Tam Otonom Araçlarda Potansiyel Siber Saldırı Kaynaklarının İncelenmesi

Investigation of Cyber Attack Sources in Fully Autonomous Vehicles

Engin Subaşı[1,2], *Muharrem Mercimek*[1]

[1]Kontrol ve Otomasyon Mühendisliği Bölümü
Yıldız Teknik Üniversitesi, Davutpaşa Kampüsü, İstanbul
enginsubasi@gmail.com, mercimek@yildiz.edu.tr

[2]Fonksiyonel Emniyet ve Siber Güvenlik Takımı
FEV Türkiye, İstanbul
subasi@fev.com

Özetçe

Otomotiv sektörü ve özellikle otonom araç teknolojisindeki hızlı gelişmelerle birlikte, araçların güvenliğini sağlamak ve olası siber saldırılara karşı korumak, araç emniyeti ve güvenliği için en önemli problemlerden biri haline gelmiştir. Bu kapsamda, tam otonom araçları hedef alan potansiyel siber saldırı kaynaklarının belirlenmesi, karşı önlemler alınabilmesi için atılacak ilk adımdır. Potansiyel saldırı yöntemlerinin kapsamlı bir şekilde incelenmesi ve analizi, oluşabilecek siber saldırı durumlarına önlem almak için en önemli ön koşuldur. Bu çalışmada ağ tabanlı saldırılar, kötü amaçlı yazılımlar, fiziksel kurcalama ve sosyal mühendislik dahil olmak üzere bilinen güvenlik tehditleri incelenerek potansiyel saldırı kaynakları ortaya konmuştur. Nihai hedef olarak bu çalışmaya esas oluşturan senaryolar üzerinden tam otonom araçların yer aldığı ulaşım sistemlerinde güvenliğin ve bu sistemlere güvenilirliğin artırılması hedeflenmektedir.

Abstract

With the rapid developments in automotive industry and especially in autonomous vehicle technology, securing vehicles and protecting them against possible cyber-attacks has become one of the most important problems for vehicle safety and security. In this context, identifying potential sources of cyber-attacks targeting fully autonomous vehicles is the first step towards taking countermeasures. Comprehensive investigation and analysis of potential attack methods is the most important prerequisite for taking precautions against cyber-attacks. In this study, known security threats, including network-based attacks, malware, physical tampering, and social engineering, were investigated. The goal is to increase the security and reliability of transportation systems with fully autonomous vehicles through the scenarios that form the basis of this study.

1. Giriş

Tam otonom araçlar [1] (otonom araç veya araç olarak anılacaktır), otomotivde devrim yaratmayı hedefleyen dönüştürücü bir teknoloji olarak ortaya çıkmıştır. Bu araçlar yol güvenliğini artırma, trafik akışını optimize etme ve gündelik hayata uygun mobilite çözümleri sağlama potansiyeline sahiptir. Bununla birlikte, devrim yaratan teknolojilerde olduğu gibi bu teknolojik gelişme de kendi riskleri ile ortaya çıkmıştır. Otonom araçlarda sürücüler ortadan kalktığı için tüm kontroller elektronik sistemlere bırakılmıştır. Bu durumda sistemlerin olası siber saldırılara karşı korunması, araç kullanıcıların güvenini kazanmak ve bu güveni sürdürülebilir şekilde tutmak için kritik önem taşımaktadır. Otonom araçlar üzerine olası bir siber saldırı durumunda aracı farklı bir yere sürme, beklenmedik hızlandırma, ani manevra yaptırma gibi tehlike senaryoları gerçekleşebilir [2].

Otonom araçların temel kontrol fonksiyonları doğru ve bozucu etkilere karşı dirençli bir şekilde tasarlansa bile dışarıdan gelebilecek siber tehditlere karşı açıkları olabilmektedir. Bu durumda ilgili sistemlerin güvenliğinden bahsetmek için ek önlemlere ihtiyaç duyulmaktadır.

Bu çalışmada otonom araçları hedef alan potansiyel siber saldırı kaynaklarının belirlenmesi konusu ele alınmaktadır. Bu kapsamda endüstri standardı olarak belirtilen ve 2021 yılında yayınlanan siber güvenlik standardında [3] siber güvenlik yönetimi için tanımlanan gerekli yollar son teknoloji yöntemler olarak kabul edilmektedir. Bu çalışmada, siber saldırı kaynaklarının incelemesi üzerinde durularak otonom araç ekosisteminde var olan güvenlik açıklarının tanımlanması hedeflenmektedir. Siber güvenliği sağlamak için ilk adım, var olan tehditleri ve bu tehditlere imkân oluşturacak atak yollarını açık bir şekilde tanımlayabilmektir.

ISO 21434 kapsamında tehditlerin belirlenmesi ve değerlendirilmesi üzerine verilen yol haritası Şekil 1'de gösterilmiştir. Bu çalışmanın çıktıları hasar senaryosu tanımlama, tehdit senaryosu tanımlama ve atak yolu analizini destekleyecek niteliktedir.

Şekil 1: ISO21434 standardına göre otonom araçlarda siber tehditlerin yönetilmesi iş akışı

Otonom araçların güvenliğini sağlamadaki önemli zorluklardan biri, kötü niyetli kişi veya grupların kullanacağı çeşitli saldırı yöntemlerini ve yollarını anlamaktır. Potansiyel riskleri etkili bir şekilde öngörmek ve azaltmak için hem geleneksel hem de yeni ortaya çıkan tehditleri dikkate almak önemli olmaktadır. Bu çalışmada ağ tabanlı saldırılar, kötü amaçlı yazılımlar, fiziksel kurcalamalar ve sosyal mühendislik tekniklerini kapsayacak şekilde, otonom araçlar için güvenlik tehditlerini incelenmektedir.

Otonom araçlar etkin bir şekilde çalışmak için çeşitli iletişim sistemlerine ve teknolojilerine ihtiyaç duymaktadır. Ağ tabanlı saldırılar önemli bir tehdit kaynaklarındandır. Bilgisayar korsanları, potansiyel olarak kritik araç işlevlerine yetkisiz erişim elde ederek veya yolcuların mahremiyetini ve güvenliğini tehlikeye atarak bu sistemlerdeki güvenlik açıklarından yararlanmaya çalışabilmektedir. Bu tür saldırı yollarını analiz etmek, ağ izinsiz girişlerine karşı güçlü savunmalar geliştirmek ve araç sistemlerinin bütünlüğünü sağlamak için önemlidir.

Kötü amaçlı yazılım ve fidye yazılımı dahil olmak üzere bu kaynaklar da otonom araçlar için tehdit oluşturmaktadır. Bu kötü amaçlı programlar, araç işlemlerini kesintiye uğratabilir, sensör verilerini manipüle edebilir ve hatta temel işlevlerin kontrolünü ele geçirerek yolda tehlikeli durumlara sebep olabilmektedir. Bu tür yazılımların otonom araçlara sızabileceği potansiyel kaynakları ve yöntemleri anlamak, kötü amaçlı yazılım saldırılarına karşı savunmalarını güçlendirmek için zorunlu olmaktadır.

Fiziksel kurcalama, tam otonom araçlar için başka bir potansiyel saldırı yollarını temsil etmektedir. Tehdit aktörleri, araç bileşenlerini fiziksel olarak manipüle etme, sensörleri tehlikeye atma veya kritik altyapıyı kurcalamaları sonucunda otonom ulaşım sistemlerinin emniyeti ve güvenilirliği için risk oluşturabilir. Bu potansiyel fiziksel saldırı kaynaklarının belirlenmesi, yetkisiz erişim ve kurcalamaya karşı koruma sağlamak için güçlü güvenlik önlemlerinin geliştirilmesini sağlamaktadır.

Ayrıca, sosyal mühendislik teknikleri, otonom araçlara yönelik olası saldırılarda çok önemli bir rol oynamaktadır. Saldırganlar güven, aldatma veya manipülasyon gibi insan kaynaklı güvenlik açıklarından yararlanarak yetkisiz erişim elde edebilir veya araç işlemlerini manipüle edebilir. Otonom araç sistemlerini tehlikeye atmak için kullanılabilecek çeşitli sosyal mühendislik yöntemlerini incelemek, kullanıcıları eğitmek, farkındalığı artırmak ve uygun önlemleri uygulamak için çok önemlidir.

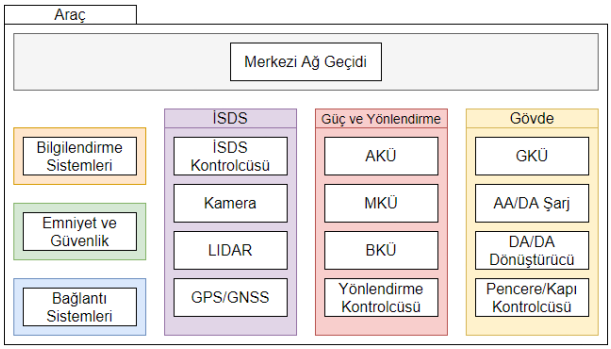
Bu çalışma kapsamında incelenen ataklardan korunmak ve atak yollarını engellemek için tasarım sürecinde çeşitli karşı önlemler alınmalıdır. Tüm bu önleyici çalışmaları yapmak dahi bir ürünün güvenliğini garanti etmeyecektir. Teknoloji ilerlediği sürece atak yollarında da yeni teknikler ve yöntemler ortaya çıkacaktır. Ürün yaşam döngüsü boyunca belirli periyotlarda bu analiz yöntemlerini tekrar etmek ve potansiyel tehditleri yeniden değerlendirmek gerekmektedir.

2. Araç Sistem Tanımlamaları

Otomotiv sektöründe sadece tek bir tip araçta bile birbirinden farklı mimariler kullanılmaktadır. Bu kapsamda çalışmanın çerçevesini belirlemek doğru bir analiz gerçekleştirmek için önemlidir. Bu kısımda üzerine çalışılacak ana yapı ve alt sistemler hakkında detaylı tanımlamalar verilmiştir.

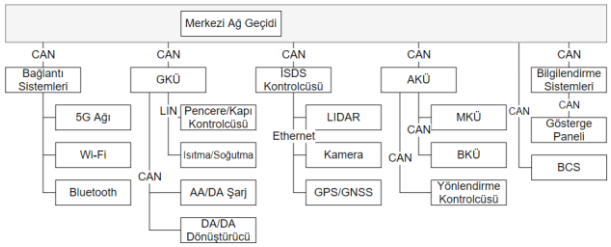
2.1. Otonom Araç Elektronik Mimarisi ve Alt Sistemleri

Otonom araç teknolojisinin araçların elektronik mimarileri üzerine büyük ve yenilikçi etkileri olmuştur. Bunları incelemek için sistemler bu çalışma kapsamında 6 ana sisteme ayrılmıştır. Bunlar gövde, güç ve yönlendirme, emniyet ve güvenlik, İSDS (İleri Sürüş Destek Sistemleri), bilgilendirme sistemleri ve bağlantı sistemleridir. İlgili kısımlar da kendi içlerinde değerlendirildiğinde Şekil 2'de verilen temel sistemlere ve alt sistemlere ayrılmaktadır.



Şekil 2: Tam otonom araç elektronik mimarisi

Analizin devamında sistemlerin detayını doğru yorumlayabilmek için araç içi elektronik mimariyi daha detaylı bir şekilde göstermek adına Şekil 3'teki mimari oluşturulmuştur.



Şekil 3: Tam otonom araç detaylı elektronik mimarisi

2.2. Araç Ağ Yapısı

Araç elektroniğinde sıklıkla kullanılan temel ağ yapıları aşağıdaki listede verilmiştir.

- CAN (Controller Area Network): Araç içi elektronik bileşenler arasında kullanılır. Hızlı ve kritik bilgi transferi gerektiren işlemlerde ilgili bileşenler arasında kullanılır. Örnek olarak mekanik güç iletim sistemleri ile ilgili bileşenler CAN hattı üzerinden haberleşir.
- LIN (Local Interconnect Network): Araç içi elektronik bileşenler arasında kullanılır. Orta/düşük hızlı, orta/düşük kritiklikteki bilgi transferi

gerektiren işlemlerde ilgili bileşenler arasında kullanılır. Örnek olarak cam açma kapama kontrolcüleri, GKÜ ile LIN hattı üzerinden haberleşir.

- FlexRay: FlexRay konsorsiyumu tarafından geliştirilen, ISO tarafından standardize edilmiş hızlı ve emniyetli bir haberleşme yapısıdır.
- Ethernet: Yüksek hız gerektiren sistemler arasında kullanılır. Otomotiv özelinde özelleşmiş standartlaştırma çalışmaları bulunmaktadır.
- MOST (Media Oriented Systems Transport): Yüksek hızda multimedya veri transferi için oluşturulmuş, otomotiv için optimize edilmiş bir haberleşme yapısıdır.

Siber saldırganlar bu ağ yapıları üzerinden çeşitli teknikler ile araçlara veya araçlar ile ilgili verilere erişip sisteme, kişilere veya alt yapılara zarar verebilmektedir. Araç elektroniğindeki iç ağlara fiziksel kurcalamalar ile erişilebileceği gibi ağ tabanlı saldırılar üzerinden de erişilerek bir siber saldırı yolu açılabilmektedir.

2.3. Dış Bağlantı ve Sensör Girişleri

Otonom araçlar, sürücü barındırmadığı için dış dünya ile tüm iletişimi de elektronik sistemler üzerinden gerçekleştirir. Bu kapsamda bağlantı yapılarını tanımlayan farklı kavramlar vardır [4].

2.3.1. V2X

V2X (Vehicle-to-everything) [5] yeni nesil araçlarda araç ile herhangi diğer bir sistemin haberleşmesini ifade eder. Bu çalışma kapsamında üzerine çalışılan sistemin de diğer araçlar, yol ve şehir altyapıları, uzaktan kontrol sistemleri, trafik işaretleri gibi yapılarla iletişimde olduğu varsayılmıştır.

V2X ifadesinin alt kırılımları aşağıdaki listede verilmiştir.

- Vehicle-to-Device (V2D): Araçlar ile cep telefonu vb. cihazların iletişimini ifade eder. Genellikle bluetooth, Wi-Fi gibi protokoller kullanılır.
- Vehicle-to-Grid (V2G): Araçlar ile akıllı şebekelerin iletişimini ifade eder. Yük dengeleme ve optimizasyon problemlerini çözmek için iletişim kurarlar [6].
  - Vehicle-to-Building (V2B): Vehicle-to-Home (V2H) olarak da anılır. Araçlar ile binalar arasındaki iletişimi ifade eder. Bu iletişim çoğunlukla şarj istasyonları üzerinden gerçekleştirilir.
  - Vehicle-to-Load (V2L): Araçlar ile ek yükler arasındaki iletişimi ifade eder. V2L teknolojisi ile araçların gerektiği yerde güç kaynağı olarak kullanılmasının önü açılmıştır [7].
- Vehicle-to-Network (V2N): Araçlar ile diğer sistemlerin haberleşme tabanlı iletişimini ifade eder.
  - Vehicle-to-Cloud (V2C): Hücresel veya Wi-Fi üzerinden bulut tabanlı servislerle olan iletişim. Güncelleme servisleri.
  - Vehicle-to-Infrastructure (V2I): Trafikteki altyapı sistemleri ile kurulan iletişim.
  - Vehicle-to-Pedestrian (V2P): Trafikte bulunan, tekerlekli sandalye veya bisiklet gibi sistemlerle olan iletişim.
  - Vehicle-to-Vehicle (V2V): Araçlar arası iletişimi ifade eder.

V2X listesinde görüldüğü gibi otonom araçlar akla gelebilecek neredeyse bütün sistemler ile iletişimde ve bir koordinasyon içerisinde çalışırlar. Bu kavram ve haberleşme yapılarının tahsis edilebilmesi için aşağıdaki bağlantı yetenekleri de otonom araçlarda olmalıdır [4].

- Hücresel: Anlık veri transferi. Yazılım güncellemesi. Bağlantılı araç teknolojileri
- Wi-Fi: Tanımlı protokoller kapsamında V2X haberleşmeleri. Park durumunda yazılım güncellemesi.
- Bluetooth: Cihaz bağlantıları. Multimedya destekleri.
- RF: Cihaz bağlantıları.
- Dedicated short-range communication (DSRC): V2X haberleşmeleri.

2.3.2. Sensör Girişleri

Otonom araçlarda sürücünün yerini doldurabilmek için birçok gelişmiş sensör kullanılmaktadır. Bunlardan öncelikli olanlar aşağıdaki listede verilmiştir [5].

- Kamera/Kızılötesi Kamera: Nesne/Engel, trafik işaretleri tespiti ve yorumlaması. Mesafe ölçümü. Yol çizgilerinin tespiti
- Kısa/Orta/Uzun Menzil Radar: Nesne/Engel tespiti
- LIDAR: Nesne/Engel tespiti
- GPS/GNSS: Küresel konumlama
- Ultrasonik Sensör: Nesne/Engel tespiti. Mesafe ölçümü

Araçlarda otonom özellikler haricinde diğer kontrol algoritmaları için de elbette yüzlerce sensör kullanılmaktadır. Bunlar daha çok sıcaklık, hız, eğim, basınç gibi genellikle tek boyutlu çıkışı olan sensörlerdir. Bu çalışma kapsamında sensör olarak ifade edilecek sistemler otonom sürüşü destekleyen, çevreyi algılamak için kullanılan sensörlerdir.

3. Siber Saldırı Kaynakları ve Bunların İncelemesi

Bu kısımda potansiyel saldırılar, saldırıların sebep olabileceği hasarlar ve tehdit senaryoları üzerine yapılan araştırmalar sonucunda atak yolları incelenmiştir.

Sonraki çalışmalarda bu bilgiler üzerinden atakların ve atak yollarının uygulanabilir olup olmadığı değerlendirmesi yapılıp, gerekli görülen güvenlik açıkları üzerine güvenlik konseptleri sunmak otonom araçların güvenliğini tahsis etmek için önem taşımaktadır. Bu aşamaları tamamladıktan sonra otonom araçlarda siber güvenliğin tahsis edilmesi konusunda büyük bir adım atılmış olur.

İncelemeler kapsamında her bir alt başlık için 2 adet hasar senaryosu üzerinden, 4 adet tehdit senaryosu ve ilgili tehdit senaryolarını gerçekleştirmek için 8 adet atak yolu incelenmiştir.

Bu çalışmada temel siber saldırı yolları olarak şu kaynakların varlığı üzerinde şekillendirilmiştir; araç ağ yapısı

olarak CAN ve LIN, dış bağlantı türleri olarak hücresel ve Bluetooth haberleşmeleri, sensör olarak da kamera ve radar cihazları.

3.1. Araç Elektronik Mimari Ağ Yapısı Üzerinden Gerçekleştirilebilecek Saldırılar

Elektronik mimari üzerine gerçekleşebilecek saldırıların ilk etapta fiziksel kurcalamalar olacağı düşünülebilir ancak diğer saldırı yöntemlerini de göz önünde bulundurarak değerlendirmek, olası gizli risklerin eksiksiz incelenmesini sağlayacaktır.

Araç elektronik mimari ağ yapısı kapsamında CAN ve LIN değerlendirilecektir. CAN protokolü üzerinden hızlı ve güvenli gitmesi gereken veriler akar. Bununla beraber daha uzun hatlar üzerinden iletilebilir. LIN protokolü üzerinden nispeten daha yavaş ve emniyet toleransı olan veriler akar. Çok basit bir genelleme ile CAN hattı güç yönetimi, emniyet, gösterge gibi ECU'ların kendi aralarında kullandığı protokoldür. LIN hattı daha çok ECU'lar üzerinden yönetilen çeşitli eyleyici ve sensörleri kontrol etmek için kullanılır. Basit bir örnek vermek gerekirse araç cam kontrolcüleri LIN üzerinden GKÜ ile haberleşir.

Verilen bilgiler ışığında CAN hattına erişim sonucunda araca çeşitli müdahalelerde bulunulabilir. LIN hattı üzerinden de araca erişmek ve müdahale etmek mümkündür. Sistem tasarımına göre değişmekle birlikte LIN hattı üzerinde nispeten daha düşük kritiklikte veriler bulunur.

Tablo 1: Elektronik mimari üzerinden ağ tehdit senaryoları

Hasar Senaryosu	Tehdit Senaryosu
HS1-Araç 60 km/s hızda giderken beklenmedik hızlanma sonucunda önde giden araca çarpabilir.	TS1-Boylamsal hareket güç iletim hattındaki CAN mesaj paketlerini manipüle ederek, motor sürücülere tam güç uygulanır ve bu durum beklenmedik hızlanmaya sebep olur.
HS1	TS2-VCU yazılım güncellemesi sırasında kötü amaçlı bir yazılım yüklenir. VCU araç seyir halinde iken CAN üzerinden beklenmedik hızlanma komutu iletmeye başlar.
HS2-Araç 120 km/s hızda giderken beklenmedik güç kesilmesi sonucunda arkadaki araç bu araca çarpabilir.	TS3-LIN üzerinden gelen beklenmedik bir mesaj üzerine GKÜ üzerinden boylamsal hareket güç iletim hattındaki CAN mesaj paketleri manipüle edilerek, motor sürücülere güç uygulama kesilir ve bu durum beklenmedik araç güç kesilmesine ve aracın durmasına sebep olur.
HS2	TS4-LIN hattındaki bir sistem CAN hattındaki mesajlara müdahale ederek güç kesilmesine ve aracın durmasına sebep olur.

Tablo 2: Elektronik mimari üzerinden ağ atak yolları

Tehdit Senaryosu	Atak Yolu
HS1-TS1	AY1-Araç park halinde beklerken CAN hattına zararlı mesajlar basabilecek bir elektronik kontrolcü takılır. Bu kontrolcü rastgele bir zamanda beklenmedik hızlanmaya neden olacak mesaj paketleri gönderir.
HS1-TS1	AY2-Araç giderken bağlantı sistemlerinin hücresel ağı üzerinden aldığı zararlı bir mesaj paketi üzerine güç iletim bileşenlerinden araca azami tork talebi gönderir.
HS1-TS2	AY3-VCU yazılımı güncel versiyonu araca yüklenirken hücresel ağ üzerinde araya girme metodu ile farklı ve zararlı bir yazılım yüklenir.
HS1-TS2	AY4-VCU yazılımı güncel versiyonu Wi-Fi ağı üzerinden araca yüklenirken aynı ağdaki başka bir bilgisayar üzerinden ağ paketleri değiştirilerek zararlı yazılım VCU'ya yüklenir.
HS2-TS3	AY5-Araç park halinde beklerken LIN hattına zararlı mesajlar basabilecek bir elektronik kontrolcü takılır. Bu kontrolcü rastgele bir zamanda beklenmedik hızlanmaya neden olacak mesaj paketlerini GKÜ üzerinden gönderir.
HS2-TS3	AY6-LIN üzerinden çalışan, kolay değiştirilebilir bir sensör, zararlı yazılım içeren bir sensör ile değiştirilerek araç harekete geçtiğinde kötü niyetli yazılım aktifleşir ve tehdit senaryosu gerçekleşir.
HS2-TS4	AY7-LIN hattı üzerinden çalışan bir sisteme güncelleme esnasında kötü niyetli bir yazılım yüklenir ve GKÜ üzerinden güç yönetim hattını bozacak mesajlar yayınlanır.
HS2-TS4	AY8-Araç park halindeyken rastgele aktifleşecek bir kısa devre etme cihazı LIN hattına takılır. Araç hareketi başladıktan belli bir süre sonra bu cihaz devreye girer genel sistemi hata moduna sokar. Hattaki kritik sinyallerden dolayı sistem kapanma moduna geçip aracı durdurur.

3.2. Dış Bağlantılar Üzerinden Gerçekleştirilebilecek Saldırılar

Dış bağlantılar siber saldırılara en açık noktaların başında gelmektedir. Eğer bir sistemde dış bağlantı özellikleri varsa bunlar araçların beklenen davranışlarını asla etkilememelidir. Bu yüzden çok net ve sağlam sınırlar çekilmelidir. İlgili standardda hücresel bağlantı üzerinden saldırı yapmak en yüksek uygulanabilirlik seviyesindedir. Bunu Wi-Fi, Bluetooth gibi bağlantılar takip eder.

Bu kapsamda ilgili hatlar üzerinden araç fonksiyonlarına müdahale etmek mümkündür. Bu fonksiyonlar çoğunlukla emniyet kritik fonksiyonlardır. Bu durumların mümkünse tamamı analizler sürecinde değerlendirilmelidir.

Tablo 3: Dış bağlantılar üzerinden tehdit senaryoları

Hasar Senaryosu	Tehdit Senaryosu
HS3-Araç şarj olurken bataryanın beklenmedik bir şekilde yüksek sıcaklığa ulaşması ile araç yanabilir.	TS5-Batarya ısıtma komutu sürekli gönderilir ve bu batarya sıcaklığının hızlıca artmasına sebep olur.
HS3	TS6-Sisteme batarya sıcaklığı çok düşük mesajı gönderilir. Bu yanlış bilgiden dolayı ısıtıcı kontrolcüsü sürekli bataryayı ısıtır.
HS4-Araç 120 km/s hızda giderken beklenmedik güç kesilmesi sonucunda arkadaki araç bu araca çarpabilir.	TS7-Kontrolcülerin CAN hattı sürekli meşgul tutulur ve sonunda araç güç uygulamayı keser ve durur.
HS4	TS8-CAN hattına sıfır güç komutu basılır ve böylece araç güç uygulamayı keser ve durur.

Tablo 4: Dış bağlantılar üzerinden atak yolları

Tehdit Senaryosu	Atak Yolu
HS3-TS5	AY9-Hücresel ağ bağlantısı üzerinden araca erişilir. Araç CAN hattı üzerinden batarya ısıtma talebi sürekli gönderilir.
HS3-TS5	AY10-Hücresel ağ üzerinden çalışan bir uzaktan gözlemleme ve kontrol uygulaması üzerinden CAN hattına sürekli ısıtma talebi gönderilir.
HS3-TS6	AY11- Araca cep telefonu bluetooth üzerinden bağlanır. Telefonda bulunan bir zararlı yazılım vasıtasıyla bluetooth üzerinden aracın ilgili hatlarına sıcaklık düşük mesajı yayınlanır.
HS3-TS6	AY12- Araç içerisine bluetooth'a otomatik veya çok düşük bir efor ile bağlanabilecek bir cihaz yerleştirilir. Bu cihaz batarya sıcaklık mesajının sürekli düşük olduğunu yayınlar.
HS4-TS7	AY13-Araçta hücresel ağ üzerinden bir güncelleme yapılırken bir ECU'nun yazılımı zararlı bir şekilde güncellenir. Bunun sonucunda araç giderken uzaktan müdahalelere karşı açık hale gelir ve bir uzak saldırı sonucunda güç kesilir ve araç durdurulur.
HS4-TS7	AY14-Araçta hücresel ağ üzerinden çevrim için çalışan bir uygulamadaki zararlı yazılım üzerinden araç ağı meşgul tutulur.
HS4-TS8-	AY15-Araca cep telefonu bluetooth üzerinden bağlanır. Sonrasında cep telefonunda var olan bir uygulama araç ağına müdahale edecek mesajlar göndermeye başlar. Bunun sonucunda CAN hattındaki mesajlar manipüle edilir ve araç durdurulur.
HS4-TS8	AY16-Araç içerisine bluetooth'a otomatik veya çok düşük bir efor ile bağlanabilecek bir cihaz yerleştirilir. Bu cihaz sürücüden habersiz araç ağına bağlanır. CAN hattını manipüle edecek sinyalleri basar.

3.3. Sensörler Üzerinden Gerçekleştirilebilecek Saldırılar

Tam otonom araçlarda sensörler araçların dış dünyaya bakan yönleridir. Bu kapsamda özel önlemler alınmadığı taktirde dış dünyadan gelebilecek aldatıcı etkiler aracı beklenmedik durumlara sürükleyebilir.

Tablo 5: Sensörler üzerinden tehdit senaryoları

Hasar Senaryosu	Tehdit Senaryosu
HS5-Araç şehir içerisinde düşük/orta hızla giderken beklenmedik şekilde yüksek hızlara çıkabilir. Bu durumda herhangi bir varlığa çarpabilir.	TS9-Aldatıcı bir görsel yapı ile araca yüksek hız limitleri tanımlanır. Araç bu hız limitlerine uyum sağlayacağı için şehir içerisinde emniyetsiz hızlara çıkar ve sonuçta bir kazaya yol açar.
HS5	TS10-Aldatıcı RF sinyaller ile araç sensörleri manipüle edilir. Önünde bir engel olmasına rağmen bunu algılayamaz ve sonuçta bir kazaya yol açar [8].
HS6-Araç yüksek hızla giderken ani frenleme yapıp arkadaki araçların bu araca çarpmasına sebep olabilir.	TS11-Aldatıcı bir görsel ile araç bir engel var gibi ani frenleme yapar ve arkadaki araçların vurmasına sebep olur [9].
HS6	TS12-Aldatıcı RF sinyaller ile araç sensörleri manipüle edilir. Önünde engel olmamasına rağmen araç bir engel var gibi aksiyon alır. Sonuçta bu araca arkadaki araç çarpar.

Tablo 6: Sensörler üzerinden ağ atak yolları

Tehdit Senaryosu	Atak Yolu
HS5-TS9	AY17-Saldırgan yol kenarına trafik işaretçilerinin kötü niyetli bir veya birkaç kopyasını yerleştirir. Bu işaretçi araç kamerası tarafından algılanır ve hız limitleri güncellenir. Bunu sonucunda araç daha hızlı ilerlemeye başlar.
HS5-TS9	AY18-Saldırgan yol kenarına yerleştireceği aldatıcı bir ekran ile sadece hedef araç yaklaştığında aktifleşen bir ekran tanımlar. Bu ekran araca yüksek hız limitleri gösterir ve aracın şehir içinde hızlı ilerlemesine sebep olur.

Tehdit Senaryosu	Atak Yolu
HS5-TS10	AY19-Saldırgan yol kenarındaki bir RF kaynağı ile araç radarlarını manipüle edecek aldatıcı sinyaller yayar. Bu sinyaller araca yolun sürekli açık olduğunu gösterir. Bu durumda araç önündeki herhangi bir engele çarparak zarar verir.
HS5-TS10	AY20-Saldırgan bir araca aldatıcı sinyaller yaymak üzere bir RF modül takar. Saldırılacak aracın ön çaprazında giderken aldatıcı sinyaller yayılır, aracın radarları manipüle edilir. Araç önünü boş sandığı için hızlanır ve önündeki araca çarpar.
HS6-TS11	AY21-Saldırgan yol kenarına yola hareketli gibi görünen bir görsel yerleştirir. Bunu gören araç kameraları ani fren yapma kararı verir ve ani frenleme etkisi ile arkadaki araç vurabilir.
HS6-TS11	AY22-Saldırgan yol kenarına yanıltıcı bir yol çalışması veya çok düşük hız görseli koyar. Bunu gören araç ani frenleme yapar ve arkadaki araç bu araca vurur.
HS6-TS12	AY23-Saldırgan yol kenarındaki bir RF kaynağı ile araç radarlarını manipüle edecek aldatıcı sinyaller yayar. Sinyaller çarpma mesafesinde bir araç var olduğunu gösterir. Bu durumda araç ani fren yapar ve arkasındaki araç bu araca vurur.
HS6-TS12	AY24-Saldırgan bir araca aldatıcı sinyaller yaymak üzere bir RF modül takar. Saldırılacak aracın önünde giderken aldatıcı sinyaller yayılır, aracın radarları manipüle edilir ve arkasından gelen araç ani frenleme yapar. Bu durumda arkasındaki araç tehdit altındaki araca çarpar.

4. Sonuçlar

Sonuç olarak, bu yayın, otonom araçları hedef alan potansiyel saldırı kaynaklarının incelenmesi üzerine literatür ve sektörel araştırmaların ışığında ortaya konmuştur. Bu kapsamda literatür araştırmaları ve sektörel araştırmaların çıktısı olan hasar senaryoları, tehdit senaryoları ve atak yolları belirlenmiştir. Çalışma içeriğinde, sistematik ve kapsamlı bir yaklaşımla saldırıların meydana gelebileceği çeşitli kaynaklar tespit edilmiştir. Otonom araç ekosistemindeki bilinen güvenlik tehditleri incelenerek, potansiyel riskler, güvenlik açıkları ve atak yolları hakkında siber güvenlik için önemli durumlar incelenmiştir.

Bu araştırmanın sonucunda ortaya çıkan atak yolları, otonom araçların korunmasında proaktif güvenlik önlemlerinin kritik önemini oluşabilecek hasar ve tehdit senaryoları üzerinden vurgulamaktadır.

Tam otonom araçların ürün yaşam döngüsü boyunca güvenli olarak kalması için siber güvenlik faaliyetlerinin de aktif bir şekilde yürütülmesi çok önemlidir. Bugün için tam olarak güvenli bir araç üretilse bile teknolojik gelişmeler sonucunda yeni ortaya çıkacak bir yöntemin araçlarını tehdit edecek olması potansiyel büyük bir risktir.

Çalışma kapsamında incelenen tehdit senaryoları ve atak yolları kapsamlı bir şekilde ele alınıp araç üreticileri ve araştırmacılar tarafından çözülmesi gereken problemleri ortaya koymuştur.

Gelecek çalışmalarda bu güvenlik zafiyetlerine ve atak yollarına karşı önlem alacak çeşitli konsept ve teknik çalışmaların yapılması, tam otonom araçların siber güvenliğini kapsamlı bir şekilde tahsis etmek için önemli iyileştirme çalışmaları olacaktır.

Kaynakça

[1] SAE, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE, 2021.

[2] C. W. Axelrod, «Cybersecurity Challenges of Systems-of-Systems for Fully-Autonomous Road Vehicles,» *13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)*, 2017.

[3] *ISO/SAE 21434:2021*, The British Standards Institution, Standards Policy and Strategy Committee, 2021.

[4] C. W. Axelrod, «Cybersecurity Challenges of Systems-of-Systems for Fully-Autonomous Road Vehicles,» *13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)*, 2017.

[5] B. Geenen, Autonomous Vehicle Technology Report, Wevolver, 2020.

[6] J. Donoghue ve A. J. Cruden, «Whole System Modelling of V2G Power Network Control, Communications and Management,» *EVS27 Symposium*, 2013.

[7] S. Kumar, B. Ramalingam ve K. B. Yadav, «A Novel Circuit Topology for Vehicle to Load (V2L) Application,» *Proceedings of the 9th International Conference on Electrical Energy Systems, ICEES*, 2023.

[8] M. A. Vu, W. C. Headley ve K. P. Heaslip, «A Comparative Overview of Automotive Radar Spoofing Countermeasures,» *IEEE International Conference on Cyber Security and Resilience (CSR)*, 22.

[9] M. Girdhar, J. Hong, Y. You ve T.-J. Song, «Anomaly Detection for Connected and Automated Vehicles: Accident Analysis,» *IEEE Transportation Electrification Conference & Expo*, 2023.