VERİ BİLİMİ DERGİSİ
www.dergipark.gov.tr/veri

Akıllı Ulaşım Sistemlerinde Kablosuz İletişim Teknolojileri: Güncel Yaklaşımlar, Güvenlik ve Gizlilik

Bora UĞURLU[1]*

[1]Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Çanakkale, Türkiye

Makale Bilgisi

Başvuru:
01/12/2024
Kabul:
22/01/2025

Özet

Akıllı ulaşım sistemi (Intelligent Transport System-ITS) modern şehirlerin trafiğini daha güvenli, verimli ve sürdürülebilir hale getirmek için geliştirilmiş ileri bir teknolojik çözümdür. Bu çözümün en önemli bir tanesi ise V2X (Vehicle to Everything) teknolojisidir. V2X teknolojisi, araçtan her şeye iletişim, araçların çevrelerindeki akıllı bütün nesneler ile iletişim kurulması adına oluşturulmuştur. Bu sayede gündelik hayattaki trafik güvenliği, verimliliği arttırmakta ve otonom sürüş sistemlerin verimliliğinin arttırılmasına yardımcı olan bir teknolojidir. Bu teknolojiden optimum yararlanabilmek için araçlardan alınan verilerin diğer araç ve nesneler ile paylaşılırken dikkat edilmesi gereken güvenlik, gizlilik ve bütünlük gibi birtakım durumlar söz konusudur. Bu çalışmada V2X ve bunun ilişkili güvenlik ve gizlilik kavramları ele alınarak incelenmiştir. Literatürdeki 29 adet çalışma sistematik olarak incelenerek kıyaslama yoluyla güvenlik ve gizliliğe yönelik bulgular, bilimsel değerlendirmeye dayanan tartışma yoluyla bu çalışmada verilmektedir.

Anahtar Kelimeler: *ITS, V2X, Güvenlik, Gizlilik*

Wireless Communication Technologies in Smart Transportation Systems: Current Approaches, Security and Privacy

Abstract

Intelligent Transport System (ITS) is an advanced technological solution developed to make the traffic of modern cities safer, more efficient and sustainable. The most important of these solutions is V2X (Vehicle to Everything) technology. V2X technology was created for vehicle-to-everything communication, and for vehicles to communicate with all intelligent objects around them. In this way, it increases traffic safety and efficiency in daily life and is a technology that helps to increase the efficiency of autonomous driving systems. In order to benefit from this technology optimally, there are some situations such as security, confidentiality and integrity that should be taken into consideration when sharing the data received from vehicles with other vehicles and objects. In this study, V2X and its related security and confidentiality concepts are examined. 29 studies in the literature are systematically examined and findings regarding security and confidentiality are given in this study through a discussion based on scientific evaluation.

Keywords: *ITS, V2X, Security, Privacy*

* İletişim e-posta: boraugurlu@comu.edu.tr

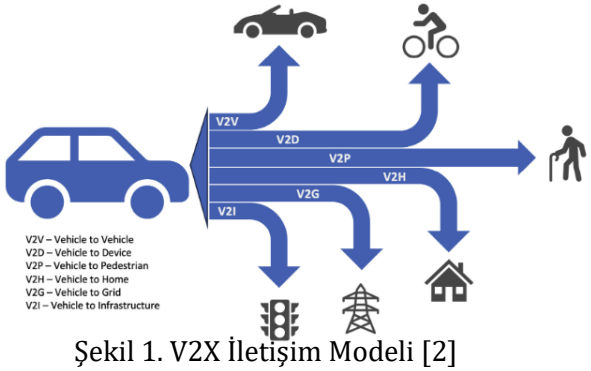
1 Giriş

Bilgi teknolojilerindeki hızlı değişim ve dönüşüm etkilerini ulaştırma sektöründe de göstermektedir. Özellikle Nesnelerin İnterneti (Internet of Things-IoT) ve Akıllı Ulaşım Sistemleri (Intelligent Transportation Sytems-ITS) arasındaki ilişki oldukça güçlüdür. IoT dünyasındaki algılayıcıların hızla gelişimi ve bu sayede hızlı, sürekli toplanan verinin olması önemlidir. Bu verinin paylaşılması sonrasında analiz edilebilmesi, ulaşım altyapılarının iyileştirilmesinde önemli bir rol oynar. Her iki kavramı veri paylaşımı, güvenlik ve etkileşim, otonom araçlar ve son olarak akıllı şehirler başlıkları altında bir araya getirmek mümkündür [1].

Özellikle günümüz modern araçları bir algılayıcı yumağı olarak nitelendirilebilir. Böylelikle hem kendileri hem de çevreleri ile ilgili birçok farklı veriyi toplayabilmektedir. Bu veriler aracın kendisi tarafından işlenebileceği gibi, bunların alt kümesi etraflarındaki diğer araçlarla da paylaşımı mümkündür. Özellikle akıllı şehir altyapıları için tasarlanmış altyapı ve sinyalizasyon sistemlerinde de benzer algılayıcı yapıları yer almaktadır. Trafik güvenliği ve akışını en üst düzeyde sağlayabilmek adına bu sistemler ile araçlar arasında da veri paylaşımı gerçekleştirilmektedir. Sürücü müdahalesine ihtiyaç duymadan çevresini algılayarak hareket edebilen araçlar olarak nitelenen otonom araçların algılayıcılardan elde edilen bu verilerle paylaşımda bulunması oldukça önemlidir. Terimsel olarak ITS, ulaşım ağlarını daha güvenli, etkili ve verimli hale getirmek için bilgi ve iletişim teknolojilerini kullanan sistemlerdir. Bu sistemler kullanılan bölgedeki trafiği yönetebilmekte, sürücülere anlık bilgi sağlayabilmektedir. Araçlar, sürücüler, yolcular, yayalar, yerel otoriteler arasında bilgi alışverişini sağlayarak ulaşım sorunlarını çözmeye yardımcı olurlar. ITS'lerin başlıca bileşenleri arasında trafik yönetim sistemleri, sürücü yardım ve güvenlik sistemleri, şehir içi toplu taşıma sistemleri, V2X teknolojileridir [2,3].

ITS'in bir bileşeni olan V2X, araçlar, altyapı, yaya gibi ögeler arasında etkileşimi kurarak trafik güvenliğini önemli ölçüde arttırılmasına yardımcı olmaktadır. Amerika Birleşik Devletleri Ulaştırma Bakanlığı (United States Department of Transportation-USDOT), yollarda meydana gelen ölüm ve ciddi yaralanmaları azaltmak için V2X teknolojilerinin güncel yayılım planını güncellemiş ve bunu sağlamak için kaynak ayırmıştır [1]. Ulusal Karayolu Trafiği Güvenliği İdaresi (Natiaonal Highway Traffic Safety Administration-NHTSA), 2017 yılında Özel Kısa Menzilli İletişim (Dedicated Short-Range Communications-DSRC) teknolojisini kullanan iki V2V uygulamasının, Kavşak Hareket Desteği (Intersection Movement Assistance-IMA) ve Sol Dönüş Desteği (Left Turn Assitance-LTA), toplam bildirilen kazaların %13 ilâ %18'ini oluşturan 439 bin ilâ 615 bin adetini önleyebileceğini ve tam olarak uygulandığında ise yılda 987 ilâ 1366 hayatı kurtarılabileceğini tahmin etmiştir. Bundan ayrı olarak kazaların önlenmesinden kaynaklı olan tasarruf ise tahmini 55 ilâ 74 milyar dolar arasındadır [1]. V2X destekli trafik yönetimi ve bununla birlikte gerçekleştirilen sinyal yönetiminin CO_2 emisyonunun %16'ya kadar azaltılabileceği belirtilmiştir [1].

Akıllı cihazlar, dijital dönüşümün temelini oluşturarak gündelik hayatımıza yenilikçi çözümler sunmaktadır. Özellikle iletişim teknolojilerindeki gelişmeler, içinde yaşadığımız şehir yaşamında ulaşım, haberleşme, alt yapı vb. birçok unsuru birbirleriyle bağlantılı hale getirmektedir. Bu bağlamda, V2X araçların çevreleriyle kurduğu etkileşimlerin temelinde yer alan kapsamlı bir teknoloji olarak karşımıza çıkmaktadır. Bu teknoloji sayesinde kara yolundaki araçlar, diğer araçlarla, yayalarla ve diğer dijital ağlarla sürekli etkileşim halinde olarak daha güvenli ve etkin bir ulaşım yapısı oluşturmaktadır. V2X kavramı birçok başlığı bünyesinde barındıran bir çatı bir kavram olarak Şekil 1'de görüldüğü gibi karşımıza çıkmaktadır. V2V (Vehicle-to-Vehicle-V2V) araçlar arasındaki iletişim teknolojisini ifade eder. Bu teknoloji, araçların hız, konum, yön gibi bilgileri çevresindeki diğer araçlarla paylaşmasına olanak tanır. Bu bilgiler araç üzerindeki uygulamalar tarafından işlenerek diğer araç sürücülerini kazalar, aşırı hız, yavaş trafik, agresif sürücüler, kör noktalar veya yol tehlikeleri konusunda uyarmaktadır.



Şekil 1. V2X İletişim Modeli [2]

Yol kenarında bulunan üniteler (RSU-Roadside Unit) yol kenarına yerleştirilmiş haberleşme ekipmanlarıdır (trafik ışıkları, sinyalizasyon cihazları, kameralar vb.). Bu üniteler yardımıyla yol üzerindeki taşıtlar altyapı ile karşılıklı etkileşim halinde bulunurlar. V2I (Vehicle-to-Infrastructure-V2I) araçtan altyapıya olan iletişim için kullanılan bir teknolojidir. Bu teknoloji, araçların RSU ile haberleşerek veri alışverişi yapmasını sağlar. V2N (Vehicle-to-Network) ise araçtan ağa olan iletişim içindir. Mobil ağlar bu teknolojide oldukça etkin olarak rol alırlar. I2N (Infrastructure-to -Network) altyapıdan ağa iletişimde kullanılır. Bu teknoloji de V2I'da olduğu gibi RSU'ların bir veri merkeziyle ekseriyetle mobil ağlar üzerinden haberleşmesinde kullanılmaktadır. Akıllı şehirlerdeki ulaşım alt yapılarının koordineli çalışabilmesi için bu I2N iletişim şekli önemli bir unsur olarak karşımıza çıkmaktadır [2,3].

V2X'in araç, yol, yaya ve diğer altyapısal üniteler ile veri paylaşımı gerçekleştirmesi beraberinde veri ve ağ güvenliği gibi başlıklarla beraber düşünülmesini gerektirmektedir. V2X alt yapısı ile donatılmış bir bölgede kötü niyetli bir araç ve/veya kullanıcı, ele geçirilmiş Yol Kenarı Ünitesi (Roadside Unit-RSU) vb. bu ağı kullanan diğer araçları yanıltıcı bilgiler yayarak trafik sıkışıkları ve/veya kazalara neden olarak sistemin kullanışsız hale gelmesini sağlayabilirler. Diğer bilgisayar ağlarında olduğu gibi V2X ağında oluşabilecek açıklar ağa entegre olan sürücü, yolcu, yayalara ait gizliliğin ihlal edilmesine sebep olabilir. Bu çalışmada ITS ve ilişkili olduğu V2X teknolojisindeki iletişim standartları ve var olan güvenlik, gizlilik tehditleri çerçevesinden incelenmiştir. Çalışmamızın ana katkısı, literatürdeki çalışmalara sistematik bir inceleme yoluyla güvenlik özelinde değerlendirme yaparak, çalışmaları kıyaslayan ve öne çıkan yönlerini vurgulayan bir yapıyı sunmasıdır. Bu makale beş bölümden oluşmaktadır. İkinci bölümde önceki çalışmalar, üçüncü bölümde ITS ile ilgili var olan standartlar, dördüncü bölümde V2X'deki güvenlik ve gizlilik kavramları ve ardından son bölümde ise sonuç ve öneriler yer almaktadır.

2 Önceki çalışmalar ve genel bakış

V2X özelinde literatürdeki çalışmaları birkaç farklı boyutta değerlendirmek mümkündür. İlk kategorideki çalışmalar ITS ve V2X'in genel olarak resmeden, var olan sorunları ve bu sorunlarla ilişkili hipotetik çözüm önerileri sunan yaklaşımlardır. Kablosuz iletişim teknolojisindeki yeni teknolojilerin DSRC ve C-V2X üzerindeki etkilerini inceleyen çalışmalardır. Son olarak ise mobil ağların V2X üzerindeki etkilerini inceleyen çalışmalar karışımıza çıkmaktadır.

Var olan DSRC, C-V2X ve bunların melez kullanımlarını ele alan bir çalışma Abboud ve arkadaşları tarafından 2016 yılında yapılmıştır[4]. Çalışmalarında hücresel ağlardaki dikey geçiş tekniklerindeki ve ağ seçim şemalarındaki zorlulara vurgu yapmışlardır. V2X ile ilgili var olan düzenlemeler, standartlar ve yapılan çalışmaların kapsamlı bir incelemesi MacHardy ve arkadaşarı (2018) tarafından yapılmıştır [5]. Çalışmada DSRC ve mobil ağlar karşılaştırılmış ve her birinin eksiklik ve zayıflıkları ortaya konulmuştur. En iyi çözümün ise hibrit bir yaklaşımın olması gerektiğine vurgu yapılmıştır.

V2X teknolojilerindeki tarihsel gelişmeleri ve bu alanda Kuzey Amerika, Avrupa ve Asya'da var olan standartları inceleyen bir çalışma Zhou ve arkadaşları (2020) tarafından yapılmıştır. Çalışmada IoV (Internet of Vehicles) teknolojisi, büyük veri odaklı olarak incelenmiştir [6].

Sonklin ve arkadaşları 2019 yılındaki çalışmasında var olan DSRC ve 4G temelli ağların araçların konularını geniş ölçekte belirlemekte yetersiz kaldığını belirterek yeni bir yaklaşım olarak Publish-Subscribe temelli olan MQTT protokolü kullanarak araçların çevrelerindeki diğer araçların konularını belirleyebilmesini sağlayan bir yaklaşım öne sürmüşlerdir. Bu amaçla bir çerçeve (framework) geliştirmişlerdir [7].

DSRC ve C-V2X üzerinde var olan eksiklikleri ve yapılması gereken iyileştirmeler içeren çalışma ise Naik ve arkdaşları tarafından 2019 yılında gerçekleştirilmiştir. Çalışmada var olan radyo erişim teknolojilerinin eksik yönleri değerlendirilmiş ve otonom sürüşlerde ilerisi için kullanılabilecek 802.11bd ve NR-(New Radio)V2X gibi iki teknoloji üzerine bir literatür incelemesi gerçekleştirilmiştir[8].

4G-LTE'nin kullanıldığı ve C-V2X veya melez V2x teknolojilerini simülasyon ortamlarında değerlendiren makaleleri bir çalışmada Hejazi ve Bakor 2021 yılında bir araya getirmiştir. İncelediklerı makaleleri kullandıkları kullandıkları simülasyon ortamlarına göre sınıflandırmışlardır. Çalışmalarının sonucunda Avrupa merkezli ve IEEE 802.11p standartı temelli olan ITS-G5'in trafik sıkışıklığının olduğu senaryolarda C-V2X'te daha başarılı olduğunu belirtmiştir [9].

5G-NR (New Radio), 5G ağları için geliştirilmiş yeni bir radyo erişim teknolojisidir. 5G-NR-V2X (New Radio Vehicle-to-Everything) ise özellikle otonom araçlar, artırılmış güvenlik ve düşük gecikmeli iletişim için tasarlanmıştır. Bu teknoloji aynı zamanda, 5G mobil ağları kullanarak araçlar arasında ve çevredeki diğer nesnelerle (yaya, altyapı, ağlar, vb.) iletişim kurulmasını sağlayan bir sistemdir. 3GPP (3rd Generation Partnership Project), 2020 yılında 5G-NR arayüzünü temel alan V2X standardını için sürüm 16'yı yayınlamıştır. 5G-NR-V2X ile kapsamlı bir incelemeyi Garcia ve arkadaşları 2021 yılında yapmış ve sürüm 17 için bazı iyileştirmeleri önermişlerdir [10].

4G-LTE ve 5G tabanlı hücresel ağ teknolojilerinin C-V2X'de var olan mevcut çalışmaları ve karşılaşılan zorlukları kapsamlı bir şekilde ele alan bir araştırma makalesi Gyawali ve arkadaşları tarafından 2021 yılında yapılmıştır [11]. Çalışmada var olan ve aktif olarak kullanılan LTE'nin geniş kapsama alanı, yüksek nüfuz etme gücü gibi açılardan C-V2X'e tercih edilme nedeni olarak sunulmuştur. Bunun yanında fiziksel katmanın yapısı ve senkronozisyon, V2X sistemlerinde gereksinim duyulan yüksek bağıl hız ve sık olan geçişler LTE'de yaşanan başlıca zorluklar olduğuna değinilmiştir. C-V2X'de ağda bulunan kullanıcılar arasındaki kaynak tahsisinin çakışmadan gerçekleştirilmesi ise bir başka zorluk olarak nitelendirilmiştir. V2X ve 5G kapsamında kullanılan radyo kaynak tahsisi ile ilgili bir çalışma ise Le ve arkadaşları tarafından 2021 yılında gerçekleştirilmiştir [12]. Çalışmada frekans kaynaklarının araç sayıları düşünülünce oldukça kısıtlı hale geldiği ve modern 5G tabanlı V2X sistemlerindeki radyo kaynak tahsisi ile ilgili zorlukları olası muhtemel çözüm önerilerini belirtmiştir.

Hur ve arkadaşlarının çalışmasında (2023) C-V2X'in 5G'ye doğru evrilirken karşılaşılan kullanımı zorluklarını ve çözüm önerilerini belirtmişlerdir. Çalışmalarında LTE'nin V2X'in bir sonraki aşamasını oluşturan LTE destekli eV2X (enhanced V2X) ve 5G temelli 5G-NR(New Radio)-V2X teknolojilerinin var olan DSRC teknolojileri ile birlikte kullanılmasının gerekliliğinden bahsedilmiştir[13].

V2X'de yer alan güncel kablosuz çözümleri ele alan bir çalışma ise Clancy ve arkadaşları (2024) tarafından yapılmıştır. Klasikleşmiş olan protokol ve standartları yeni kabul gören IEEE 802.11bd ve 5G NR protokollerini de kapsamlı olarak incelemişlerdir[14].

Gupta ve arkadaşları V2I ve I2N'de kullanılmak üzere uygulama sunucularıyla kıyaslayınca daha küçük ölçekte kalan yerel ve mobil cihazlara yakın küçük bulutları (cloudlets) önermişlerdir. Önerdikleri cloudlet yapısı sayesinde uç birimler arasında güvensiz bir veri aktarımı yerine güvenli iletişimin sağlanabildiği, kimlik doğrulama ve yetkilendirmenin (authentication and authorization) sağlanmışltır. Ayrıca geliştirdikleri ağ üzerinde transfer edilen veriler üzerinde anomali tespiti yapmaktadır[15].

Yoshizawa ve Preneel 2019 yılındaki çalışmasında V2X alanında IEEE 802.11p ve hücresel tabanlı çözümlerin olduğunu belirtmiştir. 5G mobil teknolojisinin etkilerinin V2X'te etkisini gösterdiğini ve klasikleşmiş iki standardın yanında melez yaklaşımların da V2X dünyasında ön plana çıktığını göstermiştir. Standartları ve sunduklarını güvenlik açısından incelemiştirler [16].

5G teknolojisinin taşıtlardaki iletişimdeki güvenlik ve gizlilik boyutu ele alındığı bir çalışma Sağlam ve Bahtiyar tarafından 2019 yılında yapılmıştır. Var olan saldırı türlerine göre geliştirilen mekanizmaları 4 farklı şekilde sınıflandırmışlardır. Bunlar kimlik doğrulama (authentication), gizlilik (confidentiality), hazır bulunuşluluk (availability) ve bütünlüktür (integrity) [17].

Hasan ve arkadaşları (2020), V2X ekosisteminin genel bir özetini bu ağ üzerinde güvenlik ve gizlilik açılarından incelemiştir. Var olan saldırı tehditleri, gizliliğin ihlal şekilleri ve bunların önlenmesine ilişkin çözüm önerilerini sunmuştur. Tehditler ve çözümler arasındaki kavramsal boşluklara dikkat çekmiştir [18]. 5G-V2X'de yer alan saldırı türlerinin sınıflandırılması Saulaiman ve arkadaşları tarafından (2021) yapılmıştır [19]. Yine V2X ağlarına gerçekleştirilebilecek siber saldırıları, olası sonuçları ve alınabilecek önlemler Avcı ve arkadaşları tarafından ele alınmıştır [20].

İsmail ve arkadaşları 2024 yılında yaptıkları çalışmada araçlar arasındaki güvenlik tehditlerini MAC, yönlendirme, çapraz katman seviyelerinde inceleyen bir literatür incelemesi yapmışlardır. Araştırmalarının sonucunda MAC (Media Access Control) katmanı için TDMA (Time Division Multiple Access- Zaman Bölmeli Çoklu Erişim) protokolünde ve yönlendirme protokollerinde özellikle gerçek zamanlı yapılan işlemlerde

iyileştirmeler yapılması gerektiği ortaya koymuşlardır [21].

Kwak ve arkadaşları araçların güvenliği için sürücünün doğrulanmasına odaklanarak sürücüye ait verileri araç bünyesinde bulunan ECU'dan elde ettiği verileri makine öğrenmesi ile analiz ederek aracın çalıntı bir araç olup olmadığını anlamaya yönelik bir sistem geliştirmiştir. Sistemlerinde karar ağaçları, rastgele orman, k en yakın komşu (nearest neighbor) ve çok katmanlı yapay sinir ağlarını kullanmışlarıdır [22].

V2X sistemlerindeki güvenlik ve gizliliğin arttırılmasında kökleşmiş tekniklerin yanında yenilikçi yaklaşımlar sunan çalışmalar da bulunmaktadır. Rishiwal ve arkadaşları V2X'de var olan çeşitli güvenlik tehditlerini, gizlilik ihlallerini, kötü niyetli saldırıları gibi başlıkları çalışmasında inceleyip değerlendirdikten sonra blockchain teknolojisini bahsi geçen tehditleri gidermek için yenilikçi bir çözüm olarak sunmuşturlar [23]. Blockchain teknolojisinin V2X'deki kullanımına yönelik bir diğer benzer çalışma da Roa ve arkadaşları tarafından gerçekleştirilmiştir (2023). Çalışmalarında V2X'in nesnelerin interneti (IoT) ile ilişkisi ve bu ilişkinin blok zincir (blockchain) teknolojisi ile ilişkisi incelenmiştir [24].

Var olan tehditlerin geniş bir özeti, savunma mekanizmalarının proaktif ve reaktif olarak geniş bir taksonomisi ve güvenlik hedeflerini karşılamak için yapay zekâ araçlarından yenilikçi güvenlik yaklaşımlarını ortaya koyan bir çalışma ise Sedar ve arkadaşları tarafından gerçekleştirilmiştir [25].

Bir diğer yenilikçi yaklaşım ise makine öğrenmesini esas alan ve veri zehirlenmesi saldırısına (Data Poisoning Attack) karşı bir altyapı sisteminin kullanımıdır. Wang ve arkadaşları (2024) geliştirdikleri modeli altyapı destekli savunma (IED-Infrastructure Enable Defense) olarak isimlendirmek ve kentin trafik durum ve tahmini için kullanmayı önermişleridir [26].

V2X ağındaki saldırı türlerini kapsamlı bir şekilde Gulerte ve arkadaşları (2024) incelemişleridir. Çalışmalarında V2X'deki güvenlik ile ilgili olan zorlukları ortaya koyduktan sonra karıştırma (jamming), kimlik sahtekarlığı (spoofing), dağıtık hizmet engelleme (DDOS-Distributed Denial of Service), dinleme (eavesdropping) siber saldırı türlerini V2X'de incelemişlerdir. Araştırma sonucunda V2X sistemlerinde güvenlik başlığının ileri protokol ve teknolojilere ve bu konuda patentli araştırmalara gereksinim duyduğunu belirtmişlerdir [27].

Bilgisayar ağları üzerinde etkili olan DDOS (Distributed Denial of Service) saldırıları V2X ağları üzerinde de gözlemlenmektedir. Gorine ve Agboile (2024) yaptıkları çalışmada VEINS simülasyon ortamını kullanarak Bristol şehri üzerinde DDOS saldırısının etkilerini gözlemlemiştir. Saldırının etkilerini gözlemlemek için temel ağ ölçütlerinden olan PDR (Packet Delivery Ratio-Paket Teslim Oranı), uçtan uca olan gecikme (end-to-end delay), saldırı öncesi ve saldırı anlarındaki verimi (troughput) kullanmışlarıdır. Çalışmalarında DDOS ataklarının V2X ağını ciddi derecede etkilediğini, bu tarz saldırıyı önlemek için kullanılan yöntemlerin ağın genelindeki operasyonları kısmen geri getirdiği belirtilmiştir [28].

Çalışmamızda yukarıda bahsi geçen çalışmaların gösterdiği araştırma alanı içerisinde sistematik bir inceleme yapılarak, güvenlik ve gizlilik yönelimli uygulamaları kıyaslama yoluyla kategorize eden bir bilimsel yöntem ile değerlendirme yapılmıştır. Sonraki bölümlerde buna dair detaylara yer verilmektedir.

3 ITS ve standartlar

Bu bölümde ITS hakkında literatüre geçen çeşitli standartlar ve bunların kullanım alanlarına dair detaylara yer verilmektedir. Buna göre standartlar incelenerek güvenlik ve gizlilik kapsamı sistematik yoldan ortaya konulmuştur.

3.1 802.11 temelli standartlar

Akıllı ulaşım sistemlerde Avrupa Birliği, Amerika Birleşik Devletleri (ABD) ve Japonya bazı birtakım standartların belirlenmesinde öncülük etmektedir ve bu konuda farklı standartları kabul etmişlerdir (Tablo 1).

Avrupa ve ABD'deki kuruluşların kabul ettikleri standartlarını temel alan standart ise IEEE 802.11'dir. Bu standart temel alınarak 2010 yılında ilk olarak IEEE 802.11p kabul edilmiştir [3,16]. IEEE 802.11p genellikle 5.9 Ghz frekans bandında çalışır ve menzili yaklaşık 300-500 m.'dir. Ad-hoc iletişim kurabilir. Böylelikle herhangi bir mobil ağa dahil olmadan araçlar ve altyapı arasında doğrudan bir iletişim kurabilir.

Bu nedenle IEEE 802.11'den farklılaşarak IEEE 802.11 OCB (Outside the Context of Basic Service Set) mod olarak da bilinir. Amerika Birleşik Devletleri'nde ise IEEE 802.11 OCB modu Özel Kısa Menzilli İletişim (Dedicated Short Range

Communication-DSRC) olarak isimlendirilir. Avrupa'da ise IEEE 802.11 OCB modu Akıllı Ulaşım Sistemi G5 (ITS-G5) olarak isimlendirilmektedir. Avrupa ve ABD'de kullanılan protokol yapısı yukarıda verilmiştir. Her iki sistem birbirlerine benzese (IEEE 802.11p) de özelde farklılıklar arz etmektedir [29].

Tablo 1. Akıllı ulaşım sistemlerinin Dünya genelindeki durumu

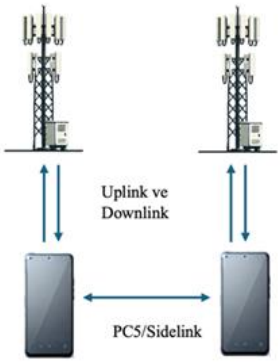
Bölge	İlgili Kurumlar	Kullanılan Protokoller	Üst Protokoller
Avrupa	**ETSI** (European Telecommunication Standards Institute) **CEN** (European Committee for Standardization))	EN 302-663	EN 302-665
ABD	**ANSI** (American National Standards Institute) **TIA** (The Telecommunications Industry Association)	IEEE 802.11p / 1609.x	WAVE (IEEE 1609)
Japonya	**ARIB** (Association of Radio Industries and Businesses) Ministry of Internal Affairs and Communications	STD 109	STD-T109

IEEE 802.11p kimlik doğrulama gerektirmemektedir. İletişimin kurulabilmesi için iletişim kurulacak kanalın frekansı ve bant genişliğinin belirlenmesi yeterlidir. Bu yapı kablosuz iletişimde fiziksel ve mac katmanlarını kapsamaktadır. Uygulama katmanına doğru ilerlemek için, IEEE tarafından WAVE olarak bilinen IEEE 1609 standardı geliştirildi. Avrupa'da ise ETSI Akıllı Ulaşım Sistemleri (ETSI ITS) komitesi, IEEE 802.11p'nin üzerine uygulamaları ve bir güvenlik çerçevesini standardize etmeye çalıştı. Bu çalışmalardan ABD'de ve Avrupa'da sırasıyla DSRC ve ITS-G5 ortaya çıkmıştır. Her ikisi de 802.11 OCB modunun üzerinde çalışan üst katman protokollerini tanımlar ve hem araçtan araca (V2V) hem de araçtan altyapıya (V2I) kısa menzilli iletişim uygulamalarını hedefler.

3.2 Hücresel temelli standartlar

3GPP'nin V2X ile ilgili çalışmaları mobil iletişim teknolojilerinin gelişimi doğrultusunda ilerlemiştir. Bu bağlamda 4G LTE'den itibaren 5G NR tabanlı V2X teknolojilerine doğru sırasıyla bazı standartlar ortaya koymuştur. 3GPP, 2014 yılında ilk defa V2X ile ilgili çalışmalara başlamıştır. 3GPP'nin önceki sürümlerinden farklı olarak ilk kez Sürüm 12 (Release 12) ile cihazlar arası (Device to Device - D2D) iletişime imkân vermiştir. D2D farklı konseptlerde uygulama alanı bulmuştur [31]. Bu servis ile mobil cihazlar birbirleriyle doğrudan herhangi bir baz istasyonuna ihtiyaç duymadan iletişim kurabilmektedir. Şekil 2'deki cihazlar arasındaki iletişim 3GPP tarafından tanımlanan sidelink veya PC5 arayüzü ile gerçekleştirilir. Böylelikle mobil cihazlar belirli bir coğrafi yakınlık içerisinde olduğu durumlarda aralarında veri alışverişi mümkün olmaktadır. Özellikle acil durumlarda ve araçlar arasında iletişimde bu durum son derece önemli bir hal almaktadır. D2D iletişim şekli Proximity Servisleri (ProSe) olarak da bilinmektedir [30,31].

Takip eden Sürüm 13(Release 13)'de LTE ve D2D teknolojilerinin performansının arttırılmasına ve kamu güvenliğine dönük iyileştirmelerde bulunulmuştur [32]. 2017 yılında yayınlanan sürüm 14 (Relase 14)'de ise 3GPP araçlar arasındaki iletişim için LTE tabanlı ilke V2X standardını tanıtmıştır[33]. Bunun bir sonucu olarak Şekil1'de ifade edilmeye çalışılan karayolundaki tüm nesneler birbirleriyle 4G LTE üzerinden haberleşebilir hale gelmiştir. Bu sürümde PC5 arayüzünde yapılan iyileştirmeler neticesinde araçlar arasındaki haberleşmesindeki gecikmeler azaltılmıştır [3,16,30,33]. Ayrıca araçlar arasında ve altyapı sistemlerinin birbirleriyle haberleşmesinde baz istasyonları olmadığından haberleşme hızı artmaktadır. Böylelikle trafik kazalarının birçoğu için önlem alınabilmekte ve karayolu üzerindeki trafik akışı daha verimli bir şekilde kontrol edilip yönlendirilebilmektedir.



Şekil 2. Cihazlar arası iletişim

5G NR'nin V2X'de kullanımına dönük ilk temeller 3GPP'nin Sürüm 15 (Release 15)'inde ele alınmıştır [34]. Takip eden Sürüm 16 ve 17'de V2X'de otonom sürüş ve işbirlikçi sürüş (cooperative drive) gibi özellikler desteklenir hale gelmiştir [35-36]. 2024 yılındaki Sürüm 18'de ise yapay zekâ destekli sürüş desteklenmesine dönük çözümlerin desteklenmesi beklenmektedir [37].

3GPP'nin Sürüm 14'ün getirdiği yenilikler otomotiv alanında bir başka kuruluşun oluşmasına neden olmuştur. 2016 yılında başta otomotiv ve telekomünikasyon olmak üzere V2X ile ilgilenen şirketler tarafından 5GAA (5G Automative Association) kurulmuştur. Özellikle otonom ve işbirlikçi sürüş, yapay zekâ destekli sistemlerin V2X'e eklemesi ile ilgili olarak 3GPP ve ETSI ile iş birliği içerisinde olup özellikle 5G NR V2X'in gelişimi için çalışmalarını sürdürmektedir. V2X ağlarının yakın (IEEE 802.11 tabanlı) ve uzak mesafe ağları (hücresel tabanlı) olmak üzere iki ana başlık altında toplandığını görmekteyiz. Özellikle PC5 arayüzü ve 5G NR ağlarındaki ProSe teknolojileri yardımıyla araçlar ve diğer yol üniteleri ile kısa mesafe iletişim kurabilmektedirler. Hem hücresel ağlar hem de kısa mesafede iletişim kurabilen IEEE 802.11p ağları hibrit kullanım şekillerini de ön plana çıkarmaktadır.

4 Güvenlik ve gizlilik

Önceki bölümde detaylı bir şekilde açıklanmaya çalışılan V2X kavramının başarılı bir şekilde uygulanabilmesinin bir ön şartı olarak bu sistemlerin güvenliği ve gizliliği gelmektedir. V2X sistemlerindeki saldırlar, bunların sınıflandırılması ve saldırı hakkında detaylı bir görünüm Tablo 2'de bulunmaktadır. Saldırıları ilk etapta aktif ve pasif olarak iki gruba ayırmak mümkündür. Aktif saldırılarda, saldırgan ağdaki veriyi aktif olarak değiştirmekte ve/veya bozulmasına neden olmaktadır. Bu tip saldırılarda V2X ağına doğrudan müdahale söz konusudur. Ağa hata kod/data eklenmesi, hizmetin engellenmesi (DoS), transfer edilen verinin değiştirilmesi aktif türde olan saldırılardır. Pasif saldırılar ise saldırganın ağa müdahale etmeden sadece verileri gizlice izlemek ve izlediği bu verilerden bilgi ederek gizliliğin ihlal edildiği saldırı türüdür. Özellikle V2X ağındaki yolculuk eden kişilerin kişisel bilgilerinin ele geçirilmesini ağırlıklı olarak hedeflendir. Pasif saldırılar kendi içerisinde araç ağ sisteminin çevrimiçi olup olmamasına göre çevrimiçi ve çevrimdışı saldırılar olarak ikiye ayrılırlar. Çevrimiçi saldırılar cihazın ayakta olduğu zamanlarda gerçekleştirilirken çevrimdışı saldırılar cihazın pasif olduğu zamanlarda ve genellikle de fiziksel erişim ile gerçekleştirilir [18].

V2X (Vehicle-to-Everything) sistemlerinde DoS saldırıları, iletişimi hedef alarak ağdaki cihazların veya araçların hizmet vermesini engellemeye yönelik olan saldırılardır. Sistemin tamamı veya bir kısmının iletişim süreçlerini kesintiye uğratmayı amaçlar. Bu saldırı türü sistemdeki ağ protokollerindeki açıkları hedef alarak farklı türlerde karşımıza çıkabilir. Replay, Jamming, Flooding DoS saldırılarının alt türlerdir (Tablo2). DoS saldırıları ağın farklı katmanlarında gerçekleşir. Ağın fiziksel katmanında gerçekleşen önemli saldırılardan bir tanesi Jamming olarak isimlendirilen frekans boğulması saldırısıdır. V2X ağına dahil olan cihazlar önceki kısımda da belirtildiği gibi (IEEE 802.11p) belirli bir frekansta haberleşirler. Jamming saldırganı sistemin çalıştığı frekans bandını hedef alarak çok fazla sayıda sinyal gönderir ve iletişim kanalını tıkar. Böyle bir durumda ise araçların birbirleriyle olan ve/veya altyapı ile olan iletişimi kesintiye uğrar. Özellikle acil durum gerektiren senaryolarda müdahale imkansızlaşır. Bu saldırgan kullandığı jammer cihazının menzili ile sınırlıdır [18].

Hizmetin engellenmesine yönelik ağ katmanında gerçekleşen saldırı türü ise Jellyfish'tir. Bu saldırıda saldırgan düğüm, başlangıçta ağdaki diğer düğümler gibi davranarak güven kazanır ve paketlerin yönlendirilmesinde önemli bir rol üstlenir. Sonrasında saldırgan düğüm paketlerin iletimini kasıtlı olarak geciktirir, yanlış sırayla iletilmesini sağlar veya paketleri rastgele düşürerek ağın işleyişini bozar.

Örneğin V2X sistemindeki araçlar yol durumu ile ilgili kritik bilgileri (kaza, yol çalışması, sıkışıklık, acil durum vb.) sürekli olarak birbirleriyle paylaştığı senaryoda trafik kazasının olduğu durumda sanki kaza olmamış gibi sağlayarak diğer araçların o yola girmesini sağlayabilir. Böyle bir senaryoda şehrin ulaşım altyapısında ciddi sıkıntılar yaşanması söz konusudur. Ayrıca bu saldırı türü otonom araçların zaman içerisinde arttığı senaryolarda daha büyük riskleri de beraberinde getirmektedir.

Tablo 2. V2X'deki aktif saldırı türleri

Saldırı İsmi	Türü	Hedef Aldığı Ağ Katmanı	Açıklama
Hizmetin Engellenmesi Saldırısı (DoS) • Frekans Boğulması (Jamming) • Denizanası (JellyFish) • Ağ Trafiğini Aşırı Yükleme (Flooding) • Yeniden Yönlendirme (Replay)	Çevrimiçi	• Fiziksel • Ağ • Ağ ve Taşıma • Uygulama katmanları	Hedef sistemin aşırı yüklenmesini sağlamak ve normal iletişimi aksatmak ya da tamamen durdurmaktır. Radyo frekansları, ağ trafiği veya protokol açıklarını hedef alarak çeşitli şekillerde gerçekleştirilebilir
Man-in-the-Middle(MITM)	Çevrimiçi	• Taşıma ve Uygulama	Ağa sızarak iki taraf arasındaki haberleşmeyi gizlice izler ve verileri değiştir.
Donanımsal yazılım (Fimware) Analizi ve Kötü Amaçlı Yazılım Yükleme	Çevrimdışı	• Fiziksel • Veri Bağı	Araçların firmwareleri ele geçirildikten sonra çevrimdışı analiz edilerek kötü amaçlı yazılım cihaza yüklenir.
Sahtekarlık (Spoofing)	Çevrimiçi	• Ağ • Veri Bağı	Sahte kimlik ve içerikle diğer tarafa bilgi gönderir.

Ağın hem ağ katmanı (network layer) hem de taşıma katmanını (transport layer) etkileyerek hizmetin engelleyen saldırı ise Flooding saldırılarıdır. Bu saldırı büyük miktarda gereksiz istek göndererek ağı işlevsiz kılmayı amaçlamaktadır. Saldırgan V2X ağındaki bir veya biden fazla hedef düğüme (araç veya yol kenarındaki sisteme dahil olan herhangi bir uç birim olabilir) çok fazla sahte veri paketi veya istek gönderir. Bu durum hedef düğümün kaynaklarını tüketir ve böylelikle sistem normal veri paketlerini işleyemez duruma gelir.

Bu saldırının ağ ve servis odaklı çalışan iki farklı alt türü bulunmaktadır. Birincisinde saldırgan ağ üzerinde sürekli ve aşırı miktarda ve trafiği oluşturarak ağın bant genişliğini tüketmektedir. Böyle bir durumda V2X sistemlerindeki araçlar, trafik lambaları, RSU'lar birbirleriyle iletişim kurmakta aksamalar yaşayacaktır. Diğer türünde ise saldırgan ağ üzerindeki araçların alt yapı veya yerel otoritelerle iletişim kurduğu belirli bir servisi hedef alırlar ve bu servise çok sayıda gereksiz istek gönderirler. Trafik bilgilerini toplayan bir sunucuya sürekli ve yoğun bir şekilde sahte istekler göndermesi neticesinde sunucu şehrin trafik yönetiminde aksamalar meydana gelecektir.

Replay saldırısı ağın taşıma ve uygulama katmanlarını hedefleyen saldırı türüdür. Bu saldırıda V2X ağında geçmişte ağda yer alan geçerli bir verinin sonradan saldırgan tarafından yeniden gönderilerek ağ üzerinde bulunan cihazların yanıltılması esas fikirdir. Böylelikle araçlar üzerinden hatalı iletişim oluşturulur. Güvenlik ve kimlik doğrulama mekanizmalarını hedefleyerek ağının güvenliğini olumsuz yönde etkiler. V2X ağındaki çarpışma uyarıları, hız bilgileri, trafik sinyalleri vb. önemli bilgiler saldırgan tarafından ağ içerinde yakalanır. Sonrasında bu mesaj tekrar hedeflenen birimlere gönderilir. Alıcı tarafından alınan paketler her ne kadar geçerli bir kaynaktan geliyor gibi görünse de tekrar eden benzer tarz mesajlar sistemin hatalı kararlar almasına neden olur. Bu tarz yanıltıcı veri paketlerinin ağ üzerinde yoğun bir şekilde tekrar etmesi trafik güvenliğini tehlikeye düşürerek kaza riskini arttırır. Ayrıca acil durumlarda yapılması gereken müdahaleleri de kesintiye uğramasına neden olur.

MITM saldırısında saldırgan V2X ağındaki cihazlar arasındaki verilere gizlice sızar ve her iki taraf arasındaki iletişimi kontrol etmeye başlar. Bu taraflar iki araç olabileceği gibi yol kontrol sistemi de olabilir. Ağa sızarak kendine yer edinen saldırgan mesajın doğrudan hedefe gitmesi yerine mesajları önce kendisine yönlendirir. Sonrasında mesajı değiştirebilir ve/veya sadece izleyebilir. Mesajların değiştirildiği durumda V2X ağına entegre olan araçların veya ilişkili olan diğer ünitelerin yanlış kararlar almalarına neden olabilir. Diğer durumda ise kullanıcıların gizliliğini ihlal ederek hassas bilgileri toplar (eavedropping). Toplanan gizli bilgiler ilk anda olmasa bile sonraki saldırılarda kullanılabilir. Bu tarz saldırı özellikle otonom araçları daha fazla etkiler. Otonom araçların aldıkları tüm kararları verilere dayalı olarak gerçekleştirmektedirler.

Taşıtlarda yer alan elektronik kontrol üniteleri (ECU-Electronic Control Units), taşıtlardaki çeşitli sistemleri kontrol eden ve yöneten birimleridir. Taşıt üzerinde birden fazla ECU bulunur ve her biri araç üzerindeki farklı bir sistemi kontrol eder. Motor sistemi, klima sistemi, fren sistemi için ayrı ayrı ECU'ları görmek mümkündür. Her bir sistemin çalışmasının kontrol edilmesi ECU üzerindeki firmware tarafından sağlanır. Firmware'ler ECU'lar üzerindeki yerleşik yazılımlardır. Bu yazılım aracın güvenliği açısından kritik öneme sahiptir. Eğer firmware üzerinde bir güvenlik açığı varsa saldırganlar bu açığı kullanarak aracı maniple edebilir. Motor, fren sistemi ve hava yastıkları gibi birincil dereceden güvenlik ile ilgili olan sistemler bu saldırılar sonucu devre dışı kalabilir. Bahsi geçen firmware'ler sadece taşıtlar üzerinde değil yol kenarındaki uç birimlerde de bulunabilir. Saldırgan tarafından bu yazılım sistemlerini hedef alarak yapılacak saldırılar neticesinde otonom araçlar ve V2X ağının farklı unsurlarından olan trafik ışıkları, GPS üniteleri kontrol edilebilir. Bu saldırı V2X ağının fiziksel ve veri bağı katmanını etkilemektedir. Ağın diğer katmanlarını ise dolaylı olarak etkileyebilir.

V2X ağında olan başka bir saldırı ise Spoofing'dir. Ağ ve veri bağı katmanlarını doğrudan hedef alan bu saldırı türünde saldırgan kendisini bir araç, trafik sinyal sistemi veya başka güvenilir kaynak olarak tanıtarak sahte veri iletir. İletilen bu verileri alan karşı taraftaki diğer bileşenler bu verileri kullanarak yanlış kararlar alırlar. Özellikle iletişim protokollerindeki kimlik doğrulamadaki açıklardan yararlanılarak gerçekleştirilen saldırı türüdür.

V2X teknolojisinde araçlar, altyapı, yayalar gibi çok çeşitli olgu birbirleriyle sürekli iletişim halindedir (Şekil 1). Bu yapıda sürücüler ve yayalar ile ilgili pek çok veri toplanır ve toplanan veriler diğer kişi veya cihazlarla analiz edilme üzere paylaşılır. Aracın konum verisi, plaka bilgisi, aracın hangi yöne doğru ilerlediği ve hangi rotayı takip ettiği, varsa araç içerisindeki yolcu bilgisi gibi bilgiler örnek olarak verilebilir. Bu tarz bilgilerle ilgili herhangi bir önlem alınmazsa gizlilik ihlalleri ortaya çıkabilir. Araçlar birbirleriyle iletişim kurarken kimlik doğrulama ve şifreleme mekanizmalarını kullanırlar. Eğer buralarda yeterli önlemler alınmazsa kötü niyetli bir kullanıcı bir aracı izleyebilir, yolcular hakkında bilgi edinebilir. Yine araçlar ve altyapı sistemleri üzerinde gerekli siber önlemler alınmadığı taktirde trafik ağına sızacak olan saldırgan araç bilgilerini ele geçirerek sistemdeki diğer araçları yanlış yönlendirebilir ve ağı kısmen veya tümüyle kullanılmaz hale getirebilir.

Tablo 3. V2X'deki gizlilik ile ilgili kuruluşlar

ABD Genelinde Gizlilik ile İlişkili Kurumlar	
Düzenleme	**Açıklama**
Federal İletişim Komisyonu (FCC)	V2X iletişimindeki spektrum tahsisi ile ilişkilidir.
Federal Ticaret Komisyonu (FTC)	V2X'de kişisel verilerin toplanması ve kullanılması ile ilgili düzenlemeler içerir.
Ulusal Karayolu Trafik Güvenliği İdaresi (NHTSA)	V2X'deki gizlilik ile ilgili düzenlemeler yayınlamıştır.
Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA)	V2X'indeki siber güvenlik standartlarını belirler.
Avrupa Genelinde Gizlilik ile İlişkili Kurumlar	
Genel Veri Koruma Tüzüğü (GDPR)	V2X'de toplanan veriler bu yönetmelik kapsamına da girmektedir.
Ağ ve Bilgi Sistemleri (NIS) Direktifi	V2X'indeki siber güvenlik için bir çerçeve belirler.
E-Gizlilik (E-Privacy)	V2X'in gizlilik standartlarının belirler.

Güvenli iletişim protokollerinin devreye alınması, V2X ağındaki mesajların gizli kalmasını ve bu tür saldırılara karşı korunmasını sağlar. V2X sistemlerindeki güvenlik ile ilgili tehditleri gizlilik konusuyla da yakından ilişkilidir. Aracın sahibinin gizliliği ve kullanılan bölgedeki yasal düzenlemeler gizlilik ile yakından ilişkilidir [6]. Amerika Birleşik Devletleri ve Avrupa Birliğinde olan yasal düzenlemeler Tablo3'te belirtilmiştir.

V2X'de gizliliği sağlamak amacıyla kullanılan mekanizmaların başında anonimleştirme gelmektedir. Bu yapıda araç ve sürücü ile ilişkili hiçbir bilgi toplanmamaktadır. Anonimleştirmede sürücü, varsa yolcu hakkındaki bilgiler araçlarla ilişkilendirilmeyerek gizlenir. Takma isimlerin kullanımı (pseudonymization), grup imzalarının kullanılması, dinamik kimlik değişimi anonimleştirmede kullanılan bazı tekniklerdir.

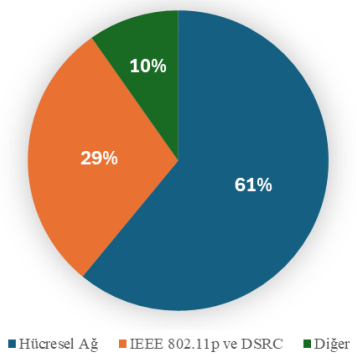
5 Sonuçlar ve öneriler

Çalışma kapsamında incelenen yayınlar (Tablo 5), V2X'in sağladığı araçlar arası (V2V), altyapı ile (V2I), yayalar ile (V2P) ve ağ ile (V2N) iletişim olanakları sayesinde, sürüş güvenliğini artırdığını ve trafik yönetiminde yenilikçi çözümler sunduğunu belirtmektedir. Özellikle V2X, çarpışma uyarıları, hız kontrolü, trafik ışığı optimizasyonu ve acil durum iletişimleri gibi uygulamalarla sürüş deneyimini daha güvenli ve konforlu hale getirmektedir.

Çalışmalar kullandıkları iletişim teknolojisi açısından hücresel tabanlı V2X (C-V2X) ve 5G destekli V2X protokollerine ağırlıklı olarak yoğunlaşmaktadır. Ayrıca, yayınlar bu teknolojinin güvenlik ve gizlilik konularını derinlemesine ele almakta; araçlar ve altyapı arasında sürekli veri akışı olduğundan, kullanıcı verilerinin korunması ve siber saldırılara karşı güvenlik önlemlerinin alınması gerektiğine dikkat çekmektedir.

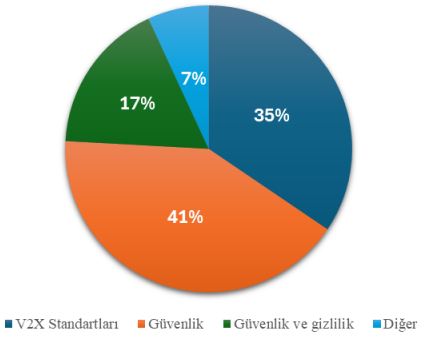
Akıllı trafik sinyalizasyonu, yol durumu tahminleri ve gerçek zamanlı navigasyon gibi uygulamalar sayesinde trafik akışının daha dinamik ve çevre dostu hale geldiği gözlemlenmiştir. Sonuç olarak, V2X teknolojisinin gelişimi, gelecekte otonom ve bağlanabilir araçların daha yaygın ve güvenilir bir şekilde kullanılmasını sağlayarak akıllı şehirlerin ulaşım sistemlerinde devrim yaratma potansiyeline sahip olduğu öngörülmektedir.

Tablo 5'te yer alan çalışmalar incelendiğinde V2X ağlarında hücresel tabanlı iletişim şekillerinin daha fazla sayıda olduğu gözlemlenmiştir (Şekil 3).



Şekil 3. Kullanılan iletişim teknolojisi

Bu çalışmalar içerisinde ele alınan konu başlıkları ağırlıklı olarak sırasıyla V2X standartları, güvenlik, güvenlik ve gizlilik olduğu görülmektedir (Şekil 4).



Şekil 4. Ele alınan konu başlıkları

Bunun yanı sıra eserler ağırlıklı olarak dergi makalesi ve konferans bildirileri şeklinde ön plana çıkmaktadır (Tablo 4).

Tablo 4. V2X ağları üzerine yapılan çalışmaların ele aldığı başlıklar

Kaynak Türü	Sayı
Dergi Makalesi	16
Konferans Bildirisi	12
Diğer	1

Tablo 5. V2X ağları üzerine yapılan çalışmaların ele aldığı başlıklar

Referans	Teknoloji	Ele Alınan Başlıklar	Açıklama
Yoshizawa ve ark.[3]	DSRC ve hücresel ağ	Güvenlik ve Gizlilik	Güvenlik ve gizliliğin ile ilgili problemlerin temel nedenleri var olan standartlar açısından ortaya konulmuştur.
Hasan ve ark.[18]	DSRC ve hücresel ağ	Güvenlik ve Gizlilik	V2X ortamı incelenerek güvenlik ve gizlilik için önerilen savunma mekanizmaları incelenmiştir.
Gupta ve ark.[15]	Hücresel ağ	Güvenlik ve Gizlilik	P2P bağlantı yerine güvenilir bir şekilde RSU'lara hücresel olarak bağlanma şekli tanıtılmıştır.
Dönmez [38]	Araç içi ağ	Güvenlik	Araç ağındaki CAN verileri ile araçtaki normal dışı durumun tespiti ve bunun araç güvenliği ile olan ilişkisi ele alınmıştır.
Wang ver ark. [26]	DSRC ve hücresel ağ	Güvenlik	V2X ağına yapılacak saldırıların trafik akışı üzerine olan etkilerini makine öğrenmesi ile çözümlenmesi açıklanmıştır.
Gorine ve Agboile[28]	Hücresel ağ	Güvenlik	V2X ağ ortamındaki DDoS saldırısı ve bunun önlemesini ele almıştır.
Yoshizawa ve Preneel [16]	DSRC ve hücresel ağ	Güvenlik	V2X standardizasyonunu güvenlik açısından incelemiştir.
Lekidis[39]	ETSI ITS G5	Güvenlik	En az etkiyle V2X ağındaki güvenlik mekanizmalarına yönelik yeni bir anomali tespit durumu açıklanmıştır.
Tu ve Shi[40]	IEEE 802.11p ve hücresel ağ	Araç ve yol altyapısın mimarisi	Araç ve yol çevresi ünitelerin birbirleriyle işbirliği içinde kullanılarak otonom sürüş için verimliliğin arttırılması.
Wu ve Yang[41]	C-V2X Ağları	C-V2X ağlarındaki erişim dilimleri	C-V2X ağının temel mimarisi ele alınarak ağ dilimlerinde kullanılan dağıtılmış merkezileştirilmiş ve dağıtılmış birimleri ele almaktadır.
Lekidis ve Morais [42]	Açık V2X platformu	Güvenlik ve gizlilik	Açık yapıya sahip olan V2X ağlarındaki güvenlik ve gizliğe ilişkin tehditler ve çözüm yöntemleri incelenmiştir.
Bodei ve ark.[43]	DSRC ve Hücresel ağ	Güvenlik ve gizlilik	V2X'de OLIVE isimli çok faktörlü yeni bir doğrulama yöntemini açıklamışlardır.
Abboud ve ark.[4]	DSRC, Hücresel Ağlar (4G) ve Hibrit Kullanım Şekilleri	V2X Standartları	V2X ağlarındaki standartlar ve geleceğe yönelik öneriler.
MacHardy ve ark. [5]	DSRC, Hücresel Ağlar (4G)	V2X Standartları	Akıllı ulaşım sistemlerindeki standardizasyon çalışmaları.
Zhou ve ark. [6]	DSRC, Hücresel Ağlar (4G)	V2X Standartları	Kuzey Amerika, Avrupa ve Asya'daki ana V2X standartları, IoV ile Büyük Veri İlişkisi Kavramı
Sonklin ve ark.[7]	MQTT Protokolü	V2X Standartları	Araçlar arasında pub-sub temelli iletişim
Naik ve ark.[8]	DSRC ve Hücresel Ağlar (5G)	V2X Standartları	Otonom sürüşler için kullanılabilecek IEEE 802bd ve NR teknolojileri
Hejazi ve Bokor [9]	4G Temelli C-V2X ve Hibrit Ağlar	V2X Standartları	V2X'deki simülasyon ortamlarının ağ kategorilerine göre değerlendirilmesi
Garcia ve ark.[10]	Hücresel Ağlar (5G-NR-V2X)	V2X Standartları	3GPP sürüm 17 için öneriler
Gyawali ve ark.[11]	Hücresel Ağlar (LTE ve 5G)	V2X Standartları	Hücresel V2X ağlarında karşılaşılan zorluklar ve çözüm önerileri

Hur ve ark.[13]	Hücresel Ağlar (LTE ve 5G-NR-V2X)	V2X Standartları	Hücresel V2X ağlarında karşılaşılan zorluklar ve DSRC ile hibrit kullanım
Clancy ve ark.[14]	IEEE 802.11bd ve 5G NR	V2X Standartları	Eski ve yeni protokollerin kapsamlı bir incelemesi
Li ve ark.[44]	Hücresel Ağlar (C-V2X)	Güvenlik	C-V2X ağlarındaki DoS saldırılarının mobil uç bilişim temelli yaklaşımlar tespiti
Dolnák ve ark. [45]	DSRC ve Hücresel Ağlar	Güvenlik	V2X ağlarındaki DNS güvenliği incelenmiştir.
Pagadala ve ark. [46]	Hücresel Ağlar (5G)	Güvenlik	5G ağı üzerindeki DDoS saldırıları ve çözüm önerilerine değinilmiştir.
Zheng ve ark. [47]	Hücresel Ağlar (C-V2X)	Güvenlik	C-V2X ağlarındaki fiziksel katman güvenliği
Twardokus ve ark.[48]	Hücresel Ağlar (C-V2X)	Güvenlik	C-V2X ağındaki fiziksel katmanın güvenliği ve DDoS saldırıları için yenilikçi bir tespit yöntemi.
Saulaiman ve ark.[19]	Hücresel Ağlar	Güvenlik	Var olan 5G-V2X iletişim teknolojileri ve bu ağ üzerindeki saldırı ve açıklar.
Avcı ve ark. [20]	DSRC veHücresel Ağ	Güvenlik	Güvenlik saldırıları ve alınabilecek önlemler.

V2X (Vehicle-to-Everything) teknolojisi, modern ulaşım sistemlerinin dijitalleşmesinde ve otonom araç ekosisteminin geliştirilmesinde kritik bir rol oynamaktadır. Birçok farklı disiplini bünyesinde barındıran bu teknolojinin gelişimi bu çatı içerisinde yer alan veri trafiğinin güvenliği ve gizliliği ile de yakından ilişkilidir. Bu nedenle, V2X teknolojik altyapısı ve standartları ile yine bu alandaki güvenlik ve gizliliğe ilişkin bir literatür incelemesi yapmak, mevcut araştırmaları ve teknolojik gelişmeleri anlamak, mevcut boşlukları tespit etmek ve yeni uygulama alanları keşfetmek için önem arz etmektedir.

Kaynaklar

[1] Intelligent Transportation Society of America. "ITS America National V2X Deployment Plan:An Infrastructure&Automaker Colloboration". Amerika Birleşik Devletleri, 2023.

[2] Oka D.K., Nadahalli S., Yost J., Bojanki R.P."Building Secure Automotive IoT Applications", Packt Publishing, 2024.

[3] Yoshizawa T., Singelée D., Muehlberg J.T., Delbruel S., Taherkordi A., Hughes D., Preneel B. "A Survey of Security and Privacy Issues in V2X Communication Systems", ACM Computing Surveys,vol 55., no.9, https://doi.org/10.1145/3558052

[4] Abboud K, Omar H. Aboubakr, Zhuang W."Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey", IEEE Transactıons On Vehıcular Technology, vol.65, no.12, pp.9457-9470,2016. doi: 10.1109/TVT.2016.2591558

[5] MacHardy Z, Khan A.,Obana K. "V2X Access Technologies: Regulation, Research, and Remaining Challenges", IEEE Communıcatıons Surveys & Tutorıals, vol. 20, no.3, pp. 1858-1877, 2018. doi: 10.1109/COMST.2018.2808444

[6] Zhou H., Xu W., Chen J., Wang W. "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities", Proceedings of the IEEE, vol. 108, no.2, pp. 308-323, 2020. doi: 10.1109/JPROC.2019.2961937

[7] Sonklin K., Wang C., Jayalath D., Feng Y. "Connected-Vehicle Data Exchanges and Positioning Computing Based on the Publish-Subscribe Paradigm", Journal of Computer and Communications, vol. 7, no. 10, pp. 82-93,2019 . doi: 10.4236/jcc.2019.710008

[8] Naik G., Choudhury B., Park J. "IEEE 802.11bd & 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications", IEEE Access, vol.7, pp. 70169-70184, 2019. doi: 10.1109/ACCESS.2019.2919489

[9] Hejazi H. , Bokor L. "A Survey on Simulation Efforts of 4G/LTE-based Cellular and Hybrid V2X Communications", 44th International Conference on Telecommunications and Signal Processing (TSP), pp. 333-339, 26-28 July 2021. doi: 10.1109/TSP52935.2021.9522665

[10] Garcia M.H.C., Boban M., Coll-Perales B. " A Tutorial on 5G NR V2X Communications", IEEE Communications Surveys & Tutorials, vol.23, no. 3, pp.1972-2026. doi: 10.1109/COMST.2021.3057017

[11] Gyawali S., Xu S., Qian Y., Hu R.Q."Challenges and Solutions for Cellular Based V2X Communications", IEEE Communıcatıons Surveys & Tutorıals, vol. 23, no. 1, pp. 222-255. doi: 10.1109/COMST.2020.3029723

[12] Le T.T.T., Moh S. "Comprehensive Survey of Radio Resource Allocation Schemes for 5G V2X Communications", IEEE Access, vol. 9, pp. 123117-123133, 2021, doi: 10.1109/ACCESS.2021.3109894

[13] Hur D., Lee D., Oh J., Won D., Song C., Cho S. "Survey on Challenges and Solutions of C-V2X: LTE- V2X Communication Technology", 14h International Conference on Ubiquitous and Future Networks (ICUFN), pp. 639-641, 04-07 July 2023. doi: 10.1109/ICUFN57995.2023.10201105

[14] Clancy J., Mullins D., Deegan B., Horgan J., Ward E., Eising C., Denny P., Jones E., Glavin M. "Wireless Access for V2X Communications:Research, Challenges and Opportunities", IEEE Communications Surveys & Tutorials, vol. 26, no.3, pp.2082-2119. doi: 10.1109/COMST.2024.3384132

[15] Gupta M., Benson J., Patwa F., Sandhu R. "Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets", IEEE Transactions on Services Computing, vol. 15, no. 4, pp.1912-1925. doi: 10.1109/TSC.2020.3025993

[16] Yoshizawa T., Preneel B. "Survey of Security Aspect of V2X Standards and Related Issues", 2019 IEEE Conference on Standards for Communications and Networking (CSCN), 28-30 October 2019. doi: 10.1109/CSCN.2019.8931311

[17] Sağlam E.T., Bahtiyar Ş. "A Survey: Security and Privacy in 5G Vehicular Networks", 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 108-112, 11-15 September 2019. doi: 10.1109/UBMK.2019.8907026

[18] Hasan M., Mohan S., Shimizu T., Lu H. " Securing Vehicle-to-Everything (V2X) Communication Platforms", IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 693-713. doi: 10.1109/TIV.2020.2987430

[19] Saulaiman M.N.E., Kozlovszky M., Csilling Á. "A Survey on Vulnerabilities and Classification of Cyber-Attacks on 5G-V2X", IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 2021, pp. 000235-000240,doi: 10.1109/CINTI53070.2021.9668440

[20] Avcı İ., Özpara C., Özdemir M., Kınacı B.F., Kara S.A. "Akıllı Ulaşım Araçlarında Siber Güvenlik Ve Çok Katmanlı Güvenlik Önlemi", Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi, Cilt: 5 Sayı: 1, 22 - 35, doi: 10.51513/jitsa.1034370

[21] İsmail T., Touati H., Hajlaoui N., Hadded M., Muhlethaler P., Bouzefrane S., Saidane L.A. "A Comprehensive Survey on Vehicular Communication Security", Journal of Cyber Security and Mobility, vol. 13, no.5, pp. 1007-1038.

[22] Kwak B.II, Woo J.Y., Kim H.K. "Know Your Master: Driver Profiling-based Anti-theft Method", 14th Annual Conference on Privacy, Security and Trust (PST), pp. 211-218, doi:10.1109/PST.2016.7906929.

[23] Rishiwal V., Agarwal U., Alotaibi A., Tanwar S., Yadav P. Yadav M. "Exploring Secure V2X Communication Networks for Human-Centric Security and Privacy in Smart Cities", IEEE Access, vol. 12, pp. 138763-138788. doi: 10.1109/ACCESS.2024.3467002

[24] Rao P.M., Jangirala S., Pedada S., Das A.K., Park Y. "Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges", IEEE Access, vol. 11, pp. 2169-3536. doi: 10.1109/ACCESS.2023.3281844

[25] Sedar R., Kalalas C., Gallego F.V., Alonso L., Zarate J.A. "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths", IEEE Open Journal of the Communications Society, vol. 4, pp. 325-391. doi: 10.1109/OJCOMS.2023.3239115

[26] Wang F., Wang X., Ban J. "Infrastructure-enabled Defense Methods against Data Poisoning Attacks on Traffic State Estimation and Prediction", Conference in Emerging Technologies in Transportation Systems (TRC-30), paper_id: 107.

[27] Gulerte K.H.M, Vargas J.A.R., Da Costa J.P.J., Da Silva A.S., Santos G.A., Wang Y., Müller C.A., Lipps C., De Souse Junior R.T., Filho W.De B.V., Slusallek P., Schotten H.D. "Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape Through Systematic Review", IEEE Access, vol. 12, pp. 72871-72895. doi: 10.1109/ACCESS.2024.3402946

[28] Gorine A.,Agboile C. "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation", International Journal of Multidisciplinary Research and Publications, vol.7, no. 3, pp.61-68.

[29] Rohde & Schwarz, "Intelligent Transportation Systems Using IEEE 802.11p: Application Note: R&S FSW, R&S FSV3000, R&S SMW200A, R&S SMBV100A.", Wan", Wand L. ve Simon M., 2019.

[30] Holma H., Toskala H., Nakamura T. "5G Technology 2nd Edition", Wiley Press, 2020.

[31] "Proximity-based Services (ProSe) UID_580059", Overview of 3GPP Release 12 v0.2.0", 3rd Generation Partnership Project.

[32] "Enhanced LTE Device to Device Proximity Services", Release 13 analytical view version Sept. 9th 2015, 3rd Generation Partnership Project.

[33] "Study on Multimedia Broadcast Supplement for Public Warning System (PWS)", Overview of 3GPP Release 14 V0.0.1, 3rd Generation Partnership Project.

[34] "Vehicle-to-Everything Communications (V2X) Improvements", 3rd Generation Partnership Project Technical Specification Group Services and System Aspects 3GPP TR 21.915 V15.0.0, 3rd Generation Partnership Project.

[35] "Advanced V2X Support", 3rd Generation Partnership Project-Technical Specification Group Services and System Aspects 3GPP TR 21.916 V16.2.0, 3rd Generation Partnership Project.

[36] "Proximity/D2D/Sidelink related and V2X", 3rd Generation Partnership Project Technical Specification Group Services and System Aspects 3GPP TR 21.917 V17.0.1, 3rd Generation Partnership Project.

[37] "Artificial Intelligence (AI)/Machine Learning (ML)", 3rd Generation Partnership Project Technical Specification Group Services and System Aspects 3GPP TR 21.918 V1.2.1 , 3rd Generation Partnership Project.

[38] Dönmez T.C.M. "Anomaly Detection in Vehicular CAN Bus Using Message Identifier Sequences", IEEE Access, vol. 9, pp. 136243-136252, 2021, doi: 10.1109/ACCESS.2021.3117038.

[39] Lekidis A. "Anomaly detection mechanisms for in-vehicle and V2X systems", 19th International Conference on Availability, Reliability and Security (ARES '24), Article 100, 1–8. https://doi.org/10.1145/3664476.3671012

[40] Tu L., Shi H. "Application and Research of V2X Vehicle Road Collaboration Technology", 3rd International Conference on Computer, Artificial Intelligence and Control Engineering, pp. 822–829. https://doi.org/10.1145/3672758.3672894

[41] Wu F., Yang B. "Research on C-V2X slice random access technology", 2024 8th International Conference on Digital Signal Processing, pp. 89-95. https://doi.org/10.1145/3653876.365388

[42] Lekidis A., Morais H. “Open V2X Management Platform Cyber-Resilience and Data Privacy Mechanisms”, 19th International Conference on Availability, Reliability and Security (ARES '24), article 139, pp.1–8. https://doi.org/10.1145/3664476.3669917

[43] Bodei C., Vincezi M.D., Matteucci I. “OLIVE: Flexible, Portable, and Sustainable V2X Multi-Factor Authentication”, 39th ACM/SIGAPP Symposium on Applied Computing (SAC '24), pp. 215–217. https://doi.org/10.1145/3605098.3636102

[44] Li Y., Hou R., Lui K.S., Li H. “An MEC-based DoS Attack Detection Mechanism for C-V2X Networks”, 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1-6, doi: 10.1109/GLOCOM.2018.8647323

[45] Dolnák I., Litvik J.J. “An overview of DNS security in V2X networks”, 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), Starý Smokovec, pp. 156-159, doi: 10.1109/ICETA48886.2019.9040111.

[46] Pagadala A., Ahmed G. “Analysis of DDoS Attacks in 5G Networks”, 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10307311.

[47] Zheng T.X., Wen Y., Liu H.W., Ju Y., Wang H.M., Wong K.K., Yuan J.“Physical-Layer Security of Uplink mmWave Transmissions in Cellular V2X Networks”, IEEE Transactions on Wireless Communications, vol. 21, no. 11, pp. 9818-9833, Nov. 2022, doi: 10.1109/TWC.2022.3179706

[48] Twardokus G., Rahbari H. “Vehicle-to-Nothing? Securing C-V2X Against Protocol-Aware DoS Attacks”, IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, pp. 1629-1638,doi: 10.1109/INFOCOM48880.2022.9796667