırılması, farklı bir topoloji benimseyen bir Ethernet veri yolu ağı ile değiştirilmek üzere, bol miktarda ek kablolama gerektirir ve pratik olmayabilir.

5. OTOMOTİV GÖMÜLÜ AĞLARIN İÇİN GÜVENLİK YÖNTEMLERİ

Bir önceki bölümde, gözlemlenen ağ trafiğine dayalı olarak araç içi otomotiv ağları için bir saldırı tespit sistemi sunduk.

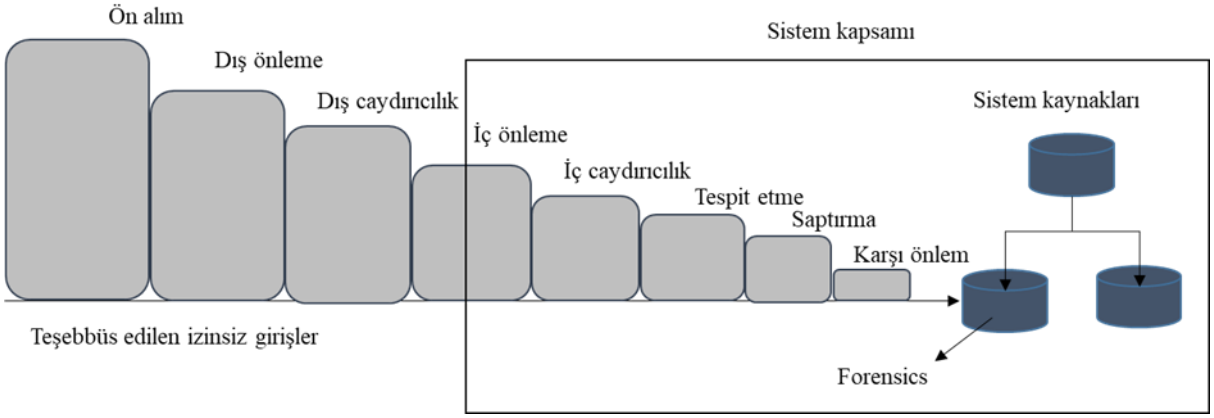
Bu nedenle, bu bölümde ilk olarak otomotiv ağlarında güvenlik mekanizmalarının geliştirilmesi ve uygulanmasına rehberlik eden genel stratejileri tartışacağız. Daha sonra otomobil için geçerli olan çeşitli bilgisayar güvenlik mekanizmalarını sunacağız (bir yandan sözde önleyici yöntemlerle, diğer yandan sözde reaktif yöntemlerle). Sonunda, özellikle V2X iletişiminde, otomobiller için bilgisayar güvenliği ile ilgili bazı Avrupa projelerini sunacağız.

5.1. SAVUNMA STRATEJİLERİ

Bir otomobilin kendi başına karmaşık bir sistem olduğunu bildiğimiz için, birbirleriyle iletişim kuran bir otomobil ağı daha karmaşık hale gelir. Bu nedenle, bir otomobil güvenlik sisteminin gerçekten etkili olması için, otomobildeki güvenlik mekanizmalarının uygulanması, ilgili sisteme genel bir bakış ile yapılmalıdır. Ancak, daha geniş çeşitlilikteki tehditlerle başa çıkmak ve bir sistemin izinsiz giriş toleransını artırmak. Daha pratik olan, sadece giriş noktalarını korumak yerine, güvenlik mekanizmalarını sistemin çeşitli seviyelerine yerleştirmektir. Bu nedenle amaç, bu mekanizmalardan biri tehlikeye girdiğinde veya bir saldırıyı durdurmak için yeterli olmadığında riskleri azaltmaktır. Halme ve BAUER [18], izinsiz girişlere karşı savunmak için altı kategori teknik tanımladılar: Önleme, ön alım, caydırıcılık, saptırma, tespit ve karşı önlem.

- **Önleme:** Sistem spesifikasyonu aşamasından güvenlik kavramlarının entegrasyonundan güvenlik açığı analiz araçlarının, anti virüsün ve hatta güvenlik duvarının kullanımına kadar, belirli izinsiz giriş girişimlerine karşı koymak için kullanılan tüm araçlar.
- **Ön alım:** Olası bir saldırıdan önce alınan önlemler. Hem korunacak sistemin kullanıcılarını veya tasarımcılarını eğitmeyi hem de potansiyel saldırgan topluluklarından bilgi almayı içerir.
- **Caydırıcılık:** Risk / ödül oranı üzerinde oynayarak bir saldırının ilgisini azaltmayı amaçlayan tüm teknikler.
- **Saptırma:** Saldırganı, bir tuzakla etkileşim halindeyken sisteme başarılı bir şekilde girdiğine inandırmak.
- **Tespit:** Sistemin hileli kullanımını meşru kullanımlardan ayırmaya çalışan teknikler.

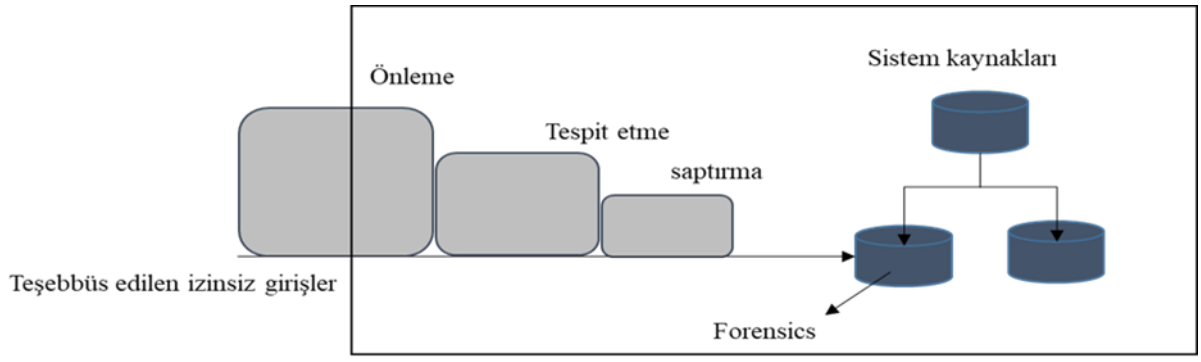
- **Karşı önlem:** Kanıtlanmış bir izinsiz giriş durumunda sistemin otomatik olarak tepki verme yeteneği.



Şekil 5-1: HALME ve BAUER'ye Göre, derinlemesine savunma

Başarılı bir izinsiz girişin olasılığını ve sonuçlarını en aza indirmek için, farklı kategorilere (korunacak sisteme ve yürürlükteki güvenlik politikalarına bağlı olarak) ait çeşitli araçlar seçen bir güvenlik mekanizması mümkündür. Böylece, bir önceki şekilde, yatay ok, sistemin derinliğindeki saldırıların ilerlemelerine karşılık gelir ve dikdörtgenler, her bir aracın başa çıkması gereken bu saldırıların oranlarına karşılık gelir. Bu durumda, bu araçlardan birinin çok etkili olduğu kanıtlanırsa, aşağıdaki araçların başa çıkması gereken daha az saldırı olacaktır. Söz değil, bir araç birkaç aşamada uygulanabilir. Örneğin sistemin içinde ve dışında yer alan caydırıcı mekanizmalar olabilir. Son olarak, bu araçların bir tamamlayıcısı olarak, sistemde olası bir uzlaşmanın nedenini bulmak için adli analizler yapılabilir.

Otomotiv endüstrisindeki bilgisayar saldırılarının riskleri ile ilgili olarak, derinlemesine savunma yaklaşımı uygun görünmektedir [2]. Derinlemesine savunma, bir güvenlik denetiminin başarısız olması veya bir güvenlik açığından yararlanılması durumunda birkaç yedekli savunma önlemi sağlayan bir bilgi güvence stratejisidir. Bir saldırıyı tek bir güçlü savunma hattıyla yenmek yerine ilerlemesini geciktirmeyi amaçlayan aynı adı taşıyan bir askeri stratejiden kaynaklanmaktadır. Böylece V2X iletişimleri için Nilsson ve Larson, [19]'te derinlemesine bir savunma modeli önerdiler. Modelleri, önceki modelde açıklanan tüm araçları içermez, ancak adli tıp (*forensics*) analizlerinin yanı sıra yalnızca önleme, tespit ve saptırma araçlarını içerir.



Şekil 5-2: NILSSON ve LARSON 'ye göre, otomobil için derinlemesine savunma

Bu bölümde, iki eksenden başlayarak, yazılımları ve yerleşik ağları hedef alan saldırılar için savunma mekanizmalarına odaklanacağız: Bir yanda sözde önleyici yöntemlerle, diğer yanda reaktif yöntemlerle.

5.2. ÖNLEYİCİ SAVUNMA MEKANİZMALARI

Önleme, sistemin güvenliğini artırarak saldırganın sisteme girmesini önlemeyi amaçlar. Bu bölümde güvenlik mekanizmalarını 3 kategoriye göre sınıflandıracağız: yazılım veri güvenliği, iletişim şifreleme ve ağ yönetimi.

5.2.1. Yazılım Verilerinin Güvenliğini Sağlama

Çoğu bilgisayar korsanının birincil amaçları olarak verilere erişimi olduğunu hepimiz biliyoruz, daha sonra bir ECU'da depolanan verileri kullanmak isteyen bir saldırganın olasılıklarını önlemek veya sınırlamak için, ECU'larda bulunan verilerin bütünlüğünü sağlayacak mekanizmalar esastır. Bu mekanizmalar esas olarak gömülü yazılımı hedefleyen saldırılara karşı koruma sağlamak için kullanılır, genel olarak sistemde herhangi bir kalıcı uzlaşmayı önlemek için. ECU'lardan akan verilerin güvenliğinin sağlanması, kod imzalama, sanallaştırma ve erişim kontrolleri yoluyla sağlanabilir.

5.2.1.1. Kod İmzalama

Kodun imzalanması, dolaşan verilerin gerçekliğinin doğrulanmasına izin vermek için ECU'lara kriptografik modüller eklenerek yapılır.

5.2.1.2. Sanallaştırma

Sanallaştırma, sanal bir sistem oluşturmak için donanımın işlevselliğini simüle eden yazılımı kullanır. Bu, belirli bir donanım platformuna bağımlılığı ortadan kaldırarak daha fazla esneklik, daha iyi kontrol ve daha iyi izolasyon sağlar. Bu soyutlamayı sağlayan yazılım katmanına genellikle hiper yönetici denir. Hipervizörler fiziksel kaynakları alır ve sanal ortam tarafından kullanılabilecek şekilde ayırır.

Otomotiv sektöründe, amaçlarından biri sanallaştırma yoluyla bir otomobilin multimedya sisteminin bütünlüğünü sağlamak olan OVERSEE projesinden bahsedebiliriz [20].

5.2.1.3. Giriş Kontrolu

Erişim kontrolü, ister insanlar ister araçlar olsun, güvenlik zincirindeki ilk savunma hattıdır. Böylece bir erişim kontrol politikası, bir öznenin bir kaynağı kullanma, okuma veya belirli bir nesneye veri yazma hakkına sahip olup olmadığına karar vermeyi mümkün kılacak farklı ayrıcalık seviyeleri tanımlar.

Otomotiv sektöründe, [21] bilgi akışlarının kontrolüne dayalı bir mekanizma önermiştir. Mekanizma, belirli veri ve kaynaklara, bu verilerin yayılımını takip etmeyi mümkün kılan bir işaretçi vermektir. Örneğin, 3'ü en güçlü seviye olan 4 gizlilik seviyesine karşılık gelen 0'dan 3'e kadar 4 işaretçi değeri vardır. Böylece erişim kontrol politikaları, verilere erişmek isteyen özneler tarafından yapılan taleplerin meşru olup olmadığını veriler üzerinde bulunan işaretleyicilerden belirleyecektir. Aksi takdirde, sistem bu verilerin gizliliğini korumak için konuya erişimi reddeder.

[22], bir veri yönetim sisteminin (DMS, *Data Management System*) tanıtılmasıyla başka bir yaklaşım önerilmiştir. Prensip, ECU'ların aralarındaki bilgi alışverişini yönetmesine izin vermek yerine, verilerin ağın belirli düğümlerinde birlikte gruplandırılmasıdır. Bu nedenle, veri gizliliğini korumak için erişim kontrol mekanizmaları DMS'ye kolayca dâhil edilebilir.

5.2.2. İletişimin Şifrelenmesi

Teknolojinin günden güne evrimi ile V2X iletişimleri veya ECU'lar arasındaki iletişim, özgünlük, bütünlük ve gizliliklerini sağlamak için güçlü şifreleme gerektirir. Bunun için üreticiler, iletişim kanalları aracılığıyla değiş tokuş edilen bilgileri şifrelemek veya imzalamak için kriptografi kullanır. Araçlar arasındaki iletişim mutlaka kablosuz olduğundan, alışverişlerin gizliliği sağlanmalıdır. Bu nedenle, V2X iletişiminden sorumlu sistem, karmaşık kriptografik işlemleri gerçekleştirebilmelidir. ECU'lar arasındaki iletişimler için, güvenli kimlik doğrulama

yöntemlerinin eklenmesi, mesajların gerçekliğinin sağlanmasına yardımcı olabilir, bunları imzalama yeteneği de bütünlüğü sağlar ve şifreli mesajlar göndermek, gizliliğe izin verir.

İki ana şifreleme kategorisi vardır: simetrik şifreleme (gizli anahtar) ve asimetrik şifreleme (ortak anahtar). Şu anki araçlarda kriptografi kullanan güvenlik mekanizmalarının zaten mevcut olduğunu belirtmek gerekir. Örneğin, aracın sinyalin doğru anahtar tarafından verildiğinden emin olmasına izin vermesi gereken bir sorgulama-tepki tipi sisteme dayanan uzaktan açma sistemleri durumu. İmmobilizer sistemleri de bu sisteme dayanmaktadır, bu sefer birkaç ECU arasında uygulanmaktadır [2].

5.2.3. Ağ Yönetimi

Bu kategori, ağ ile etkileşime giren her türlü saldırıyı önlemeyi amaçlar. Ancak araçlardaki iletişim sistemlerinin evrimi ile, görünüşte bariz bir çözüm, dışarısı ile iletişim ara yüzlerini içeren ağları, aracın düzgün çalışmasından sorumlu kritik ağlardan tamamen ayırmak olacaktır, hatta kritiklik seviyelerine göre izole ağlardaki ECU'ları gruplandırın [2]. Bu sayede dışarıdan gelecek bir saldırı kritik araç ağlarını etkilemeyecektir. Gerçekten de, yerleşik bir ağa karşı başlatılan bir saldırının etkisi, ağ topolojisi ve mevcudiyeti kritik araç unsurlarını kontrol edebildiği için, mevcut giriş noktalarının sayısına ve çeşitliliğine bağlı olarak değişir. Miller ve Valasek, bir saldırganın araçları ağ topolojilerine göre kontrol etmede karşılaşacağı zorluğu değerlendirmeye çalışarak bu gerçeği [23] iyi bir şekilde göstermektedir.

Bağlantı izleme ve hatta bilgi aktarmanın yasal olup olmadığını belirlemek için çerçevelerin içeriğini incelemek için, otomotiv sınıfı bir güvenlik duvarı işi yapabilir [24]. Yine de, güvenlik duvarının etkinliği, ağın topolojisi ve ağdaki konumu ile ilgilidir.

5.3. REAKTİF SAVUNMA MEKANİZMALARI

Saldırgan sisteme başarılı bir şekilde sızdığında, önleyici savunma mekanizmaları artık sistemi koruyamaz. İşte burada reaktif savunma mekanizmaları devreye giriyor. Reaktif savunma mekanizmaları için IDS ve forensics analizlerden bahsedeceğiz.

5.3.1. Saldırı Tespit Sistemleri

Artık modern bilgi işlemde yaygın olan izinsiz giriş tespit sistemleri (IDS), saldırganın izinsiz girişten sonra eylemlerinin ne olduğunu belirlemek için önleyici savunma sistemlerinden

devralır. Otomotiv saldırı tespit mekanizması, tespit mekanizmasının sistem içinde nasıl kullanıldığına bağlıdır. Anormallikler, imzalar, spesifikasyonlar ve melezlere dayanan dört kategori içerir. İmza ve spesifikasyon tabanlı teknikle karşılaştırıldığında, anormallik tabanlı IDS, otomotiv IDS'de kullanılan en yaygın ve gelecek vaat eden yaklaşımdır [17].

5.3.1.1. Anomali Tabanlı Yaklaşım

Anomali tabanlı IDS [25] bir sistemin faaliyetlerini gerçek zamanlı olarak gözlemler ve bunları bir profilde kaydedilmiş normal davranışlarla karşılaştırır. Bu durumda, profilin normal davranışından sapma belirli bir eşiğe ulaştığında, alarmı tetikler. Bir eğitim aşamasından geçtikten sonra bu anormallik tabanlı yaklaşım, yeni saldırıları etkili bir şekilde tespit edebilir. Bir eğitim aşamasından geçtikten sonra bu anormallik tabanlı yaklaşım, yeni saldırıları etkili bir şekilde tespit edebilir.

- **Frekansa dayalı yöntem:** [26] Song ve ark. CAN paketlerinin frekanslarına saygı gösteren çok hafif bir algoritma benimsemiştir [27]. Bilgi işlem gücü tüketimini azaltırken izinsiz girişlere daha hızlı yanıt verebilmesi için algılama algoritmasını basitleştirdiler. Yöntem, son paketlerin varış zamanından, genellikle 0,2 ms'den daha kısa olan zaman aralığını hesaplayarak çalışır. Zaman aralığı belirli bir eşikten daha kısaysa, IDS izinsiz girişlerin gerçekleştiğini belirleyecektir.
- **Öğrenmeye dayalı yöntem:** Öğrenmeye dayalı yöntem, girdi verilerinden özelliklerin temsilini öğrenmeye çalışan denetimli veya denetimsiz bir kategoriye girer. CAN veri yolu sisteminin değerlendirilmesinde saldırı davranışlarını tahmin etme ve üretmedeki zorluklar ve ayrıca CAN protokolünün tescilli ortamı ile uygun genelleme ihtiyacı, bu nedenle araştırmacıları denetimli veya yarı denetimli anormallikleri tespit etmek için yöntemler önermeye teşvik eder. Örneğin Wasicek ve Weimerskirch, ECU'lardaki parametreleri veya flash bellekleri değiştirmeye çalışan saldırıları tespit etmek ve CAN ağının trafiğinin anormal şekilde davranmasını sağlamak için yeni donanımı entegre etmek için çip ayarlamaya dayalı yarı denetimli bir yöntem tasarladı [28].
- **İstatistik tabanlı yöntem:** İstatistik tabanlı yöntem, mevcut istatistiksel gözlemi önceden belirlenmiş istatistiksel gözlemle karşılaştırır. Örneğin, [29], modellenen sistemde olağandışı davranışları bulmak için istatistiksel özellikleri (ortalama, varyans ve standart sapma) kullandı.

5.3.1.2. İmza Tabanlı Yaklaşım

İmza tabanlı yaklaşım, ağ veya sistem etkinliğini IDS'de depolanan saldırı kalıplarıyla karşılaştırır ve depolanan kötü amaçlı kalıplarla eşleşirse alarmı tetikler. Ancak bu yaklaşım, büyük ölçüde saldırı imzası veri tabanına dayandığından, bilinmeyen bir saldırıyı tespit etmede etkisiz hale gelir [30].

5.3.1.3. Spesifikasyona Dayalı Yaklaşım

Spesifikasyön tabanlı yaklaşım [31], beklenen bir ağ davranışı belirlenen spesifikasyonlardan saptığında saldırıları tespit ederek çalışır. Bu yaklaşım, anomali temelli yaklaşımla aynı amaca hizmet eder. İki yöntem arasındaki tek önemli fark, her bir belirtim ve kuralın bir insan uzman tarafından manuel olarak tanımlanması gerektiğidir [17].

5.3.1.4. Hibrit Yaklaşım

Adından da anlaşılacağı gibi, birkaç yöntemin bir kombinasyonu yaklaşımıdır. Birkaç IDS tekniğini (örneğin ağ tabanlı IDS ve ana bilgisayar tabanlı IDS) birbiriyle iletişim kuran ve merkezi sunucu tarafından izlenen büyük bir ağ üzerinde birleştirir [32]. Wang et al. CAN veri alanı dizilerini öğrenirken çok sayıda CAN zaman serisi girişini çalıştırabilen bellek tabanlı bir sistem olan Hiyerarşik Zaman Belleği (HTM, *Hierarchical temporal memory*) kullanılarak hibrit anormallik tespiti geliştirildi [33]. Yöntem, önceki öğrenme durumuna dayanan çevrimiçi bir şekilde çalıştı.

5.3.2. Adli Analizler (Forensics Analysis)

Otomobillere yönelik bilgisayar saldırılarının ortaya çıkmasıyla, bir olayın yerleşik bilgisayarlara yönelik bir saldırıyla bağlantılı olma riski artık sıfır değil ve bu da adli analize olan ihtiyacın artmasına neden oluyor. Örneğin, bir saldırıyı basit bir kazadan ayırt etmeye yardımcı olmak için. Ancak bunun için bu analizlerin yapılması için gerekli verilerin güvenli bir şekilde toplanıp saklanabilmesinin sağlanması önemlidir. Çünkü saldırgan, değiştirmek için bu verilere erişmeyi başarırsa, bu veri toplama gereksiz hale gelecektir.

[34]'e göre, birkaç gömülü bileşen analizi, genellikle adli analiz için uygun olan beş veri sınıfı tanımlamıştır:

- **Firmware:** Bu, ECU'da kurulu bir yazılım monolitidir. Firmware veri analizi, ECU'daki değişiklikleri algılamak için uygundur.

- **Haberleşme Verileri:** Hem araç içinde hem de araç içerisinde başka bir alıcıya iletilen tüm verilerdir.
- **Kullanıcı verileri:** Bu, kullanıcı tarafından okunan veya değiştirilen tüm verilerdir.
- **Güvenlik verileri (*safety*):** (Bu, güvenlik verileridir (aracın ve bileşenlerinin güvenlik durumuna ilişkin veriler gibi). Güvenlik olayları, manipülasyonun bir göstergesi olarak kullanılabilir.
- **Güvenlikle ilgili veriler (*security*):** bu, güvenlikle ilgili verilerdir (doğrudan güvenlik olaylarıyla ilgili bilgiler gibi). Güvenlik olayları, aracın veya çevresinin yanlış kullanımı veya olası manipülasyonu ile ilgili bir bilgi kaynağı sağlar.

5.4. BAZI AVRUPA PROJELERİ

Bu bölümde, araçlara uyarlanmış savunma mekanizmalarının uygulanmasına katkıda bulunan bazı Avrupa projelerinden [35]örnekler sunuyoruz.

PRESERVE (1 Ocak 2011 - 30 Haziran 2015), PRESERVE'in (*Preparing Secure Vehicle-to-X Communication Systems*) amacı, V2X iletişimleri için piyasa kısıtlamalarına uyarlanmış ve önceki projelere devam ederek gelecekteki deneyler için doğrudan kullanılabilen bir güvenlik modeli sunmaktır.

SEEDS (1 Mart 2021 - 28 Şubat 2025), Özellikle, SEEDS'in genel amacı, V2X ağları için çok katmanlı güvenilir ve sağlam bir güvenlik tasarımı elde etmek ve güvenlik sorunlarına yanıt vermek için araştırma bilgisinin Avrupa ülkeleri ve ortakları arasında transferini ve dağıtımını hızlandırmaktır. Yani gizlilik, bütünlük, mahremiyetin korunması, güven ve ölçeklenebilirlik.

CARAMEL (1 Ekim 2019 - 30 Haziran 2022), CARAMEL projesi, yollarda siber güvenlikle ilişkili güvenlik risklerini azaltmak için yapay zeka ve makine öğrenimi tekniklerine dayalı proaktif bir yöntem uyguluyor. Avrupa otomotiv endüstrisi için yenilikçi korsanlıkla mücadele saldırı tespit / önleme sistemlerini tanıtmayı amaçlamaktadır.

nIoVe (1 Mayıs 2019 - 30 Nisan 2022),Bunu yapmak için proje, nIoVe makine öğrenimi platformunu ve IoV(*Internet of Vehicule*) ekosistemindeki tehdit analizi ve durumsal farkındalık araçlarını besleyecek bir dizi yerleşik ve V2X veri toplayıcı geliştiriyor.

6. DENEYSEL ÇALIŞMA

Bu bölümde internetten indirdiğimiz bir veri tabanını inceleyeceğiz [36]. Veri tabanı bir enjeksiyon saldırısını göstermektedir. Veri kümeleri, mesaj enjeksiyon saldırıları devam ederken gerçek bir araçtan OBD-II portu üzerinden CAN trafiği kaydedilerek oluşturulmuştur. İlk olarak, deneysel protokolü sunuyoruz. Sonra, değerlendirdiğimiz sistemi ve incelemeye çalıştığımız parametreleri açıklıyoruz.

6.1. DENEYSEL VERİ

DoS attack, Fuzzy attack, Drive Gear Spoof ve Gauge Spoof (RPM ve gear) içeren araba hack veri setlerimiz var. Mesaj enjeksiyon saldırıları devam ederken gerçek bir araçtan OBD-II portu üzerinden CAN trafiği kaydedilerek veri setleri toplanmıştır. Veri kümelerinin her biri 300 mesaj enjeksiyon izinsiz girişi içerir. Her izinsiz giriş 3 ila 5 saniye arasında gerçekleştirildi ve her bir veri seti toplam 30 ila 40 dakikalık CAN trafiğine ulaştı. Kaydedilen CAN veri yolu trafiği, Hyunday YF Sonata Modeline dayalı bir CAN veri yolu mesaj yorumuyla CAN 2.0 spesifikasyonuna karşılık gelir.

6.1.1. Dos Saldırıları

Hizmet reddi veya DoS (*Denial of Service*) saldırısı, bir bilgisayar sunucusunu hatalı isteklerle aşırı derecede bombardımana tutarak işleyişini bozmayı veya tamamen felç etmeyi amaçlar [37]. Amaç, sistem kaynaklarından birini doyurarak çevrimiçi bir hizmeti veya bir şirketin ağını etkilemek olabilir: bant genişliği, depolama alanı, bir veri tabanının işlem kapasitesi, işlemcilerin hesaplanması, RAM...

DoS saldırıları için, CAN ID olarak “0000” olan mesajlar her 0,3 milisaniyede bir enjekte edilir. En baskın onlar.

6.1.2. Fuzzy Saldırılar

Bulanık saldırı, neyin bozulduğunu görmek için bir sisteme rastgele nesneler atarak bir sistemin her ayrıntısını öğrenmenin kesin sürecidir. Siber güvenlik dünyasında, fuzzing, bu permütasyonlardan biri bir güvenlik açığı ortaya çıkarana kadar bir hedef programa rastgele farklı

veri permütasyonlarını ekleyerek kötü amaçlı yazılım hatalarını bulmanın genel olarak otomatikleştirilmiş sürecidir [38].

Bulanık saldırılar için her 0,5 milisaniyede bir tamamen rastgele CAN ID ve DATA değeri mesajları enjekte edilir.

6.1.3. Tahrik Dişlisi Sahtekârlığı Ve Gösterge Sahtekârlığı (RPM / Gear)

Spoofing, bilinmeyen bir kaynaktan gelen bir iletişimin bilinen ve güvenilir bir kaynaktan geliyormuş gibi gösterilmesidir. Kimlik hırsızlığı, bir hedefin kişisel bilgilerine erişim sağlamak, virüslü bağlantılar veya ekler aracılığıyla kötü amaçlı yazılım yaymak, ağ erişim denetimlerini atlamak veya bir reddetme saldırısı gerçekleştirmek için trafiği yeniden dağıtmak için kullanılabilir.

RPM ve gear spoofing için, RPM/gear bilgileriyle ilgili belirli CAN ID'lerinden her 1 milisaniyede bir mesajlar enjekte edilir.

6.2. UYGULANMA

Birkaç teknik seçim yapıldı. Aşağıda, en önemlilerini açıklıyoruz:

- **Python 3.8.5:** Programlama dili seçimi Python'dur. Nesne yönelimli, öğrenmesi kolay, makine öğrenimi için en çok kullanılan dillerden biridir. Python'un çok sayıda kitaplığı vardır: veri analizi, bilimsel hesaplama, görselleştirme ve makine öğrenimi;
- **Pandas:** analiz ve ön işleme için verilerimizi kolayca manipüle etmemize izin veren bir Python kitaplığıdır;
- **Numpy:** Numpy kitaplığı, Python ile sayısal hesaplamalar yapmanızı sağlar;
- **Matplotlib:** Matplotlib, verileri çeşitli grafik formlarında çizmenize ve görselleştirmenize izin veren bir Python kitaplığıdır;
- **Seaborn:** Matplotlib ile erişilemeyen bazı işlevleri tamamlayan bir kütüphanedir;
- **Scikit-Learn:** GitHub'daki en önemli projelerden biridir. Sınıflandırma, regresyon, kümeleme, boyut indirgeme, model seçimi ve veri ön işlemeyi sağlayan bir makine öğrenme kütüphanesidir;
- **Jupyter Notebook:** Aynı belgede metin, resim, matematiksel formül ve çalıştırılabilir Python kodunu toplayabilen elektronik defterler olan Jupyter defterlerini kullandık;

- **Anaconda3:** Yukarıda bahsedilen kütüphanelerin kurulumu için Python kütüphaneleri dahil çok sayıda paketi entegre eden ücretsiz bir platform olan Anaconda'yı kullandık.

6.2.1. Veri Kaynağı

Aşağıdaki şekilde bir kayıttan bir alıntı gösterilmektedir.

	Timestamp	CAN ID	DLC	DATA[0]	DATA[1]	DATA[2]	DATA[3]	DATA[4]	DATA[5]	DATA[6]	DATA[7]	Flag
0	1.478196e+09	0545	8	d8	00	00	8a	00	00	00	00	R
2	1.478196e+09	0002	8	00	00	00	00	00	01	07	15	R
3	1.478196e+09	0153	8	00	21	10	ff	00	ff	00	00	R
4	1.478196e+09	0130	8	19	80	00	ff	fe	7f	07	60	R
5	1.478196e+09	0131	8	17	80	00	00	65	7f	07	9f	R

Şekil 6-1: Bir veri tabanı kaydından ayıklayın.

Her satır, ağdaki bir çerçevenin iletimine karşılık gelir. Sütunlar sırasıyla şunları açıklar:

- Timestamp: çerçevenin zaman damgası (saniye cinsinden);
- CAN ID: onaltılık biçimde çerçeve tanımlayıcısı;
- DLC: kontrol başlığına göre veri alanının boyutu (0'dan 8'e kadar);
- DATA [1~7] : veri alanının içeriği, değerler bayt ile gruplandırılır ve onaltılık gösterimde gösterilir;
- Flag: T veya R, T enjekte edilen mesajı temsil ederken, R normal mesajı temsil eder.

Bölüm 1'de sunduğumuz saldırı senaryolarına karşılık gelen kayıtları içeren 4 dosyamız var. Bu kayıtların içerdiği çerçevelerin sayısı tablo 6-1'da açıklanmıştır ve tablo 6-2 her bir saldırı türünün sıklığını göstermektedir.

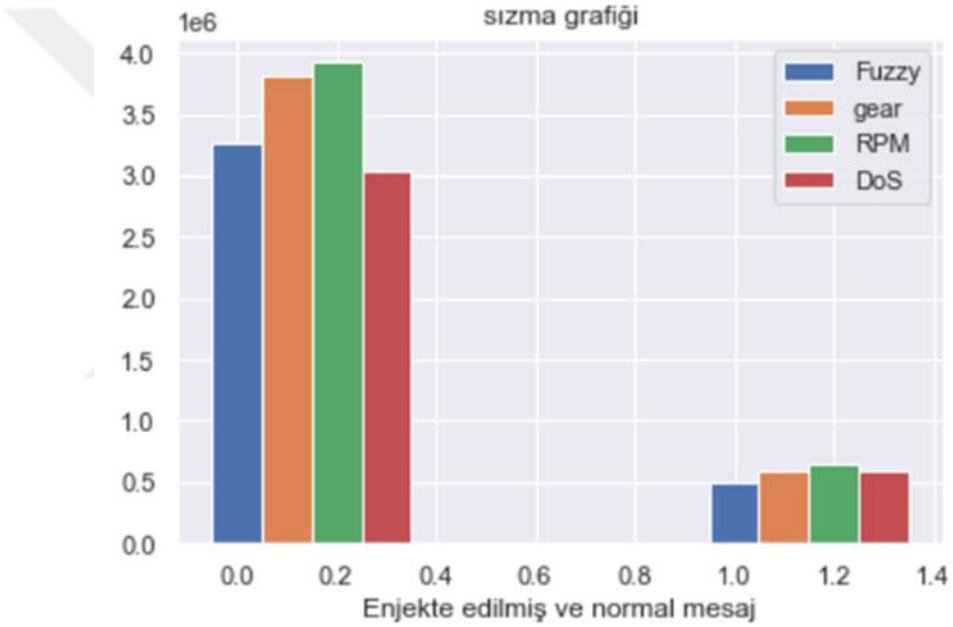
Tablo 6-1: Saldırıların açıklaması

CAN Message	Fuzzy	Gear	RPM	DoS
R	3259177	3805725	3925329	3047062
T	491847	597252	654897	587521
Total	3751024	4402977	4580226	3634583

Tablo 6-2: Saldırıların sıklığı

CAN Message	Fuzzy	gear	RPM	DoS
R	86.89	86.44	85.7	83.84
T	13.11	13.56	14.3	16.16

Bu iki tabloda, DoS tipi enjeksiyonların en sık ve Fuzzy tip enjeksiyonların en az sıklıkta olduğunu görüyoruz. Aşağıdaki şekil bu pasajı iyi bir şekilde özetleyebilir.



Şekil 6-2: Enjekte edilmiş ve normal mesaj grafiği

6.3. VERİ ANALİZİ

Veri analizi için, en basit sinir ağı türü olan çok katmanlı algılayıcıyı (veya MLP Multi-Layer Perceptron için) kullandık.

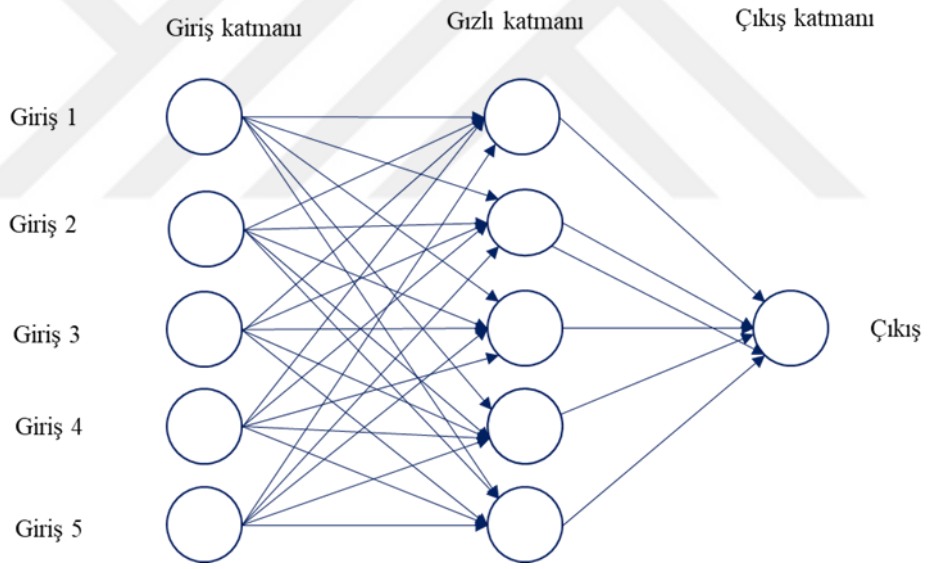
6.3.1. Sinir Ağları Modeli

Bir sinir ağı, insan beyninin bilgiyi nasıl işlediğinin basitleştirilmiş bir modelidir. Nöronların soyut versiyonlarına benzeyen çok sayıda birbirine bağlı işlem birimini simüle ederek çalışır [39].

İşlem birimleri katmanlar halinde düzenlenmiştir. Bir sinir ağının genel olarak üç bölümü vardır:

- Bir giriş katmanı (giriş alanlarını temsil eden birimlerle);
- Bir veya daha fazla gizli katman;
- Bir çıkış katmanı (hedef alan(lar)ı temsil eden bir veya daha fazla birim ile).

Üniteler farklı bağlantı güçleri (veya ağırlıkları) ile bağlanır. Girdi verileri ilk katmana sunulur ve değerler sonraki katmandaki her nörondan her nörona yayılır. Son olarak, çıkış katmanından bir sonuç çıktısı alınır.



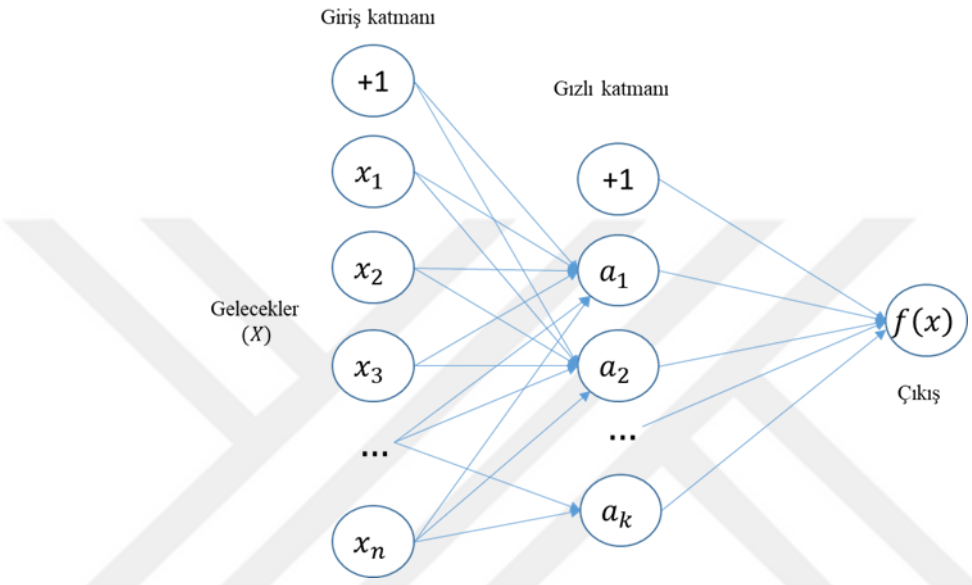
Şekil 6-3: Sinir ağı örneği

6.3.2. Multi-layer Perceptron (MLP)

Çok Katmanlı Algılayıcı (MLP), bir veri kümesi üzerinde eğitim vererek bir işlevi öğrenen denetimli bir öğrenme algoritmasıdır; burada ***n***, giriş için boyut sayısı ve ***o***, çıkış için boyut sayısıdır.

$$f(\cdot): R^n \rightarrow R^0 \tag{6.1}$$

Bir özellik seti $\boldsymbol{X = x_1, x_2, \cdots x_n}$ ve bir hedef $\boldsymbol{y}$ verildiğinde, sınıflandırma veya regresyon için doğrusal olmayan bir fonksiyon tahmincisi öğrenebilir. Lojistik regresyondan farklıdır, çünkü giriş katmanı ile çıkış katmanı arasında, gizli katmanlar olarak adlandırılan bir veya daha fazla doğrusal olmayan katman olabilir [40].



Şekil 6-4: Çok katmanlı perceptron (mlp) örneği

Giriş katmanı olarak adlandırılan en soldaki katman, giriş özelliklerini temsil eden bir dizi nörondan oluşur.

$$\{x_i | x_1, x_2, \ldots, x_n\} \tag{6.2}$$

Gizli katmandaki her bir nöron, bir önceki katmanın değerlerini ağırlıklı bir lineer toplama ile dönüştürür.

$$w_1 x_1 + w_2 x_2 + \cdots + w_n x_n \tag{6.3}$$

Bir aktivasyon fonksiyonu tarafından takip edilir. Aktivasyon fonksiyonları tercihen katı bir şekilde artan ve sınırlı olmalıdır. Geleneksel olarak kullanılan işlevler, doğrusal işlev, hiperbolik tanjant ($\boldsymbol{f_1}$) ve standart sigmoid işlevidir ($\boldsymbol{f_2}$) :

$$f_1(x) = tan\,h(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{6.4}$$

$$f_2(x) = \frac{tan\,h(x) + 1}{2} \tag{6.5}$$

Çıkış katmanı, son gizli katmandan değerleri alır ve bunları çıktı değerlerine dönüştürür.

Özetlemek gerekirse, bir algılayıcı nöron, giriş vektörü $\boldsymbol{x}$ ile ağırlık olarak adlandırılan bir parametre vektörü $\boldsymbol{w}$ arasında bir nokta çarpım gerçekleştirir, buna bir önyargı $\boldsymbol{b}$ ekler ve çıktısını belirlemek için bir aktivasyon fonksiyonu $\boldsymbol{f}$ kullanır [41].

$$y = f(x \cdot w + b) \tag{6.6}$$

6.3.3. Modelimiz

MLP'mizi eğitmek için aşağıdaki parametreleri kullandık:

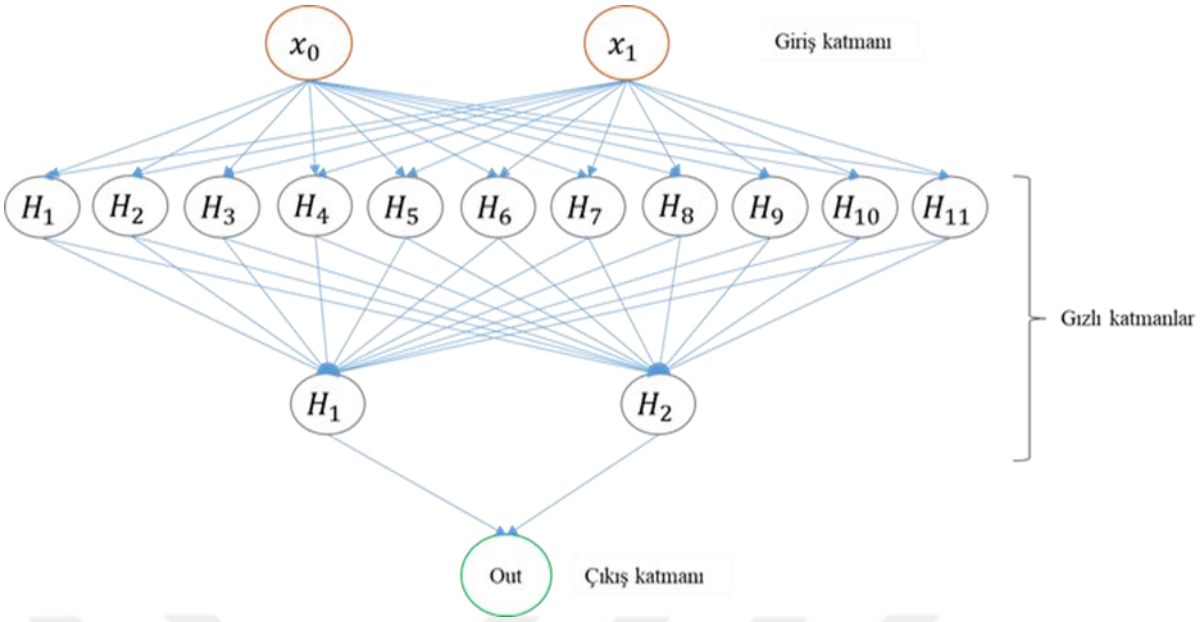
- **hidden_layer_sizes:** bu parametre ile Neural Network Classifier'da olmasını istediğimiz katman sayısını ve düğüm sayısını belirleyebiliriz. Dizinin her bir elemanı, i'nin dizinin indeksi olduğu i. konumundaki düğümlerin sayısını temsil eder. Böylece dizinin uzunluğu, sinir ağındaki toplam gizli katman sayısını gösterir;
- **max_iter:** Dönemlerin sayısını gösterir;
- **activation:** Gizli katmanlar için etkinleştirme işlevi;
- **solveur:** bu parametre, düğümlerdeki ağırlığı optimize etmek için algoritmayı belirtir.

```
Entrée [26]: #using Neural Network
             mlp_clf= MLPClassifier(hidden_layer_sizes=(11,2),
                                    max_iter = 300,activation = 'relu',
                                    solver = 'adam')
             mlp_clf.fit(trainX_scaled,Y_train)

Out[26]: MLPClassifier(hidden_layer_sizes=(11, 2), max_iter=300)
```

Şekil 6-5: MLP classifier kodları

İşlem sırasında oluşturulan ağ yapısı şöyle görünecektir.



Şekil 6-6: MLP mimarisi

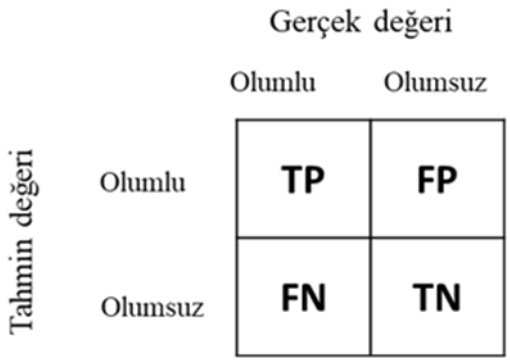
Bir MLP ağı oluşturmak için veriler her zaman ölçeklendirilmelidir çünkü ona karşı çok hassastır [42].

6.3.4. Modelimizin Değerlendirilmesi

Modelimizi değerlendirmek için bir karışıklık matrisi kullandık. Karışıklık matrisi genellikle sınıflandırma modellerini değerlendirmek için kullanılır. Bir karışıklık matrisi, bir sınıflandırma modelinin performansını değerlendirmek için kullanılan bir N x N matrisidir; burada N, hedef sınıfların sayısıdır [43]. Matris, gerçek hedef değerleri makine öğrenimi modeli tarafından tahmin edilen değerlerle karşılaştırır. Bu bize, sınıflandırma modelimizin nasıl performans gösterdiğine ve yaptığı hata türlerine dair bütünsel bir görüş sağlar.

Bizim durumumuz için bir ikili sınıflandırma problemimiz var, bu nedenle aşağıda gösterildiği gibi 2 x 2 matrisimiz var.

Burada TP (gerçek pozitif) ve TN (gerçek negatif), sırasıyla saldırı veya normal olarak doğru şekilde sınıflandırılan mesajların sayısıdır ve FP (yanlış pozitif) ve FN (yanlış negatif), sırasıyla saldırı veya normal olarak yanlış sınıflandırılan mesajların sayısıdır [44].



Şekil 6-7: 2x2 karşıklık matrisi

İşte Doğruluğu (*Accuracy*) nasıl hesaplayacağız:

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FN} \tag{6.7}$$

Modelimizin güvenilir olup olmadığını belirlemek için *Precision*'ımız var. Bize doğru tahmin edilen kaç vakanın pozitif çıktığını anlatıyor. Aşağıdaki gibi hesaplanır:

$$Precision = \frac{TP}{TP + TF} \tag{6.8}$$

Modelimizle kaç tane gerçek pozitif vakayı doğru bir şekilde tahmin edebildiğimizi bilmek için, Geri Çağırma (*Recall*) bize bildirmek için oradadır. Geri çağırma şu şekilde hesaplanır:

$$Recall = \frac{TP}{TP + FN} \tag{6.9}$$

F1 puanı (*f1-score*), *Precision* ve *Recall'nın* harmonik bir ortalamasıdır ve bu nedenle bu iki ölçüm hakkında birleşik bir fikir verir. Kesinlik, Geri Çağırmaya eşit olduğunda maksimumdur [43].

$$F1 - score = \frac{2}{\frac{1}{Recall} + \frac{1}{Precision}} \tag{6.10}$$

Bu nedenle, şekil 6-8 bize her bir saldırı türü için modelimiz tarafından oluşturulan sınıflandırma oranını ve şekil 6-9 bize kayıp eğrisini göstermektedir.

	precision	recall	f1-score	support
0	1.00	1.00	1.00	609498
1	1.00	1.00	1.00	117419
accuracy			1.00	726917
macro avg	1.00	1.00	1.00	726917
weighted avg	1.00	1.00	1.00	726917

DoS

	precision	recall	f1-score	support
0	0.99	1.00	1.00	652264
1	0.99	0.96	0.98	97941
accuracy			0.99	750205
macro avg	0.99	0.98	0.99	750205
weighted avg	0.99	0.99	0.99	750205

Fuzzy

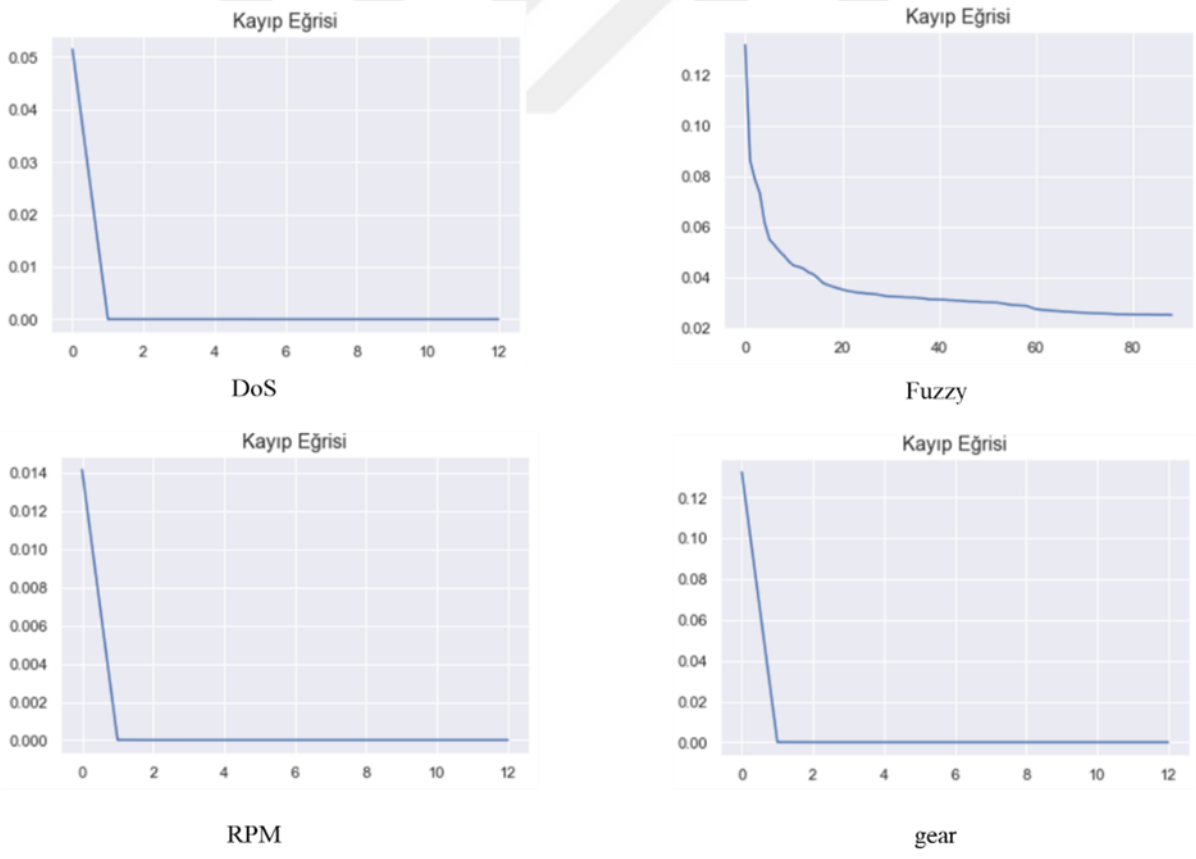
	precision	recall	f1-score	support
0	1.00	1.00	1.00	784967
1	1.00	1.00	1.00	131079
accuracy			1.00	916046
macro avg	1.00	1.00	1.00	916046
weighted avg	1.00	1.00	1.00	916046

RPM

	precision	recall	f1-score	support
0	1.00	1.00	1.00	118986
1	1.00	1.00	1.00	761610
accuracy			1.00	880596
macro avg	1.00	1.00	1.00	880596
weighted avg	1.00	1.00	1.00	880596

gear

Şekil 6-8: Bildiri saldırıların sınıflandırması



Şekil 6-9: Kayıp eğrisini

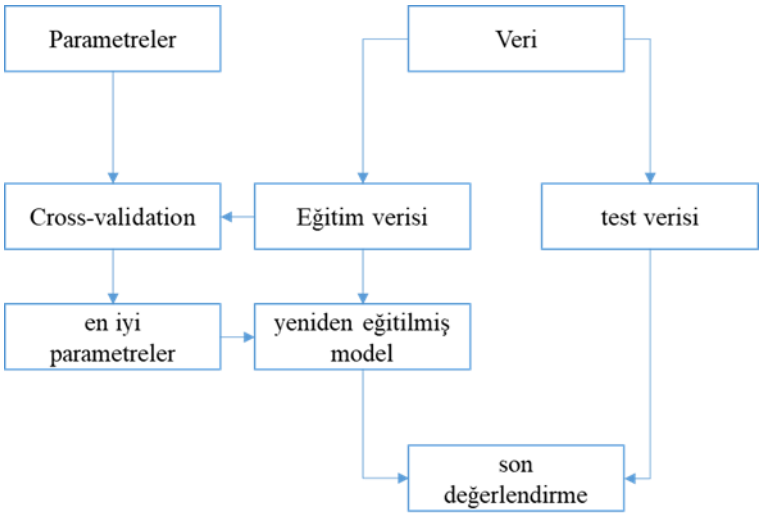
Modelimizin değerlendirilmesinden sonra aşağıdaki tabloda temsil edilen sonuçları bulduk.

Tablo 6-3: Analiz sonuçları tablosu

Attaque type	Accuracy	Precision	Recall	F1-score
DoS	1,00	1,00	1,00	1,00
Fuzzy	0,99	0,99	0,96	0,98
RPM	1,00	1,00	1,00	1,00
gear	1,00	1,00	1,00	1,00

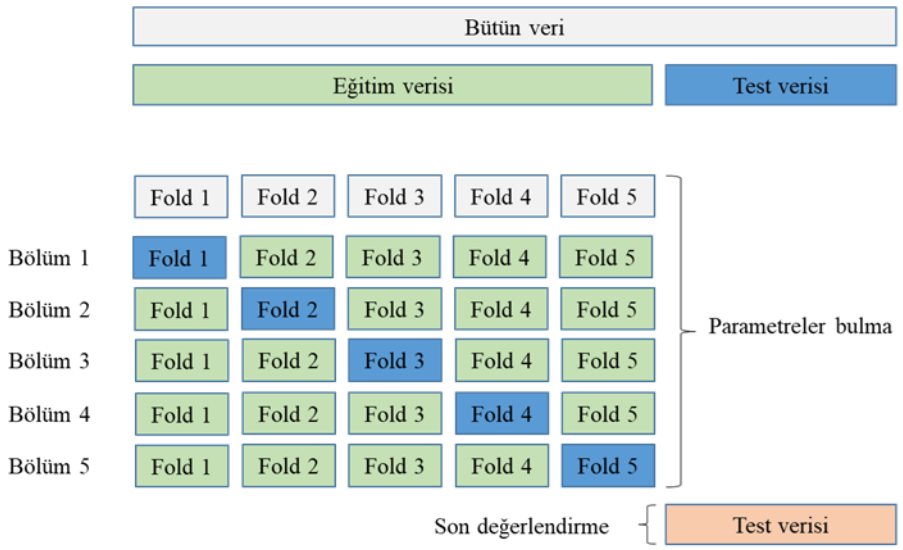
6.3.5. 5 Fold Cross Validation

Modelimize fazla uymamak için çapraz doğrulama yaptık. Çünkü bir tahmin fonksiyonunun parametrelerini öğrenmek ve aynı veriler üzerinde test etmek metodolojik bir hatadır. Çapraz doğrulama, model değerlendirmesinde önemli bir adımdır [45]. Bu, modeli eğitmek için kullanılan veri miktarını en üst düzeye çıkarır, çünkü eğitim sırasında model yalnızca eğitilmez, aynı zamanda mevcut tüm veriler üzerinde test edilir. Şekil 6-10'de gösterildiği gibi:



Şekil 6-10: Cross validation

Bizim durumumuzda, farklı veri türlerinde 5 katlı çapraz doğrulama (5-fold cross validation) kullanacağız. Bu 5 katlı çapraz doğrulama tekniğinde veri seti 5 eşit büyüklükte parçaya bölünür. Her bölüme "Fold" denir. Yani elimizde 5 parça olduğu için 5-Fold diyoruz.



Şekil 6-11: 5 fold cross validation

Bir Fold doğrulama seti olarak kullanılır ve diğer Fold'lar biçimlenme seti olarak kullanılır. Teknik, her Fold doğrulama seti ve kalan Fold'lar eğitim seti olarak kullanılana kadar 5 kez tekrarlanır. Modelin nihai doğruluğu, doğrulama verilerinin ortalama doğruluğu alınarak hesaplanır.

6.3.6. LSTM ve GRU

Karşılaştırma için modelimizin puanını LSTM ve GRU modellerinin puanı ile karşılaştıracağız.

6.3.6.1. LSTM

Uzun-kısa süreli bellek veya LSTM (Long Short-Term Memory) modelleri, RNN (Recurrent Neural Network) mimarisinin bir çeşididir. Bir sinir ağının LSTM olarak sınıflandırılabilmesi için en az 1 LSTM katmanına sahip olması gerekir. Temel olarak, aynı yinelenen davranışa sahiptirler. Ancak, LSTM düğümleri sıradan RNN düğümleri gibi değildir [46]. LSTM düğümlerinin üç ek kapısı vardır: giriş kapısı, çıkış kapısı ve unutma kapısı. Bu ek kapılar, basit RNN'lerden dört kat daha fazla parametreye sahip LSTM'lerle sonuçlanır.

6.3.6.2. GRU

Kapalı tekrarlayan birimler GRU (Gated Recurrent Unit), tekrarlayan sinir ağı tasarımının başka bir çeşididir. GRU hücreleri, LSTM hücrelerine benzer. Geleneksel bir sinir ağındaki bir

hücre veya düğümden farklı olarak, GRU'lar ayrıca kapılar içerir. Bir giriş kapısı ve bir unutulma kapısı içerirler. LSTM'lerin aksine, GRU'lar çıkış kapıları içermez. GRU'lar ilk olarak 2014 yılında LSTM'lere alternatif olarak tanıtıldı [47]. Çoğu zaman benzer performans gösterirler, ancak daha az eğitim parametresine sahiptirler. GRU'ların, daha düşük veri hızına sahip daha küçük veri kümeleri gibi bazı veri kümelerinde LSTM'lerden daha iyi performans gösterdiği gösterilmiştir.

Farklı modellerimizi derledikten sonra, aşağıdaki tabloda temsil edilen puanları bulduk:

Tablo 6-4: Karşılaştırma tablosu

Model	**DoS**	**Fuzzy**	**RPM**	**gear**
MLP	1	0,99	1	1
5Fold-CV	0,83	0,86	0,85	0,86
LSTM	0,83	0,86	0,85	0,86
GRU	0,83	0,86	0,85	0,86

Bu çalışmada bir CAN veri yoluna enjekte edilen saldırı mesajlarını öğrenmek için bir öğrenme modeli uyguladık. MLP öğrenme algoritmasını kullandık. Modeli, farklı saldırı türlerini içeren dört açık kaynaklı araç hack veri setinde test ettik, yani: DoS saldırısı,Bulanık saldırı(Fuzzy), Sürücü dişlisi sahtekârlığı ve gösterge sahtekârlığı (RPM ve gear). İlk önce modelimizi tek bir saldırı türü olan veri kümeleri üzerinde kullandık. Sonra modelimizi bir karışıklık matrisi ile değerlendirdik. Böylece, Fuzzy saldırısı için 0.99, DoS saldırısı için 1.00 ve tahrik dişlisinin yanıltması ve göstergenin (RPM ve gear) yanıltması için 1.00 puan elde ettik.

Modelimize fazla uymamak için çapraz doğrulama yaptık (cross validation). Böylece, Fuzzy saldırısı için 0.86, DoS saldırısı için 0.83, tahrik dişlisinin yanıltması RPM için 0,85 ve göstergenin yanıltması (gear) için 0.86 puan elde ettik.

7. SONUÇ VE ÖNERİLER

Gömülü sistemler, çok sayıda işlevsellik sunabilen ve hesaplanamaz miktarda görev gerçekleştirebilen çok güçlü araçlardır. Ancak bu sistemler, tasarım karmaşıklığı ve sürekli kararsız ortamı nedeniyle kullanıcılarına operasyonel güvenilirliği ve maksimum güvenliği garanti edemez. Gerçekten de, çok iyi tasarlanmış bir koruma aracı, örneğin tasarımı sırasında henüz bilinmeyen yeni teknikler sayesinde bazen atlatılabilir. Bu durumda, güvenlik politikalarının uygulanması, ilgili sistemlere ve onları hedefleyebilecek saldırıların çeşitliliğine genel bir bakış sağlanarak yapılmalıdır.

Bu tezde ilk olarak otomotiv gömülü sistemler özelliklerini sunduk, özellikle yazılım kısmına ve günümüzde en çok kullanılan iletişim protokollerine (CAN) odaklanmak. Ardından, modern otomobillerin yerleşik ECU'larını hedef alabilecek farklı saldırı senaryolarını inceledik. Ondan sonra, gözlemlenen ağ trafiğine dayalı olarak gömülü otomotiv ağları için bir saldırı tespit sistemi sunduk. Ardından, yerleşik otomotiv ağlarını korumak için mevcut veya planlanmış çeşitli bilgisayar güvenlik mekanizmalarını sunduk. Son olarak, bir CAN veri yoluna enjekte edilen saldırı mesajlarını öğrenmek için bir öğrenme modeli uyguladık. MLP öğrenme algoritmasını kullandık. Modeli, farklı saldırı türlerini içeren dört açık kaynaklı araç hack veri setinde test ettik, yani: DoS saldırısı, Bulanık saldırı(*Fuzzy*), Sürücü dişlisi sahtekârlığı ve gösterge sahtekârlığı (RPM ve gear). Bu alandaki araştırmamız, lojistik regresyon (*Logistic regression*) veya çok terimli sınıflandırıcı Naive Bayes (*multinomial Naive Bayes classifie*) gibi başka bir modelle devam edebilir... Ve böylece, farklı veri tabanlarımızdan öğrenmek için hangi modellerin en uygun olduğunu bulmak için sonuçları karşılaştırırız.

Bu çalışma, gömülü sistemlerin üyeliğini ve ekini otomotiv alanında göstermektedir, kullanımlarında belirgin bir artış ile güvenlik, konfor veya doğrudan operasyon gibi farklı alanlar aracın. Bu nedenle, bu sistemlerin yardım ve uyarı işlevleri aracılığıyla kullanıcısına ek bir güvenlik düzeyi sağladığını ancak başarısız olduklarında ne yazık ki bir tehlike oluşturabileceğini gördük. Sonuç olarak, yerleşik bilgisayarların özelliklerinin sayısındaki sürekli artış ve otomobillerin artık donatıldığı çoklu iletişim yetenekleriyle, üreticilerin yanıt vermesi gereken birçok güvenlik sorunu ortaya çıktı.

Benim için modern bir araba karmaşık bir sistemden oluşur. Gerçekten etkili güvenlik için, bu karmaşıklığın tüm yönlerini hesaba katan bir güvenlik stratejisi uygulamaya konmalıdır.

8. KAYNAKLAR

[1] THALES, «SÉCURITÉ DES VOITURES CONNECTÉES : L'IMPORTANCE DE LA MÉTHODE,» 27 07 2016. [Çevrimiçi]. Available: https://www.thalesgroup.com.

[2] İ. STUDNIA, Détection d'intrusion pour des réseaux embarqués automobiles : une approche orientée langage, Toulouse: Institut national des sciences appliquées de Toulouse, 2015.

[3] ESILV, «lingenieur-systemes-embarques-incontournable-dans-lautomobile-et-laeronautique,» 27 12 2019. [Çevrimiçi]. Available: https://www.esilv.fr.

[4] F. SIMONOT-LION ve N. NAVET, «Les réseaux temps réel embarqués dans les véhicules,» %1 içinde *Systèmes temps réel – Volume 2*, Paris, Lavoisier, 2006, p. 281.

[5] . F. BOITTIAUX, «La production automobile mondiale à - 15,8 % en 2020,» 26 Nısan 2021. [Çevrimiçi]. Available: https://pro.largus.fr.

[6] BIBLIO TECHNO, «Voitures connectées : les nouveaux défis du test électronique,» 21 OCAK 2016. [Çevrimiçi]. Available: https://www.actutem.com/.

[7] M. T. GIORGIO, «Véhicule autonome : on distingue 5 niveaux d'autonomie,» 26 Eylül 2020. [Çevrimiçi]. Available: https://www.visite-medicale-permis-conduire.org.

[8] M. A. M. OUBRAHIM, K. TAHIRY ve A. FARCHI, Architecture réseaux et électroniques embarqués automobiles, Casablanca: Ecole Supérieure de Technologie de Casablanca (Maroc), Institut Universitaire de Technologie d'Aix-Marseille (France), 2019.

[9] ISO, «ISO 26262-1:2018 Road vehicle engineering (Vocabularies),» Decembre 2018. [Çevrimiçi]. Available: https://www.iso.org.

[10] A. BENKHELIFA, «Les systèmes embarqués dans l'automobile,» Haute École de Gestion de Genève (HEG-GE), Genève, 2018.

[11] F. SOMMER, J. DURRWANG ve R. KRIESTEN, «Survey and Classification of Automotive Security Attacks,» *MDPI*, p. 148, 219.

[12] S. CHECKOWAY, D. MCCOY, B. KANTOR, D. ANDERSON, . H. SHACHAM, S. SAVAGE, K. KOSCHER, A. CZESKIS, F. ROESNER ve T. KOHNO, «Comprehensive Experimental Analyses of Automotive Attack Surfaces,» 2011.

[13] RTL-SDR, «STEVE MOULD HACKS INTO HIS CAR WITH A HACKRF,» 9 Decembre 2020. [Çevrimiçi]. Available: http://www.rtl-sdr.com.

[14] C. MILLER ve C. VALASEK, «Black Hat USA 2015: The full story of how that Jeep was hacked,» 6 Ağustos 2015. [Çevrimiçi]. Available: https://www.kaspersky.com/.

[15] T-SYSTEMS, «Intrusion Detection System : gardien des voitures connectées,» 1 Janvier 2021. [Çevrimiçi]. Available: https://www.t-systems.com/.

[16] M. MÜTER, A. GROLL ve F. C. FREILING, «A structured approach to anomaly detection for in-vehicle networks,» %1 içinde *2010 Sixth International Conference on Information Assurance and Security*, Atlanta, 2010.

[17] S.-F. LOKMAN, A. T. OTHMAN ve M.-H. ABU-BAKAR, «Système de détection d'intrusion pour le système de bus CAN (Controller Area Network) automobile : un examen,» *Journal EURASIP sur les communications et les réseaux sans fil*, p. 184, 2019.

[18] L. R. HALME ve K. R. BAUER, AINT misbehaving : A taxonomy of anti-intrusion techniques., San Jose: Arca Systems, Inc., 1995.

[19] D. K. NILSSON ve . U. E. LARSON, «A Defense-in-Depth Approach to Securing theWireless Vehicle Infrastructure,» *JOURNAL OF NETWORKS,* pp. 552-564, 7 Septembre 2009.

[20] A. GROLL, J. HOLLE, C. RULAND, M. WOLF, T. WOLLINGER ve F. ZWEERS, «OVERSEE A Secure and Open Communication and Runtime Platform for Innovative Automotive Applications,» In 7th Embedded Security in Cars Conference , Düsseldorf, 2009.

[21] A. BOUARD, H. SCHWEPPE, B. WEYL ve C. ECKERT, «Leveraging In-Car Security by Combining Information Flow Monitoring Techniques,» *Second International Conference on Advances in Vehicular Systems Technologies and Applications (VEHICULAR 2013),* pp. 1-7, 2013.

[22] S. SCHULZE, M. PUKALL, G. SAAKE, T. HOPPE ve J. DITTMANN, «On the need of data management in automotive systems.,» *BTW*, pp. 217-226, 2009.

[23] C. MILLER ve C. VALASEK, «A survey of remote automotive,» 27 JUILLET 2014. [Çevrimiçi]. Available: https://ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf.

[24] ARILOU, «Feasible Car Cyber Defense.,» %1 içinde *10th Embedded Security in Cars*, 2012.

[25] P. GARCIA-TEODORO, J. E. DIAZ-VERDEJO, G. MACIA-FERNANDEZ ve E. VAZQUEZ, «Anomaly-based network intrusion detection: Techniques, systems and challenges,» *Computers & Security*, pp. 18-28, 2008.

[26] C. MILLER ve C. VALASEK, «Adventures in automotive networks and control units,» %1 içinde *DEF CON 21*, 2013.

[27] H. M. SONG, H. R. KIM ve H. K. KIM, «Intrusion Detection System Based on the Analysis of,» %1 içinde *2016 international conference on information networking (ICOIN)*, Kota Kinabalu, 2016.

[28] A. WASICEK ve A. WEIMERSKIRCH, «Recognizing Manipulated Electronic Control Units,» %1 içinde *SAE 2015 World Congress & Exhibition*, 2015.

[29] A. Avalappampatty Sivasamy ve B. SUNDAN, «A Dynamic Intrusion Detection System Based on Multivariate Hotelling's T2 Statistics Approach for Network Environments,» *The Scientific World Journal*, p. 1–9, 2015.

[30] J. D. HOWARD ve T. A. LONGSTAFF, «A common language for computer security incidents,» Sandia National Lab, 1998.

[31] C.-Y. TSENG, P. BALASUBRAMANYAM, C. KO, R. LIMPRASITTIPORN, J. ROWE ve K. LEVITT, «A specification-based intrusion detection system for AODV,» *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, p. 125–134, 203.

[32] D. KRISHNAN ve M. C. CHATTERJEE, «An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework,» %1 içinde *International Conference on Security in Computer Networks and Distributed Systems*, 2012.

[33] C. WANG, Z. ZHAO, L. GONG, L. ZHU, Z. LIU ve X. CHENG, «A distributed anomaly detection system for in-vehicle network using HTM,» *IEEE Access (Volume: 6)*, pp. 9091-9098, 2018.

[34] K. K. G. BUQUERIN, C. CORBETT ve H.-J. HOF, «A generalized approach to automotive forensics,» *Forensic Science International: Digital Investigation*, 2011.

[35] CORDIS, «CORDIS research results,» 23 novembre 2021. [Çevrimiçi]. Available: https://cordis.europa.eu.

[36] E. SEO, H. M. SONG ve H. K. KIM, «GIDS: GAN based Intrusion Detection System for In-Vehicle Network,» *Vehicular Communications*, pp. 1-6, 2018.

[37] F. Tech, «Déni de service : qu'est-ce que c'est ?,» 2021. [Çevrimiçi]. Available: https://www.futura-sciences.com.

[38] A. GREENBERG, «Hacker Lexicon: What Is Fuzzing?,» 2 Juin 2016. [Çevrimiçi]. Available: https://www.wired.com.

[39] IBM, «SPSS Modeler 18.1.1,» [Çevrimiçi]. Available: https://www.ibm.com/. [Erişildi: 16 ocak 2022].

[40] Scikit learn, «Neural network models (supervised),» [Çevrimiçi]. Available: https://scikit-learn.org. [Erişildi: 02 Decembre 2021].

[41] D. E. RUMELHART ve J. L. McClelland, «Parallel Distributed Processing: Explorations in the Microstructure of Cognition,» *MIT Press,* p. 567, 1987.

[42] M. FUCHS, «NN - Classificateur Perceptron multicouche (MLPClassifier),» 2021.

[43] A. BHANDARI, «Tout ce que vous devez savoir sur la matrice de confusion pour l'apprentissage automatique,» 17 Avril 2020. [Çevrimiçi]. Available: https://www.analyticsvidhya.com/.

[44] V. S. BARLETTA, D. CAIVANO, A. NANNAVECCHIA ve M. SCALERA, «A Kohonen SOM Architecture for Intrusion Detection on In-Vehicle Communication Networks,» *Applied Sciences,* 2020.

[45] Scikit-learn, «Cross-validation: evaluating estimator performance,» [Çevrimiçi]. Available: https://scikit-learn.org.

[46] Y. TANG, «Long Short-Term Memory (LSTM) in Keras,» 31 Aralık 2021. [Çevrimiçi]. Available: https://pythonalgos.com.

[47] Y. TANG, «Build a GRU RNN in Keras,» 2 Ocak 2022. [Çevrimiçi]. Available: https://pythonalgos.com.

[48] J. LI, «Cansee-an automobile intrusion detection system,» %1 içinde *In Presentation slides on Hack In The Box Security Conference (HITBSecConf),* 2016.

ÖZGEÇMİŞ

Kişisel Bilgiler		
Adı Soyadı		
Doğum Yeri		
Doğum Tarihi		
Uyruğu		
Telefon		
E-Posta Adresi		
Web Adresi		

	Eğitim Bilgileri
	Lisans
Üniversite	
Fakülte	
Bölümü	
Mezuniyet Yılı	

Yüksek Lisans	
Üniversite	
Enstitü Adı	
Anabilim Dalı	
Programı	

Makale ve Bildiriler