AUSUD
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
JITSA

Derleme Makalesi

Ulaştırmanın Beşinci Modu: Hyperloop Sistemi ve Siber Güvenlik

Esma Dilek[1,*], Özgür Talih[2], Bahadır Fatih Yıldırım[3]

[1]Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Bölümü, Gazi Üniversitesi, Ankara, Türkiye
[2]Fen Bilimleri Enstitüsü, Akıllı Ulaşım Sistemleri ve Teknolojileri Tezli Yüksek Lisans Programı, Bandırma Onyedi Eylül Üniversitesi, Balıkesir, Türkiye
[3]Ulaştırma ve Lojistik Fakültesi, Ulaştırma ve Lojistik Bölümü, İstanbul Üniversitesi, İstanbul, Türkiye
*Correspondence: esma.dilek@gazi.edu.tr
DOI: 10.51513/jitsa.1511769

Özet: Hyperloop; kapsül adı verilen bileşenin manyetik kaldırma teknolojisi yardımıyla havada süzüldüğü, bir tüp içerisinde çok yüksek hızla hareket ettiği ve kapsülün kalkış ile varışlarının kontrol edildiği terminallerden oluşan yenilikçi bir kara ulaştırma modudur. Ultra yüksek hızlı, sürekli bir ulaştırma sistemi olan hyperloop; birbiri ile entegre ve birlikte çalışan birçok alt sistem içerdiğinden sağlam bir haberleşme altyapısına ihtiyaç duymaktadır. Haberleşme, entegrasyon ve dijitalleşme teknolojilerinin yoğun kullanıldığı ulaştırmanın bu modunun, emniyetli ve güvenli bir şekilde hizmet verebilmesi için hyperloop sistemini oluşturan haberleşme türlerinin siber saldırılara ve tehditlere karşı güvenli olması gerekmektedir. Bu çalışmada, hyperloop teknolojisine genel bir bakış yapılarak ulaştırmanın bu türünü oluşturan unsurların, kendi içinde ve dış dünya ile haberleşmesini sağlayan ağ altyapısı incelenmiştir. Hyperloop sistemini oluşturan haberleşme türleri, teknolojileri, ağ altyapısını oluşturan ağ katmanları ele alınarak haberleşme yöntemleri ve zorlukları değerlendirilmiştir. Hyperloop sistemini hedef alabilecek siber güvenlik saldırıları, siber güvenlik tehditleri ve risk azaltıcı stratejiler araştırılarak literatüre katkı sağlanması hedeflenmiştir. Ayrıca Türkiye'de hyperloop sistemi geliştirme girişimleri özetlenerek bu sistemin siber güvenliğini sağlamak için öneriler sunulmuştur. Bu çalışma, hyperloop teknolojisine, bu sistemi oluşturan haberleşme türlerine ve bunların siber güvenliği konularına odaklanan, güvenli bir hyperloop sistemi geliştirme çabalarına katkı sunmayı amaçlayan literatürdeki nadir çalışmalar arasındadır.

Anahtar Kelimeler: Hyperloop; haberleşme; siber güvenlik; siber saldırı; Türkiye

Fifth Mode of Transportation: Hyperloop System and Cyber Security

Abstract: Hyperloop is an innovative mode of land transport, in which the component called capsule floats in the air with the help of magnetic levitation technology, moves at very high speed in a tube and consists of terminals where the departure and arrival of the capsule are controlled. Hyperloop, which is an ultra-high-speed continuous transport system, requires a robust communication infrastructure as it includes many subsystems that are integrated with each other and work together. In order for this mode of transportation, where communication, integration and digitalization technologies are used intensively, to provide safe and secure service, the communication types that make up the hyperloop system must be secure against cyber attacks and threats. In this study, an overview of hyperloop technology is made and the network infrastructure that enables the elements that make up this mode of transport to communicate within themselves and with the outside world is examined. The communication types, technologies, network layers that make up the hyperloop system, communication methods and difficulties are evaluated. It is aimed to contribute to the literature by investigating cyber security attacks, cyber security threats and risk mitigation strategies that may target the hyperloop system. In addition, hyperloop system development initiatives in Türkiye are summarized and recommendations are presented to ensure the cyber security of this system. This study is one of the rare studies in the literature that focuses on hyperloop technology, the communication types that make up this system and their cyber security issues, aiming to contribute to the efforts to develop a secure hyperloop system.

Keywords: Hyperloop; communication; cyber security; cyber attack; Türkiye

ORCID: 0000-0002-7994-0294, 0000-0002-5899-2511, 0000-0002-0475-741X
Received 06.07.2024; Received in revised form 02.12.2024; Accepted 03.12.2024
Peer review under responsibility of Bandirma Onyedi Eylul University.

1. Giriş

Sürdürülebilir ve yaşanabilir dünya hedeflerini gerçekleştirmek için ülkelerin belirlediği yol haritalarında, farklı disiplinlere sahip birçok sektöre, oldukça önemli görevler düşmektedir. Bu doğrultuda, küresel iklim hedefleri ile sürdürülebilir şehirler ve toplumlar konusunda yoğun çalışmalar yapılan öncelikli alanlardan biri ulaştırma sektörü olup yolcu ve yüklerin taşınmasına yönelik ulaştırma hizmetlerine ve faaliyetlerine ilişkin yöntemler; gelişime, değişime ve dönüşüme açıktır. Ayrıca ulaştırma faaliyetlerinin hedefleri arasında; hız, güvenlik, emniyet, konfor, etkin maliyet gibi toplumsal ihtiyaçları ve beklentileri karşılayarak çevresel olumsuz etkilerin azaltılması ile enerji ve kaynak verimliliği konularına önem verilmesi yer almaktadır. Bu hedeflerin gerçekleşmesi ise ulaştırma ve hareketlilikte kullanılan geleneksel yöntemlerin iyileştirilmesini ve günümüzde yenilikçi yaklaşımların benimsenmesini gerektirmektedir. Özellikle havayolu taşımacılığı ile motorlu karayolu ve gemi taşımacılığı emisyonlarında meydana gelen artış, alternatif sürdürülebilir ulaştırma ve hareketlilik yöntemleri arayışlarını yoğunlaştırmıştır.

Dünya genelinde, özellikle yüksek hızlı kara yolu taşımacılığı sektöründe, toplu taşıma sistemlerinin faydalarını daha üst düzeye çıkarmak için mevcut ulaştırma sistemlerini değiştirmeye yönelik çalışmalar yapılmaktadır. Bu çerçevede son gelişmelerden biri Elon Musk tarafından tasarlanan, ultra yüksek hızlı (Mitropoulos vd., 2021), yenilikçi kara ulaştırması modu olan hyperloop sistemidir (Premsagar & Kenworthy, 2022). Özellikle son yıllarda özel sermaye yatırımlarındaki hızlı artış, hyperloop taşımacılığına yönelik araştırma ve geliştirmeler için kitle kaynak ve bazı kamu fonları oluşturulması, test pistlerinin inşası ve farklı ülkelerde ticari hatların işletilmesi projeleri, vakum tüpü taşımacılık teknolojileri ve ultra yüksek hızlı ulaşımın fizibilitesi ile performansı konularında büyük beklentiler ortaya çıkarmıştır (Hansen, 2020).

İlk kez 2013 yılında orta menzilli veya şehirler arası seyahat için yenilikçi bir ulaştırma modu olarak önerilen hyperloop teknolojisini geliştirme çalışmaları; İspanya (zeleros, 2024), Hollanda (HARDT, 2024), Amerika Birleşik Devletleri (ABD)-İsviçre (swisspod, 2024), İsviçre (euroTUBE, 2024), Kanada-Fransa (TRANSPOD, 2024), ABD-Fransa (HyperloopTT, 2024), Hindistan (DGWHyperloop, 2024), Polonya (NEVOMO, 2024), ABD (Virgin Hyperloop One), Almanya (TUM Hyperloop, 2023), İtalya (Hyperloop Italia, 2024), Çin, Birleşik Krallık (Kale, 2019), Suudi Arabistan, Rusya ve İsveç gibi birçok ülkede, özel girişimler tarafından sürdürülmektedir. Bu girişimlere ek olarak Avrupa genelinde hyperloop sistemi geliştirmek için iş birliği yapan 25'ten fazla özel sektör kuruluşu ve araştırma enstitüsünü bir araya getiren bir kamu-özel sektör ortaklığı olarak Hyperloop Geliştirme Programı (Hyperloop Development Program, 2024) geniş bir ekosistemi temsil etmektedir (Nøland, 2024). Hyperloop teknolojisinin savunucuları hem yolcu taşımacılığı hem de yük taşımacılığı bakımından zaman tasarrufu, kolaylık, hizmet kalitesi ve enerji verimliliği gibi potansiyel faydalarına işaret etmektedir. Sistem elektrikle çalışacak şekilde tasarlandığından, yenilenebilir enerji kaynaklarını kullanımını ve enerji depolamayı içeren stratejilere odaklanmaktadır (U.S. Department of Energy, 2021). Hyperloop fikri, geleneksel yük ve yolcu taşımacılığında kullanılan kara, demir, deniz ve havadan oluşan ulaştırma modları alışkanlıklarına alternatif olabilecektir. Aynı zamanda ulaştırma ve hareketlilik paradigma değişiminin benzersiz bir örneği olmaya aday bir yaklaşımdır.

Hyperloop ulaştırma sisteminin dünyanın herhangi bir yerinde inşa edilmesi kararı; sistemin sürdürülebilirlik, ekonomi, güvenlik ve yolcu taleplerine cevap verme gibi özelliklerine bağlıdır (Özbek & Çodur, 2021). Son yeniliklerle birlikte hyperloop sistemi; sürdürülebilir, kendi kendine çalışan, yüksek hızlı, güvenli ve gelecek için umut verici bir ulaştırma modu olarak tanımlanabilmektedir, ancak içerdiği eksiklikler nedeniyle değişiklik, iyileştirme ve geliştirmelere ihtiyaç bulunmaktadır (Armağan, 2020).

Hyperloop konusunda literatürde birçok araştırma bulunmakta olup farklı disiplinlerden birçok araştırmacının konuya ilgi duyduğu görülmektedir. Hyperloop sistemi ve altyapısı, tüp yapısı, tüp-kapsül ara yüzü, kapsül gibi hyperloop sisteminin fiziksel bileşenlerine ilişkin bilimsel çalışmaların olduğu gözlenmektedir. Hyperloop ağ yapıları, iletişim teknolojileri, enerji, emniyet, güvenlik, çevre gibi konularda da çeşitli araştırmalar bulunmaktadır. Hyperloop sistemine ilişkin tartışma ve gelişmeler de araştırma konusu olarak çalışılmıştır (Gkoumas, 2021).

Bu çalışmada; hyperloop sisteminde yer alan haberleşme ağı, haberleşme türleri, haberleşme teknolojileri, bu sistemi hedef alan siber güvenlik tehditleri ile risk azaltıcı stratejiler ele alınarak genel bir bakış açısıyla incelenmiştir. Hyperloop sistemi, henüz küresel olarak herhangi bir yerde tam anlamıyla işlevsel bir teknoloji olmadığından; bu sistemin faydaları, zorlukları ve karşılaşılan sorunlar, varsayımlara dayanmaktadır. Hyperloop sisteminin güvenli ve emniyetli bir şekilde yük ve yolcu taşımacılığında kullanılabilmesi amacıyla mevcut yaklaşımlar incelenmiş, hyperloop haberleşmesi ve siber güvenliğiyle ilgili literatür çalışmaları gözden geçirilmiştir.

Bu çalışmanın temel özellikleri ve önceki çalışmalardan farkları, aşağıda özetlenmiştir:

- Hyperloop teknolojisi ve fiziksel bileşenlerindeki gelişmeler, genel bir bakış açısıyla ele alınmıştır.
- Fiziksel bileşenlerin haberleşme gereksinimleri, bunu nasıl sağlayacakları ve bu kapsamdaki sınırlılıkların neler olduğu incelenmiştir.
- Hyperloop bileşenlerinin birbirleri ve dış dünya ile haberleşmesinin yanında yolcu, kullanıcı ve sürücülerin seyahatleri esnasında dijital fırsatlardan nasıl yararlanabileceği araştırılmıştır.
- Hyperloop teknolojisine yönelen siber güvenlik zafiyetleri, karşılaşılan siber saldırı türleri, kullanılan siber güvenlik standartları ve yaşanan zorluklar, bütüncül bir bakış açısıyla sunulmuştur.
- Türkiye'de hyperloop sistemi için test merkezlerinin kurulması sürecinde ya da bir pilot uygulamada; haberleşme ve siber güvenlik bileşenlerini ele alacak şekilde tasarım modelinin belirlenmesi önerilmiştir.

Bu çalışmanın geri kalan bölümü şu şekilde organize edilmiştir: İlk olarak 2. bölümde, bu çalışmada uygulanan metot özetlenmiş, 3. bölümde hyperloop teknolojisine genel bir bakış yapılarak hyperloop sisteminin haberleşme ağı, haberleşme yöntemleri, zorlukları ve çözüm önerileri incelenmiştir. Hyperloop sisteminin siber güvenliğine odaklanan 4. bölümde, siber güvenlik saldırıları ve siber riskleri azaltma stratejilerine yer verilmiştir. Son olarak 5. bölümde, sonuç ve öneriler paylaşılmıştır.

2. Metot

Bu çalışma, hyperloop teknolojisinde yer alan haberleşme sistemleri ile muhtemel siber saldırı aktörlerine ışık tutmak amacıyla literatür çalışmalarının incelenmesine dayanmaktadır. Çalışma kapsamında; Web of Science, IEEE, ProQuest, Google Scholar, DergiPark Akademik elektronik veritabanlarında "hyperloop cyber security", "hyperloop and cyber security", "hyperloop cyber attacks", "hyperloop communication systems", "cyber security performance measurement", "hyperloop siber güvenliği", "hyperloop ve siber güvenlik", "hyperloop siber saldırıları", "hyperloop haberleşme sistemleri" ve "siber güvenlik performans ölçümü" anahtar kelimeleri kullanılarak yapılan arama sonucunda ulaşılan kaynaklar ile internet üzerinden erişilebilen açık erişim kaynaklar kullanılarak inceleme yapılmıştır. Araştırmalardan elde edilen sonuçlara ve değerlendirmelere çalışmada yer verilmiş, literatürdeki güncel çalışmalar ve sektörel gelişmeler göz önünde bulundurulmuştur.

3. Hyperloop teknolojisine genel bir bakış

Genellikle yeni bir ulaştırma sistemine büyük bir yatırım yapıldığı durumlarda, aynı ölçüde ölçülebilir getirisi ve faydalarının olması beklenmektedir. Mevcut ve alternatif ulaştırma modları ile kıyaslandığında, hyperloop sisteminin; güvenlik, emniyet, hız, düşük maliyet, konfor gibi faydalarının daha fazla olmasının yanında; hava koşullarına karşı dirençlilik, depreme karşı dayanıklılık, güzergâh üzerinde bulunan varlıklar için zararsız olma ve sürdürülebilir bir şekilde kendi enerjisini sağlayabilme özellikleriyle çok daha efektif bir ulaştırma sistemi olması beklenmektedir. Kara, hava, demir ve denizyolunda kullanılan mevcut araçlar ve altyapının ötesinde, bu kriterleri karşılayabilen ve uygulanabilir olan hyperloop teknolojisi, ulaştırmanın beşinci modu olarak ortaya çıkmıştır (Musk, 2013).

Hyperloop sistemi, ilk olarak 1904 yılında mucit ve roket bilimci Robert Goddard tarafından, Massachusetts'teki Worcester Politeknik Enstitüsü'nde birinci sınıf fizik öğrencisiyken bir vakum tüplü tren fikri olarak ortaya çıkmıştır (Li vd., 2024). Fikir, 1906 yılında Scientific American'a sunulmuş olup

1972-1978 yıllarında Amerikalı fizikçi Robert M. Salter, son olarak da 2013 yılında Elon Musk tarafından ele alınmıştır. Bu konuda başka girişimler de bulunmaktadır, ancak Musk'ın önerisine en yakın olanı Salter'in yaklaşımıdır. Salter'in önerileri, farklı olarak proje inşaatına ilişkin tahminleri ve 1972-1978 yılları için gelir elde etmek ve maliyetleri dengelemek amacıyla yolculara ödenecek nakliye ücretlerini de içermektedir (Thompson, 2019). Elon Musk'ın buradaki temel amacı, vakumlu boru hattıyla ulaştırma konsepti ortaya koymak olduğundan, Hyperloop One'ı kurarak maglev kapsül treninin vakum ortamında tam ölçekli bir testini tamamlamıştır. Akabinde Southwest Jiaotong Üniversitesi, 2014 yılında dünyanın ilk vakum tüplü ultra yüksek hızlı maglev tren prototip test platformunu geliştirmiş, AviChina tarafından 2017 yılında "*yüksek hızlı uçan tren*" projesi başlatılmış ve Hyperloop Ulaştırma Teknolojisi (Hyperloop Transportation Technologies, HyperloopTT) (HyperloopTT, 2024), 2018 yılında, Çin'in ilk ticari vakum tüp ultra-yüksek hızlı demiryolu hattının Tongren'de inşa edileceğini duyurmuştur. Vakumlu tüp trenler için günümüze kadar ulaşan normal elektromanyetik kaldırma düzeni, pnömatik/kalıcı manyetik kaldırma düzeni ve yüksek sıcaklıkta süper iletken manyetik kaldırma düzeninden oluşan üç ana teknik çözüm bulunmaktadır (Li vd., 2024).

Hyperloop sistemi; Los Angeles-California ve San Francisco-California arasındaki mesafeyi, 35 dakikalık bir sürede katetmek için bir ulaştırma ve hareketlilik konsepti olarak önerilerek 2013 tarihli, alfa seviyedeki bir tasarım dokümanı ile Elon Musk tarafından ortaya koyulmuştur. Hyperloop sistemi, tüpün uzunluğu boyunca hem düşük hem de yüksek hızlarda taşınan kapsüllerin bulunduğu, düşük basınçlı bir tüpten oluşmaktadır. Kapsüller, basınçlı hava ve aerodinamik kaldırma özelliğine sahip bir hava yastığı üzerinde taşınmaktadır. Kapsüller, her kapsülde bulunan döndürücülerle düşük basınçlı tüp üzerinde, çeşitli istasyonlarda sabitlenmiş manyetik bir doğrusal ivmelendirici aracılığıyla hızlandırılmaktadır. Hyperloop aracına tüpün uçlarında bulunan istasyonlardan ya da tüp uzunluğu boyunca uzanan bölümlerden giriş-çıkış yapılabilmektedir (Musk, 2013).

Hyperloop ulaştırma teknolojisi henüz kavramsal aşamada olsa da bu sistem, performansı yüksek hızlı demiryolu ve hava taşımacılığı sisteminden daha üstün olabilir ve aynı zamanda seyahat süresini, nakliye maliyetlerini ve enerji tüketimini azaltabilme potansiyeline sahiptir.

Hyperloop vakum treni, (i) manyetik veya hava levitasyonu, (ii) doğrusal motor bölümü ve (iii) vakum tabanlı taşıma sisteminden oluşan üç temel parçaya dayanmaktadır. Ulaştırmanın bu teknolojisindeki temel unsurları; biri ileri, diğeri tam tersi yönde hareket eden iki tüp ve yolcuların taşınmasında kullanılan kapsüller oluşturmaktadır (Rob vd., 2019). Sistem; birçok farklı bileşen içermekte olup kapsül, tüp, tahrik sistemi, altyapı ile coğrafi ve geometrik yapıyı temsil eden rota, bunların en temel olanlarıdır (Musk, 2013). Kapsül (pod), sistemin ana omurgasıdır ve bir uçak gövdesine benzemekte olup yolcuların konfor ve emniyeti düşünülerek tasarlanmış iç mekân ve güç sistemi temel bileşenlerinden oluşmaktadır. Altyapı bileşenini ise kapsülü tüm çevresel koşullara karşı koruyan tüp, noktadan noktaya bağlantıyı sağlayan yüksek hızlı anahtarlar, sürgülü valflerle donatılmış hava kilitleri, basınç bakım sistemi, levitasyon arayüzleri, tahrik ya da itki ara yüzleri gibi cihazlar oluşturmaktadır (Delft Hyperloop, 2019; Mitropoulos vd., 2021). Ayrıca haberleşme sistemi ve test pistleri de hyperloop teknolojisinin gelişiminin önemli unsurlarıdır (Mitropoulos vd., 2021).

Geliştirilme çalışmaları devam eden yenilikçi ulaştırma modu olan hyperloop, olumsuz hava şartlarından veya diğer dış koşullardan korunmayı sağlayan ve çok yüksek hızlarda emniyetli bir seyahati mümkün hale getiren, düşük basınçlı ortam veya manyetik levitasyon gibi yeni ya da gelişmekte olan teknolojileri içermektedir (CEN, 2023). Bu teknoloji, bir demiryolu ulaşım hizmetinin 1.200 km/saat potansiyel hızda çalışmasını sağlayabilmektedir. Hyperloop ulaştırma modunun iddialı hız hedefi, zaman-mekân boyutunu küçültme potansiyeline sahiptir; böylece birbirine uzak şehirleri, büyük ölçüde kısaltılmış seyahat süreleriyle daha erişilebilir hale getirebilmektedir (Premsagar & Kenworthy, 2022).

Hyperloop teknolojisinin küresel ölçekte, henüz uygulanan tam bir örneğinin olmaması, birçok etkisinin araştırılması ve karşılaştırılması noktasında, sınırlılıklar ortaya çıkarmaktadır. Bu ulaştırma ve hareketlilik yönteminin fiziksel, teknik, ekonomik, çevresel etkileri ile enerji, hız, konfor, insan ve ulaşım planlaması gibi konularda potansiyel etkilerinin kapsamlı değerlendirilmesi, değişkenlerin kısıtlı olması nedeniyle henüz varsayım olarak kalabilmektedir. Bu varsayımlar, bu etkilerin olumlu ve olumsuz yanlarını içerebilmektedir (Premsagar & Kenworthy, 2022). Örneğin çevresel etki tartışmaları,

operasyonlar sırasındaki emisyonlara odaklanma eğilimindedir ve güzergâh inşası sırasındaki tüm diğer yaşam döngüsü emisyonlarını göz ardı edebilmektedir. Ayrıca hyperloop sisteminin sunduğu çok yüksek hızların, yolcular için konforlu olup olmayacağı henüz netlik kazanmamıştır (Catherine vd., 2016). Diğer taraftan hyperloop teknolojisi geliştirme çalışmaları halen devam etmektedir. Farklı girişimciler ve şirketler; 700 km/saat'in üzerinde, henüz tam ölçekte veya ses hızına yaklaşan yüksek seyir hızları için test edilmemiş çözümler üzerinde çalışmaktadır. Hyperloop sisteminin geleceğe yönelik konsepti; şu anda emniyet, güvenlik, mühendislik açısından uygulanabilirlik ve ekonomik yapılabilirlikle ilgili endişeler nedeniyle zorluklar içermektedir. Kapsül başına düşen yolcu sayısı da açık bir konudur; zira daha büyük araçlar daha fazla iş hacmi oluştururken, daha küçük araçların tasarımı daha kolay olmakla birlikte, her bir kapsül arasındaki mesafenin daha kısa olmasını telafi etmek durumunda kalınacaktır (Nøland, 2024).

Hyperloop sisteminin potansiyeline ilişkin ilk tartışmalar, yolcu taşımacılığına odaklanarak yük taşımacılığını ikinci plana atarken, hyperloop şirketleri tarafından sağlanan daha yeni bilgiler ise yük taşımacılığına odaklanmaktadır. Böyle bir gelişme belki de petrol, doğal gaz ve su gibi belirli gaz ve sıvı maddelerin taşınmasında boru hatlarının oynadığı mevcut rolün doğal bir uzantısıdır. Köprü inşa etmeyi engelleyen mesafelerde, su üzerindeki kargo sevkiyatı için yalnızca yüksek maliyetli, ancak hızlı hava taşımacılığı ile uygun maliyetli, ancak yavaş deniz yolu taşımacılığı kullanılmaktadır. Bu açıdan bakıldığında, lojistik faaliyetleri için de ilave bir taşıma moduna ihtiyaç bulunmaktadır. Kargo taşımacılığı için süper yüksek hızlar, kendi başlarına hyperloop sisteminin zorlayıcı özelliği olmamakla birlikte; belirli bir tüp boyutu için daha yüksek verim sağlayabilmektedir (Catherine vd., 2016). Hyperloop yük ve yolcu taşımacılığı konsepti; günümüzde, daha kısa seyahat süresi ve yolcu gelir kilometresi başına daha düşük yakıt tüketimi vaat edebilen kısa mesafeli uçak yolculukları için potansiyel bir alternatif olarak görülmektedir (Nøland, 2021).

Hyperloop teknolojisinin geliştirilmesi, projelendirilerek hizmete sunulabilmesi için standartların belirlenmesi ve topolojinin çıkarılması önemli bir husustur. Avrupa Standardizasyon Komitesi (European Committee for Standardization, CEN) ve Avrupa Elektroteknik Standardizasyon Komitesi (European Committee for Electrotechnical Standardization, CLC, CENELEC) tarafından yayınlanan CEN/CLC/TR 17912:2023, bu teknolojide yer alan sistemlere ilişkin bir standardizasyon yol haritası sunmaktadır. Yol haritası, çeşitli alanlardan uygulanabilir standartlar, değiştirilmesi gerekenler ve yeni geliştirilebilecekler hakkında rehberlik etmektedir (CEN, 2023).

Hyperloop sistemi, dünyadaki gelişmelerin yanında, Türkiye'de henüz yeni bir kavram olarak araştırma kurumları, akademi ve özel sektör tarafından üzerinde çalışmalar yapılan bir teknolojidir. Bu doğrultuda, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Raylı Ulaşım Teknolojileri Enstitüsü (TÜBİTAK RUTE) tarafından başta üniversite öğrencilerinin projeleri olmak üzere akademik çalışmalar, yenilikçi ulaştırma teknolojilerinin geliştirilmesi ve araştırılması çerçevesinde desteklenmektedir. TÜBİTAK RUTE öncülüğünde, hyperloop geliştirme yarışma kategorisi, TEKNOFEST kapsamında ilk defa 2022 yılında gündeme gelmiş olup manyetik levitasyon teknolojileri, sürtünmenin etkisinin azaltıldığı yenilikçi ulaştırma araçlarının geliştirilmesi ve yeni nesil ulaştırma teknolojileri konularında lisans ve lisansüstü öğrencilerinde farkındalık oluşturulması amaçlanmaktadır. Gazi Üniversitesi TURKUAZ, Selçuk Üniversitesi SÜ Kapsül Hyperloop ve Yeditepe Üniversitesi HyperHawk, 2022 yılındaki yarışmada sırasıyla ilk üçe giren takımlar olmuştur. Hyperloop geliştirme yarışmasında 2023 yılında ise sırasıyla Selçuk Üniversitesi Selçuk Kapsül Hyperloop ve Gebze Teknik Üniversitesi Alfa ETA-H takımları, ilk ikiye girerken Yeditepe Üniversitesi HyperHawk ve İstanbul Teknik Üniversitesi HyperBee üçüncülüğü paylaşmıştır (TEKNOFEST, 2022). TÜBİTAK tarafından düzenlenen Hyperloop Geliştirme Yarışmasının üçüncüsü ise TÜBİTAK Gebze Yerleşkesi'nde gerçekleştirilmiştir (TEKNOFEST, 2024).

Gazi Üniversitesi bünyesinde 2022 yılında kurulan Turkuaz Hyperloop ekibi tarafından yüksek hızlı bir hyperloop aracı tasarlanmıştır. Bu tasarımda; kesintisiz haberleşme ve tam otonom sürüşe olanak sağlayan yer kontrol ara yüzü, fotoelektrik sensörlerle tünel içinde hassas konum takibi, pnömatik ve rejeneratif fren sistemi, çok noktalı çekiş ve tork kontrolü bulunmaktadır (Gazi Üniversitesi, 2022).

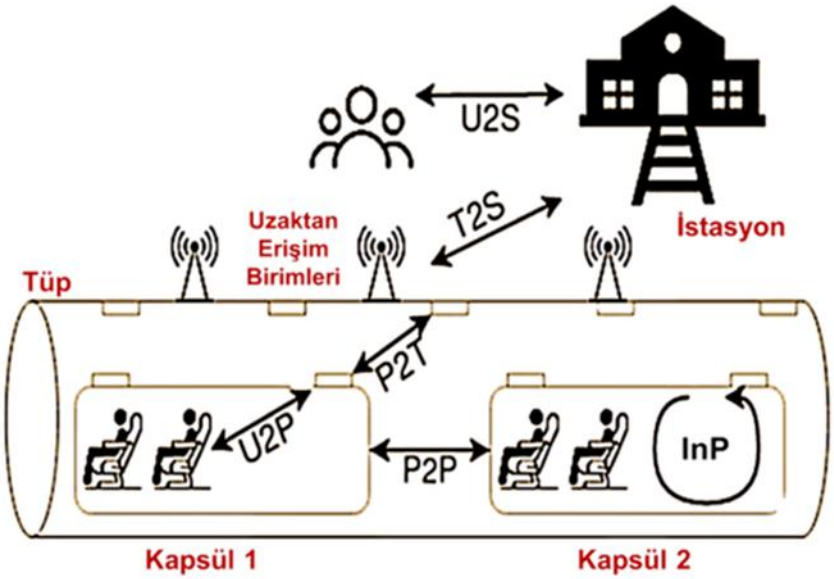
Türkiye'de hyperloop teknolojisinin gelişiminde yatırımcı ve tedarikçi rolü olan özel sektör kuruluşları da bulunmaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020). Erciyas Holding, 2017

yılından bu yana iş birliğinde olduğu, merkezi ABD'de bulunan HyperloopTT şirketiyle 2022 yılında imzaladığı anlaşma (UTİKAD, 2022) sayesinde, Hyperloop teknolojisi ile yolcu ve kargo taşımacılığı projesinin tedarikçisi ve yatırımcısı olmuştur (PLATİN, 2023).

Sonuç olarak dünyadaki gelişmeler incelediğinde, hyperloop sisteminin Avrupa ülkelerinde önemli ölçüde gelişme gösterdiği, ancak maglev konusundaki uzmanlığın genel olarak Asya ülkelerinde olduğu gözlenmektedir. Asya ülkeleri, aynı zamanda hyperloop uygulamaları ve gösterimlerine ev sahipliği yapmaktadır. Bu nedenle, arzu edilen hedef hızlarda bir hyperloop ulaştırma sisteminin hayata geçirilmesinde karşılaşılan önemli teknik ve mali zorluklarının üstesinden gelebilmek için bilgi transferi yapmak oldukça önemlidir. Ayrıca hyperloop geliştirme çalışmalarında, çok sayıda temel deneysel araştırmanın da göz ardı edilmemesi gerekmektedir (Nøland, 2024).

3.1. Hyperloop sisteminde haberleşme türleri ve ağ altyapısının incelenmesi

Hyperloop ulaştırma modunun, kapalı ve kısmi vakumlu tüplerde çalışan kapsül gibi bileşenleriyle çok yüksek hızlı, sabit rotalı, şehirler arası kara taşımacılığına yönelik bir konsept olma potansiyeli bulunmaktadır (Catherine vd., 2016). Bu ulaşım teknolojisindeki otonom kapsüller birbirleriyle, kontrol merkeziyle ve dış dünyayla sürekli iletişim halindedir. Veri ve bilgi iletimini yönetmek için sistem altyapısı tarafından çeşitli yöntemler kullanılmaktadır (Delft Hyperloop, 2020). Hyperloop teknolojisindeki bileşenler ve haberleşme türleri, Şekil 1'de gösterilmiş ve aşağıda özetlenmiştir (Brighente vd., 2022, 2024).

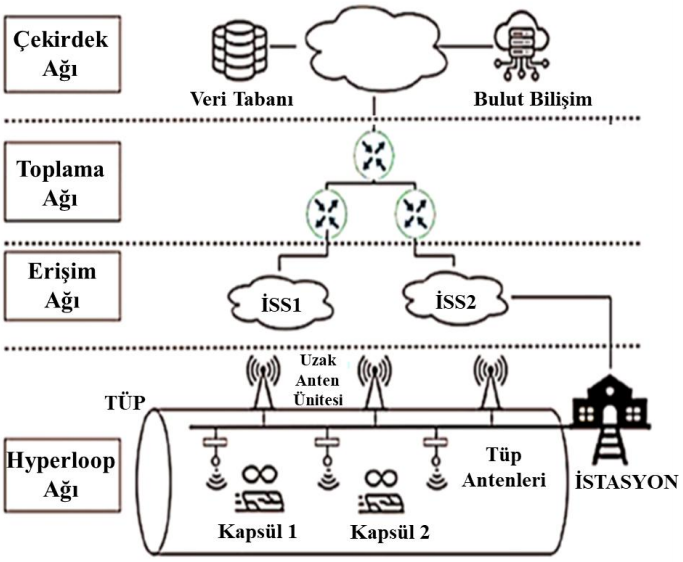


Şekil 1. Hyperloop sisteminde haberleşme türleri

- ***Kapsülden Kapsüle (Pod-to-Pod, P2P)***: Çarpışmalardan kaçınmak için kapsüllerin birbirlerinin varlığını ve göreceli konumunu tespit etmesi gerekmektedir. Bu amaçla kapsüller, konumları ve hızları hakkındaki bilgileri karşılıklı paylaşabilmektedir. Yüksek hızlı kapsüller arasında veri iletimi, araçtan araca haberleşme için kullanılan tahsis edilmiş kısa mesafeli haberleşme (Dedicated Short Range Communications, DSRC) benzeri ad-hoc protokollerle desteklenebilir.
- ***Kapsülden Tüpe (Pod-to-Tube, P2T)***: P2T bağlantısı sayesinde tüp, kapsülün hareket ve manevrasını yapabilmesi için gereken manyetik veya hava kuvvetlerini kontrol edebilir ve yönetebilir. Bunun tersi olarak kapsül, yerleşik (onboard) motor tarafından üretilen hareket için manyetik veya hava kuvvetlerini uygulayabilir. Bu durum, altyapı ve yolcuların güvenliği açısından büyük ihtimam gerektirebilir. P2T bağlantısı, kapsülün durumu ve konumu hakkında bilgi paylaşmak için de kullanılabilir. Bu bilgiler, basınç düzenlemesi ile motor yönetimi gibi amaçlar doğrultusunda merkez istasyona tüpten istasyona (T2S) bağlantısı sayesinde iletilebilir.

- ***Tüpten İstasyona (Tube-to-Station, T2S)***: Kapsüllerin bir istasyondan diğerine güvenli bir şekilde seyahat edebilmesini sağlamak için tüpün faaliyetlerinin merkezi bir birim tarafından yönetilmesi gerekmektedir. Bu faaliyetler arasında, yakın vakum ortamı tesis eden vanaların çalıştırılması ve ihtiyaç halinde acil çıkışların açılması gibi durumlar yer almaktadır. Bununla birlikte kapsüllerin planlanan zamanlara göre hareketinin sağlanması ve raporlamaların yapılması, tüpün görevleri arasındadır. T2S bağlantısı, gecikme süresi ve güvenilirlik açısından gereksinimlere bağlı olarak kablolu veya kablosuz olabilir.
- ***Kullanıcıdan Kapsüle (User-to-Pod, U2P)***: Seyahat sırasında bilgi-eğlence sistemi hizmeti sunabilmek için kapsül dahili bir kablosuz ağ altyapısı ile donatılmıştır. Böylece kullanıcılar yolculuk durumu, mevcut konumları ve beklenen varış zamanı ile ilgili bilgileri alabilmekte, ayrıca internete erişebilmektedir. Bu bağlantı, tüp boyunca kurulmuş olan uzaktan erişim birimleri (Remote Access Units) sayesinde internete erişim sağlayan P2T haberleşmesi ile garanti edilmektedir. Birçok erişim noktası, internet erişimi sağlayan çekirdek ağa bağlanabilmek için yerel bir internet servis sağlayıcısına (İSS'ye) bağlanmaktadır.
- ***Kapsül İçi Haberleşme (In-Pod Communication, InP)***: Her bir kapsül, denetleyicilerin ve çalıştırıcıların, temel kapsül fonksiyonlarını düzenlediği dahili bir ağ altyapısı ile donatılmıştır. Tüm bu birimler, güvenliği sağlamak için verileri sürekli olarak izleyen kapsül güvenlik denetleyicisine bağlıdır. Bu ağ altyapısı, aynı zamanda kapsülün farklı bileşenlerine güç sağlamak için de kullanılmaktadır.
- ***Kullanıcıdan İstasyona ve İstasyondaki Erişilebilen Tüm Cihazlara (User-to-Station, U2S)***: Hyperloop sistemi çerçevesinde istasyon, kullanıcılar ve altyapı arasındaki haberleşmenin kapsamı önemli bir durumdur. Kullanıcılar, akıllı cihaz ve uygulamalar sayesinde bu sistemle, ihtiyaçları çerçevesinde çeşitli şekillerde iletişime geçebilir. Bu doğrultuda bilet satın alma işlemi için kapsüllerdeki koltukların uygunluk durumunu gerçek zamanlı olarak doğrulayan ad-hoc terminallerden yararlanılabilir. Turnikeler, kullanıcıların yolculuk alanına erişimini yönetmek ve erişimi kolaylaştırmak için kullanıcıların biyometrik bilgilerini kullanabilir. Ekranlar, kapsüller için gecikmeleri ve kalkış saatlerini göstererek kullanıcıların uygun kapıyı bulmalarına yardımcı olabilir. U2S haberleşme kapsamında, kullanıcıların uzaktan bilet satın almalarını ya da rezervasyon yapabilmelerini sağlayan uygulamalar ve internet hizmetleri de bulunmaktadır.

Hyperloop sistemi ağ altyapısını (i) çekirdek (core), (ii) toplama (aggregation), (iii) erişim (access) ve (iv) hyperloop ağı olmak üzere dört ana katmana ayırmak mümkündür (Brighente vd., 2022, 2024; Hedhly vd., 2021; T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020). Hyperloop ağ altyapısını oluşturan katmanlar Şekil 2'de gösterilmiştir (Brighente vd., 2022, 2024; Hedhly vd., 2021).



Şekil 2. Hyperloop ağ altyapısını oluşturan ağ katmanları

Erişim ağı katmanı, toplama ağı ve hyperloop ağını birbirine bağlamakta olup aynı zamanda tüp boyunca yerleştirilen, uzaktan iletimi destekleyen çeşitli uzak anten birimleri (Remote Antenna Units, RAU) arasındaki bilgilerin toplanmasından ve bunların bir veya daha fazla İSS'ye bağlanmasından sorumludur. Tüpün uzunluğunun farklı ülke sınırları boyunca uzanabiliyor olması nedeniyle coğrafi bölgeye göre İSS'ler de farklılık gösterebilmektedir (Brighente vd., 2022, 2024). Ağın ön kısmını oluşturan ve doğrudan kullanıcı ekipmanına, yani hyperloop trenine bağlı olan bu katman; sinyallerin alımı ve iletimi, kodlama ve kod çözme, modülasyon ve demodülasyon gibi işlevleri yürütmektedir. Başta uydu iletişimi, kablosuz veri ve hücresel ağlar olmak üzere çeşitli teknolojiler kullanarak çalışan bu katmanda benimsenen teknolojiye bağlı olarak bu işlevler, tek bir birimde yürütülebilmekte veya üniteler arasında dağıtılabilmektedir (Hedhly vd., 2021).

Toplama ağı, farklı İSS'ler arasındaki bilgileri toplayıp yönlendirerek erişim ağını çekirdek ağa bağlamaktadır. Ağda, yaklaşan paketlerin bir paket anahtarlama işleminin ardından hedeflerine iletildiği bir kavşağı temsil etmektedir (Hedhly vd., 2021). Ethernet ve fiber optik (Fokum & Frost, 2010) ile asimetrik sayısal abone hattı (Asymmetric Digital Subscriber Line, ADSL), Wi-Fi bu katmanda kullanılan haberleşme teknolojileri arasındadır (Brighente vd., 2022, 2024).

Çekirdek ağı veya omurga ağ, ağın farklı bileşenlerini birbirine bağlayan (Brighente vd., 2022, 2024) ve ara bağlantı kuran kısımdır (Hedhly vd., 2021). Bu ağ, aynı zamanda hesaplama işlemleri için veri tabanı, bulut gibi çeşitli hizmetlere erişim sağlamaktan sorumludur (Brighente vd., 2022, 2024).

Hyperloop ağı, tüp ve seyahat kapsülünden oluşmaktadır. Erişim ağı ile tüp arasındaki haberleşme, hızlı iletişim ve kısa gecikme gereksinimlerini karşılamak için kablosuz veya kablolu olabilmektedir. Antenler, tüpün tavanına yerleştirilmektedir ve transfer sürecini kolaylaştırmak ya da bu sürece yardımcı olmak için kapsülün üzerine yerleştirilen bir veya iki antenle iletişim kurmaktadır. Tren kontrol ünitesinden ve yolcuların kişisel cihazlarından gelen sinyaller, kapsül duvarları üzerinden iletim sırasında sinyallerin zayıflamasını önlemek için kapsülün içine monte edilen tren erişim terminali tarafından alınmaktadır (Hedhly vd., 2021).

Hyperloop kapsülleri, kablosuz haberleşme sistemlerini ve yerel alan ağı (Local Area Network, LAN) altyapısını kullanarak birden fazla varlıkla iletişim kurabilmektedir. Araçtan her şeye (Vehicle-to-Everything, V2X) konseptini benimseyen bir kapsülden her şeye (Capsule-to-Everything, C2X) haberleşme çerçevesi, bilgilerin iletilmesi için omurga sağlayacaktır. C2X sistemi; kapsülden altyapıya (Capsule-to-Infrastructure, C2I), kapsülden şebekeye (Capsule-to-Grid, C2G), kapsülden yolcuya (Capsule-to-Pedestrian, C2P), kapsülden kapsüle (Capsule-to-Capsule, C2C) ve kapsülden ağa (Capsule-to-Network, C2N) gibi diğer daha spesifik haberleşme türlerini içermektedir. C2X, kablosuz yerel alan ağı (Wireless Local Area Network, WLAN)/Wi-Fi 6 ve beşinci nesil hücresel yeni radyo (5G New Radio, 5G NR) gibi temel haberleşme teknolojileri tarafından desteklenebilir (Tavsanoglu vd., 2021).

Bir haberleşme sisteminin istenilen verimlilikte çalışabilmesi için bant genişliği, internet hızı ve gecikme süreleriyle ilgili minimum sistem özelliklerini karşılaması önemlidir. Hyperloop teknolojisini oluşturan tüm cihazların ve bileşenlerin haberleşmesinin sağlanmasında kullanılan bant genişliği, verilerin gerçek zamanlı iletimi ve gönderilen sinyallere verilen cevaplar arasındaki zaman farkının minimum seviyelerde olması, ulaştırma sisteminin konforu, güvenliği ve emniyeti için gereklidir. Hyperloop hızında haberleşme ihtiyacını ve teknolojilerini destekleyecek kablosuz iki temel standart, (i) 5G NR ve (ii) 802.11ax ağları (Tavsanoglu vd., 2021) olarak değerlendirilebilmektedir. Bu nedenle mevcut hyperloop altyapısında, dahili antenler ve kapsüller arasında, bu standartların kullanılmaları muhtemeldir.

Hyperloop ulaştırma modunun çok yüksek hız ve benzersiz teknolojik altyapısı göz önüne alındığında, hyperloop haberleşme sisteminin performansı; seyahat emniyeti ve güvenliği açısından önem arz etmektedir. Hyperloop sisteminin düzgün ve verimli çalışması da haberleşme sisteminin çalışmasından doğrudan etkilenebilmektedir. Bu çerçevede, hyperloop ulaştırma sisteminin haberleşmesinde göz önünde bulundurulması gereken farklı boyutları ele alan bir sınıflandırma modeli, Şekil 3'te yer almaktadır (Hedhly vd., 2021).

Şekil 3. Hyperloop sistemi haberleşmesinde farklı boyutlar

3.2. Hyperloop sistemi haberleşme yöntemlerinin zorlukları ve çözüm önerileri

Hyperloop sisteminde kapsüller ve altyapı haberleşmesi çerçevesinde, yüksek hızlı bağlantının kurulması, kapsül haberleşmesi ve verilerin toplanması gibi bazı zorluklar bulunmaktadır (Delft Hyperloop, 2019; Mitropoulos vd., 2021; Qiu vd., 2020; Tavsanoglu vd., 2021; Zhang vd., 2020). Ayrıca bu sistemlerde kablosuz haberleşme tasarımında; tüpteki yayılma özellikleri, hızlı ve sık devirler, doppler frekans kayması, yüksek penetrasyon kaybı ve frekans spektrumsuz ortam gibi konular, temel zorlukları oluşturmaktadır (Qiu vd., 2020).

Yüksek hızlar nedeniyle hyperloop sistemi kapsülleri, genellikle haberleşme hücreleri arasında geçiş yapmaktadır ve bu işlem devir (handover) olarak adlandırılmaktadır. Yüksek devir sıklığı, devir hatası olasılığını artırarak geçici bir haberleşme kaybına neden olabilmektedir. Bu nedenle hyperloop haberleşme sistemi, güvenilir devir yeteneklerine sahip olmalıdır. Ayrıca, hyperloop sisteminde yer alan çelik boru, kablosuz sinyallerin kapsüle ulaşmasını engelleyebileceğinden, bu sorunu aşmak için haberleşme sistemi hem kablolu hem de kablosuz çözümleri bir araya getirmektedir (Delft Hyperloop, 2020).

Vakum tüplü trenler için tren ve yer arası kablosuz haberleşme kapsamında, frekans değişimi ve şiddetli doppler etkisinin ortaya çıkarması muhtemel olan sorunların üstesinden gelmek amacıyla mobil hücreye ve sızıntı dalga kılavuzuna dayalı, çok seviyeli bir kablosuz veri iletim mimarisi kullanılabilmektedir. Bu mimaride, vakum tüplü ultra yüksek hızlı tren kablosuz haberleşme sistemi için uygun olan devir gecikmesinin etkili bir şekilde azaltılabildiği ve aktarım gücünün artırılabildiği, simülasyonlar ile doğrulanabilmektedir (Li vd., 2024).

Yüksek hızlı demiryollarında kullanılan mevcut haberleşme sistemleri ve teknolojileri arasında yer alan sinyalizasyon sistemleri, mobil iletişim için küresel sistem (GSM), üçüncü nesil (3G) ve dördüncü nesil (4G) haberleşme sistemleri (Gheth vd., 2021), hyperloop sisteminin hız seviyeleri ve güvenilirlik gereksinimleri için uygun performansa sahip olmayabilir. Buradaki başlıca zorluk, kapsül ile dış dünya arasında veri alışverişi için gerekli olan haberleşmenin sağlanmasıyla ilgili ihtiyaçtan kaynaklanmaktadır. Fiber optik altyapının iyileştirilmesi ve 5G gibi yeni haberleşme protokollerinin geliştirilmesi, bu zorluklara çözüm olarak değerlendirilmektedir. Ancak yeni teknolojilerin gelişimi belirsiz olduğundan, mevcut teknolojilerin yüksek hızlı ulaştırma faaliyetlerine uygun hale getirilmesi ve iyileştirilmesinde fayda bulunmaktadır (Delft Hyperloop, 2019).

Hyperloop sistemi için haberleşme çözümlerinde doppler etkisi, sık devirler gibi sebeplerle ortaya çıkması muhtemel zorlukların üstesinden gelebilecek yaklaşımlar geliştirmek önemlidir. Bu doğrultuda hyperloop haberleşmesine yönelik olası çözümler (i) anten, (ii) radyo, (iii) ağ ve (iv) yazılım tabanlı çözümler olmak üzere dört temel kategoriye ayrılabilir. Bunun yanında hyperloop haberleşmesini

sağlamak için milimetre dalga ve terahertz teknolojisi ile boş alan (free space) optik haberleşmesi gibi bazı yeni teknolojiler potansiyel olabilir (Hedhly vd., 2021). GSM-R (Global System for Mobile Communications-Railway), yüksek hızlı tren için birincil haberleşme teknolojisi tercihi olmakla birlikte, uzun süreli gelişim (Long Term Evolution, LTE), kullanılan diğer bir yöntemdir (Delft Hyperloop, 2019; Sniady & Soler, 2014) ve hyperloop için de uygun olması muhtemel haberleşme teknolojileri arasındadır.

Demiryolu ortamlarında olduğu gibi hyperloop sistemi boyunca, belirli aralıklarla yerleştirilen özel antenler ile bir radyo ve fiber haberleşme ağının en son 802.11 Wi-Fi standartlarını kullanarak kapsülde kurulu bir donanım ile iletişime geçilebilmektedir. Yüksek bant genişliğine sahip bu kablosuz ağ bağlantısı, daha sonra kapsülün yerleşik ağı aracılığıyla yolculara ve yerleşik sistemlere iletilmektedir (Icomera, t.y.; Mitropoulos vd., 2021). Hyperloop kablosuz iletişim sisteminin kurulumu ve performans analizi için kesin ve ayrıntılı geniş bant kablosuz kanal karakterizasyonu ön koşul olup ayrıca daha ileri düzeyde haberleşme teknolojilerinin ve kaynak yönetiminin etkili bir şekilde değerlendirilmesini sağlamaktadır (Zhang vd., 2020).

4. Hyperloop sisteminde siber güvenliğe genel bir bakış

Ulaştırma altyapıları ve sistemleri, siber saldırılar çerçevesinde ele alındığında, nüfus ve çevre için felaketle sonuçlanabilecek güvenlik sorunlarını içeren kritik altyapılardır. Hyperloop ulaştırma modunun temsil ettiği kritik altyapının ve sistemin performans gereksinimleri dolayısıyla güvenlik ve emniyet konularının dikkatli bir şekilde ele alınması gerekmektedir (Brighente vd., 2024). Bu yenilikçi ulaştırma modunda, mevcut ulaştırma modlarında tecrübe edilenlerin yanında, kendine özgü muhtemel güvenlik sorunlarının öngörülmesi gerekmektedir. Hyperloop sisteminin haberleşmesi ve güvenliği konusunda altyapı, tüp, kapsül ve ara yüzler gibi bileşenler arasındaki ilişkilerin iyi tanımlanması ve fonksiyonel prosedürlerin belirlenmesine ihtiyaç duyulmaktadır.

Ulaştırma ağının içinde olduğu kritik altyapılar, çoğunlukla siber saldırılara açık (Gkoumas & Christou, 2020) olup hyperloop teknolojisindeki muhtemel siber güvenlik zafiyetlerinin, sistemi oluşturan insan unsuru dahil olmak üzere tüm bileşenler arasındaki haberleşmeden kaynaklanabileceği değerlendirilmektedir. Uzun mesafelerin izlenebilirliği zorlaştırması ve muhtemel siber saldırıların ciddi sonuçlarının olabilmesi nedeniyle hyperloop sisteminde siber güvenliğe ilişkin tüm risklerin adreslenmesine ve azaltılmasına yönelik tedbirlerin alınması önem arz etmektedir.

4.1. Siber saldırı türleri

Hyperloop sistemlerine yönelebilecek siber saldırı türlerinden bazıları, potansiyel etkileri ve güvenlik önlemleri aşağıda özetlenmiştir (Brighente vd., 2022, 2024; Turrin, 2023):

- *Hizmet Reddi (Denial of Service, DoS) saldırısı*, makineler arasındaki iletişimi bozmak için sistem kaynaklarını aşırı tüketerek cihazları kullanılamaz hale getirir. Genellikle yaygın bir teknik, paket taşmasıdır (flooding) ve paketler birçok farklı kaynaktan üretilirse, bu durum dağıtık hizmet reddi (Distributed Denial of Service, DDoS) olarak tanımlanır. Bu saldırı, bazı cihazları durdurarak kullanılamaz hale getirebilir ve endüstriyel kontrol sistemlerinde (EKS'de) beklenmedik davranışlara yol açabilir. Endüstriyel cihazlar genellikle eski ve düşük hesaplama gücüne sahip olduğundan, düşük miktarda paket taşması, normal işleyişlerini durdurabilir. DoS saldırısı, hyperloop bilgi-eğlence sisteminin kesintiye uğramasına ve güvenlik açısından kritik veri akışlarının gecikmesine yol açabilir. Ayrıca bir DoS saldırısı paket alışverişini engelleyebilir, öngörülemeyen bir enerji aktarım davranışına yol açabilir veya bundan yararlanacak kapsül sayısını sınırlayabilir. Kötü niyetli bir kullanıcı, diğer kullanıcıların sistemi kullanmasını engellemek için bir DoS saldırısı oluşturabilir. Kapsül; tüpün içinde korumalı olduğundan, bu iletişim kanalının zarar görmesi, tüpün dışındaki tüm haberleşmenin durdurulması anlamına gelebilir. Ayrıca kötü niyetli bir aktör, kısıtlamaları aşmak için başka bir kullanıcının kimliğini ele geçirebilir ya da diğer kullanıcıların erişim noktasına bağlanmasını önlemek için kimlik doğrulama sistemine DoS saldırısı yapabilir. Bir DoS saldırısı sistemin kullanılabilirliğini tehlikeye atabilir ve T2S haberleşmesinde mesaj alışverişini engelleyebilir. Kapsül içerisinde ortaya çıkan bir DoS saldırısı, kaynakların tüketilmesine yol açabilir, kritik mesajların alınmasını engelleyebilir veya geciktirebilir. Bu acil mesajlar, acil durdurma veya

yangın sensörleri gibi kritik sistemleri kontrol etmektedir. DoS saldırılarını önlemek çok zordur. Yaygın stratejiler arasında kaynak yöneticilerinin belleği kritik süreçlere doğru şekilde tahsis etmesi ve bir DoS saldırısı tespit edildiğinde, kaynakları yeniden dağıtması yer almaktadır. Ağ saldırılarını önlemek için yaygın bir çözüm, kötücül davranışları erken tespit etmek ve sistemi korumak için doğru kararlar almak üzere saldırı tespit sistemlerinin (Intrusion Detection System, IDS) uygulanmasıdır. Ayrıca ağın çevresel korumasını artırmak için ağın stratejik noktalarına güvenlik duvarı uygulamak mümkündür. Bir kapsülün bağlantısını kesmeye zorlamanın bir başka yolu da DoS'a yol açan bir taşma saldırısı olabilir. Bu, bir kapsülü diğer kapsüllerden mesaj alamaz hale getirerek hyperloop sistem bileşenlerinin doğru çalışmasını engelleyebilir.

- *Gizlice Dinleme (Eavesdropping) saldırısı* çerçevesinde, belirli bir kullanıcının kapsül erişimi izlenerek profilini çıkarmak üzere U2P iletişimi gizlice dinlenebilir. Aynı erişim noktasına bağlı kullanıcı sayısı göz önüne alındığında, kötü niyetli bir unsur, örneğin iletişimi gizlice dinlemek ve hassas bilgileri çalmak için diğer kullanıcılara saldırmaya çalışabilir.
- *Fiziksel Kurcalama (Physical Tampering) saldırısı*, hyperloop sisteminin dağıtık yapısı nedeniyle fiziksel altyapıda bulunan potansiyel güvenlik açığı alanlarını hedeflemektedir. Fiziksel kurcalamayı önlemek için en yaygın çözüm, girişimleri tespit eden sensörlerle donatılmış kurcalama önleyici mekanizmaların oluşturulmasıdır. Diğer bir çözüm yöntemi, anomali tespit yazılımı kullanarak güvenlik ihlalinin olduğu bileşenlerin tespit edilmesi şeklindedir.
- *Taşma (Flooding) saldırısı*, bir kapsülün bağlantısını kesilmeye zorlayacak şekilde DoS saldırısına yol açabilmektedir. Kapsül, yer istasyonuna ve İSS'ye ulaşmak için verileri tüp üzerinden iletmektedir. Taşma saldırısı gerçekleştiren bir saldırgan, kapsülün bilgi alışverişini engelleyebilir veya geciktirebilir.
- *Mahremiyet ihlali (Privacy violation)* doğrultusunda belirli bir kullanıcının alışkanlıklarına ilişkin bilgiler, profil oluşturmaya veya kullanıcı takibine yol açarak ihlallere neden olabilir.
- *Ortadaki Adam (Man-in-the-middle, MitM) saldırısı*, sistemde birbiriyle iletişim kuran tarafların ortasına bir saldırganın girmesi şeklindedir. Saldırgan daha sonra haberleşme yönlerini kolayca değiştirebilir, komutlar ekleyebilir ya da paketleri kesebilir. EKS'ye yönelik MitM saldırıları, ağ bağlantısı kurulmasını gerektiren kablolu haberleşmeyi veya antenler kullanarak kablosuz haberleşmeyi engelleyebilir. MitM saldırıları, kapsüle ilişkin yanlış bilgiler içerecek şekilde paketleri değiştirebilir veya yenilerini oluşturabilir. Bu durum, yakındaki diğer kapsüllerde yanlış tepkiler ortaya çıkarabilir. Örneğin saldırı altındaki bir kapsül, bir önceki kapsüle yakın olduğunu söyleyerek hızlanmasına ya da kazalara neden olabilir. MitM saldırısı, bir kapsülü konvoydan ayırmak için kötücül mesajlar göndermek için de kullanılabilmektedir. Bir MitM saldırısı, kapsülün tüpün kenarlarına veya tabanına çarparak raydan çıkmasına yol açacak şekilde gücünü artırmak veya azaltmak için levitasyon mekanizmasını manipüle edebilir. Bir kapsülün kaçırılması da mümkün olabilir. Yüksek hızlı anahtarlama sistemi sayesinde bir saldırgan, herhangi bir kapsülü konvoydan ayırmak ve yanlış yönlendirmek için bir anahtarı tetikleyebilir. MitM saldırısı, şifrelenmemiş haberleşmeler için mümkün olup şifrelenmiş verileri izleyerek saldırganların faaliyetleri hakkında trafik analizi uygulanabilir. Kapsül içi ağda MitM yeteneği kazanan bir saldırgan, yanlış mesajlar yayarak kapsülün durumunda tutarsızlıklar, dolayısıyla yanlış alarm mesajları oluşturabilir. MitM ve gizli dinleme sayesinde kötü niyetli kişiler tarafından hassas veriler çalınabilir.
- *Sybil saldırısı,* bir saldırganın, farklı sensörler arasında tutarsızlık oluşturmak için var olmayan bir kapsülden veri göndermesi ile başlamaktadır.
- *Kara Delik (Blackhole Attack) saldırısı* ile bir saldırgan, paket iletimini engelleyerek P2P iletişim paketlerini ele geçirebilir.
- *Oltalama-Kimlik Avı (Phishing) saldırısı:* Hyperloop sistemleri, zehirlenme saldırılarına (poisoning attacks) karşı savunmasız olabilir ve bu da kimlik avı saldırılarına ve kimlik

bilgilerinin sızmasına neden olabilir. Kötü niyetli bir kullanıcı, belirli bir kullanıcının kapsül erişimini izlemek ve profilini çıkarmak için U2P haberleşmesini de gizlice dinleyebilir.

- *Tekrarlama saldırısı (Replay Attack),* ağda daha önce görülen geçerli bir mesajın, yeniden iletilmesine dayanmaktadır. Bu saldırının tespit edilmesi zordur ve sistemde arızalara yol açabilir. Bu saldırı, meşru iletişimi kopyalamak için daha önce iletilmiş ve gizlice dinlenmiş bir mesajı, ardışık iletişimde yeniden kullanmayı amaçlar. Yolcular ve erişim noktası arasındaki iletişimi gizlice dinleyerek kullanıcı gizliliğini tehlikeye atar.
- *Sahtecilik (Spoofing) saldırıları* ile hyperloop sistemini tehlikeye atmak için kapsülün konumu, sahte olarak bir saldırgan tarafından değiştirilmeye çalışılabilir. Sahteciliği önlemek için şifreleme ve kimlik doğrulama gibi geleneksel yöntemler kullanılmaktadır. Bunun yanında haberleşmeye yönelen sahteciliğe engel olmak için bir mesafe sınırlama protokolü kullanılabilir. Bu protokol, beklenen yanıt süresini analiz ederek bir varlığın fiziksel mesafesini ölçer. Bu şekilde, verilerin manipüle edilmesiyle veya sahte bir konumla eklenen gecikme, alıcı tarafından tespit edilebilir. Bu protokol yaygın olarak röle saldırılarını (relay attacks) ve küresel konumlama sistemi (Global Positioning System, GPS) sahteciliğini önlemek için kullanılmaktadır.
- *Konum sahteciliği (Location Spoofing);* kapsüllerin yakınındaki tüm kapsülleri uyarmak için konumlarını periyodik olarak yayınladığı varsayıldığında, diğer tüm kapsüllerin ihtiyaç duyulmasa bile mola verme veya hızlanma ve yavaşlama gibi yanlış eylemlerde bulunmasına neden olabilir. Bu durum, gecikmelerin olması gibi verimsizliğe veya kazalara yol açabilir.
- *Kimlik doğrulama sistemine saldırılar (Attacks to Authentication System),* saldırganların hassas verilere ve işlevlere erişim sağlamasına olanak tanıyabilir. Bu saldırı, hyperloop sisteminde bulunan kimlik doğrulama ile ilgili yöntemlerdeki güvenlik açıklarını hedef alır ve daha fazla istismar için ek saldırı yüzeyi oluşturabilir.

Hyperloop haberleşme sistemlerini hedeflemesi muhtemel siber saldırı türleri, tehditler, muhtemel etkileri, alınabilecek önlemler ve etki düzeyleri Tablo 1'de gösterilmiştir (Brighente vd., 2022, 2024):

Tablo 1. Hyperloop haberleşmesini hedef alan siber saldırılar (yazarlar tarafından uyarlanmıştır)

Haberleşme Türü	Siber Saldırı Türleri	Tehditler	Muhtemel Etkileri	Karşı Önlemler	Etki Düzeyi
Kullanıcıdan İstasyona (U2S)	– MitM – Gizlice Dinleme	– Özel Veri Sızıntısı	– Kullanıcıdan hassas bilgileri çalmak	– Şifreleme – Kimlik doğrulama – VPN	Düşük
	– Sahtecilik – Kimlik doğrulama sistemine saldırılar	– Manipülasyon – Sistem Bozulması – Hizmet Kaybı	– Bir bileti yanlış kullanıcıya fatura etme – Bilet rezervasyonunu engelleme – Doğru kapsüle ulaşılmasını engelleme	– Şifreleme – Dijital imza	Düşük
	– Mahremiyet ihlali	– Özel Veri Sızıntısı	– Kullanıcı kapsül erişimlerini izleme – Kullanıcı profillerini çıkarma	– Veri anonimleştirme	Düşük

Tablo 1. Hyperloop haberleşmesini hedef alan siber saldırılar (devamı)

Kapsülden Kapsüle (P2P)	– MitM – Sahtecilik – Röle – Tekrarlama	– Kimlik Taklidi (Impersonation) – Bilgi Toplama – Güvenlik Açığı – İstismarı – Manipülasyon – Sistem Bozulması (Corruption) – Hizmet kaybı	– Kapsül çalışma prosedür ve fonksiyonunda bozulmalar – Kazalar	– Kimlik doğrulama – Şifreleme	Yüksek
	– DoS – Taşma Saldırısı – Sybil – Kara Delik	– Sistem Bozulması – Hizmet kaybı	– Kapsül veri alışverişinde bozulma – Veri iletiminde gecikmeler – Kullanılamaz hale gelen bilgiler – Haberleşme ağında düzensizlik – Sensör tutarsızlığı	– Kaynak yönetimi kurtarma – Saldırı tespit sistemi	Orta
	– Konum sahteciliği	– Manipülasyon – Sistem Bozulma	– Kapsüllerin hatalı konum bilgisi iletimi sonucu kazalar, gecikmeler ve verimsizlik	– Mesafe sınırlaması – Dijital İmza – Konum bilgisi gizliliğini koruma	Yüksek
Kullanıcıdan Kapsüle (U2P)	– MitM – Gizlice Dinleme Kimlik doğrulama sistemine saldırılar	– Özel Veri Sızıntısı – Hizmet Kaybı	– Kullanıcıların dış ağ bağlantısını ele geçirme ve engelleme – Hassas bilgileri çalma – Satın alınan biletlerin kullanımı ve kapsüle erişimi engelleme	– Saldırı tespit sistemi – Şifreleme – Kimlik doğrulama – Veri anonimleştirme	Düşük
	– DoS – Kimlik doğrulama sistemine saldırılar	– Sistem Bozulması – Hizmet Kaybı	– Kullanıcıların kapsüle ve dolayısıyla internete erişimini engelleme	– Kaynak yönetimi kurtarma – Kimlik doğrulama – Güvenlik duvarı	Düşük
	– Mahremiyet ihlali – Oltalama	– Özel Veri Sızıntısı	– Kullanıcıların özel bilgilerini çalma	– Şifreleme – Kimlik doğrulama	Düşük

Tablo 1. Hyperloop haberleşmesini hedef alan siber saldırılar (devamı)

Kapsülden Tüpe (P2T)	– MitM – Röle – Tekrarlama	– Kimlik Taklidi – Bilgi Toplama – Güvenlik Açığı – İstismar – Manipülasyon – Sistem Bozulması – Hizmet Kaybı	– Kapsüle veya tüpe sahte komutlar gönderme – Kapsülü raydan çıkarma – Kapsülü kaçırma	– Kimlik doğrulama – Şifreleme – Saldırı tespit sistemi	Yüksek
	– DoS – Taşma Saldırısı	– Sistem Bozulması – Hizmet Kaybı	– Tüp ve kapsül arası veri alışverişini devre dışı bırakma ya da geciktirmek – Tüp ve kapsül arası enerji aktarımını önleme	– Kaynak yönetimi kurtarma – Saldırı tespit sistemi	Orta
	– Konum Sahteciliği	– Manipülasyon, – Sistem Bozulması	– Kapsülün konum bilgisiyle ilgili tutarsızlıklar oluşturma	– Mesafe sınırlaması – Dijital imza – Konum bilgisi gizliliğini koruma	Orta
	– Mahremiyet ihlali	– Özel Veri Sızıntısı	– Kapsül konum bilgisini ve kullanıcıların kimlik bilgilerini takip etme	– Veri anonimleştirme – Şifreleme	Düşük
Kapsül İçi Haberleşme (InP)	– MitM – Sahtecilik – Röle – Tekrarlama	– Bilgi Toplama – Güvenlik Açığı – İstismarı – Manipülasyon – Sistem Bozulması – Hizmet Kaybı	– Kapsül içi tüm sistemleri tehlikeye atma (bilgi-eğlence, havalandırma, ışık, acil çıkışlar, yangın dedektörleri ve yangın söndürücüler gibi)	– Saldırı tespit sistemi – Bütünlük kontrolü	Orta
	– DoS – Taşma Saldırısı	– Sistem Bozulması – Hizmet Kaybı	– Kaynakları tüketme – Kritik mesajların alınmasını önleme veya geciktirme	– Güvenlik duvarı – Saldırı tespit sistemi	Yüksek

Tablo 1. Hyperloop haberleşmesini hedef alan siber saldırılar (devamı)

Tüpten İstasyona (T2S)	– MitM – Sahtecilik – Röle – Tekrarlama	– Bilgi Toplama – Güvenlik Açığı – İstismarı – Manipülasyon – Sistem Bozulması – Hizmet kaybı	– Tüpe kötücül kontrol mesajları gönderme – Anomaliler oluşturma – Kapsül bilgilerinde sahtecilik yapma – Tüpün bazı bölümlerini kapatma – Var olan anomalileri gizleme	– Kimlik doğrulama – Şifreleme – Saldırı tespit sistemi	Yüksek
	– DoS	– Sistem Bozulması	– Tüp istasyon arası iki yönlü mesaj alışverişini önleme	– Güvenlik duvarı – Saldırı tespit sistemi – Belleğin kritik süreçlere doğru şekilde tahsis edilmesi – Kaynakların yeniden dağıtılması	Orta
	– Fiziksel Kurcalama	– Sistem Bozulması – Hizmet Kaybı	– Kablolu iletişimi kesme – RAU'ları manipüle etme – Hizmeti kesintiye uğratma	– Kurcalama önleyici malzemeler kullanma – Anomali tespit dedektörü	Orta

4.2. Siber riskleri azaltma stratejileri ve siber güvenlik mekanizmaları

Hyperloop sisteminin veri iletimi ve diğer ihtiyaçları doğrultusunda haberleşmesi, çeşitli yöntemler ile sağlanabilmektedir. Ancak bu verilerin dış tehditlerden ve siber saldırılardan korunması önemlidir. Bu nedenle siber güvenliği geliştirmeye yönelik önlemlerin alınması gerekmektedir. Bu doğrultuda bilgi sistemleri, eğlence sistemleri ve güvenlik için ayrı haberleşme ağlarının kullanılması, sistem açısından kritik verilerin korunmasını sağlayabilir. Altyapı boyunca fiber optik ağ kurulması ile haberleşme sinyallerinin bilgisayar korsanları tarafından fiziksel olarak ele geçirilmesi önlenebilir (Delft Hyperloop, 2020).

Hedeflenen siber güvenlik performansını ölçmek için literatür çalışmalarında kullanılan bazı metrikler bulunmaktadır. Bu metrikler dikkate alınarak hyperloop sisteminin siber güvenliği için de stratejiler geliştirilebilir. Siber güvenlik performans ölçümü ya da metriği olarak Tablo 2'deki anahtar performans göstergeleri (Key Performance Indicator, KPI) kullanılabilir (RiskXChange, 2023).

Tablo 2. Siber güvenlik performans ölçümü için KPI'lar

KPI	Açıklama
Hazırlıklı olma seviyesi	Siber olayı önleme, müdahale etme ve kurtarmaya yönelik bir stratejiye sahip olunması, uygulanması ve takibiyle ilgilidir.
Saldırı girişimleri	Saldırı girişimlerini takip etmek; mevcut güvenlik açıklarına, güvenlik önlemlerine ve müdahale ekiplerinin hazır olup olmadığına dair bir görünüm sunmaktadır.
Ortalama tespit süresi	Bir siber güvenlik riskini veya siber tehdidini tespit etmek için geçen ortalama süre ile ilgili olup temel amaç, bu hedefe mümkün olan en kısa sürede ulaşmaktır.
Ortalama yanıt süresi	Bir siber güvenlik riskine veya tehdide yanıt vermek için geçen ortalama süre ile ilgili olup temel amaç, bu hedefe mümkün olan en kısa sürede ulaşmaktır.
Ortalama kontrol altına alma süresi	Bir siber güvenlik riskinin veya tehdidin kontrol altına alınması için geçen ortalama süre ile ilgili olup temel amaç bu hedefe mümkün olan en kısa sürede ulaşmaktır.
Güvenlik olayları	Sistem donanımı veya yazılımı aracılığıyla güvenliğin ihlal edilmesiyle ilgili sorunlar ya da önlemlerin yeterliliği ölçülebilir. Siber güvenlik ekipleri, güvenlik olaylarını sürekli izleyerek her olasılığa hazırlıklı olmalıdır.
Güvenlik derecelendirmeleri	Gelişmiş risk ölçüm yöntemlerini kullanarak gerçek zamanlı risk derecelendirmeleri ve analizler sunulması, tüm hyperloop ekosistemindeki siber riskleri ölçerek proaktif bir şekilde riskleri azaltmaya yardımcı olabilir.
İnsan dışı trafik	Bot'lar tarafından tetiklenen insan dışı trafik miktarının ölçülmesi ve takibidir.
Virüs izleme	Sistem yazılımları, haberleşme ağı veya donanımıyla ilgili potansiyel virüsleri veya kötücül yazılım sorunlarını tespit etmeye yöneliktir.

Hyperloop haberleşme sistemlerine yönelen siber güvenlik tehditlerine karşı kullanılan yöntemlerden bazıları aşağıdaki gibi sıralanabilir:

- Kuantum kriptografi (National Security Agency, 2020)
- Yazılım Tanımlı Ağ (Software Defined Networking, SDN) (Kaur vd., 2014)
- Mesafe sınırlama (distance bounding) protokolü
- Veri toplama ve veri anonimleştirme (data aggregation and data anonymization)
- IDS
- Kaynak yönetimi kurtarma (resource management recovery)

Genel olarak bilişim sistemlerinin siber saldırılardan korunmasında temel koruma önlemleri, sistemin tasarım aşamasından itibaren en iyi güvenlik uygulamalarını ve tüm paydaşlar tarafından kullanılması gereken güvenlik standartlarının takip edilmesini içermektedir. Hyperloop sistemi yeni bir teknoloji olduğu için henüz tasarım aşamasında olan bu sistem özelinde, siber güvenlik konusunu adresleyen bir standart bulunmamaktadır. Hyperloop ulaştırma moduna yönelik siber güvenlik çözümleri geliştirmede; otomotiv, raylı sistemler ve havacılık gibi diğer sektörlerdeki tecrübeleri içeren; CEN-CENELEC yol haritasında belirtilen mevcut standartlar (CEN, 2023), Uluslararası Standardizasyon Örgütü'nün (International Organization for Standardization, ISO) ISO/IEC 27000 serisi gibi bilgi güvenliğine yönelik genel standartlar (ISO, 2018), Uluslararası Otomasyon Topluluğu (International Society of Automation, ISA) ve Uluslararası Elektroteknik Komisyonu (International Electrotechnical

Commission, IEC) tarafından yayınlanan ISA/IEC 62443 otomasyon ve kontrol sistemleri özelindeki standartlar (ISA, 2019), CLC/TS 5071 demir yoluyla ilgili uygulamalara yönelik siber güvenlik standartları (CLC, 2023), ISO Otomotiv Mühendisleri Topluluğu (Society of Automotive Engineers, SAE) tarafından hazırlanan ISO/SAE 21434:2021 karayolu taşıtlarının siber güvenlik standartları (ISO, 2021), Ulusal Siber Güvenlik Merkezi tarafından yayınlanan güvenlik prensipleri (National Cyber Security Centre, 2019), Otomotiv Açık Sistem Mimarisi (AUTomotive Open System Architecture, AUTOSAR) topluluğunun oluşturduğu güvenliğe yönelik standartları ve prosedürleri içeren genel bakış dokümanları (AUTOSAR, 2023) gibi kaynaklardan da faydalanılabilir (Brighente vd., 2024).

5. Sonuç ve Öneriler

Ulaştırma için kullanılan tüm modlar, dış dünya ile sürekli iletişim halindedir. Uydular aracılığıyla konum tespiti, radyo dalgaları aracılığıyla eğlence sistemlerinin kullanımı ve mobil ağlar aracılığıyla internete erişilmesi gibi hizmetler, ulaştırma sistemlerinde kullanılmaktadır. Ulaştırma ve hareketliliğin sağlanmasında yenilikçi bir mod olan hyperloop teknolojisinde de yer alan tüm bileşenlerin ve altyapının, bir ağ üzerinden kontrol merkezine sürekli bağlantılı olması gerekmektedir. Bu nedenle diğer tüm ulaştırma modlarında olduğu gibi hyperloop teknolojisi de etkin ve verimli bir haberleşme sistemine ihtiyaç duymaktadır. Bu çalışmada, hyperloop teknolojisinde kullanılan haberleşme ağı, haberleşme türleri, haberleşme teknolojileri ve yöntemleri ile bu sistemleri hedef alan siber güvenlik tehditleri ve siber güvenlik risklerini azaltıcı stratejiler incelenmiştir.

Haberleşme teknolojileri, güvenilir ve yüksek hızlı bir haberleşme imkânı sağlayarak yolculukların konforlu, güvenilir ve emniyetli olmasına katkı sunmaktadır. Hyperloop sisteminin haberleşme gereksinimlerini karşılamak için kablolu ve kablosuz birçok teknolojiden faydalanılmaktadır. Bu gereksinimler, olası siber güvenlik tehditlerini ve zorlukları da beraberinde getirmektedir. Hyperloop sisteminde, çelikten yapılmış kalın tüp kablosuz haberleşme için engeller oluştururken vakumlu ortam, bakım ve onarım gibi işleri zorlaştırmaktadır. Hyperloop sisteminin yüksek hıza sahip olması ve yolculuk boyunca kapsüldeki süreklilik arz eden devir nedeniyle sistemin bütün olarak haberleşmesinin verimli şekilde sağlanması için tüpün başka bölümlerine bağlantının aktarılması gerekebilmektedir. Bu aktarımların güvenilir olması önemli olup yüksek hızda seyahat sırasında doppler etkisinin ortaya çıkması da muhtemeldir.

Dünyada olduğu gibi Türkiye için de hyperloop sistemi; araştırılması, incelenmesi ve uygulamaya alınması zorluklar içeren ve ekonomik açıdan maliyetli bir ulaştırma modudur. Bu teknolojiyi oluşturan sistemlerin, mekanizmaların, haberleşme çözümlerinin, uçtan uca güvenlik ve emniyet ihtiyacı gibi birçok varlığın geliştirilmesi ile sonrasında yönetilmesi, kapsamlı süreçler içermektedir. Hyperloop teknolojisinin geliştirilmesi için test mekanizmalarının ve alanlarının, yani bu teknoloji özelindeki laboratuvarların oluşturulması, ulaştırma ve hareketliliğin yeni bir boyut kazanması açısından önem arz etmektedir.

Dünyadaki hyperloop sistemi geliştirme çalışmaları göz önünde bulundurularak Türkiye'nin bu alanda teknolojik gelişime öncülük edebilmesi için prototip düzeyde de olsa, ekonomik ve teknik açıdan minimum ölçekli bir hyperloop uygulama projesinin, çok paydaşlı bir yaklaşımla kamu-özel sektör iş birliği ile başlatılmasının uygun olacağı değerlendirilmektedir. Bu çerçevede ihtiyaç duyulan mevzuat, kurallar ve prosedürler, organizasyon yapısı, yer seçimi ve benzeri öncelikli konuların belirlenmesi gerekmektedir. Sistemin karmaşık yapısı ve çok kapsamlı bileşenleri olması nedeniyle çok farklı sektörleri bir araya getirmesi gerekeceği için planlama ve projelendirmenin doğru bir şekilde yapılması, ayrıca kritik bir konudur. Yol altyapısı, hyperloop tüpü, kapsülü, istasyonu, kontrol merkezi, haberleşme sistemleri, sensör ağları, uygulama yazılımları ve daha birçok varlık, ulaştırmanın beşinci modunun pilot bir uygulamasında yerini alacak olup bu varlıkların, güvenli ve güvenilir bir sistem oluşturacak şekilde çalışabilmesi için hyperloop sistemini oluşturan haberleşme türlerinin uçtan uca güvenliği, önemli bir husus olarak öne çıkmaktadır. Bu nedenle pilot uygulamalarda, olası siber saldırılar ve bu saldırılara karşı alınabilecek önemler de göz önünde bulundurulmalıdır.

Türkiye'de hyperloop sistemindeki gelişmeler ile haberleşme altyapısı ve siber güvenlik çözümlerinin mevcut durumu araştırılarak bu teknolojinin kurulumu ve pilot uygulaması için analiz yapılması, gelecek çalışmalar için potansiyel bir araştırma konusu olabilir. Türkiye'deki hyperloop sistemi

geliştirme çabalarının hız kazanması amacıyla test merkezlerinin kurulması ya da kentsel veya kurumsal ihtiyaçlar çerçevesinde prototip bir model geliştirilmesi, haberleşme ve siber güvenlik bileşenlerini de ele alacak şekilde tasarlanarak modellenmesi önerilmektedir. İzleyen çalışmalarda, olası siber saldırı senaryoları üzerinden siber saldırıları azaltmaya yönelik stratejilerin ve yöntemlerin seçimine ve uygulanmasına yönelik çözümler geliştirilebilir. Tasarlanacak pilot hyperloop sisteminin siber saldırılara karşı dayanıklılığını, literatürde yer alan siber güvenlik ölçüm KPI'larına göre analiz edecek bir model geliştirilebilir.

Araştırmacıların Katkı Oranı Beyanı

Sorumlu yazar ve ikinci yazar tarafından araştırmanın ilk versiyonu hazırlanmış, tüm yazarlar tarafından düzenlenerek gözden geçirilmiştir.

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

Armağan, K. (2020). The fifth Mode of Transportation: Hyperloop. *Journal of innovative transportation*, *1*(1), 1105.

AUTOSAR. (2023). Explanation of Safety Overview. https://www.autosar.org/fileadmin/standards/R23-11/FO/AUTOSAR_FO_EXP_SafetyOverview.pdf

Brighente, A., Conti, M., Donadel, D., & Turrin, F. (2022). Hyperloop: A Cybersecurity Perspective. *arXiv preprint arXiv:2209.03095*.

Brighente, A., Conti, M., Donadel, D., & Turrin, F. (2024). Hyperloop: A Cybersecurity Perspective. https://doi.org/10.1109/EuroSPW61312.2024.00045

Catherine, T., Barr, L. C., & By Hyde, D. J. (2016). *Hyperloop Commercial Feasibility Analysis : High Level Overview*. https://rosap.ntl.bts.gov/view/dot/12308

CEN. (2023). JTC 20-CEN/CLC/TR 17912:2023, Hyperloop systems- Standards Inventory and Roadmap. https://www.cencenelec.eu/news-and-events/news/2023/eninthespotlight/2023-02-13-a-first-step-in-the-standardization-of-the-european-hyperloop-industry/

CLC. (2023). CLC/TS 50701:2023, Railway applications-Cybersecurity, European Committee For Electrotechnical Standardization, Brussels, Belgium.

Delft Hyperloop. (2019). *The Future of Hyperloop*. https://hyperloopconnected.org/2019/06/report-the-future-of-hyperloop/

Delft Hyperloop. (2020). Safety Framework for the European Hyperloop Network. Içinde *Hyperloop Connected*. https://hyperloopconnected.org/2020/07/report-safety-framework-for-the-european-hyperloop-network/

DGWHyperloop. (2024). *Developing the future of high-speed transportation.* Erişim tarihi 25 Kasım 2024, https://www.dgwhyperloop.in/careers.html

euroTUBE. *(2024). Hyperloop A new mode of transport.* Erişim tarihi 25 Kasım 2024, https://eurotube.org/hyperloop/

Fokum, D. T., & Frost, V. S. (2010). A survey on methods for broadband internet access on trains. *IEEE communications surveys & tutorials*, *12*(2), 171-185.

Gazi Üniversitesi. (2022). *TEKNOFEST'te Üniversitemiz Teknoloji Fakültesi Öğrencilerinden Büyük Başarı "Türkiye'nin En Hızlısı Turkuaz Hyperloop"*. https://gazi.edu.tr/view/news/289802/teknofest-

te-universitemiz-teknoloji-fakultesi-ogrencilerinden-buyuk-basari-turkiye-nin-en-hizlisi-turkuaz-hyperloop-

Gheth, W., Rabie, K. M., Adebisi, B., Ijaz, M., & Harris, G. (2021). Communication systems of high-speed railway: a survey. *Transactions on Emerging Telecommunications Technologies*, *32*(4), e4189.

Gkoumas, K. (2021). Hyperloop Academic Research: A Systematic Review and a Taxonomy of Issues. *Applied Sciences*, *11*(13). https://doi.org/10.3390/app11135951

Gkoumas, K., & Christou, M. (2020). Hyperloop in Europe: State of Play and Challenges. *Proceedings of the 8th Transport Research Arena, TRA*.

Hansen, I. A. (2020). Hyperloop Transport Technology Assessment and System Analysis. *Transportation Planning and Technology*, *43*(8), 803-820. https://doi.org/10.1080/03081060.2020.1828935

HARDT. (2024). *Hyperloop is the most environmentally friendly solution.* Erişim tarihi 24 Eylül 2024, https://www.hardt.global/

Hedhly, W., Amin, O., Shihada, B., & Alouini, M.-S. (2021). Hyperloop Communications: Challenges, Advances, and Approaches. *IEEE Open Journal of the Communications Society*, *2*, 2413-2435.

HyperloopTT. (2024). *Hyperloop Transportation Technologies*. Erişim tarihi 25 Kasım 2024, https://www.hyperlooptt.com/

Hyperloop Development Program. *(2024). The Hyperloop development program.* Erişim tarihi 25 Kasım 2024, *https://www.hyperloopdevelopmentprogram.com/questions-hdp*

Hyperloop Italia. (2024). *Firma del contratto tra cav e hyper builders per lo studio di fattibilità del progetto futuristico hyperloop in italia.* Erişim tarihi 24 Eylül 2024, https://hyperloopitalia.com/media/comunicati-stampa/firma-del-contratto-tra-cav-e-hyper-builders-per-lo-studio-di-fattibilita%e2%80%a8del-il-progetto-futuristico-hyperloop-in-italia/

Icomera. (2021). *HyperloopTT Connects with Icomera TraXsideTM for Wireless Communications.* Erişim tarihi 12 Mart 2024, gönderen https://www.icomera.com/hyperlooptt-connects-with-icomera-traxside-for-wireless-communications/

ISA. (2019). ISA/IEC 62443 Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

ISO. (2018). ISO/IEC 27000:2018 Information technology-Security techniques-Information security management systems-Overview and vocabulary, Geneva. https://www.iso.org/standard/73906.html.

ISO. (2021). ISO/SAE 21434:2021- Road vehicles- Cybersecurity engineering, International Organization for Standardization, Geneva, CH, Standard. https://www.iso.org/standard/70918.html

Kale, S. (2019). Hyperloop: Advance Mode of Transportation System and Optimize Solution on Traffic Congestion. *International Journal for Research in Applied Science and Engineering Technology*. 7. 539-552. 10.22214/ijraset.2019.7085.

Kaur, K., Singh, J., & Ghumman, N. S. (2014). Mininet as software defined networking testing platform. *International conference on communication, computing & systems (ICCCS)*, 139-142.

Li, P., Niu, Y., Wu, H., Han, Z., Wang, Y., Wang, N., Zhong, Z., & Ai, B. (2024). Scheduling of Millimeter Wave Communications for Ultra-High-Speed Vacuum Tube Train. IEEE Transactions on Vehicular Technology.

Mitropoulos, L., Kortsari, A., Koliatos, A., & Ayfantopoulou, G. (2021). The Hyperloop System and Stakeholders: A Review and Future Directions. *Sustainability*, *13*(15), 8430.

Musk, E. (2013). Hyperloop Preliminary Design Study Technical Section. *Hyperloop Alpha*. https://www.tesla.com/sites/default/files/blog_images/hyperloop-alpha.pdf

National Cyber Security Centre. (2019). Secure design principles. https://www.ncsc.gov.uk/collection/cyber-security-design-principles

National Security Agency. (2020, Eylül 16). *Kuantum Anahtar Dağıtımı ve Kuantum Kriptografi*. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

NEVOMO. (2024). *Projects for a new passenger and freight.* Erişim tarihi 24 Eylül 2024, https://www.nevomo.tech/en/vehicles/

Nøland, J. K. (2021). Prospects and Challenges of the Hyperloop Transportation System: A Systematic Technology Review. *IEEE Access*, *9*, 28439-28458. https://doi.org/10.1109/ACCESS.2021.3057788

Nøland, J. K. (2024). A Reality Check on Maglev Technology for the Hyperloop Transportation System: Status Update After a Decade of Development. IEEE Access.

Özbek, R., & Çodur, Y. M. (2021). Comparison of Hyperloop and Existing Transport Vehicles in Terms of Security and Costs. *Modern Transportation Systems and Technologies*, *7*(3), 5-29. https://doi.org/https://doi.org/10.17816/transsyst2021735-29

Platin. (2023). *Sürdürülebilir ve çevre dostu yeni ulaşım konsepti Hyperloop'ta Türk imzası*. https://www.platinonline.com/sektorler/surdurulebilir-ve-cevre-dostu-yeni-ulasim-konsepti-hyperloopta-turk-imzasi-1087505

Premsagar, S., & Kenworthy, J. (2022). A Critical Review of Hyperloop (Ultra-High Speed Rail) Technology: Urban and Transport Planning, Technical, Environmental, Economic, and Human Considerations. *Frontiers in Sustainable Cities*, *4*. https://doi.org/10.3389/frsc.2022.842245

Qiu, C., Liu, L., Han, B., Zhang, J., Li, Z., & Zhou, T. (2020). Broadband wireless communication systems for vacuum tube high-speed flying train. *Applied Sciences*, *10*(4), 1379.

RiskXChange. (2023). *A guide to cybersecurity metrics and KPIs*. https://riskxchange.co/1006911/a-guide-to-cybersecurity-metrics-and-kpis/

Rob, M. A., Sagar, A. S. M., & Uddin, M. N. (2019). Prospects of Hyperloop Transportation Technology: A Case of China. *International Journal of Engineering and Management Research*.

Sniady, A., & Soler, J. (2014). Capacity gain with an alternative LTE railway communication network. *2014 7th International Workshop on Communication Technologies for Vehicles (Nets4Cars-Fall)*, 54-58. https://doi.org/10.1109/Nets4CarsFall.2014.7000913

swisspod. (2024). *Preliminary Testing For World's Longest Hyperloop Mission.* Erişim tarihi 24 Eylül 2024, https://www.swisspod.com/our-journey

Tavsanoglu, A., Briso, C., Carmena-Cabanillas, D., & Arancibia, R. B. (2021). Concepts of Hyperloop Wireless Communication at 1200 km/h: 5G, Wi-Fi, Propagation, Doppler and Handover. *Energies*, *14*(4), 983.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). *Yeni Nesil Ulaşım Teknolojisi Hyperloop*. https://cbddo.gov.tr/SharedFolderServer/Genel/3.Aras%CC%A7t%C4%B1rma-Raporu-Yeni-Nesil-Ulas%CC%A7%C4%B1m-Teknolojisi-Hyperloop.pdf

TEKNOFEST. (2022). *Hyperloop Geliştirme Yarışması*. https://www.teknofest.org/tr/yarismalar/hyperloop-gelistirme-yarismasi/

TEKNOFEST. (2024). Geleceğin Ulaşım Teknolojisi TÜBİTAK Hyperloop Geliştirme Yarışması Sona Erdi. https://www.teknofest.org/tr/yarismalar/hyperloop-gelistirme-yarismasi/

Thompson, P. J. (2019). *A Scientific and Economic Analysis of the Hyperloop as it Pertains to Mass Transportation*. http://rave.ohiolink.edu/etdc/view?acc_num=case1560510307453676

Turrin, F. (2023). *Cybersecurity of Modern Cyber-Physical Systems*.

U.S. Department of Energy. (2021). *Effect of Hyperloop Technologies on the Electric Grid and Transportation Energy*. USDOE Office of Energy Efficiency and Renewable Energy (EERE), Washington …. https://www.osti.gov/biblio/1773025/

UTIKAD. (2022). *Erciyas ve Çimtaş, Hyperlooptt'e Tedarikçi ve Yatırımcı Oldu*. https://www.utikad.org.tr/Detay/Sektor-Haberleri/30900/erciyas-ve-cimtas-hyperlooptt-e-tedarikci-ve-yatirimci-oldu

TRANSPOD. (2024). *TransPod system*. Erişim tarihi 24 Eylül 2024, https://www.transpod.com/transpod-system/

TUM Hyperloop. (2023). *Ultra-fast connections between mobility hubs*. Erişim tarihi 25 Kasım 2024, https://tumhyperloop.com/about-hyperloop/

zeleros. (2024). *We develop hyperloop Technologies.* Erişim tarihi 24 Eylül 2024, https://zeleros.com/hyperloop/

Zhang, J., Liu, L., Han, B., Li, Z., Zhou, T., Wang, K., Wang, D., & Ai, B. (2020). Concepts on train-to-ground wireless communication system for hyperloop: Channel, network architecture, and resource management. *Energies, 13*(17), 4309.