AUSUD
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
JITSA

Araştırma Makalesi

Akıllı ulaşım araçlarında siber güvenlik ve çok katmanlı güvenlik önlemi

İsa Avcı[1,*], Cevat Özarpa[2], Muammer Özdemir[1], Bahadır Furkan Kınacı[3], Seyit Ali Kara[2]
[1]Karabük Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Karabük, Türkiye
[2]Karabük Üniversitesi, Mühendislik Fakültesi, Makine Mühendisliği, Karabük, Türkiye
[3]Karabük Üniversitesi, Mühendislik Fakültesi, Raylı Sistemler Mühendisliği, Karabük, Türkiye
*Correspondence: isaavci@karabuk.edu.tr
DOİ: 10.51513/jitsa.1034370

Özet: Teknolojide yaşanan hızlı gelişmelerle günümüzde kullanımı hızlı artan akıllı ulaşım araçları, artan talep ve sağladıkları kolaylıklar sebebiyle kısa zamanda dünya çapında önemli bir yere sahip olacaktır. Akıllı ve otonom ulaşım araçları alanındaki teknolojik gelişmeler söz konusu olduğunda hızlı bir ivme kazanıldığı göz ardı edilemez. Gelişmiş makine öğrenimi ve yapay zekâ tekniklerinden yararlanan yarı otonom ve otonom arabaların ortaya çıkmasıyla birlikte potansiyel riskler ve siber güvenlik zorlukları artmaktadır. Dahası, akıllı ulaşım sistemlerinin ve otonom araçların konuşlandırılması için gerekli Araçtan Araca (V2V) ve Araçtan Altyapıya (V2I) ara yüzler, potansiyel saldırı yüzeyini ve saldırı vektörlerini büyük ölçüde genişlettikleri için güvenlik risklerini daha da artırmaktadır. Yapay zekâ ve yazılımla çalışan bu araçlar her ne kadar sürücü güvenliği ve konforunu artırsa da dışarıdan gelebilecek siber saldırılardan dolayı büyük ölçekte can ve mal kaybına da sebep olabilmektedir. Bu nedenle, akıllı ulaşım araçları ile ilgili tehditleri ve siber güvenlik risklerini analiz etmek ve bu son derece karmaşık, heterojen ve değişken ortamın özelliklerini dikkate alarak bu riskleri ele almak için güvenlik önlemleri ortaya koymak son derece önemli hale gelmektedir. Bu çalışmada akıllı ulaşım araçlarına yapılan siber güvenlik saldırıları, doğabilecek sonuçlar ve alınabilecek güvenlik önlemleri açıklanmaya ve analiz edilmeye çalışılacaktır. Ayrıca bu sistemlerde kullanılan çok katmanlı savunma sistemi incelenerek değerlendirilmiştir.

Anahtar Kelimeler: Akıllı ulaşım araçları, Siber saldırı, Siber güvenlik önlemleri, Çok katmanlı savunma teknolojisi

Cyber security and multi-layered security measures in smart transportation vehicles

Abstract: Smart transportation vehicles are increasing rapidly today with the rapid developments in technology. It will soon have an important place in the world due to the increasing demand and the convenience they provide. When it comes to technological developments in the field of smart and autonomous vehicles, it cannot be ignored that rapid acceleration has been gained. With the advent of semi-autonomous and autonomous cars that leverage advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity challenges are increasing. Moreover, the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces required for the deployment of intelligent transportation systems and autonomous vehicles further increase security risks as they greatly expand the potential attack surface and attack vectors. Although these vehicles, working with artificial intelligence and software, increase driver safety and comfort, they can also cause large-scale loss of life and property due to cyber attacks that may come from outside. Therefore, it becomes extremely important to analyze the threats and cybersecurity risks related to smart vehicles and to put forward security measures to address these risks by taking into account the characteristics of this highly complex, heterogeneous, and variable environment. In this study, cyber security attacks against smart vehicles and the consequences that may arise are examined. In addition, the security measures that can be taken are explained and analyzed. The Multi-Layer Defense System used in these systems was examined and evaluated in detail.

Keywords: Intelligent vehicles, Cyber-attack, Cybersecurity measures, Multi-Layer defense technology

* Corresponding author. İsa Avcı
E-mail address: isaavci@karabuk.edu.tr
ORCID: 0000-0001-7032-8018[1], 0000-0002-1195-2344[2], 0000-0002-3866-7041[3], 0000-0001-6872-2630[4], 0000-0003-1275-1242[5]
Received 08.12.2021; accepted 10.01.2022
Peer review under responsibility of Bandirma Onyedi Eylul University.

1. Giriş

İlk Akıllı Ulaşım Sistemleri (AUS) çalışmaları 1960'ların sonu 1970'lerin başında Japonya'da CACS (Comprehensive Automobile Traffic Control Systems-Kapsamlı Otomobil Trafik Kontrol Sistemleri), ABD'de ve Almanya'da ERGS (Electronic Route Guidance System - Elektronik Rota Kılavuzluk Sistemi) ile başlamıştır. 1980'lerin ortasından itibaren haberleşme teknolojilerinde yaşanan gelişmeler AUS uygulamalarına ivme kazandırmıştır. Devlet ve sanayi ortaklığı ile büyük projeler başlatılmış, bu projelerle 90'lı yıllarda elektronik ücret toplama sistemleri, akıllı kavşak kontrol sistemleri, yolcu ve sürücü bilgilendirme sistemleri ve trafik kontrol merkezleri gibi uygulamalarla genişleyen AUS, ayrı bir disiplin olarak kabul görmeye başlamıştır. İlk olarak AUS kongresi 1994 yılında Paris'te düzenlenmiş ve her yıl düzenli olarak farklı ülkelerde yapılmaya devam etmiştir. Bu yapılan kongreler ile birlikte AUS organizasyonlarını kurulmuştur. Ulusal ölçekte kurulan organizasyonların yanısıra ERTICO, Akllı Ulaşım Topluluğu (ITS) Amerika, ITS Asya Pasifik gibi bölgesel yapılanmalar da bulunmaktadır (AUS Eylem Planı, 2020).

Günümüzde akıllı ulaşım araçlarının sayısı hızla artmakta ve yaşamımızda önemli bir yer edinmeye başlamıştır. Akıllı ulaşım araçları konfor ve güvenlik alanında önemli ölçüde etkisini göstermektedir. Bu araçlar, Wi-Fi erişim noktaları ve Bluetooth cihazlarıyla güvenli ve keyifli bağlantılı sürüşü hâlihazırda bizlere sunuyor. Bu avantajları ile beraber kullanımı daha da artan akıllı ulaşım araçları kötü amaçlı saldırganlar tarafından birer hedef haline gelmektedir. Araçlarda artan özerklik ve bağlanabilirlik, işlevsellik ve rahatlık açısından birçok iyileştirmeyi beraberinde getirirken, beraberinde yeni bir siber tehdidi de getiriyor (Eiza ve Ni, 2017). Akıllı ulaşım araçlarını hedef alan saldırılar, aracın hareketsiz kalmasına, yol kazalarına, mali kayıplara, hassas ve / veya kişisel verilerin ifşasına yol açabilir ve hatta otoyoldaki kullanıcıların güvenliğini tehlikeye atabilir.

Akıllı araçların gelişimi ve üretimi ülkeler açısından stratejik bir konu haline gelmiştir. Özellikle son yıllarda ülkemizde üretilmesi planlanan akıllı araçların bir çok ülke tarafından gelişmeler takip edilmektedir. Bir ürün geliştirmek sadece onu üretmekle değil onun lojistiği ve ihracatı aynı derece öneme sahip olmaktadır. Akıllı araçlar açısından üretim sonrası onların sahip oldukları akıllı teknolejilerin güvenliğide dikkate alınmalıdır. Teknoloji üretmek aynı zamanda ona ait olan güvenlik unsurlarının korunmasını sağlamakla mümkündür. Güvenlik kavramı donanımsal ve yazılımsal olarak ele alınarak bir bütün olarak çözümler üretilmelidir. Özellikle bu çalışmada veri iletişimde kullanmak güvenlik katmanlar ele alınmıştır ve güvenli bir iletişimi yöntemleri önerilmiştir. Ayrıca bu çalışmada siber güvenlik açısından yaşanabilecek saldırılar açıklanarak bu saldırılara karşı alınabilecek savunma metatları verilmiştir.

Bu çalışmada, akıllı ulaşım araçlarından kısaca bahsedilmiş, ikinci bölümde akıllı ulaşım ve akıllı ulaşım araçlarının yapısı anlatılmış ve yapılan siber saldırılar türlerinden örnekler verilmiştir. Yine ikinci bölümde siber saldırılara karşı tasarlanan çok katmanlı güvenlik modeli tanıtılmış ve son bölümde akıllı ulaşım araçlarında siber saldırıların sonuçları ve önerilere yer verilmiştir.

2. Literature Review

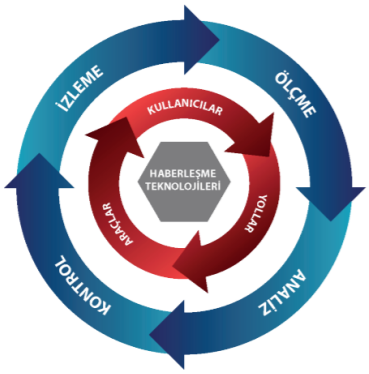
Son yıllarda akıllı ulaşım araçlarına yapılan siber saldırılar ve önlemleri konusunda hazırlanan çalışmalarda akıllı ulaşım araçlarının genel yapısı ele alınmış ve çeşitli saldırı önleme yöntemleri önerilmiştir. Eiza ve Ni 2017 yılında yayınlanan "Köpek Balıkları ile Sürüş" adlı makalelerinde karşılaşılan siber tehditler ve OTA (Over The Air), Bulut Tabanlı Çözüm, Tek Katmanlı Çözüm gibi saldırı önleme yöntemleri önermişlerdir (Eiza ve Ni, 2017).

Limbasiya ve Das, bir araç kullanıcısı ile bir RSU arasında yol kenarı ve diğer ilgili verileri yer degiştirmek için EC konseptini ve tek yönlü karma işlevini kullanan bir V2R veri iletim protokolü önermektedir (Limbasiya ve ark., 2019). Astarita ve ark. tarafından blockchain teknolojisinin hala erken bir aşamada olduğunu, ancak gıda takibi ve mevzuata uygunluğu, akıllı araçların güvenliği ve arz-talep eşleşmesi gibi birçok alanda yapılan çalışmalar son derece umut verici olduğu vurgulanmaktadır. Ayrıca, bu teknolojinin gıda israfını sınırlamak, egzoz gazı emisyonlarını azaltmak, doğru kentsel gelişmeyi desteklemek ve genel olarak yaşam kalitesini iyileştirmek için tetikleyici olabileceğini gösteren blok zinciri sürdürülebilirlik bağlantısı araştırılmıştır (Astarita ve ark., 2020). Gupta ve arkadaşları da

2020 yılında yayınladıkları çalışmada; doğrudan uçtan uca iletişim yerine ayrıt altyapıları kullanarak güvenli ve güvenilir bir V2V ve V2I iletişim yaklaşımı sunuyor (Gupta ve ark., 2020). Mollah ve arkadaşları tarafından hazırlanan başka bir makalede; heterojen bir Akıllı Ulaşım Sistemi ağı için blok zincir destekli bir güvenlik çerçevesi önerilmiştir (Mollah et al. 2021). Chen yapmış olduğu çalışmada iki kritik modüle odaklanmaktadır. Bunlardan birincisi sensör ve yerelleştirme, ikincisi ise engellere çarpma veya araçtan inme gibi uçtan uca güvenlik etkilerine neden olabilecek yeni ve pratik sensör/fiziksel dünya saldırılarını nasıl tespit edilebileceğine okaklanmıştır (Chen, 2021).

3. Akıllı Ulaşım

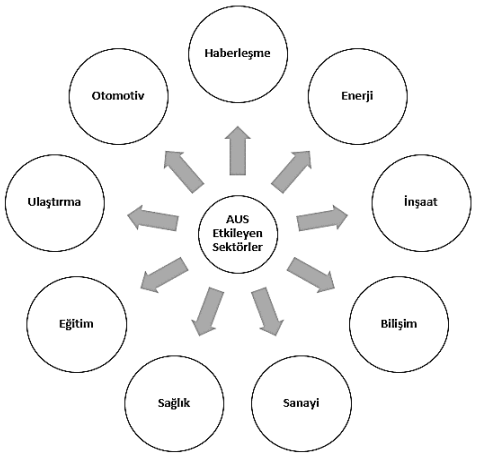
Akıllı ulaşım, Bilgi ve İletişim Teknolojileri destekli ve entegre ulaşım sistemleridir. Bir noktadan bir noktaya gitmeye çalışan insanların 360 derece tüm ihtiyaçlarını gideren daha kolay, daha verimli, daha konforlu ulaşımlarını sağlayan her türlü alt yapının bütününe akıllı ulaşım diyebiliriz. Seyahat sürelerinin azaltılması, trafik güvenliğinin arttırılması, mevcut yol kapasitelerinin optimum kullanımı, mobilitenin arttırılması, enerji verimliliği sağlanarak ülke ekonomisine katkısı ve çevreye verilen zararın azaltılması gibi amaçlar doğrultusunda geliştirilen, kullanıcı, araç, altyapı ve yolcu arasında çok yönlü veri alışverişi ile, izleme, ölçme, analiz ve kontrol içeren sistemler olarak tanımlanan Akıllı Ulaşım Araçları otomotiv sektöründen ulaştırma sektörüne, sağlıktan çevreye ve haberleşmeden bilişim, yazılım sektörüne dek pek çok sektörü ilgilendiren ve bu sektör ya da sektörlere katkı sağlayan yapısıyla disiplinler arası bir kavram olarak karşımıza çıkıyor (Tektaş ve Tektaş, 2019).



Şekil 1. *Akıllı ulaşım sistemi tanımı (AUS Eylem Planı, 2020).*

3.1. Akıllı Ulaşımdan Etkilenen Sektörler

Akıllı ulaşım sistemleri gelişirken etkilenen sektörlerde birlikte etkilenmektedir. Bu sektörlerin gelişimi ulaşıma bağlı olarak ekonomik büyümeye, insan kaynağına, üretime ve teknolojik olarak gelişmektedir.



Şekil 2. *Akıllı ulaşım sisteminden etkilenen sektörler (AUS Eylem Planı, 2020).*

3.2. Akıllı Ulaşım Araçlarını Tanımı ve Çeşitleri

İnternet ile bir şekilde iletişim kuran ve veri alışverişi yapan, yapay zeka ile görüntü tanımlama yapan, diğer araç veya nesnelerle iletişim kuran bağlantılı araçlara akıllı ulaşım aracı diyebiliriz.

Akıllı Ulaşım Araçlarını; Araçtan Araca Bağlantı (V2V), Araçtan Altyapıya (V2I), Araçtan Her Şeye (V2X), Araçtan Ağa (V2N), Araçtan Şebekeye (V2G) ve Platooning (Konvoylama) sınıflarına ayrılmaktadır.

3.2.1. Araçtan Araca Bağlantı (V2V)

Araçtan araca iletişim teknolojisi genellikle V2V olarak tanımlanır. Araç verilerinin bir araçtan diğerine değiş tokuşunu sağlayan akıllı bir teknolojidir. V2V teknolojisi için iletişim, özel kısa menzilli iletişimle (DSRC) dayanmaktadır. Bu tam olarak yeni bir teknoloji değil, onlarca yıl önce de bulunmaktadır. Ancak V2V sistemleri yaygın olarak kullanıldığında, araç güvenliği uygulamaları üzerinde en büyük etkiye sahip olacaktır. Örneğin çarpışmadan kaçınma uygulamalarını ilerletmek gibi çalışmalardır. V2V iletişimi, motorlu araçların Wi-Fi'ye benzer bir kablosuz iletişim protokolü kullanarak çevresindeki diğer V2V özellikli araçların hızı ve konumu hakkındaki bilgilere

erişmesini sağlar. Bu veriler daha sonra sürücüleri olası tehlikelere karşı uyarmak için kullanılır.

Kazaların ve trafik sıkışıklığının azaltılmasına yardımcı olmaktadır. V2V, tehlikeli trafik ve yol koşullarını, arazi sorunlarını ve hava muhalefetlerini 300 metrelik bir mesafede algılayabilir. V2V, sürüşü yoldaki herkes için daha öngörülebilir ve güvenli bir aktivite haline getirme imkanı sunmaktadır.

3.2.2. Araçtan Altyapıya Bağlantı (V2I)

V2I veya araç-altyapı teknolojisi, trafik sıkışıklığı, hava durumu uyarıları, köprü açıklık seviyeleri, trafik ışıklarının durumu gibi verileri yakalar ve ardından sürücülerin güvenli ve hızlı sürüş gerçekleştirmeleri için koşullar hakkında bilgilendirmeyi kablosuz olarak iletir. V2I tarafından desteklenen akıllı trafik sinyalleri, sürücülerin trafik koşullarını daha iyi anlamalarına yardımcı olarak, sürücüler ve toplu ulaşım aracı kullanan insanlar arasındaki iletişimi iyileştirebilecek doğru varış sürelerini de tahmin etmeye yardımcı olur.

3.2.3. Araçtan Her Şeye Bağlantı(V2X)

Araçtan her şeye olarak da bilinen V2X, hem V2V hem de V2I teknolojisini kapsar. V2X teknolojisi, diğer arabalar ve altyapı dahil olmak üzere trafik sistemiyle "iletişim kurma" gücü vererek yoldaki her otomobili daha akıllı ve daha güvenli hale getirir. V2X, sürücüleri tehlikeli hava koşulları, yakınlardaki kazalar ve trafik sıkışıklığı ve yakın mesafede meydana gelen diğer tehlikeli davranışlar hakkında bilgilendirebilir. V2X, kullanıcı olarak bizim için mevcut olan birçok bilgiyi doğrudan arabaya veya araca sağlar ve sürücünün yanıt vermesi için gereken tepki süresini azaltır.

V2X ayrıca geçiş ücretleri ve park etme ödemelerini otomatikleştirerek sürüş sürecini kolaylaştırır. V2X iletişimi, otonom sürüşün geleceği olarak görülmekte, ancak V2X pazarının hala uzun bir yolu bulunuyor. V2I ve V2V teknolojisine benzer şekilde, her kamyon, otobüs, araba, motosiklet ve hatta bisikletin bu bağlantılı araç teknolojisiyle beraber bir standart olarak gelmesi halinde V2X bu alanda en etkili teknoloji olacaktır.

3.2.4. Araçtan Ağa Bağlantı (V2N)

Araçtan Ağa (V2N) - LTE gibi kablosuz ağlar üzerinden araçtan araca iletişimi sağlamaktadır. V2N araçlar ile V2X yönetim sistemi ve ayrıca V2X AS (Uygulama Sunucusu) arasında hem yayın hem de tek noktaya yayın iletişiminin gerçekleşmesini sağlamaktadır. Bu, LTE ağ altyapısından ve E-UTRA'dan yararlanılarak elde edilir. Araçlar, yolun ilerisindeki kazalarla ilgili yayınlanmış uyarıları veya planlanan rotadaki tıkanıklık veya kuyruk uyarılarını alabilmektedir.

3.2.5. Araçtan Şebekeye Bağlantı(V2G)

V2G teknolojisi hala geliştirilmektedir, elektrikli otomobillerde ve kamyonlarda akülerin (pillerin), güç için gerçek zamanlı taleplere dayalı elektrik şebekelerinde, bir güç kaynağı olarak kullanılması fikrine odaklanmaktadır.

3.2.6. Platooning (Konvoylama)

Bir konvoy, birlikte güvenli bir şekilde seyahat eden bir grup araçtır. Her araç en az iki şerit içi araçla iletişim kurabilir ve takımdaki araçlardan biri lider olarak hareket eder ve takımın hızını ve yönünü kontrol eder. Konvoy fikri, katılan araçların uyumlu olduğu alt sistemler aracılığıyla bir kooperatif sistemi oluşturmaktır. Bağlı araçların takım oluşturması, trafik akış verimliliğini artırabilir ve diğerlerinin yanı sıra daha güvenli sürüşe, gelişmiş otoyol kullanımına ve verimli yakıt tüketimine katkıda bulunabilir (Zeadally, Guerrero, and Contreras 2020).

3.3. Akıllı Ulaşım Araçlarının Yapısı

Akıllı ulaşım araçları, iletişimin sürekli kontrol altında olması ve iletişimin bağlı olması gereken akıllı araçlardır. Bu sebeple, birden fazla yöntemle bağlantı noktası oluşturabilirler. Akıllı ulaşım araçları, içerik akışından konum tabanlı yardıma ve akıllı acil durum desteğinden elektronik kontrol birimlerinin (ECU'lar) uzaktan yazılım güncellemelerine kadar uzanan bağlantılı hizmetlerini kullanırlar. Her ne kadar sadece kullanıcısı ile etkileşim halinde olduğu düşünülse de trafikte olan diğer bütün akıllı ulaşım araçları ile de iletişim halindedirler.

Akıllı ulaşım araçlarına ait istatistiklerde yer alan bir bilgide, küçük işletmelerin %55'inin önümüzdeki yirmi yıl içinde tamamen otonom bir filoya sahip olacağına inanıyor (Alex, 2021). Bu açıdan gelecekte saldırıya açık daha fazla akıllı aracın olacağı anlamına da geliyor. Ticari açıdan bakıldığında, bir filoya yapılan saldırının maddi olarak kayıplarının fazla olması kaçınılmazdır.

Bir akıllı aracın kullandığı servisler ve genel IoT (Internet of Things) yapısı Şekil 1'de gösterilmiştir. Akıllı araçların sayıları arttıkça, ağda olan otomobiller, siber saldırganların genişleyen isabet listesine potansiyel hedef olarak eklenebilir (Okul, 2018).

Akıllı araçlar nesnelerin internet açısından güvenliği değerlendirildiğinde ele geçirelecek verinin önemi önemli hale gelmektedir. Güvenlil açısından sistemsel olarak bulutta bulundurulan veya yerli olmayan bağlantı yazılımları kullanmaktan kaçınılmalıdır. Verilerin kişisel ve özel veriler olması gizlilik ve ifşası açısından dikkat edilmesi bir konudur. Bu verilerin çalınması maddi ve itibar açısından çok boyutlu sorunlar ortaya çıkarcaktır.

Şekil 3. *Akıllı araç genel IoT yapısı*

3.4. Akıllı Araçlarda Siber Saldırı Türleri

Bir saldırgan, kablosuz arabirimlerdeki zayıflığından yararlanarak çarpışma veya kontrol kaybına neden olarak bir otomobilin ECU'larına saldırabilir. Gizlilik istilasına neden olan Telematik Kontrol Birimindeki (TCU) güvenlik açıklarını sömürerek bir arabanın özel görüşmelerini engelliyor olabilir. Çoğunlukla sürücüleri yönlendirmek ve yönetmek için kullanılan ve gizlilik ihlallerine neden olan GPS navigasyon sisteminden istifade ederek bir arabayı izleyebilir. Bir saldırgan, düşman başka bir ülke tarafından da büyük çaplı çarpışmalara ve kritik yaralanmalara neden olan tam uzaktan kumandayla zayıf otomobillerden ödün vermek suretiyle ulusal ulaşım yollarına ve banliyölerine karşı bir siber savaş başlatabilir (Eisenbarth ve ark., 2009).

Bir arabaya başarılı bir şekilde saldırmak için bir saldırganın dahili ağa fiziksel olarak, OBD-II bağlantı noktası, medya oynatıcısı veya USB bağlantı noktaları yoluyla veya kablosuz olarak Bluetooth veya hücresel arabirimler aracılığıyla erişmesi gerekir. Bir saldırganın aracın dahili ağına girmesi saldırı için gerekli imkânı verecektir. Araçları etkileyen saldırıların sınıflandırılması örnekler ile aşağıda açıklanmaktadır.

3.4.1. DoS Saldırısı

Aracın V2V (Vehicle To Vehicle) bağlantısı aracılığıyla diğer araçlara iletişim halinde bulunması saldırganın bu araca çok sayıda veri ve istek göndererek aracın cevap verebilirliğini engelleyerek, diğer araçlar ile olan iletişimin aksamasına sebep olacak kesintiyi sağlamasıdır (Abdollahi ve ark., 2018). Ayrıca aracın gerekli hız limitlerine uyamamasından kaynaklı can ve mal kayıplarına sebep olabilmektedir. Flooding saldırıları ise, bant genişliği, CPU, güç ve diğer benzer araçlar gibi ağ kaynaklarını tüketmek için trafik oluşturur. Flooding saldırıları iki gruba ayrılabilir; veri taşması ve yönlendirme kontrol paketlerinin taşması (Sakiz ve Sen, 2017).

3.4.2. Yalancı Veri Enjeksiyonu (FDI)

Bir FDI saldırısında, saldırgan, kapalı döngü kontrol sistemini tehlikeye atmak için normal sensör çıktılarını değiştirmek için kötü niyetli ölçümler enjekte eder. Otonom sürüş uygulamalarında, konum ölçümü, FDI enjekte edilmiş veriler tarafından başka bir şeride yönlendirilebilir (Wang ve ark., 2021). Bu saldırının bir örneği hız göstergesinde hatalı bir hız göstermek olabilir. Bir saldırgan ilk önce akıllı araca gönderilen gerçek hız güncelleme paketini kesip sonra sahte hız sahip olan değiştirilmiş bir paket gönderebilir. Buna ek olarak, bir saldırgan hava yastığı sisteminin gerçek durumunu, hava yastığı arızalı veya çıkarılmış olsa bile sorunsuz görünmesi için veriyi değiştirebilir.

3.4.3. Gizlilik İstilası

Saldırgan, TCU'daki hücresel ara yüze erişilerek araç içerisi dinlenebilir veya gönderilen ve alınan verileri kopyalayabilir. Saldırgan, seçilen kurban düğümlerinden gelen ve bu düğümlere giden trafiği ele geçirmek için

yönlendirme bilgilerini değiştirir. Bu, trafik analizi yapmak için kullanılabilir ve paketlerin seçici filtrelenmesiyle birleştirilebilir ve bu da, seçilen yönlendiricilerin "kaybolmasını" sağlamak için kullanılabilir (Jakobsson ve ark, 2003).

3.4.4. Bluetooth Üzerinden Zararlı Yazılım Enjeksiyonu

Saldırgan, aracın Bluetooth ağına zararlı truva atı göndererek aracın sistemini ele geçirebilir. Ele geçirilen araçta ABS sistemi gibi güvenlik açısından kritik ECU'lar ile iletişim kurabilir. Araştırmacılar, Bluetooth kontrol kodunun, eşleştirilmiş herhangi bir Bluetooth cihazından kodun yürütülmesine izin veren potansiyel bir bellek istismarı içerdiğini belirlediler (Parkinson ve ark., 2017).

3.4.5. CAN Bus Protokolüne Erişme ve Bu Protokolden Yararlanma

Bir otomobildeki CAN (Controller Area Network) veri yolu, aracın sensörleri ile çeşitli elektronik kontrol üniteleri (ECU'lar) arasındaki iletişimi sağlayan ağdır. Modern araçlar, motoru, hava yastıklarını, kilitlenme önleyici fren sistemini, arka lambaları, eğlence sistemini ve daha fazlasını kontrol eden 70 veya daha fazla ECU'ya) sahip olabilir (Payne, 2019). CAN'ın kendisi, çok uluslu elektronik ve mühendislik şirketi Bosch tarafından 1991'de CAN spesifikasyonu 2.0 olarak standartlaştırılan mesaj tabanlı bir protokoldür. Araçlar, dahili veri yolu üzerinde güvensiz bir şekilde iletişim kuran bir bilgisayar ağına benzer. Bu, bilgisayar korsanlarının CAN veri yolu üzerinde çok sayıda denetleyici alan ağı paketini (hem normal paketler hem de tanılama paketleri) dahili bileşenlere göndererek bir aracı ele geçirebileceği anlamına gelir. Kötü niyetli paketler olağan paketlerden önce ECU'lara ulaşırsa, bu bileşenler onları geçerli kabul eder. Saldırgan kabul edilen bu paketlerle araç ağına sızmış olur.

3.4.6. Tersine Mühendislik Saldırısı

Bir tersine Mühendislik saldırısında, saldırganlar yeniden yürütme ve aktarma saldırıları gibi gelecekteki saldırıları gerçekleştirmek için güvenlik açıklarını bulmak için araç sistemlerini bozabilir ve araç donanım yazılımını çıkarma ve değiştirme yoluyla tersine mühendislik yapabilir (El-Rewini ve ark., 2020).

3.4.7. Jamming (Karıştırma) Saldırısı

Bu saldırı türü, lazerle aynı frekans bandını kullanan araçtaki tarayıcı ünitesine doğrudan ışık yayar. Bir aracın LiDAR sensörünü sıkıştırmak için bir Raspberry Pi ve düşük güçlü bir lazere sahip düşük maliyetli, kullanıma hazır bir sistem kullanabilir saldırgan. En sık kullanılan sensörlerin (hız, sıcaklık, vites konum bilgileri, hız sabitleyici ayarı ve pil durumu) Elektronik Kontrol Ünitesi (ECU) ile iletişim kurmasını ve ayrıca EV (Electric Vehicle) araçlarında da bu bilgileri sunucuya göndermesini önlemek için karıştırma saldırısı başlatılabilir (Fraiji ve ark., 2018). Saldırı ile sürücü araç koşullarını tahmin edemeyecek ve araç sürücünün kontrolünden çıkacaktır.

3.4.8. Sybil Saldırısı

Sybil saldırısı, araç ağlarındaki en tehlikeli saldırılardan biri olarak sınıflandırılıyor. Saldırı, ağın normal işleyişini bozmak için aracın/kullanıcının kimliğinin tahrif edilmesini içerir (Nanda ve ark., 2019). Saldırı, ya yanlış bilgi sağlamak için birden fazla kimliği kullanır ve bilginin birden fazla cihazdan geliyormuş gibi görünmesini sağlayarak ya da başkasının kimliğini taklit ederek ve yanlış bilgi vererek iki şekilde gerçekleştirilebilir. Saldırı, ağın sürekli değişen topolojisinden ve hareketliliğinden yararlanır ve aracın konumu hakkında yanlış bilgi sağlayabilir; bunu kullanarak, bu konumlardaki olaylar hakkında da yanlış bilgi verebilir.

3.4.9. Tekrar Saldırısı

Saldırgan, önceki bir mesajı yeniden yayınlayabilir ve tekrar saldırısında bir olay ortaya çıkarabilir. Bu tepki, saldırganın bilgi sistemini savunmasız bir duruma (örneğin, bir sistem sıfırlaması) zorlamasına veya daha fazla saldırıya izin vermek için bilgi toplamasına (şifreli paketler gibi) izin verebilir. Tekrarlar en başta bütünlükten taviz verir, ancak kimlik doğrulama, erişim kontrolü ve inkar edilemezliği de tehlikeye atabilirler (Yağdereli, Gemci ve Aktaş, 2015). Seçilen tekrar saldırıları ayrıca kullanılabilirliği ve gizliliği de etkileyebilir.

3.4.10. Anahtarlıkla ve Anahtarsız Aracı Ele Geçirme

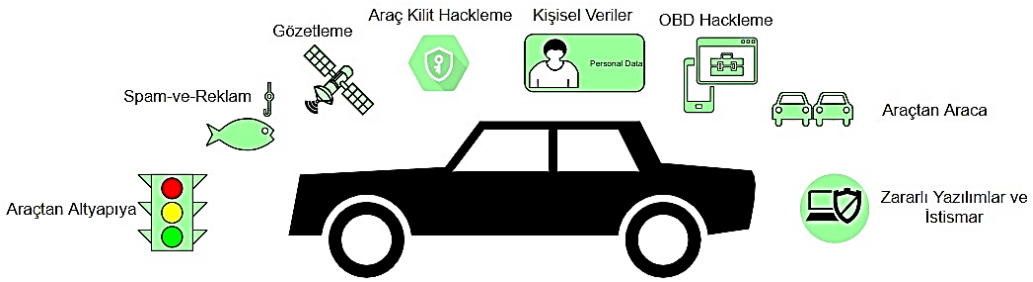
Araca girmek için, anahtarlıkla veya anahtarsız giriş olmak üzere iki yol vardır. Saldırgan, sürücü aracını kilitlemeye çalıştığında

anahtarlığın sinyallerini engelleyebilir. Bu cihazlar çalılıklara gizlendikten ve uzun süreler boyunca etkin kaldıktan sonra, anahtarlığın sinyalleri otoparkların veya caddelerin tüm alanlarında engellenecektir. Saldırgan, anahtarsız girişe sahip bir aracın sinyalini engelleyemez. Fakat bu değişmeyen sinyal, bir araca erişmek için yakalanabilir ve çoğaltılabilir. Araçların çalıştırılmasına ve çalınmasına izin vermek için alarm ve immobilizer devre dışı bırakılabilir (Sun ve ark., 2021).

3.4.11. Fiziksel Müdahale

Başka bir saldırı türü, üretim düzeyinde kötü niyetli içeriden veya gözetimsiz bir araçta dışarıdan biri tarafından (örneğin, belirli araç sensörlerini başka sensör ile değiştirerek veya bozarak) araç donanımı veya yazılımı ile oynamadır (Amoozadeh ve ark., 2015).

İletişim kanalı güvenli olsa ve CAV'da son teknoloji güvenlik mimarisi kullanılmış olsa bile, yerleşik donanım/yazılım kurcalanmış veya hatalıysa, sisteme giriş bilgileri doğru olmayacaktır.



Şekil 4. *Akıllı araç saldırı türleri (Processors tackle cybersecurity in connected cars - Electronic Products n.d.)*

3.5. Akıllı Araçlarda Siber Saldırılara Karşı Alınacak Önlemler

Araçların güvenli ve başarılı bir şekilde sürüşe devam edebilmesi için dinamik ve tehditlere duyarlı olması gerekir. Güvenliğe yönelik tehditler mümkün olduğu kadar savunulabilir olmalıdır; başka bir deyişle, tehditlere karşı erken önlem alan bir yaklaşım, karşılanması gereken temel bir gereklilik olmalıdır. Bununla birlikte, ağa yönelik tüm olası tehditleri tahmin etmek imkansız olduğundan, cevap veren yaklaşımlar etkili olmalı ve hızlı ve verimli bir şekilde devreye alınmalıdır. Kullanıcıların bir saldırı sonucunda olabildiğince az kesinti yaşaması önemlidir (Dibaei ve ark., 2019).

İşbirlikçi teknoloji V2X, konum, hız ve yön gibi bilgileri ortaya çıkaran işaretlerin yayınlanmasına olanak sağladığından, doğası gereği kısa vadeli konum takibine olanak tanır. Yolcuların uzun vadeli mahremiyetini korumak için, bir takma ad yönetim sistemi uygulamak, saldırıyı hafifletme tekniğidir. Bu nedenle araç, yeterli düzeyde güvenlik ve mahremiyet sağlayan gizlilik politikalarına göre takma adları değiştirecektir. Otonom sürüş görevi üzerinde doğrudan bir sonuç olmadığı için bu, otomasyon sistemini kendi başına etkilemez. Bu nedenle, bu tehdit ortalama bir saldırı olarak kabul edilir, ancak yine de kullanıcının dikkatini çekmek için ele alınmalıdır (Petit ve Shladover, 2015).

Araç içi ağ saldırılarını savunmak için bu saldırıların türlerine göre farklı stratejiler vardır; Uzaktan sensör saldırılarını savunmak için, kimlik doğrulama, tutarlılık kontrolü, sensör birleştirme ve Mekân-zamansal sorgulama-tepki dahil olmak üzere birkaç etkili çözüm vardır. Ultrasonik sensörlerin güvenliğini artırmak için, Xu, fiziksel düzeyde sinyalleri doğrulamak için kullanılan tek sensör tabanlı fiziksel kaydırma doğrulaması ve sistem düzeyinde sinyalleri doğrulamak için birden çok sensörün kullanıldığı çoklu sensör tutarlılık kontrolleri olmak üzere iki savunma stratejisi önerdi (Xu ve ark., 2018). GPS yanıltma saldırılarını savunmak için, önyargı tahmini menzil kontrolü, hızlar tutarlılık kontrolü, istatistiksel test, en az mutlak küçülme ve seçim operatörü ve küresel navigasyon uydu sistemi büyütme dahil olmak üzere çeşitli stratejiler vardır. Konum izleme saldırılarını savunmak için k-anonymity, mix-zone, yazılım tanımlı ağlar, lokasyon perturbation ve perturbation-hidden yöntemleri bulunuyor. En yakın güvenlik açıklarını savunmak için, şifreleme ve kriptografik sağlama toplamı dahil olmak üzere

çeşitli stratejiler vardır. Bluetooth için; kriptografik tekniklerle birkaç güvenli Bluetooth protokolü geliştirilmiştir. Ancak, çoğu ticari ürün, kullanılabilirlik üzerinde olumsuz etkileri olan bu güvenli protokolleri benimsememektedir. Bu güvenlik protokolleri, güven oluşturmak için kriptografik algoritmayı kullanır. Bluesniff gibi bazı açık kaynaklı araçları kullanarak saldırı savunulmaktadır. Ne yazık ki, kötü niyetli düğümlerin bellek istismarı ile yürütülmesini önlemek için önlem almamakta. Lastik Basıncı İzleme Sistemi için; TPMS'nin güvenilirliğini ve güvenliğini artırabilecek birkaç yöntem vardır. İlk olarak, TPMS üzerinde çalışan yazılım, temel güvenilir tasarım ilkelerine uymalıdır. İkinci olarak, TPMS paketleri basit bir kriptografik algoritma ile şifrelenmelidir. Ayrıca paketin güncelliğini sağlamak için pakete fazladan bir sıra numarası alanı eklenmelidir. Ayrıca, mesaj sahteciliğini önlemek için, Döngüsel Artıklık Kontrolü sağlama toplamından önce ekstra bir şifreleme sağlama toplamı eklenmelidir.

Anahtar ve Anahtarsız ele geçirmeler için; anahtarlık etkinleştirildiğinde, sürücünün aracın sinyali aldığını gösteren ışıkların yanıp söndüğünden emin olması gerekir. Ardından sürücü, bir kapı kolunu kaldırarak aracın kilitli olup olmadığını kontrol eder. Premium Audi RS4 araçlarında, saldırgan araçlara fiziksel erişim sağlarsa sisteme yeni bir anahtar eklenebilmektedir. Ağ Bölümlenmesi, CAN veri yolu için güvenlik sağlamanın kolay bir yoludur. Daha sonra kritik ve kritik olmayan ECU'lar ayrılır. Düşman kritik ECU'lara kolayca erişemez. Ağlar arasındaki bağlantı, bir ağ geçidi ECU'suna dayanır. Ancak, ağ geçidi ECU'su manipüle edilebilir. Ağ geçidi ECU'su ilgili kimlikleri alt ağa iletmek üzere programlanmışsa, alt ağa ait bir düğümün kimliğine sahip kötü niyetli bir CAN çerçevesi geçirilerek kandırılabilir. Dezavantaj ise, ağ bölümlenmesinde bakım zorluğu artmasıdır.

DoS saldırılarının tespit edilebilmesine rağmen düzeltilmesi zordur. Erken tespit, saldırıları önlemeye veya sürücüyü bazı etkili önlemler alması için uyarmaya yardımcı olacaktır. DoS saldırılarına karşı koymak için, kayan mod ve uyarlanabilir tahmin, bant genişliği ve entropi ve kayan pencerelerin benzerliği dahil olmak üzere bazı stratejiler vardır. Ohira ve arkadaşları, DoS saldırılarını önlemek için kullanılabilecek bir paket algılama algoritması önerdiler. Sürgülü pencerelerin benzerliğine dayalı olarak, her bir DoS saldırısını tespit etmek için geliştirilmiş bir DoS saldırı tespit stratejisi tasarlanmıştır (Ohira ve ark., 2020).

Khateeb, Bayes tahmin teknikleri aracılığıyla davranış analizi kavramlarını kullanarak siber tehdit önleme için proaktif anomali tespiti için bir yaklaşım sunmuş, bu çalışma esnekliğin önemli ölçüde arttığını ve yeni kötü niyetli amaçları tahmin etmek için denetimli makine öğreniminin gerektirdiği zaman maliyetini azalttığını göstermiştir (Al-Khateeb ve ark., 2018).

Altyapı saldırılarını savunmak için ise; siber güvenlik mimarisi, güvenli toplama, yazılım tanımlı güvenlik ve kimlik doğrulama dahil olmak üzere birkaç strateji vardır. Bulut tabanlı yöntem, CAV (Connected and Autonomous Vehicles)'lerin altyapısındaki siber saldırıları tespit etmek ve azaltmak için kullanılır. İslam, araçtan altyapıya uygulamalara yönelik siber saldırıları tespit edip önleyebilen yeni bir araçtan altyapıya siber güvenlik mimarisi tasarladı (Islam ve ark., 2018). CAV'lerin altyapısı için yeterli düzeyde koruma sağlamak için, güvenlik mekanizmalarını donanım katmanından bir yazılım katmanına soyutlayarak yazılım tanımlı güvenlik kullanılabilir.

Kritik birimler de dahil olmak üzere ağın geri kalanına erişmek için bir bileşendeki güvenlik açıklarından yararlanan tehdit aktörlerinden kaçınmak için ağ bölümlendirilmesi uygulanabilir. CAN veri yolu aracılığıyla bağlanan herhangi bir bileşen için kimlik doğrulama veya yetkilendirme uygulanmalıdır.

CAN veri yolundaki trafiğin şifrelenmesi büyük önem arz etmektedir. Güvenlik çalışmaları ayrıca siber saldırıları önlemek için anormallik algılama mekanizmalarının uygulanmasını önermektedir. Bir anormallik algılama mekanizması, araçtaki herhangi bir bileşen için "normal" davranış kalıplarından yararlanabilir. Bu taban çizgisinden herhangi bir sapma analiz edilmeli ve karşı önlemler potansiyel olarak etkinleştirilebilir.

Antivirüs yazılımı, kötü amaçlı yazılımları tespit etmek, engellemek ve sistemden kaldırmak için dosyaları tarayan bir güvenlik çözümüdür. Kötü amaçlı yazılımdan koruma, bilinen ve bilinmeyen kötü amaçlı yazılımları algılamak için buluşsal yöntemler, genel ve özel imzalar kullanır (Huq ve ark., 2020).

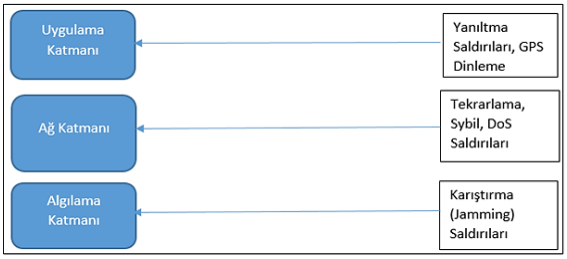
Kaspersky firmasının sadece bağlı akıllı araçlar için ürettiği güvenlik çözümleri; güvenli yazılımın yürütülmesini sağlar ve siber saldırı ile kötü amaçlı yazılımın yanı sıra rastgele yazılım hatalarına karşı koruma sağlamakta ayrıca araçlara ilişkin siber güvenlikle ilgili eksiklikleri ortaya çıkarmaya, analiz etmeye ve gidermeye yardımcı olmaktadır. Ancak antivirüs benzeri yazılımlar genel olarak güvenlik açısından hiçbir zaman yüzde yüz güvenlik sağlamazlar.

3.6. Çok Katmanlı Savunma Sistemi

Bağlantılı araç ve bilgisayar korsanlarının varlığı artık hayatın bir parçası bu nedenle güvenlik, akıllı araç tasarımının ayrılmaz bir parçası olmaktadır. Araç güvenliği büyük bir konu ve bunu yönetilebilir parçalara (zaman ve elektrik ekseninde) ayırabiliriz (Birnie ve Van Roermund, 2016). Çok katmanlı yapıya sahip olan savunma sistemi, farklı katmanlarda güvenlik sağlayarak asla aracın sürüş kontrolünün elde edilememesini ve sürekli kimliklendirme ve farklı katmansal korumalarla tam güvenliği hedefliyor. Günümüzde bu sistemin en önemli görevi, her koruma katmanının etkin olup olmadığını iki kez kontrol etmek olacaktır (Denman, 2012).

3.6.1. Çok Katmanlı Savunma Sisteminin Yapısı

Akıllı Ulaşım Araç ağları, temel olarak, veri toplamak için çeşitli sensörlerle birlikte araçlar arası iletişim sistemlerinden oluşur. Herhangi bir ağda olduğu gibi, araç ağları da katmanlı bir mimariye sahiptir; ancak geleneksel ağ katmanlı yapıdan farklıdır. Birlikte çalışabilirlik, ölçeklenebilirlik, güvenilirlik ve modülerlik gibi özellikleri ele almak için açık ve esnek katmanlı bir yapıya ihtiyaç vardır. Çok Katmanlı Savunma Sistemi, üç katmandan oluşmaktadır; Algılama Katmanı, Ağ Katmanı ve Uygulama Katmanı.



Şekil 5. *Çok katmanlı savunma sisteminde katmanlara göre saldırılar*

3.6.1.1. Algılama Katmanı

Algılama katmanı, üç katmanlı mimaride en alttaki katmandır. Bu sistemde, fiziksel ve veri bağlantı katmanları birlikte algılama katmanını oluşturur. Bu katman, mevcut sensörler aracılığıyla çevre hakkında bilgi toplamaktan sorumludur. Toplanan veriler sürüş düzenleri, çevre koşulları, araç durumları ve çok daha fazlasıyla ilgili olabilir. Bu katman, RFID etiketleri, kablosuz sensör ağları (WSN'ler) ve NFC gibi çok sayıda algılama teknolojisinden oluşur. Bu katmanda gerçekleştirilen ana görevler:

- Nesneler hakkında veri toplayarak çevredeki fiziksel nesneleri akıllı aracın bir parçası olarak benzersiz şekilde tanımlama.
- Algılanan verilerin dijital sinyallere dönüştürülmesi.
- Çevredeki nesnelerden toplanan verilerin ağ iletimi ve işlenmesi için üst katmanlara gönderilmesidir.

3.6.1.2. Ağ Katmanı

Alt katmandan alınan veriler işlenir ve uygulama katmanına iletilir. Bol miktarda veri, LAN, kablosuz/kablolu ağlar ve Wi-Fi, Bluetooth veya Zigbee gibi bir iletim ortamı gibi ağ teknolojileri kullanılarak işlenir. Bu katman, bağlantıyı sağlamaktan sorumlu olduğu için uygun bir şekilde iletişim katmanı olarak adlandırılır. Bu katman, araçtan diğer araçlara (V2V), altyapıya (V2I), yayaya (V2P) ve diğer sensörlere (V2S) kadar tüm iletişimi yönetir. Bu katman tarafından kullanılan iletişim ortamı, kesintisiz bağlantı sağlamak için Wi-Fi, Bluetooth, GSM, LTE vb. içerebilir. Bu katmanın görevleri:

- Algılama katmanı bilgileri ağ desteği tarafından işlenir.
- İşlenen sensör verileri alınır/üst katmana iletilir.
- Güvenli veri iletimi, fiziksel nesnelere IPV6 adreslemesi atar.

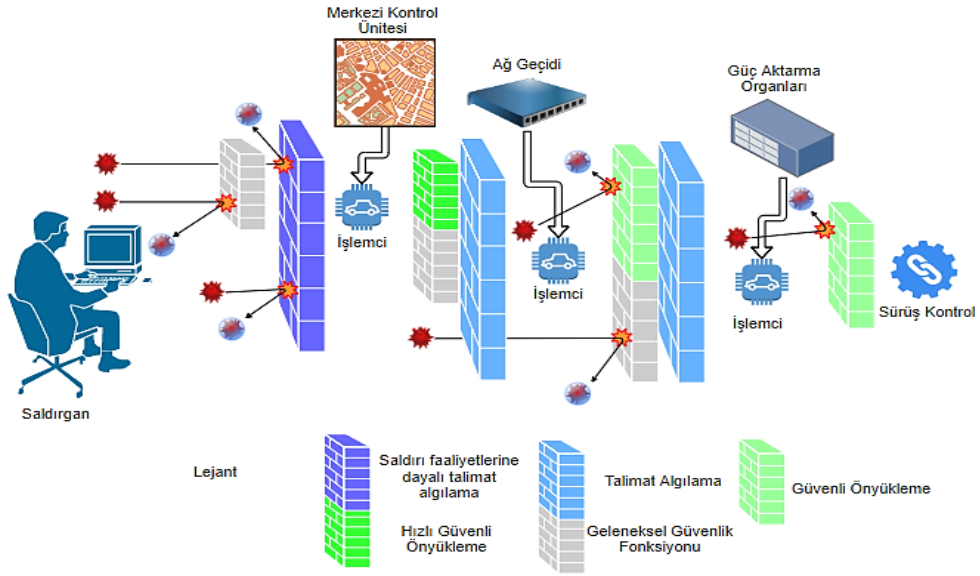
3.6.1.3 Uygulama Katmanı

Uygulama katmanı, veriler için hem depolama hem de işlemlere kaynak sağlayan güç merkezidir. Ana sorumluluklar veri yönetimi, depolama, işleme ve hatta karar vermeyi içerir. Katman ayrıca büyük veri analizi, WSN'ler, bulut bilişim vb. için destek sağlar. Bu katman ayrıca uygulama katmanı ve iş katmanına

bölünebilir. Bu katman, tüm akıllı ulaşım araç platformu için bir ön uç görevi görür. Bu katmanın ana işlevi, farklı uygulamaların yönetimini kolaylaştırmaktır. Taşıt uygulaması dağıtım platformları, ulaşım, sağlık ve bankacılık gibi çeşitli uygulamalar arasında ayrım yapmak için kullanılır. Ayrıca, iş alt katmanı, son verileri yönetir ve veri güvenliği ile ilgilenmektedir.

3.7. Çok Katmanlı Güvenlik Sisteminin İncelenmesi

Çok katmanlı savunma sistemi, otomotiv ana ünitesini ve bu ünitenin araç üzerinde tam kontrole sahip olup olmadığını izleyerek siber saldırıları tespit ediyor. Öncelikle, otomotiv ana ünitesi, aracın internete olan ana bağlantısıdır. Buna dikkat etmek, aracı siber saldırılardan korumanın anahtarıdır. Ayrıca, arka planda sürekli çalışan bilgisayar güvenlik programlarının aksine, bu teknoloji yalnızca kötü niyetli siber saldırı mevcut olduğunda aktif hale gelerek sistem işlem yükünü azaltır. Ayrıca, Fast Secure Boot teknolojisi sayesinde sistem yüzde 90 daha hızlı açılıyor ve otomobilin otomotiv ana ünitesine gömülü yazılımının bütünlüğünü doğrulamak için daha hızlı ve daha güvenli önyüklemelere izin veriyor.



Şekil 6. *Çok katmanlı savunma sistemi görseli*

Çok katmanlı savunma teknolojisi, halihazırda mevcut olan güvenlik işlevlerini güçlendirerek bağlantılı araçlar için güvenlik önlemlerini artırmayı amaçlıyor. Daha önce geliştirilen endüstriyel teknolojilerden uyarlanan sistemin dikkat çeken özellikleri ise aşağıdaki gibi sıralanabilir:

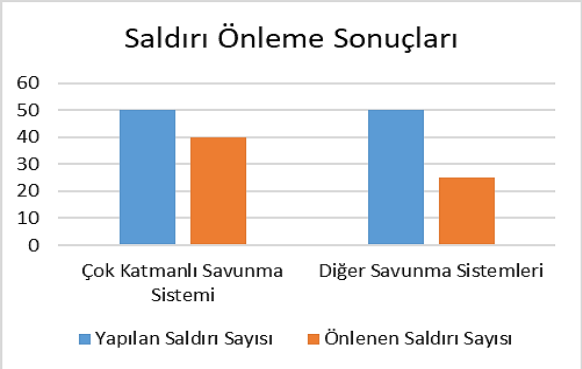
- Aracın kontrolünü ve konsolunu ele geçirme odaklı siber saldırıları tespit ediyor ve bunu sisteme mümkün olduğunca az yük bindirerek yapmayı amaçlar.
- Standart bir başlama (boot) sürecine sadece %10'dan az bir süre ekleyerek sistem çalışmaya başlıyor. Sistem açılışına etkisinin kısa olması teknolojiyi kullanılabilir yapan detaylardan belki de en önemlisi.
- Aracın internet ve diğer bağantılarını da kontrol ederek olası bir atağı başlamadan engellemeyi amaçlar.
- Çok katmanlı savunma teknolojisi, aracın internet ile ana bağlantısı olan otomotiv ana ünitesinin güvenlik işlevlerini güçlendirerek aracın güvenliğinin artırılmasını sağlar. Geliştirilen teknoloji, sınırlı makine kaynaklarına ihtiyaç duyan elektrik gücü, doğalgaz, su, kimyasallar ve petrol sistemleri gibi kritik altyapılar için geliştirilmiş çok katmanlı savunma teknolojilerinden ilham alınarak uyarlanmıştır.

Bu sistemde her katmanda gerçekleştirilen saldırı tespit edildiği anda katman olarak veya sistem kendini yeniden başlatma sürecine girer.

Çok katmanlı savunma teknolojisinde katmanın yeniden başlaması bütün sistemin başlatılması engellenerek daha hızlı bir başlatma gerçekleştirilir.

4. Bulgular ve Değerlendirme

Çok Katmanlı Savunma Teknolojisi, güvenli önyükleme özelliği, önyükleme işlemi sırasında yazılımın bütünlüğünün doğrulanmasını sağlamaktadır. Geleneksel bir güvenli önyükleme, işlem için nispeten zaman dezavantajına sahiptir, çünkü tüm yazılımların yüklenmesi ve doğrulanması gerekir. Çok katmanlı savunma sistemi, sorunu çözmek için yazılımın temel parçalarına odaklanarak doğrulama gerektiren veri miktarını azaltmaktadır. Çok katmanlı mimari sistemlerde verilerin iletimi ve korunması katmanlar arasındaki donanımsal ve yazılımsal uygulamalara bağlı olarak değişmektedir.



Şekil 7. *Çok katmanlı savunma sistemi ve diğer savunma sistemlerinin grafiği*

Bu yeni teknoloji, normal bir önyükleme dizisi için zamanın %10'undan daha azına ihtiyaç duymaktadır. Çok katmanlı Savunma Sistemini kullanan 50 adet akıllı ve bağlantılı araca gerçekleştirilen saldırıların %80'ni başarılı şekilde önlendiği gözlemlendi farklı siber saldırı önleme sistemine sahip araçlara yapılan saldırıların ancak %50'si önlenebilmiştir.

5. Sonuç

Akıllı ulaşım araçlarında son yıllarda gelişen teknolojilere bağlı olarak güvenlik sorunları ön plana çıktığı tespit edilmiştir. Bu araçlarda güvenlik sağlanmadığı durumlarda ortaya can ve mal güvenliği sorunları beraberinde gelmektedir. Akıllı ulaşım sistemlerinin ve otonom araçların konuşlandırılması için gerekli Araçtan Araca (V2V) ve Araçtan Altyapıya (V2I) ara yüzler, potansiyel saldırı yüzeyini ve saldırı vektörlerini büyük ölçüde genişlettikleri için güvenlik risklerini daha da artırmaktadır. Sonuç olarak, çok katmanlı savunma sistemi her ne kadar yeniden başlatma ile %10'luk bir zaman maliyetine sahip olsa da yapılan siber saldırıları önleme konusunda diğer savunma sistemleri veya siber saldırı önleme teknolojilerinden daha başarılı sonuçlar elde etmiştir. Bu kapsamda, gelişmekte olan akıllı ve bağlantılı ulaşım araçlarında bu yeni siber saldırı önleme teknolojisinin araştırılması ve geliştirilmesi için daha fazla bütçe ayrılması planlanmakta ve yapılan saldırılardan doğabilecek her türlü zararın da minimum seviyeye çekilmesi hedeflenmektedir. Artan akıllı ulaşım aracı pazarı ile birçok araç üretici firma bu konu üzerinde AR-GE çalışmaları yapmakta ve büyük ölçekli bütçeler ayırmaktadır. Son olarak bu araç üretici firmalarının güvenliğin sağlanması amacı ile AR-GE çalışmalarında ayıracakları yatırım bütçeleri yıl bazında arttırılması gerekmektedir. Bu artışlara ilave olarak bu alanda yetkin personellerin sayısının arttırılması ayrıca önem kazanmış durumdadır ve bu konuda yapılacak yatırımlar için devlet politikaları mutlaka desteklemelidir.

Araştırmacıların Katkı Oranı Beyanı

Yazarların çalışmadaki katkı oranları eşittir.

Destek ve Teşekkür Beyanı

Çalışma herhangi bir destek almamıştır. Teşekkür edilecek bir kurum veya kişi bulunmamaktadır.

Çıkar Çatışması Beyanı

Çalışma kapsamında herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.

Kaynakça

Abdollahi, B., Zoleikha, S. D., and Pierluigi, P., (2018). "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems." *IEEE Transactions on Intelligent Transportation Systems*, 19(12): 3893–3902.

Al-Khateeb, H. et al., (2018). "Proactive Threat Detection for Connected Cars Using

Recursive Bayesian Estimation." *IEEE Sensors Journal,* 18(12): 4822–31.

Alex, K., (2021). "Self Driving Car Statistics for 2021| Policy Advice." Erişim: 04 Nisan 2021,https://policyadvice.net/insurance/insights/self-driving-car-statistics/.

Amoozadeh, M. et al., (2015). "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving." *IEEE Communications Magazine*, 53(6): 126–32.

Astarita, V., Giofrè, V. P., Mirabelli, G., & Solina, V. (2020). A review of blockchain-based systems in transportation. *Information*, 11(1): 21.https://doi.org/10.3390/info11010021

AUS, Akıllı Ulaşım Sistemleri Strateji Belgesi 2020,https://www.utikad.org.tr/Images/Duyuru/05082020ulusalakilliulasimsistemleristratejibelgesive20202023eylemplani1610274.pdf, 08.01.2022.

Birnie, A., and Timo, V. R., (2016). "A Multi-Layer Vehicle Security Framework." *NXP White Paper*: 1–18.

Chen, A. Q. (2021). Towards Secure and Robust Autonomy Software in Autonomous Driving and Smart Transportation. *Association for Computing Machinery*, New York, NY, USA:1.https://doi= 10.1145/3457339.3457978,

Denman, S., (2012). "Why Multi-Layered Security Is Still the Best Defence." *Network Security 2012,*(3): 5–7.

Dibaei, M. et al., (2019). "An Overview of Attacks and Defences on Intelligent Connected Vehicles." *arXiv* (July).

Eisenbarth, T., Kasper, T., Moradi, A. and Paar, C., (2009). 5677 On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. ed. Shai Halevi. Berlin, Heidelberg: *Springer Berlin Heidelberg.*

Eiza, M. H., and Ni, Q., (2017). "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity." *IEEE Vehicular Technology Magazine*, 12(2): 45–51.

El-Rewini, Z. et al., (2020). "Cybersecurity Attacks in Vehicular Sensors." *IEEE Sensors Journal*, 20(22): 13752–67.

Fraiji, Y., Lamia Ben Azzouz, L. B., Trojet, W., and Azouz, S. L., (2018). "Cyber Security Issues of Internet of Electric Vehicles." *IEEE Wireless Communications and Networking Conference*, WCNC 2018-April: 1–6.

Gupta, M., Benson, J., Patwa, F., and Sandhu, R., (2020). "Secure V2V and V2I Communication in Intelligent Transportation Using Cloudlets." *IEEE Transactions on Services Computing*, 1374(c): 1–1.

Huq, N., Gibson, C., and Rainer Vosseler, R., (2020). "Driving Security Into Connected Cars: Threat Model and Recommendations." *Trend Micro.*

Limbasiya, T., & Das, D., Sahay, S. K. (2019). Secure communication protocol for smart transportation based on vehicular cloud. *In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*: 372-376.

Mhafuzul, I, Chowdhury, M., Hongda Li, H., and Hu, H., (2018). "Cybersecurity Attacks in Vehicle-to-Infrastructure Applications and Their Prevention." *Transportation Research Record*, 2672(19): 66–78.

Jakobsson, M., Wetzel, S., and Yener, B.,(2003). "Stealth Attacks on Ad-Hoc Wireless Networks." *IEEE Vehicular Technology Conference,* 58(3): 2103–11.

Mollah, M. B. et al., (2021). "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey." *IEEE Internet of Things Journal*, 8(6): 4157–85.

Nanda, A., Puthal, D., Joel J.P.C. Rodrigues, and Kozlov, S. A., (2019). "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions." *IEEE Wireless Communications*, 26(4): 60–65.

Ohira, S. et al., (2020). "Normal and Malicious Sliding Windows Similarity Analysis Method for Fast and Accurate IDS against DoS Attacks on In-Vehicle Networks." *IEEE Access*, 8: 42422–35.

Okul, Ş., (2018). "Akıllı Araçlarda Güvenlik Ataklarının Analizi." İstanbul Üniversitesi Fen Bilimleri Enstitüsü, *Yüksek Lisans Tezi*.

Parkinson, S., Ward, P. Wilson, K., and Miller, J., (2017). "Cyber Threats Facing Autonomous and Connected Vehicles: Future

Challenges." *IEEE Transactions on Intelligent Transportation Systems*, 18(11): 2898–2915.

Payne, B. R., (2019). "Car Hacking : Accessing and Exploiting the CAN Bus Protocol Car Hacking : Accessing and Exploiting the CAN Bus Protocol." *Journal of Cybersecurity Education, Research and Practice,* 2019(1): 5.

Petit, J., and Shladover, S. E., (2015). "Potential Cyberattacks on Automated Vehicles." *IEEE Transactions on Intelligent Transportation Systems*, 16(2): 546–56.

"Processors Tackle Cybersecurity in Connected Cars - Electronic Products." Erişim: 03 Nisan 2021, https://www.electronicproducts.com/processors-tackle-cybersecurity-in-connected-cars/#

Sakız, F., and Şen, S., (2017). "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV." *Ad Hoc Networks*, 61(March): 33–50.

Sun, X., Yu, F. R., and Peng Zhang, P., (2021). "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs).": 1–20.

Tektaş, M., and Tektaş, N., (2019). "Akıllı Ulaşım Sistemleri(AUS) Uygulamalarının Sektörlere Göre Dağılımı." *Akıllı Ulaşım Sistemleri ve Uygulamaları Degisi*, 2(1): 2.

Wang, Y. et al. (2021). "Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation." *IEEE Transactions on Intelligent Transportation Systems*, 1–13.

Xu, W. et al. (2018). "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles." *IEEE Internet of Things Journal*, 5(6): 5015–29.

Yağdereli, E., Gemci, C., and Aktaş, A. Z., (2015). "A Study on Cyber-Security of Autonomous and Unmanned Vehicles." *Journal of Defense Modeling and Simulation*,12(4): 369–81.

Zeadally, S., Guerrero, J. and Contreras, J., (2020). "A Tutorial Survey on Vehicle-to-Vehicle Communications."*Telecommunication Systems,* 73(3): 469–89.