AUSUD
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
JITSA

Araştırma Makalesi

Akıllı ulaşım sistemlerinde siber saldırılar ve önlemler

İsa Avcı*
*Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Karabük Üniversitesi, Karabük, Türkiye
*Correspondence:isaavci@karabuk.edu.tr
DOI: 10.51513/jitsa.1224909

Özet: Teknolojinin kullanımı ve gelişimi ile şehirlerin ana faaliyet alanları olan trafik ışıklarından su dağıtımına, trafik, çevre, sosyal eylemler, sağlık, eğitim, şehircilik, güvenlik ve kamu yönetimine kadar her şeyi kontrol etmek mümkündür. Teknolojinin uygulanması bilgi, veri, donanım ve uygulama güvenliği açısından güvenlik zafiyetleri beraberinde getirmektedir. Bu çalışma, AUS siber güvenlik tehditlerini ve alınması gereken güvenlik önlemlerini analiz etmeyi amaçlamaktadır. Bu amaçla, AUS iletişimi mimarisi, kullanımı alanları, faydaları ve siber güvenlik açısından saldırı yöntemleri analiz edilmiştir. AUS donanım ve uygulamalarda en çok yaşanan siber saldırılar dağıtık hizmet engelleme (Distrubuted Denial of Service Attack-DDoS), Ortadaki Adam Saldırısı (Man in the Middle-MitM) ve zararlı yazılım (Malicious Software-Malware) saldırıları yöntemleri yapılan araştırmalarda olarak tespit edilmiştir. Siber güvenlik saldırılarına karşı erişim kontrol yönetimi, güncel uygulama ve güvenlik yazılım kullanımı, kullanıcı eğitimi ve güvenlik donanımların kullanılması alınabilecek tedbirlerin başında gelmektedir. Son olarak, AUS sistemlerinin güvenliğini artırmak için daha önce yaşanan siber saldırılar ve gelecekte yaşanabilecek saldırılar analiz edilerek güvenli modeller incelenmiştir. Güvenli modeller çerçevesinde ülkemizde altyapı ve uygulama açısından en uygun olan modeller incelenerek uygulama ve sistemlere entegre edilmesi önemlidir. Teknolojik açıdan yapay zeka ile geliştirilmiş ve güvenlik algoritmaların uygulandığı saldırı tespit ve önlemek sistemleri kullanılarak sistemler ve uygulamaların güvenliği arttırılması gerektiği analiz edilmiştir.

Anahtar Kelimeler: Akıllı ulaşım sistemleri, akıllı şehirler, siber güvenlik

Cyber-attacks and measures in smart transportation systems

Abstract: With the use and development of technology, it is possible to control everything from traffic lights, which are the main activity areas of cities, to water distribution, traffic, environment, social actions, health, education, urbanism, security, and public administration. The application of technology brings security vulnerabilities in terms of information, data, hardware, and application security. This study aims to analyze ITS cyber security threats and security measures to be taken. For this purpose, ITS communication architecture, usage areas, benefits, and attack methods in cyber security are analyzed. The most common cyber-attacks in ITS hardware and applications have been identified as Distributed Denial of Service Attacks (DDoS), Man in the Middle (MitM), and Malicious Software (Malware) attacks methods. Access control management, use of up-to-date application and security software, user training, and use of security hardware are among the leading measures that can be taken against cyber security attacks. Finally, previous and future cyber-attacks were analyzed to increase ITS systems' security, and secure models were examined. Within the framework of safe models, it is important to examine the most suitable models in terms of infrastructure and application in our country and integrate them into applications and systems. It has been analyzed that the security of systems and applications should be increased by using intrusion detection and prevention systems, which have been developed with artificial intelligence in terms of technology and where security algorithms are applied.

Keywords: Intelligent transportation systems, smart cities, cybersecurity

* Corresponding author.
E-mail address:isaavci@karabuk.edu.tr
ORCID: 0000-0001-7032-8018
Received 27.12.2022; accepted 20.03.2023
Peer review under responsibility of Bandirma Onyedi Eylul University.

1. Giriş

Akıllı Ulaşım Sistemleri (AUS), dünya üzerinde çeşitli politika ve eylem planlarının odak noktası haline gelmiştir. AUS çalışmalarının temelleri incelendiğinde ilk olarak 1960'ların sonu 1970'lerin başında Japonya'da Kapsamlı Otomobil Trafik Kontrol Sistemleri, ABD ve Almanya'da Elektronik Rota Kılavuzluk Sistemi ile başlamıştır. Bu yıllardan sonra ilk olarak 1980'lerin ortasında AUS uygulamaları yaygınlaşmaya başlamıştır. Daha sonra 1990 yıllarında akıllı kavşak kontrol sistemleri, yolcu ve sürücü bilgilendirme sistemleri, elektronik ücret toplama sistemleri ve trafik kontrol merkezleri gibi uygulamalar hayata geçirilmiştir. Bu uygulamalar ile devlet ve özel sektör iş birliği başlayarak ortak projeler geliştirilmeye başlanmıştır (Lamssaggad vd., 2021). Uluslararası ölçekte çalışmalar önem kazanmaya başladıktan hemen sonra, 1994 yılında Paris'te ilk AUS kongresi düzenlenmiş ve daha sonra her yıl düzenli olarak farklı bir ülkede bu organizasyonlar yapılmaya devam edilmiştir. Bu tarz etkinlikler ve AUS alanında yapılan akademik çalışmalar neticesinde ortaya çıkan teknolojik gelişmeler, bunun yanı sıra elde edilen bilgi ve ihtiyaçlar doğrultusunda ülkeler kendi AUS organizasyonlarını kurmaya başlamışlardır. Ulusal ölçekte kurulan organizasyonların yanı sıra ERTICO, AUS Amerika, AUS Asya Pasifik gibi bölgesel yapılanmalar da kurulmaya başlanmıştır (Suryadithia vd., 2021).

2015 yılından sonra gelişen teknolojilere bağlı olarak birçok ülke AUS'un ulusal ve uluslararası pazarında pay sahibi olmak amacıyla yoğun olarak çalışmalara başlamıştır. Bu çalışmalar ile birlikte AUS alanında yeni proje çalışmalarının, altyapı ve teknoloji alanında finansal yatırımların artması, devlet desteklerinin her geçen gün güçlenmesi ve ülkelerin kendi oluşturdukları stratejilerine AUS'un doğrudan yansıması oluşan rekabetin en önemli göstergelerinden olmuştur (Özarpa vd., 2022). Özellikle bilgi ve iletişim teknolojilerinde yaşanan hızlı değişime paralel olarak AUS teknolojileri ve uygulamaları çeşitlenerek farklı alanlarda da yaygınlaşmaktadır. Bu alanlar arasında havayolu, demiryolu, karayolu ve deniz yolu taşımacılık alanları bulunmaktadır.

AUS uygulamalarında telekomünikasyon ve bilgi işlem teknolojileri ulaşım sektörüyle entegre edilmektedir. Bu entegrasyon haberleşme, haritalama, konum belirleme gibi sistemlerin entegre bir şekilde çalışmasını ve AUS'da kullanılan uygulamaların teknik altyapısının olanaklı hale gelmesine imkân tanımaktadır. AUS'da sistemler arasındaki haberleşme; araç-araç (V2V) haberleşmesi, araç-altyapı (V2I) haberleşmesi, altyapı-altyapı (I2I) haberleşmesi ve araç-nesne (V2X) haberleşmesi olarak sınıflandırılmaktadır (Telang vd., 2021).

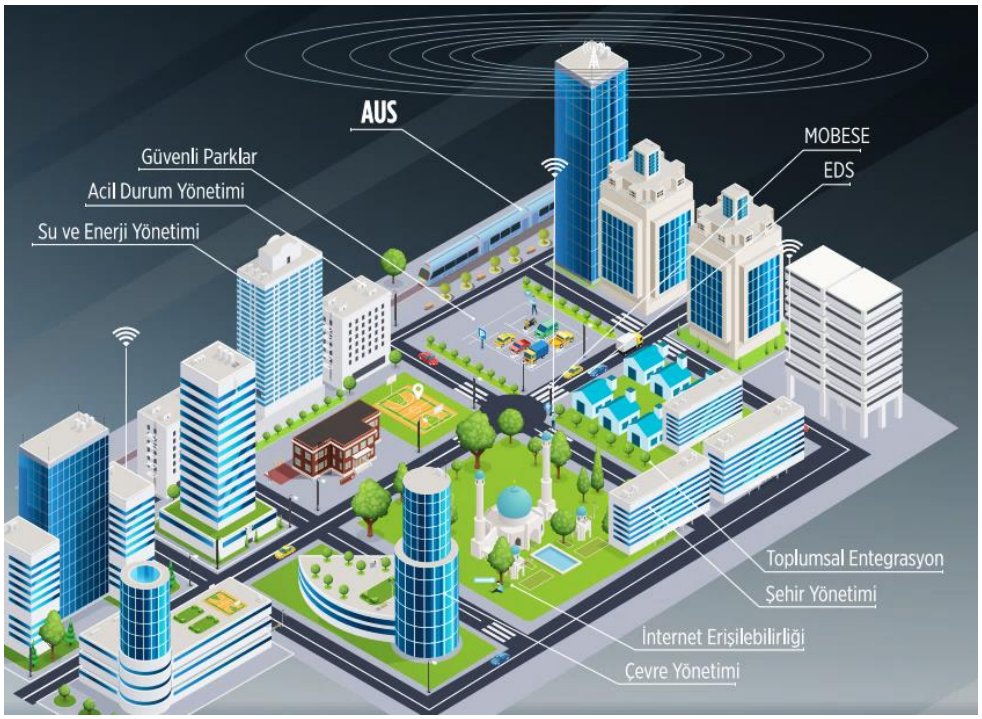
Uluslararası Telekomünikasyon Birliği (ITU)'nin "Yükselen Teknoloji Eğilimleri Raporu"na göre AUS'da siber güvenlik, yapay zeka, blok zincir, büyük veri, bulut bilişim, akıllı şehir, nesnelerin internet, finansal teknoloji, dijital sağlık ve dijital altyapı özellikle önemlidir. Bu teknolojiler arasındaki siber güvenlik yapay zekâ, blokzincir ve büyük veri gibi hızla gelişen yeni nesil teknolojiler ve bu teknolojilerin sektörel uygulamaları açısından da büyük önem taşımaktadır. Örneğin, yapay zekâ gibi yeni nesil teknolojilerin ve cihazlarının sistemleri ele geçirerek kötüye kullanılmasına karşı koruma sağlayacak çözümlerin geliştirilmesi büyük önem arz etmektedir (Zeba vd., 2022).

AUS açısından son on yıl incelendiğinde bilgisayarların, internetin, taşınabilir akıllı telefonların, tabletlerin ve kablosuz teknolojinin yaygınlaşması ile verilerin kullanılabilirliği, sistem ve cihaz bağlantısı, ve birlikte çalışabilirlik konularında muazzam bir büyümeye gerçekleşmiştir. Bu sistemler artık günlük hayatımızın ayrılmaz bir parçası olmuştur ve bu sistemlere yönelik siber saldırı potansiyeli oldukça artmıştır. Tüm sistemlerin merkezi bir noktadan control edilmesi ve izlenilmesi önemlidir. Gelişen Teknoloji ile birlikte kritik altyapıya sahip sistemleri güvenlik açısından koruma gereksinimi artmıştır. Özellikle AUS birçok teknolojinin bir arada çalışmasını sağladığından saldırılara karşı bu sistemlerin korunması gerekmektedir. Bu hayati sistemleri ve içerdikleri bilgileri korumak için artık siber güvenlik kavramı önem kazanmıştır. Bu çalışmada, AUS iletişimi ve mimarisi, faydaları, AUS' da yaşanan siber saldırılar ve alınması gereken önlemler detaylı olarak analiz edilmiştir. Ayrıca, AUS' da siber güvenlik açısından saldırı vektörleri ve siber saldırı yöntemleri anlatılmıştır.

2. Akıllı ulaşım sistemleri

AUS, bilgi ve iletişim teknolojilerinin ulaşım sistemlerine entegre edilmesidir. Tramvay, otobüs, metro, araba, deniz ve hava ulaşımı, bisiklet ve yayalar dahil olmak üzere sürdürülebilir, güvenli ve birbirine bağlı ulaşım sistemlerini kapsayan bir veya birden fazla biçimi vardır. Akıllı ulaşımın amacı, trafik yönetimi, yol güvenliği ve diğer birçok husus dahil olmak üzere ulaşım sistemine farklı ve daha akıllı

bir bakış açısı sağlamaktır. Taşımacılık hizmetleri, hem kendi sahasında, artan yük ve yolcu taşımacılığına, daha güvenli ve daha çevreci bir odaklanmaya odaklanır. Gelişen AUS uygulamaları özellikle bilgiye hızlı ve verimli bir şekilde ulaşılmasını sağlayarak, ekonomik, çevresel ve sosyal açıdan sürdürülebilir çözümler üretmektedir (Tufan, 2014). AUS genel olarak incelendiğinde araçlar, trafik akış kontrolü, karayolu raporlama sistemi, ödeme uygulamaları, yönetim uygulamaları, iletişim uygulamaları, şehir yönetimi, enerji yönetimi vb. sistemleri kapsamaktadır. Bu sistemler AUS uygulamalarını oluşturan en temel sistemlerdir ve bu sistemler Şekil 1'de detaylı olarak gösterilmektedir.



Şekil 1. Akıllı ulaşım sistemi (UAB, 2023)

2.1. AUS uygulamalarının faydaları

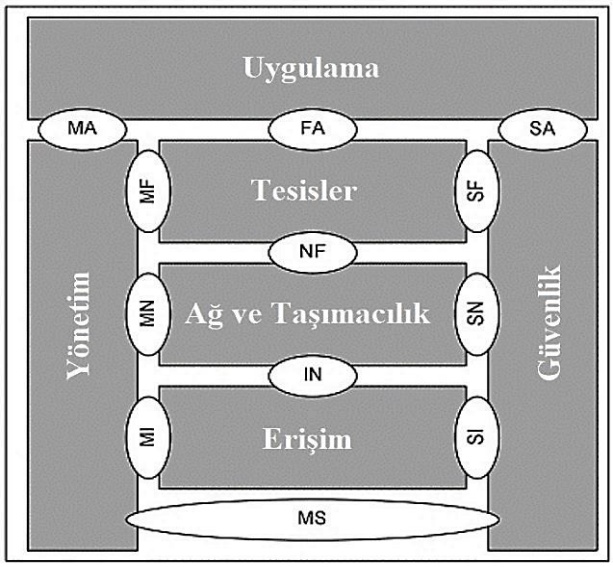
Gelişmiş ulaşım sistemlerinin sağladığı faydaların beraberinde getirdiği dezavantajları ortadan kaldırmak veya azaltmak için ulaşım sistemlerinin daha verimli, çevre dostu, güvenli, ekonomik bir şekilde çalışmasını sağlamak amacıyla AUS kavramı ortaya çıkmıştır (Katanalp, et al. al., 2018). Gelişen teknoloji ile birlikte yaygınlaşan AUS uygulamalarının faydalarının birçok faydası bulunmaktadır ve AUS'un en önemli faydaları aşağıda verilmiştir.

- Düşük CO2 emisyonu,
- Azaltılmış trafik kazası,
- Azaltılmış ulaşım süresi,
- Azaltılmış trafik sıkışıklığı,
- Alt yapı sorunlarının giderilmesi,
- Çevre dostu sistemlerin geliştirilmesi,
- Toplu taşımaya yönelimin artırılması,
- Yolların kapasiteye uygun kullanımı,
- İnsan-araç-altyapı-veri merkezi arası çok yönlü veri alışverişinin sağlanması,
- Hareketliliği artırmak için altyapının oluşturulması,
- Sürücü güvenliğini ve kaza yönetimini iyileştirmek,
- Transitte üstünlüğü olan araçlara öncelik verilmesi,
- Trafik yoğunluğunun belirlenmesi,

- Farklı sistemler arası veri entegrasyonu,
- İnsanların yaşam kalitesinin yükseltilmesi.

2.2. AUS istasyon iletişimi referans mimarisi

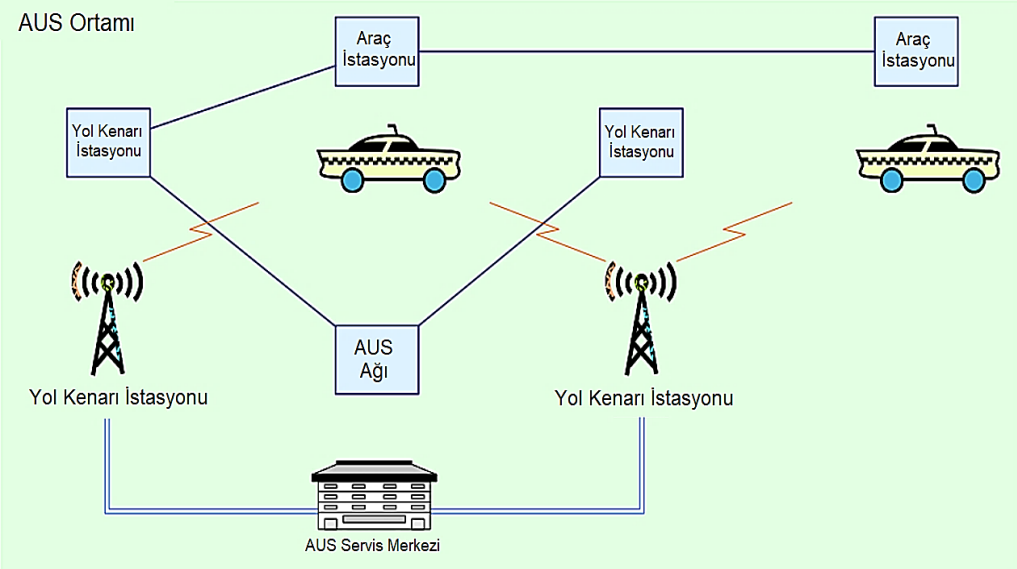
AUS referans mimarisi ETSI EN 302 663' de aşağıdaki şekilde tanımlanan dört işleme katmanına dayanan bir AUS istasyon mimarisini tanımlamaktadır (ETSI 302 663, 2022). AUS mimarisi OSI referans modeli temel alınarak 4 katmandan oluşmaktadır. Bunlar erişim katmanı, ağ ve taşıma katmanı, tesisler katmanı ve uygulama katmanlarıdır. Şekil 2'de AUS istasyon referans mimarisi gösterilmiştir.



Şekil 2. AUS İstasyon referans mimarisi (EN 302 665, 2022)

EN 302 665 standardına göre AUS istasyon iletişim referans mimarisinin erişim katmanında gruplandırılmış OSI fiziksel katmanını ve veri bağlantı katmanını tanımlamaktadır. Avrupa'da farklı frekans bantları için önceden ağ kurulumu olmaksızın mobil istasyonlar arasında veri alışverişini destekleyen ITS-G5 iletişim sisteminin bir parçasıdır. ETSI 302 663 göre ilgili frekans aralıkları aşağıda verilmiştir (ETSI 302 663, 2022):

- ITS-G5A: 5.875 GHz-5.905 GHz frekans aralığında güvenlikle ilgili uygulamalar için AUS'da ayrılmış frekans bantlarıdır.
- ITS-G5B: 5.855 GHz-5.875 GHz frekans aralığında AUS güvenlik dışı uygulamalarına ayrılmış Avrupa AUS frekans bantlarıdır.
- ITS-G5D: 5.905 GHz – 5.925 GHz frekans aralığında AUS uygulamaları için çalışma frekans aralıklarıdır. ITS-G5 teknolojisi, IEEE 802.11-2012 ve IEEE/ISO/IEC 8802-2-1998 standartlarını temel almaktadır.



Şekil 3. AUS iletişim ortamının görünümü (ETSI TR 102 638 ITS BSA, 2009).

AUS iletişimi mimarisi, ulaşım altyapısını ve ulaşım araçlarını (araba, tren, uçak, gemi) verimli ve güvenli bir şekilde kullanmak amacıyla mal ve insan taşımacılığını bilgi ve iletişim teknolojileri ile destekleyen sistemlerdir. Şekil 3'de AUS iletişim ortamının görünümü, araç ve yol kenarı istasyon haberleşme örneği gösterilmiştir. AUS uygulamaları açısından iletişim davranışları incelendiğinde kullanımı örnekleri, adresleme tipi, atlama metodu, frekans, yön ve oturum durumları Tablo 1' de detaylı olarak gösterilmiştir. Bu bilgiler, belirli AUS uygulamaları kategorisini tanımlamaktadır. Örnek olarak, işbirlikçi farkındalık, statik yerel tehlike uyarıları, etkileşimli yerel tehlike uyarıları, alan tehlike uyarıları, reklamı yapılan hizmetler, yerel yüksek hızlı tek noktaya yayın hizmetleri, yerel çok noktaya yayın hizmetleri, düşük hızlı tek noktaya yayın hizmetleri ve dağıtılmış (ağ bağlantılı) hizmetlerdir.

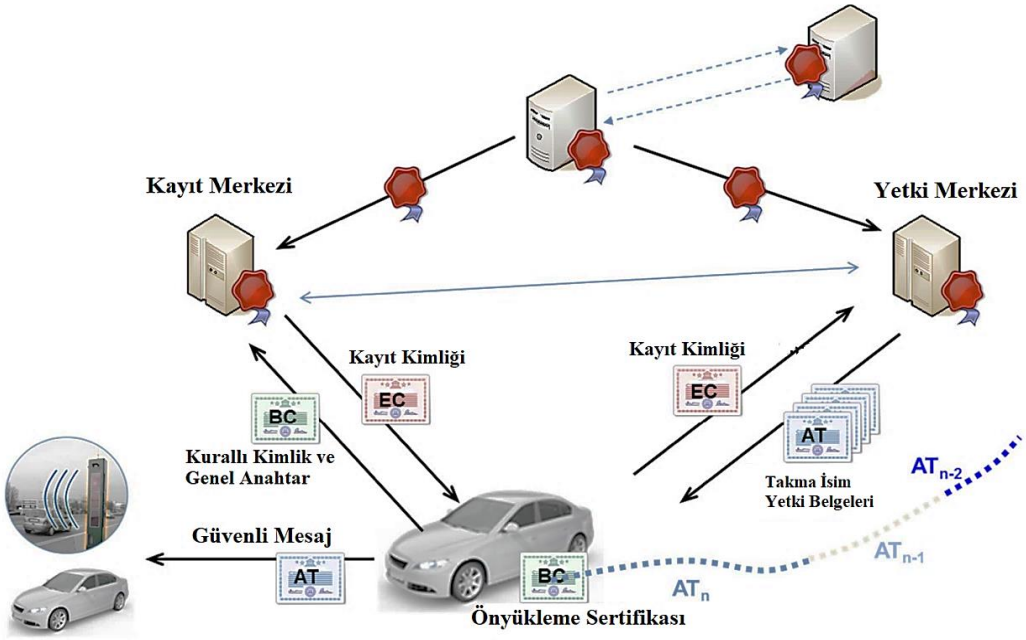
Tablo 1. AUS uygulamaları iletişim davranışı

Kullanım Örneği	Adresleme	Atlamalar	Frekans	Yön	Oturum
Acil araç uyarısı	Broadcast	Tek	Yüksek	V2V/V2I	Hayır
Yavaş araç göstergesi	Broadcast	Tek	Yüksek	V2V	Hayır
Çapraz trafik dönüşü çarpışma riski uyarısı	Broadcast	Tek	Yüksek	V2V	Hayır
Birleştirme Trafik Dönüşü Çarpışma Riski Uyarısı	Broadcast	Tek	Yüksek	V2V/I2V	Hayır
Kooperatif birleştirme yardımı	Broadcast	Tek	Yüksek	V2V/I2V	Hayır
Kavşak çarpışma uyarısı	Broadcast	Tek	Yüksek	V2V/I2V	Hayır
İşbirlikçi önden çarpışma uyarısı	Broadcast	Tek	Yüksek	V2V	Hayır
Şerit Değiştirme Manevrası	Broadcast	Tek	Yüksek	V2V	Hayır
Acil durum elektronik fren lambaları	Broadcast	Çoklu	Düşük	V2V	Hayır
Yanlış yönde sürüş uyarısı (altyapı tabanlı)	Broadcast	Tek	Düşük	I2V	Hayır
Duran araç- kaza	Broadcast	Çoklu	Düşük	V2V/V2I	Hayır
Duran araç- araç sorunu	Broadcast	Çoklu	Düşük	V2V/V2I	Hayır
Trafik durumu uyarısı	Broadcast	Çoklu	Düşük	V2V/I2V	Hayır
Sinyal ihlali uyarısı	Broadcast	Tek	Yüksek	I2V	Hayır
Yol çalışması uyarısı	Broadcast	Çoklu	Düşük	I2V	Hayır
Merkezi olmayan gezici araba verileri-Tehlikeli konum	Broadcast	Çoklu	Düşük	V2V/I2V	Hayır

Merkezi olmayan gezici araba verileri-Yağışlar	Broadcast	Çoklu	Düşük	V2V	Hayır
Merkezi olmayan gezici araba verileri-Yol tutuşu	Broadcast	Çoklu	Düşük	V2V	Hayır
Merkezi olmayan gezici araba verileri-Görünürlük	Broadcast	Çoklu	Düşük	V2V	Hayır
Merkezi olmayan gezici araba verileri-Rüzgâr	Broadcast	Çoklu	Düşük	V2V	Hayır
Hassas yol kullanıcısı uyarısı	Broadcast	Tek	Düşük	V2V/I2V	Hayır
Çarpışma öncesi algılama uyarı-Göstergesi	Broadcast	Tek	Yüksek	V2V	Hayır
Çarpışma öncesi algılama uyarı-Veri alışverişi	Unicast	Tek	Yüksek	V2V	Evet
Kooperatif parlama azaltma	Broadcast	Tek	Düşük	V2V/I2V	Hayır
Düzenleyici/bağlamsal hız sınırları bildirimi	Broadcast	Tek	Düşük	I2V	Hayır
Yamaç/Eğri Uyarı	Broadcast	Tek	Orta	I2V	Hayır
Trafik ışığı optimum hız tavsiyesi	Broadcast	Çoklu	Orta	I2V	Hayır
Trafik bilgisi ve önerilen güzergâh-Reklam	Broadcast	Tek	Düşük	I2V	Hayır
Trafik bilgisi ve önerilen güzergâh-Hizmet	Unicast/Multicast	Çoklu	Orta	I2V	Evet
Toplu taşıma bilgileri-Hizmet	Broadcast	Tek	Düşük	I2V	Hayır
Toplu taşıma bilgileri-Reklam	Multicast	Çoklu	Orta	I2V	Evet
Araç içi ekran	Broadcast	Tek	Orta	I2V	Hayır
İlgi çekici nokta bildirimi-Reklam	Broadcast	Tek	Düşük	I2V	Hayır
İlgi çekici nokta bildirimi-Hizmet	Multicast	Tek	Düşük	I2V	Evet
Otomatik erişim kontrolü ve park yönetimi-Reklam	Broadcast	Tek	Düşük	I2V	Hayır
Otomatik erişim kontrolü ve park yönetimi-Hizmet	Unicast	Tek	Düşük	I2V/V2I	Evet
ITS yerel elektronik ticaret	Unicast	Tek	Düşük	I2V/V2I	Evet
Medya indirme	Unicast	Tek	Düşük	I2V/V2I	Evet
Sigorta ve finansal hizmetler	Unicast	Tek	Düşük	I2V/V2I	Evet
Filo yönetimi	Unicast	Tek	Düşük	I2V/V2I	Evet
Yükleme bölgesi yönetimi	Unicast/Multicast	Tek	Düşük	I2V/V2I	Evet
Hırsızlıkla ilgili hizmetler/Hırsızlık sonrası araç kurtarma	Unicast	Çoklu	Düşük	I2V/V2I	Evet
Araç yazılımı/veri sağlama ve güncelleme	Unicast	Tek	Düşük	I2V/V2I	Evet
Araç ve RSU veri kalibrasyonu	Unicast	Tek	Düşük	I2V/V2I	Evet

2.3. AUS iletişim güvenliği mimarisi ve güvenlik yönetimi

AUS iletişim güvenliği ve güvenlik yönetimi açısından uluslararası standartlar referans alınmaktadır. En önemli güvenlik sorunlarından biri siber güvenlik açısından AUS uygulamaları ve sistemlerinin korunmasıdır. Bu konuda Avrupa İletişim Standart Enstitüsü olan ETSI (European Telecommunications Standards Institute) güvenli bir model önermektedir. Bu model ETSI 102 940 iletişim güvenlik mimarisi ve yönetimi adlı standart ile detayları belirtilmiştir. Bu standart iletilen bilgilerin korunması ve temel güvenlik parametrelerinin yönetimi için bir dizi güvenlik hizmetinin rollerini ve durumlarını tanımlamaktadır. Bunlar, tanımlayıcı ve sertifika yönetimini, Açık Anahtar Altyapısı (Public Key Infrastructure-PKI) süreçlerini, arayüzlerini ve güvenlik oluşturulmasına yönelik temel ilkeleri ve yönergeleri içermektedir (ETSI 102 940, 2022). Şekil 4'te ETSI 102 940 standardında oluşturulmuş olan AUS güvenli iletişim modeli gösterilmiştir.



Şekil 4. ETSI AUS güvenli iletişim model (ETSI 102 940, 2022).

3. AUS ve siber güvenlik

Son on yıl içinde bilgisayarların, internetin ve kablosuz teknolojinin yaygın bir şekilde kullanımı artmıştır. Bu sistemler günlük hayatımızın ayrılmaz bir parçası haline geldikçe, bu sistemlere yönelik saldırı potansiyeli de artmaktadır. Siber güvenlik, bu hayati sistemleri ve içerdikleri bilgileri korumayı sağlar. Siber terörizm riskinin artması, yalnızca kurumsal veya sivil verileri etkilemekle kalmıyor, aynı zamanda güvenlik açısından bir tehdit unsurudur. 2019'da Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), ulaşım sektörüyle ilgili olarak siber güvenlik için Avrupa Birliği (EU) yasal çerçevesi hakkında endişelerini dile getirmiştir. AUS uluslararası siber güvenlik konularında özel sektör firmaları ve kamu sektörü kuruluşlarının yanı sıra aşağıdaki kuruluşlar siber güvenlik araştırmalarında ortak çalışmalar yapılmaktadır (Markovčić Kostelac, 2019; ENISA, 2022).

- Ulusal Standartlar ve Teknoloji Enstitüsü,
- İç Güvenlik Departmanı,
- Savunma Bakanlığı,
- Enerji Bölümü,
- Federal Karayolu İdaresi,
- Federal Motorlu Taşıt Güvenliği İdaresi,
- Federal Transit İdaresi,
- Ulusal Karayolu Trafik Güvenliği İdaresi,
- Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA),
- ISO/IEC 27000 Bilgi Güvenliği Standartları Ailesi
- İnternet Güvenliği Merkezi (CIS) kontrolleri ve kıyaslamaları,
- Çok Devletli Bilgi Paylaşımı ve Analiz Merkezi.

3.1. AUS siber saldırı metotları

AUS'a yapılan siber saldırılar kurumlara, hükümetlere ve kritik altyapılara saldıranlar ile benzer özellikleri taşımaktadır. Bu durum AUS altyapısının güvenli olmasının kolay olduğu izlenimi verse de, gerçekte bu durum çok kolay olmamaktadır. AUS ekosistemi her gün gelişmekte ve buna paralel olarak siber saldırı vektörleride o derece farklılaşmaktadır. Böylece AUS altyapılarını siber saldırılara karşı koymak oldukça güç hale gelmektedir. AUS ekosistemlerine yapılan siber saldırılar genellikle finans

açısından değil saldırıların etkisinin yüksek olması ve herkes tarafından duyularak itibar kayıplarının yaşanması hedeflenmektedir. Bu tarz olaylar da birçok saldırganı harekete geçirmek için yeterli durum olmaktadır. AUS ekosistemlerine yapılan siber saldıranların ilk 5 amacına bakıldığında DDoS, MitM, fidye, veri hırsızlığı, bilgi savaşı ve terörizm olduğu görülmektedir. AUS ekosisteminin öne çıkan önemli bileşenleri araçlar, otoyol raporlama sistemleri, trafik akış kontrolü, ödeme sistemleri yönetim uygulamaları ve sistemleri, iletişim uygulamaları ve sistemleri kötü niyetli saldırganların hedef noktaları olarak tespit edilmiştir. AUS siber saldırı tehditleri araştırıldığında en çok yaşanan siber saldırı tehditleri aşağıdaki gibidir (Mikhalevich, 2022; Freng vd., 2022; Gaurav vd., 2022, Trenmicro, 2022; Avcı, 2021):

- Gizlice dinleme yapma,
- Hırsızlık,
- Sistem ayarlarını kurcalama/değiştirme,
- Yetkisiz kullanım/erişim,
- Dağıtılmış hizmet reddi saldırısı,
- Ortada adam saldırısı,
- İtibar kaybı,
- Donanım arızası,
- Operatör/kullanıcı hatası,
- Yazılım hataları,
- Kullanıcı desteğin sona ermesi/eskime,
- Doğa olayları,
- Çevresel ve fiziksel olaylar.

AUS siber güvenlik saldırıları açısından araştırıldığında sistemleri tehdit eden üç çeşit saldırının olduğu görülmektedir. Bu saldırılar ağ saldırıları, kablosuz saldırılar ve fiziksel saldırılardır. AUS' da yaşanmış ve yaşanabilecek siber saldırılar incelendiğinde en tehlikeli saldırıların ağ saldırıları olduğu görülmektedir (Trendmicro, 2022). AUS siber atak vektörleri Şekil 5'te verilmiştir.

Şekil 5. AUS siber atak vektörü (Trendmicro, 2022).

3.2. AUS Dünya genelinde yaşanan siber olaylar

23 Mayıs 2016'da Teksaslı bir saldırgan otoyol tabelasını hackleyerek şaka olarak "Drive Crazy Yall" yazmıştır. Bu saldırıyı yapan kişi tespit edilerek tutuklanmıştır. Bu saldırgan, tabela için giriş bilgilerini tahmin ettiğini ve yolda yol yapım çalışma olmasından dolayı araçları uyarmak için orijinal mesajı sildiğini açıklamıştır. Ayrıca, bu saldırada şaka mesajını mizahi amaçlarla yazdığını itiraf ettiği belirtilmektedir. Şekil 6'da saldırıya uğramış trafik mesaj panosu detaylı olarak gösterilmiştir.

Şekil 6. Saldırıya uğramış trafik mesaj panosu (Realclear, 2022).

6 Haziran 2016 tarihinde Dallas eyaletinde mesaj panoları haklenerek Donald Trump, Bernie Sanders ve Harambe hakkında panolara mesaj olarak "Gorilla deserved" yazısı yazılmıştır. Teksas Ulaştırma Bakanlığı, saldırıya uğramış bu mesaj panoların özel yüklenici firmaya ait olduğunu belirtmiştir. Şekil 7'de Washington'da saldırıya uğramış trafik mesaj panosu detaylı olarak gösterilmiştir.

Şekil 7. Saldırıya uğramış trafik mesaj panosu (Washington Post, 2022).

26 Kasım 2016 tarihinde, San Francisco Belediye Ulaştırma dairesinin (MUNI), bilgisayar korsanının mesajını sistemlerinde görüntüleyen bir kripto fidye yazılımı saldırısına uğramıştır. Mesaj, HDDCryptor gibi kötü amaçlı yazılım (Malware) türevlerine sahip bir saldırı olduğu tespit edilmiştir. Bu mesajla birlikte Muni metro istasyonlarındaki ücret ödeme makinelerinde "Hizmet Dışı" mesajı görülmüştür. Yolculardan ücret alamayan MUNI, yolcuların ücretsiz olarak seyehat etmelerine izin vermiştir. Şekil 8'de güvenliği ihlal edilmiş otomatik ücret ödeme sistemleri gösterilmiştir.

Şekil 8. Güvenliği ihlal edilmiş otomatik ücret ödeme sistemleri (Sfexaminer, 2022).

27 Ocak 2017 tarihinde, Washington Post, Washington'da polis gözetim kameralarından veri kaydeden depolama cihazlarının %70'ine, Başkan Donald Trump'ın göreve başlamasından sekiz gün önce bilgisayar korsanları tarafından fidye yazılımı saldırısı yapılmıştır. Bu fidye yazılımı saldırısı (ransomware) yerel polisi 12-15 Ocak tarihleri arasında kameraları kayıt yapamaz hale getirdiği ve saldırı 187 ağ video kaydedicisinden 123'ünü etkilemiştir (Sputniknews, 2022).

21 Nisan 2017 tarihinde RP Online tarafından, Rheinbahn'ın (Düsseldorf, Almanya'daki toplu taşıma şirketi) seyehat yönlendirme ve zamanlama sisteminde planlı bir çalışmada uygulama ve sistem güncellemesinde hata meydana geldiği belirtilmiştir. Bu hata sonucunda otobüs ve tren hizmetlerinde büyük gecikmelere ve iptallere yol açıldığı görülmüştür. Bu nedenle halkın yolculukta problem yaşamasına neden olduğu belirtilmiştir. Bu olay sonucunda 80'den fazla rotada toplam 832 araç etkilenmiştir. Böylece, araçlarda bazı seferler iptal edilmiş ve bazı araçlar geri dönmek zorunda kalmıştır. Bu bir AUS siber saldırısı olmasa da, bu tür olayların benzer şekilde olumsuz sonuçları olabileceğini açıkça göstermektedir (Report-d, 2022).

13 Mayıs 2017 tarihinde Radio Liberty tarafından, Rus Demiryolları bilgisayarlarına WannaCry fidye yazılımının bulaştığını belirtilmiştir. WannaCry, ilk saldırıdan hemen sonra bir gün içinde 150 ülkede 200.000'den fazla bilgisayara bulaştığı belirtilmektedir. Rus Demiryolları, saldırının local olduğunu ve demiryolu taşımacılığının etkilenmediğini bildirmiştir. The Telegraph, WannaCry'nin Alman tren istasyonlarına etkilediğini ve yolcu bilgi monitörlerinin fidye penceresini görüntülediğini bildirdi. Deutsche Bahn, "Bir Truva atı saldırısı nedeniyle çeşitli alanlarda sistem arızaları var" dedi. WannaCry, yama uygulanmamış sistemleri yaymak ve bulaştırmak için bir SMB güvenlik açığından (MS17-010) yararlanan ve şifre çözme için bitcoin olarak 300 $ fidye talep eden bir fidye (ransomware) yazılımıdır. Bir hafta içinde ödeme yapılmadığı takdirde sistemdeki tüm şifreli dosyalar silinir mesajı verilmiştir. Windows'un yamasız veya daha eski sürümlerini çalıştıran herhangi bir kuruluş, WannaCry'ın kurbanı olması kaçınılmazdır. Şekil 9'da Deutsche Bahn tren istasyonunda WannaCry saldırısı ekran görüntüsü verilmiştir.

Şekil 9. Deutsche Bahn tren istasyonunda WannaCry saldırısı (Telegraph, 2022).

4 Ağustos 2017 tarihinde Autoblog tarafından, bir grup üniversite araştırmacısı sokak tabelalarına çıkartma etiketler yapıştırarak sürücüsüz arabaları nasıl hackleyecekleri duyurulmuştur. Araştırmacılar, kendi kendini süren arabalarda görüş sistemleri tarafından kullanılan görüntü sınıflandırma algoritmalarını analiz edilerek makine öğrenimi modellerini yanlış yorumlamaları için farklı etiketler kullanarak sokak işaretlerini görsel olarak manipüle etmişlerdir. Bir örnek çalışmada, otonom bir arabanın görüş sistemini kandırarak bunun yerine bir "DUR" (STOP) işaretini saatte 45 mil işareti olarak okuması için çıkartmalar kullandılar. Bu tür basit saldırıların sonuçları gerçek dünyada büyük maddi hasarlara ve hayati tehlikelere neden olabilmesi mümkündür. Şekil 10'da trafik işeratlerini manupule edilmesi örnek olarak gösterilmiştir.

Şekil 10. Trafik işeratlerini manupule etmek (Autoblog, 2022).

4 Ağustos 2017 tarihinde, Kaliforniya'da birden fazla otoyol mesaj panosu siber saldırıya uğramıştır. Saldırganlar tarafından yayınlanan mesajlar şunları içerir: "Trump'ta uçuk var" ve "Dikkat Asyalı sürücüler." Bu olayda, elektronik mesaj panosu bir parola kullanılarak güvenlik hale getirildiği, ancak bilgisayar korsanları yine de parolayı ele geçirerek mesajlarını yayınlamayı başardıkları açıklanmıştır. Bunlar şaka olsa da sürücülerin dikkatini dağıtabilir ve yol güvenliğini tehlikeye atması mümkündür. Şekil 11'de bir saldırıya uğramış otoyol mesaj panosu gösterilmiştir.

Şekil 11. Saldırıya uğramış otoyol mesaj panosu (Fox40, 2022).

3.3. AUS siber saldırılara karşı alınması gereken önlemler

AUS donanım ve uygulamaların çevresinde fiziksel güvenlik önlemleri başta olmak üzere birçok önlemler aynı anda uygulanmalıdır. Bu tarz alanlara yetkisiz personellerin girişlerinin engellenmesi ve rol bazlı yetki erişim sisteminin uygulanması önemlidir. Kullanılmayan ve yazılımları güncel olmayan cihazlar mutlaka tesislerden uzaklaştırılmalıdır ve kullanılmamalıdır. Özellikle ağ segmantasyonu, güvenlik sıkılaştırması, IP bazlı gruplama yapılması, katmanlar arasında güvenlik duvarlarının kullanılması, IPS ve IDS sistemlerinin temin edilmesi, uygulama yama yönetimi ve log yönetimi vb. birçok konuda gerekli önlemlerin alınarak güvenlik bir koruma gerçekleştirilmesi mümkündür. Ayrıca, yapay zeka tabanlı saldırı önleme sistemleri kullanılması daha fazla koruma sağlayacaktır. Aşağıda

alınabilecek önlemler sıralanmıştır (Zhang vd., 2022; Kukkala vd., 2022; Srivastava vd., 2022; Falahati ve Shafiee, 2022). Tablo 2'de AUS'da siber güvenlik açısından alınacak önlemler ve uygulama alanları gösterilmiştir.

Tablo 2. AUS uygulamaları iletişim davranışı

Alınacak Önlemler	**AUS Uygulama Alanı**
Sanal özel ağların kullanımı	Ağ uygulamaları
Verilerin şifrelenmesi	Sunucu ve bilgisayar
Çok faktörlü kimlik doğrulama	Tüm uygulamalar
Ağ saldırı tespit sistemlerinin kullanılması	Ağ uygulamaları
Fiziksel korumanın devreye alınması	Tüm ağ ve donanımlar
Erişim kontrolü	Tüm uygulamalar ve sistemler
Alarmlar ve 7/24 izleme	Tüm uygulamalar ve sistemler
Bir bilgi güvenliği politikasının uygulanması	Tüm uygulamalar ve sistemler
Etkinlik günlüklerinin oluşturulması	Tüm uygulamalar ve sistemler
Yedekleme ve bakımı	Tüm uygulamalar, donanım ve sistemler
Düzenli denetim yapılması	Tüm uygulamalar ve sistemler
Kapatma prosedürleri	Tüm uygulamalar ve sistemler
KPI'ların izlenmesi	Tüm uygulamalar ve sistemler
Donanım yedekliliği	Tüm donanımlar
Bakım planlaması	Tüm uygulamalar ve sistemler
Müdahale ekipleri	Tüm uygulamalar ve sistemler
Kalite güvencesi	Tüm uygulamalar ve sistemler
Raporlama prosedürleri	Tüm raporlama sistemleri
Hata ayıklama prosedürleri	Tüm uygulamalar ve sistemler
Etkinlik günlüklerinin oluşturulması	Tüm uygulamalar ve sistemler
Operatör/kullanıcı eğitimi	Tüm kullanıcılar
Farkındalık eğitimleri	Tüm kullanıcılar
Standart ve prosedürlerin takibi	Tüm kullanıcılar
Yanıt prosedürleri	Tüm uygulamalar ve sistemler
Hata günlükleri	Tüm uygulamalar ve ağlar
Donanım/yazılım arızalarının teşhisi	Tüm uygulamalar ve sistemler
Olay raporlama sistemi	Tüm uygulamalar ve sistemler
Düzenli olarak altyapıların yenilenmesi	Altyapı sistemleri
Güvenlik açısından dayanıklılığın arttırılması	Tüm uygulamalar ve sistemler
Cihaz özelliklerinin uzaktan devre dışı bırakılması	Ağ uygulamaları ve sunucular
Acil durum bakım ekipleri	Tüm uygulamalar ve sistemler
Cihaz güvenlik sıkılaştırması	Ağ ve donanım
Erken uyarı sistemleri/tahmin	Tüm uygulamalar ve sistemler
Olağanüstü durum kurtarma süreçleri/merkezleri	Tüm uygulamalar ve sistemler
Altyapı tehdit değerlendirmeleri	Tüm uygulamalar ve sistemler
Risk yönetimi	Tüm uygulamalar ve sistemler
Yama yönetimi	Tüm uygulamalar ve sistemler
Log yönetimi	Ağ uygulamaları ve sunucular
Varlık yönetimi	Tüm uygulamalar ve sistemler
Uygulama lisans yönetimi	Tüm uygulamalar
Siber istihbarat servislerinin kullanılması	Tüm uygulamalar ve sistemler
Güvenlik duvarı kullanılması	Ağ ve uygulamalar

4. Sonuç ve tartışma

Modern ulaşım sistemleri sürekli gelişmekte ve akıllı sistemler olması nedeni ile birden çok faydalar sağlamaktadır. AUS teknolojisi, yeni yollar inşa etmek yerine, belediyelerin yeni yol altyapısı inşa etme maliyetinin çok altında bir oranda mevcut yolların kullanımını önemli ölçüde artırmasına olanak tanımaktadır. Şehirlerimizin altyapısında dijitalleşme ve birbirine bağlanabilirlik daha belirgin hale geldikçe, siber terörizmin yükselişi, farklı türden akıllı ulaşım sistemlerine yönelik tehditler oluşturmaktadır. AUS'un bağlantılı otomasyon sistemlerine sahip olması yenilik ve rahatlık için yeni fırsatlar sunarken, aynı zamanda saldırı yüzeyini genişletebilir ve kötü niyetli saldırganların yararlanabileceği yeni fırsatlar sağlayabilmektedir. Bu fırsatlar genellikle kullanıcıların, şirketlerin ve ülkelerin itibar ve finans kayıplarına neden olmaktadır. Mevcut geleneksel çok katmanlı AUS mimarisi artık siber güvenlik tehditlerine karşı koyamaz durumdadır. Siber terörizm tehdidi altında üç ana zorluk tespit edilmiştir: zayıf güvenlik farkındalığı, güvensiz veri alışverişi, AUS varlık yönetiminin yapılamaması ve rol bazlı yetkilendirmede yaşanan karmaşıklıklardır.

AUS'un ulusal ve uluslararası ihtiyaçlar açısından doğrudan atılan ilk adım 2014 yılında Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi (2014-2023) ve 2014-2016 Eylem Planı'dır. AUS alanında atılan bir diğer önemli çalışma ise 2020 yılında hazırlanan Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı'dır. Bu çalışmalar ile bir önceki çalışmalarda bulunan eksiklikler giderilerek daha kapsamlı bir strateji planı hazırlanması hedeflenmiştir. Bu planlar sayesinde, diğer ülkeler ile rekabet edebilmek ve AUS'a ayak uydurabilmek mümkündür. Bu çalışmalarda AUS'un geliştirilmesine yönelik Türkiye'nin ihtiyaç duyduğu bütün bilgiler yer almaktadır. Dünya ve Türkiye AUS yatırımları ve uygulamaları gelecek yıllarda oldukça önem arz edecektir (Tektaş ve Tektaş, 2019b).

Bu çalışmada, AUS iletişimi mimarisi ve katmanları, siber güvenlik açısından tehditler ve güvenlik açıkları analiz edilmiştir. Bu güvenlik sorunlarının temel nedenlerini belirlemek için yapılan çalışmalar ve uluslararası standarlara dayalı olarak AUS'daki güvenlik sorunları belirlenmiştir. Ayrıca, mevcut güvenlik çözümlerinin tasarımındaki eksik güvenlik öğelerini belirlemek için olası saldırıları da araştırılmıştır. Özellikle, AUS uygulamalarında yaşanan siber saldırı olayları açısından öğrenilen dersleri çıkarmak için mevcut çözümlerin güçlü ve zayıf yönlerini vurgulayan karşılaştırmalı bir çalışma yapılmıştır. Ayrıca, yapılan araştırmalara sonucunda AUS alanında kullanılan uygulamalar ve sistemler güvenlik açısından uluslararası standartlara dayanarak güvenlik modeller kullanılmalıdır. Bu modellerin takibi ve uygulanması sistemlerin güvenli olması, tehditlerden korunması ve sürekli çalışır durumda kalması açısından önemlidir. Siber güvenlik açısından yapılan incelemelerde en önemli saldırı yöntemleri DDoS, MitM ve Malware saldırılarıdır. Geleneksel yöntemler ile korunma yerine gelişmiş teknolojiler kullanarak korunma yolları tercih edilmelidir. Özellikle bu saldırılara karşı alınması gereken önlemler uygulanarak gerekli gereksinimlerin sağlanması önemlidir. Güvenlik denetimleri, ağ trafiğini izleme, personelin farkındalık eğitimleri, yapay zeka ile geliştirilen uygulamaların kullanılması, anamoli tarama, ulusal ve uluslararası standartları takip etmek ve geliştirilen teknolojik koruma yöntemlerini kullanmak vb. adımlar AUS'u güvenli yapmak için takip edilmelidir.

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

Annamalai, C. (2022). Combinatorial and Multinomial Coefficients and its Computing Techniques for Machine Learning and Cybersecurity. *The Journal of Engineering and Exact Sciences, 8*(8), 14713-01i.

Autoblog. Erişim: 10 Aralık 2022, https://www.autoblog.com/2017/08/04/self-driving-car-sign-hack-stickers/.

Avcı, İ. (2021). Investigation of cyber-attack methods and measures in smart grids. *Sakarya University Journal of Science, 25*(4), 1049-1060.

Çelik, U. (2018) Akıllı Ulaşım Sistemleri ve Büyük Veri, *1st International Conference on Intelligent Transportation Systems (BANU-ITSC'18)*, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye, 202-211.

ENISA, Erişim: 15 Aralık 2022, https://www.enisa.europa.eu/

European Telecommunications Standards Institute. *ETSI 302 663 - G5*. Erişim: 11 Aralık 2022,https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf.

European Telecommunications Standards Institute. *ETSI 102 940*. Erişim 12 Aralık 2022,https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf.

European Telecommunications Standards Institute. *ETSI TR 102 638 ITS BSA*. Erişim: 13 Aralık 2022,https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf.

European Telecommunications Standards Institute. *ETSI 302 665*. Erişim 11 Aralık 2022,https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf.

Falahati, A., & Shafiee, E. (2022). Improve Safety and Security of Intelligent Railway Transportation System Based on Balise Using Machine Learning Algorithm and Fuzzy System. *International Journal of Intelligent Transportation Systems Research*, *20*(1), 117-131.

Fox40. Erişim: 11 Aralık 2022, http://fox40.com/2017/08/03/road-sign-in-solano-county-hacked-to-say-trump-has-herpes/.

Feng, Y., Huang, S. E., Wong, W., Chen, Q. A., Mao, Z. M., & Liu, H. X. (2022). On the Cybersecurity of Traffic Signal Control System With Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems*.

Gaurav, A., Gupta, B. B., & Chui, K. T. (2022). Edge Computing-Based DDoS Attack Detection for Intelligent Transportation Systems. In *Cyber Security, Privacy and Networking* (pp. 175-184). Singapore: Springer Nature Singapore.

Katanalp, B. Y., Yıldırım, Z. B., Eren, E., & Uz, V. E. (2018, November). Akıllı Ulaşım Sistemleri Üzerine Bir Değerlendirme. *In 2nd International Symposium on Innovative Approaches in Scientific Studies*, SETSCI Conference Indexing System (Vol. 3, pp. 1503-1506).

Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2022). Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consumer Electronics Magazine*.

Lamssaggad, A., Benamar, N., Hafid, A. S., & Msahli, M. (2021). A survey on the current security landscape of intelligent transportation systems. *IEEE Access*, *9*, 9180-9208.

Markovčić Kostelac, M. (2019). EU raises cyber-security awareness in transportation. *Safety4Sea*. Retrieved December 7, 2022 from https://safety4sea.com/eu-raises-cyber-security-awareness-in-transportation.

Mikhalevich, I. F. (2022, March). Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems. In *2022 Systems of Signals Generating and Processing in the Field of on Board Communications* (pp. 1-7). IEEE.

Özarpa, C., Avci, İ., Kinaci, B.F. (2022). Cyberattack Measures in Smart Cities and Grids. In: Marques, G., González-Briones, A. (eds) Internet of Things for Smart Environments. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-09729-4_7.

Realclear. Erişim: 05 Kasım, 2022, http://www.realclear.com/offbeat/2016/05/24/great_prank_leads_to_truly_terrible_advice_on_hacked_texas_road_sign_13439.html.

Report-d. Erişim: 8 Aralık 2022, https://www.report-d.de/Duesseldorf/Verkehr/Duesseldorf-zwischen-Update-und-Absturz-Schwarzer-Donnerstag-bei-der-Rheinbahn-Tausende-kamen-zu-spaet-75475.

Sfexaminer. Erişim:5 Aralık 2022, http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-cashes.

Suryadithia, R., Faisal, M., Putra, A. S., & Aisyah, N. (2021). Technological developments in the intelligent transportation system (ITS). *International Journal of Science, Technology & Management*, *2*(3), 837-843.

Sputniknews. Erişim: 7 Aralık 2022, https://cdn2.img.sputniknews.com/images/105598/15/1055981593.jpg.

Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Maddikunta, P. K. R., Yenduri, G., ... & Gadekallu, T. R. (2022). XAI for Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions. *arXiv preprint arXiv:2206.03585*.

Tektaş, M., & Tektaş, N. (2019b). Akıllı Ulaşım Sistemleri (AUS) Uygulamalarının Sektörlere Göre Dağılımı. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi*, 2(1), 32-41.

Telang, S., Chel, A., Nemade, A., & Kaushik, G. (2021). Intelligent transport system for a smart city. In *Security and Privacy Applications for Smart City Development* (pp. 171-187). Springer, Cham.

Telegraph. Erişim: 9 Aralık 2022, http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-targetdeutsche/.

Tufan, H. «Akıllı Ulaşım Sistemleri Uygulamaları ve Türkiye için Bir AUS Mimarisi Önerisi,» T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ankara, 2014.

Trendmicro. Erişim: 12 Aralık 2022, https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf.

UAB. Erişim:17 Mart 2023, https://www.uab.gov.tr/uploads/announcements/ulusal-akilli-ulasim-sistemleri-strateji-belgesi-v/ulusal-akilli-ulas-im-sistemleri-strateji-belgesi-ve-2020-2023-eylem-plani.pdf.

Washington Post. Erişim: 3 Aralık 2022, Somebody keeps hacking these Dallas road signs with messages about Donald Trump, Bernie Sanders and Harambe the gorilla - The Washington Post.

Zeba, G., Dabić, M., Čičak, M., Daim, T., & Yalcin, H. (2021). Technology mining: Artificial intelligence in manufacturing. *Technological Forecasting and Social Change*, *171*, 120971.

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *arXiv preprint arXiv:2208.14937*.