Avrupa Bilim ve Teknoloji Dergisi
Sayı 27, S. 1038-1049, Kasım 2021

Derleme Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 27, pp. 1038-1049, November 2021

Review Article

Denetleyici Alan Ağının Güvenliğinin Sağlanması için Derin Öğrenme Tabanlı Saldırı Tespit Sistemleri Üzerine Bir Derleme

Zinnet Duygu Akşehir[1*], Sedat Akleylek[2]

[1*] Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Samsun, Türkiye, (ORCID: 0000-0002-6834-6847), duygu.aksehir@bil.omu.edu.tr
[2] Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Samsun, Türkiye (ORCID: 0000-0001-7005-6489), sedat.akleylek@bil.omu.edu.tr

(İlk Geliş Tarihi 26 Temmuz 2021 ve Kabul Tarihi 15 Kasım 2021)

(**DOI:** 10.31590/ejosat.974582)

ATIF/REFERENCE: Akşehir, Z. D. & Akleylek, S. (2021). Denetleyici Alan Ağının Sağlanması için Derin Öğrenme Tabanlı Saldırı Tespit Sistemleri Üzerinde Bir Derleme. *Avrupa Bilim ve Teknoloji Dergisi*, (27), 1038-1049.

Öz

Nesnelerin interneti fikrinin otomotiv alanına girmesi ile birlikte araçların interneti kavramı ortaya çıkmıştır. Araçların interneti hem araç içi ağ iletişimini hem de araçların diğer nesnelerle olan iletişimini kapsamaktadır. Araç içi ağ iletişimi, araç içi çeşitli işlevleri sağlayan Elektronik Kontrol Birimleri arasındaki güvenilir bir iletişimi sağlamakta olup araç içi ağlar arasında en yaygın kullanılanı denetleyici alan ağlarıdır. Denetleyici alan ağı, araç içi ağ için güvenli bir iletişim ortamı sunarken siber saldırılara karşı savunmasızdır. Bu derleme çalışmasında araç içi denetleyici alan ağının güvenliğinin sağlanması için derin öğrenme yöntemini kullanan saldırı tespit sistemleri üzerine odaklanılmıştır. Bu kapsamda veritabanları üzerinde sistematik bir literatür taraması gerçekleştirilerek literatüre yön veren çalışmalar belirlenmiştir. Belirlenen çalışmalar kullanılan yöntem, veri kümesi, seçilen öznitelik ve odaklanılan saldırı bakımından detaylı bir şekilde incelenmiştir. Ayrıca incelenen çalışmalarda önerilen saldırı tespit modelinin performansının nasıl değerlendirildiği ifade edilmekle birlikte önerilen modelin diğer yöntemlerle yapılan karşılaştırmalar detaylandırılmıştır.

Anahtar Kelimeler: Nesnelerin interneti (IoT), Araçların interneti (IoV), Araç içi ağ (IVN), Güvenlik, Denetleyici alan ağı (CAN), Saldırı tespit sistemi (IDS), Derin öğrenme.

A Review on Deep Learning Based Intrusion Detection Systems for Ensuring Security of Controller Area Network

Abstract

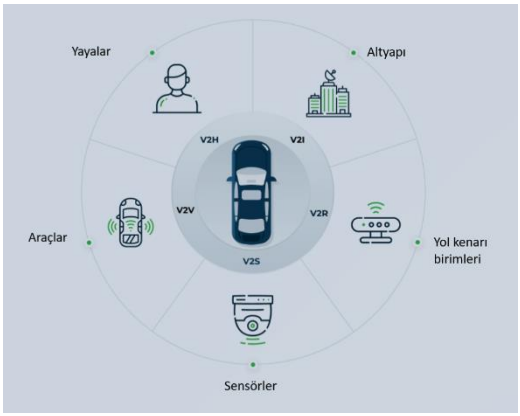
The concept of the Internet of vehicles emerges with the definition of the Internet of things idea into the automotive field. The internet of vehicles covers both in-vehicle network and the communication of vehicles with other things. The in-vehicle network provides reliable communication between Electronic Control Units providing various in-vehicle functions, and the most widely used among in-vehicle networks is the controller area networks. The controller area network is vulnerable to cyber-attacks while providing a secure communication environment for the in-vehicle network. This survey paper focuses on intrusion detection systems that use deep learning to secure the in-vehicle controller area network. In this context, systematic literature research is conducted on scientific/academical databases, and papers are determined that has an effect on the literature. The studies are examined in detail in terms of the used method, dataset, selected attribute, and focused attack. In addition, the previous studies are compared with the others in detail.

Keywords: Internet of things (IoT), Internet of vehicles (IoV), In-vehicle network (IVN), Security, Controller area network (CAN), Intrusion detection system (IDS), Deep learning.

[*] Sorumlu Yazar: duygu.aksehir@bil.omu.edu.tr

1. Giriş

İletişim teknolojilerinin ve internetin gelişmesiyle birlikte Nesnelerin İnterneti olarak ifade edilen IoT (Internet of Things) kavramı ortaya atılmıştır. IoT, akıllı nesneleri birbirine bağlayan ve bu nesnelerin birbirleriyle iletişim kurarak veri alışverişinde bulunmalarını sağlayan bir ağ olarak tanımlanmaktadır (Sharma vd., 2018). IoT'nin bir alt ağı olarak ifade edilen Araçların İnterneti (İnternet of Vehicles-IoV) ise farklı iletişim ortamları aracılığıyla araç ve çevresi arasında bilgi alışverişini sağlayan bir platformdur. Şekil 1'de gösterildiği gibi IoV, araçtan araca (V2V), araçtan yol kenarı birimine (V2R), araçtan altyapıya (V2I), araçtan sensöre (V2S) ve araçtan yayalara (V2P) olmak üzere farklı türlerde araç iletişimini içinde barındırmaktadır. Dolayısıyla IoV araç, insan ve sensörler gibi birçok kaynak türünü içeren heterojen bir ağ sistemi olarak ifade edilmektedir (Kaiwartya vd., 2016). Ayrıca IoV, araç içi ağ, kablosuz yerel alan ağı (WLAN), araçsal tasarsız ağlar (VANET) ve hücresel ağ dahil olmak üzere bu ağların birleşimi olarak nitelendirilen büyük bir ağ haline gelmiştir (Wang ve Liu, 2018).



Şekil 1. IoV Heterojen Ağ Mimarisi

Günümüzde araç içi işlevsellik, birbirine bağlı Elektronik Kontrol Birimleri (ECU) tarafından kontrol edilmektedir (Bozdal vd., 2020). Modern araçların, araç içi çeşitli işlevlerini yöneten ve mekanik kontrol birimlerinin yerini alan yüzden fazla ECU ile donatıldığı belirtilmektedir. Bu sayının gelecek yıllarda daha da artması öngörülmektedir (Hira, 2017). Her bir ECU'nun genellikle bir işlevi (direksiyon açısının kontrolü gibi) vardır ve bu ECU'lar aracın her tarafına dağıtılarak birbirleri ile iletişim kurabilir, bilgi alışverişinde bulunabilir. Araç içi ağ, ECU'lar arasındaki veri paylaşımını kolaylaştırmaktadır. Modern araç iletişim sistemlerinde kullanılan farklı araç içi ağlar olmakla birlikte en yaygın kullanılanı CAN'dir (Controller Area Network) (Al-Jarrah vd., 2019; Khatri vd., 2021). Denetleyici Alan Ağı olarak ifade edilen CAN, ECU'lar arasında iletişimi sağlamak için 1980'lerin ortasında Robert Bosch tarafından geliştirilen seri iletişim protokolüdür (Bosch, 2014). CAN, güvenlik için değil güvenilir iletişim sağlamak amacıyla tasarlanan bir protokoldür. Dolayısıyla siber saldırılara karşı savunmasızdır (Bozdal vd., 2020; Al-Jarrah vd., 2019). Örneğin, hava yastığı veya fren sistemine (ABS – Anti-lock Braking System) yapılan saldırı nedeniyle sürücünün ve yolcuların güvenliği tehlikeye girebilir. Bu durum otomobil üreticisinin itibarını, geri çağırma gibi önemli finansal sonuçlarla etkileyebilir. Gerçek hayattan örnek verilirse, Miller ve Valasek Jeep Cherokee aracına saldırı gerçekleştirerek aracı uzaktan kontrol etti. Bu durum 1,4 milyon aracın geri çağrılmasına neden oldu (Miller, 2019). Araç içi ağ sisteminde mevcut olan bu tehditler sadece hedef aracın güvenliğine değil, aynı zamanda diğer araçlar, yayalar ve altyapılar dahil olmak üzere yol ortamına da zarar verebilir (Song ve Kim, 2021).

CAN protokolünde mevcut olan bu güvenlik açığının temel iki nedeni vardır: şifreleme ve kimlik doğrulama eksikliği. CAN'deki bu güvenlik açıklarına olası çözümler bulmak için kapsamlı çalışmalar yapılmış ve çalışmalar sonucunda şifreleme, kimlik denetimi ve saldırı tespit sistemleri önerilmiştir (Bozdal vd., 2020).

1.1. Motivasyon ve Kapsam

Bu derleme çalışması için yapılan literatür taraması sonucunda hem araç içi CAN güvenliğine hem de derin öğrenme tabanlı saldırı tespit sistemlerine odaklanan ulusal çalışmalara rastlanmamıştır (Çalışır vd., 2019; Kalkan ve Sahingoz, 2020; Baki ve Tutkun, 2021). Bu sebeple yabancı güncel kaynaklara odaklanılmıştır.

Bu çalışma kapsamında araç içi CAN güvenliğinin sağlanması için derin öğrenme yöntemlerini kullanan saldırı tespit sistemleri (Intrusion Detection System-IDS) incelenmiştir. Bunun için öncelikli olarak araç içi CAN güvenliği kapsamında yapılan derleme çalışmaları araştırılmış ve 2017-2021 yılları arasında 8 çalışma detaylı olarak incelenmiştir. Elde edilen bu derleme çalışmaları aşağıda belirtilen 5 kriter üzerinden değerlendirilmiş olup bu değerlendirme Tablo 1'de ifade edilmiştir:

- Derleme çalışmasında incelenecek çalışmalar için veritabanları üzerinden taramalar nasıl yapılmış, bunlar hakkında istatistiksel bilgiler verilmiş mi, dolayısıyla yapılan derleme çalışması sistematik midir?
- IDS'ler için öznitelik seçimi detaylandırılmış mı?
- Derin öğrenme tabanlı IDS'lere odaklanılmış mı?
- CAN'e yapılan saldırılar hakkında bilgi verilmiş mi?
- Derleme çalışması kapsamında incelenen çalışmalar için performans karşılaştırılması yapılmış mı?

İncelemeler sonucunda 8 derleme çalışmasının hiçbirinde sistematik literatür taramasının yapılmadığı, dolayısıyla derlemelerde incelenen çalışmaların nasıl belirlendiği ile ilgili bilgilerin yer almadığı görülmüştür. Derlemelerin çoğunda incelenen çalışmaların, IDS için öznitelik seçimini nasıl yaptığı ve önerilen IDS modelinin diğer yöntemlere bir üstünlük sağlayıp sağlamadığı konusunda da detaylı bilgilerin olmadığı tespit edilmiştir. Ayrıca derlemelerin çoğu CAN-IDS modeli için derin öğrenme yöntemlerine odaklanmayıp bazıları ise makine öğrenimi tabanlı IDS başlığı altında derin öğrenmeye yüzeysel olarak değinmiştir. Bunların yanısıra incelenen derleme çalışmalarının neredeyse tümü CAN'e yapılan saldırılar hakkında genel bilgiler vermiştir.

İncelenen derleme çalışmalarında, sistematik literatür taramasının nasıl yapıldığı, çalışmaların nasıl belirlendiği, derin öğrenme yöntemlerinden hangilerine odaklanıldığı, öznitelik seçiminin ve önerilen IDS modellerinin performans karşılaştırmasının nasıl yapıldığı hakkındaki bilgilerin detaylı olarak verilmediği görülmüştür. Bu çalışma kapsamında, incelenen derlemelerdeki bu eksiklikler giderilmiş olup belirlenen 5 kriter hakkında detaylı bilgiler verilmiştir.

Tablo 1. Derleme Çalışmalarının Değerlendirilmesi

Çalışma	Yıl	Sistematik	Öznitelik seçimi	Derin öğrenme	Saldırılar	Performans karşılaştırması
Cyber security attacks to modern vehicular systems (Pan vd., 2017)	2017	Hayır	Hayır	Hayır	Evet	Hayır
Review of secure communication approaches for in-vehicle network (Hu ve Luo, 2018)	2018	Hayır	Hayır	Hayır	Kısmen	Kısmen
Survey of automotive controller area network intrusion detection systems (Young vd., 2019)	2019	Hayır	Hayır	Hayır	Hayır	Kısmen
Intrusion detection systems for intra-vehicle networks: A review (Al-Jarrah vd., 2019)	2019	Hayır	Evet	Hayır	Evet	Evet
Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review (Lokman vd., 2019)	2019	Hayır	Kısmen	Kısmen	Evet	Hayır
A survey of intrusion detection for in-vehicle networks (Wu vd., 2019)	2020	Hayır	Hayır	Evet	Kısmen	Evet
Evaluation of can bus security challenges (Bozdal vd., 2020)	2020	Hayır	Hayır	Hayır	Evet	Kısmen
Cyberattacks and countermeasures for in-vehicle networks (Aliwa vd., 2021)	2021	Hayır	Kısmen	Hayır	Evet	Hayır
Bu çalışma	2021	Evet	Evet	Evet	Evet	Evet

1.2. Organizasyon

Çalışma şu şekilde organize edilmiştir: Bölüm 2'de CAN için altyapı sağlanmış olup öncelikle araç içi ağ iletişimi ifade edilmiş ardından CAN'in güvenlik açıklarından ve veri çerçeve formatından bahsedilmiştir. Bölüm 3'te, derleme çalışmasının belirlenen hedefe ulaşması için incelenecek olan çalışmaların nasıl belirlendiği detaylandırılmış ve Bölüm 4'te bu çalışmalar belirlenen araştırma soruları kapsamında detaylı bir şekilde incelenmiştir. Son bölümde ise incelenen çalışmaların genel bir değerlendirmesi yapılmıştır.

2. Denetleyici Alan Ağı

Bu bölümde öncelikle araç içi iletişimin nasıl gerçekleştirildiği, bu iletişimin gerçekleştirilmesi için hangi ağların kullanıldığı ile ilgili bilgiler verilmiş ve bu araç içi ağların karşılaştırılması yapılmıştır. Ardından derleme çalışması kapsamında odaklanılan CAN detaylandırılmış, araç içi ağ iletişimi için kullanılan veri çerçeve formatlarından bahsedilmiş ve CAN'in güvenlik açıklarına değinilmiştir.

2.1. Araç İçi Ağ İletişimi

Gelişen teknolojinin araç üreticileri tarafından hızla benimsenmesi ile birlikte modern araçların işlevselliğinde de büyük artışlar meydana gelmektedir. Bu durum, modern araçlardaki ECU sayılarının artışına neden olmaktadır. ECU'lar arasında verimli bir iletişimin sağlanması için LIN (Local Interconnection Network), CAN, FlexRay, Ethernet ve MOST (Media Oriented System Transport) gibi çeşitli araç içi ağ iletişim protokolleri kullanılmaktadır. Tablo 2'de bu beş araç içi ağ protokolü bant genişliği, kullandıkları topolojiler, güvenlik tehditleri, avantaj ve dezavantajları açısından karşılaştırılmıştır. LIN, düşük seviyede güvenlik tehditine ve maliyete sahip olmasına rağmen araç içinde düşük hızda bir iletişim sağlamaktadır. Bununla birlikte hata toleransı da oldukça düşüktür. Diğer taraftan FlexRay, Ethernet ve MOST, LIN'den daha yüksek bant genişliğine sahip olmasına rağmen bu ağ protokolleri LIN'den daha yüksek seviyede güvenlik tehditine ve yüksek maliyete sahiptir. 1980'lerin ortasında Robert Bosch tarafından geliştirilen CAN, maliyetinin düşük olması, güvenilir haberleşme sağlaması, ölçeklenebilir olması ve düşük ağ karmaşıklığı nedeniyle araç içi ağlar arasında yaygın olarak kullanılmaktadır (Al-Jarrah vd., 2019; Khatri vd., 2021). CAN seri iletişim protokolü başlangıçta otomotiv uygulamaları için

geliştirilmiş olsa da asansör kontrol sistemleri, askeri uygulamalar, tekstil endüstrisi gibi pek çok alanda yaygın olarak kullanılmaktadır (Al-Jarrah vd., 2019).

2.2. CAN Veri Çerçevesi

CAN, araç içindeki çeşitli ECU'lar arasında veri yolu aracılığıyla CAN paketlerinin iletilmesine yardımcı olur ve yayın iletişimine dayanır. Başka bir deyişle veri yoluna bağlı her ECU, veri yolundan mesaj alabilir ya da veri yoluna mesaj gönderebilir. CAN paketlerinin ECU'lar arasındaki iletimi için kullanılan CAN 2.0A standart veri çerçevesi Şekil 2'de ifade edilmiştir. Standart veri çerçeve formatında denetim alanı içerisinde bulunan 11 bitlik CAN ID bilgisinin 29 bite genişletilmesiyle birlikte CAN 2.0B genişletilmiş veri çerçeve formatı elde edilmektedir. Dolayısıyla, bu iki veri çerçeve formatı arasındaki fark denetim alanlarının uzunluğundan kaynaklanmaktadır. Her iki veri çerçeve formatı 7 kısımdan oluşmaktadır (Song ve Kim, 2021; Khatri vd., 2021; Liu vd., 2017; Hossain vd., 2020):

- *Çerçeve başlangıcı (Start of Frame-SOF):* Bir bitlik SOF bilgisi yeni bir mesajın başlangıcını belirterek tüm düğümleri senkronize etmek için kullanılır.
- *Denetim alanı (Arbitration field):* Bu alanda CAN ID olarak bilinen kimlik bilgisi yer almaktadır. CAN mesajında gönderici veya alıcı düğüm hakkında herhangi bir bilgi bulunmamaktadır. Dolayısıyla CAN ID bilgisi, mesajda hangi araç bilgilerinin tutulduğunu belirtmek için kullanılmaktadır. Ayrıca mesaj önceliği de bu alana göre gerçekleştirilmekte olup düşük CAN ID'ye sahip mesajlar daha yüksek önceliklidir.
- *Kontrol alanı (Control field):* Bu alan kaç byte verinin gönderileceğini belirtmekle birlikte bunun dışında rezerve edilmiş bitler de mevcuttur.
- *Veri alanı (Data field):* Bu alan, CAN veri çerçeveleri ile iletilecek olan veriyi içermektedir. İletilen bu veriler maksimum 64 bit (8 bayt) uzunluğundadır.
- *CRC alanı:* Veri iletimi sırasında meydana gelen hataları tespit etmek için kullanılmaktadır.
- *Onay alanı (Acknowledge field):* Verinin iletilmesi sırasında oluşabilecek hataları tespit etmenin bir yolu da gönderilen mesaj için bir onay istenmesidir. Bu alan, alıcı düğüm tarafından verinin hatasız bir şekilde alındığını belirtmek için kullanılmaktadır.
- *Çerçeve sonu alanı (End of Frame-EOF):* Veri çerçevesinin sonlandığını belirtmek için EOF alanı kullanılmaktadır.

Şekil 2. CAN 2.0A Standart Veri Çerçeve Formatı

Tablo 2. Araç İçi Ağ Protokollerinin Karşılaştırılması

Ağ protokolü	Bant genişliği	Güvenlik Tehditi	Ağ Topolojisi	Avantaj	Dezavantaj
LIN	1 Kbps -1 Mbps	Düşük	Bus	Düşük maliyet, gerçeklemesi kolay	Düşük hız
CAN	125 Kbps- 20 Kbps	Düşük-Orta	Çoğunlukla Bus	Düşük maliyet	Düşük bant genişliği
FlexRay	10 Mbps	Yüksek	Bus, Yıldız veya Hibrid	Hata toleransı LIN ve CAN'den daha iyi	Yüksek maliyet
Ethernet	100 Mbps	Orta-Yüksek	Uçtan uca	Yüksek hız (CAN'den 100 kat daha hızlı)	Yüksek maliyet
MOST	24 Mbps	Orta	Halka	Yüksek hız	Çok yüksek maliyet

2.3. CAN'deki Güvenlik Açığı

CAN, siber saldırılara karşı savunmasızdır (Bozdal vd., 2020; Al-Jarrah vd., 2019). CAN protokolünde mevcut olan bu güvenlik açığı, mesajların şifrelenmemesi ve kimlik doğrulamanın yapılmamasından kaynaklanmaktadır. CAN, tasarım gereği ağ üzerinden iletilen mesajların/verilerin saldırgan tarafından ele geçirilmesine izin veren yayın protokolüdür. Dolayısıyla yayınlanan mesajlar şifrelenmediği için saldırgan tarafından veriler kolaylıkla elde edilebilir. Ayrıca CAN protokolü mesajların kaynağını doğrulamak için bir kimlik doğrulama mekanizması sağlamadığından saldırgan, CAN'e eriştikten sonra ağ üzerinden araç sistemini yanıltıcı mesajlar gönderebilir (Al-Jarrah vd., 2019). Literatürde, bu güvenlik açıklarına olası çözümler olarak şifreleme, kimlik doğrulama ve saldırı tespit sistemleri üzerine odaklanılmıştır. Gerçekleştirilen derleme çalışması kapsamında araç içi CAN için önerilen saldırı tespit sistemleri incelendiğinden bu bölümde CAN'e yapılan siber saldırılar detaylandırılmıştır.

- *Hizmet Reddi Saldırıları (Denial of Service (DoS) attacks):* CAN mesajlarının ID bilgisine göre öncelik mekanizmasına sahip olmalarından dolayı CAN DoS saldırılarına karşı savunmasızdır. Tüm ECU düğümleri tek bir veri yolu paylaştığı için saldırganlar, CAN veri yolunda yüksek öncelikli mesajlar ilettiğinde diğer ECU düğümlerinin mesaj göndermesine izin vermez. Dolayısıyla saldırgan tarafından gerçekleştirilen DoS saldırıları, CAN veri yolunda gecikmelere neden olmaktadır. Bir aracın, sürücünün komutlarına

zamanında yanıt vermemesi DoS saldırılarına örnek olarak verilebilir (Khatri vd., 2021; Liu vd., 2017).

- *Bulanık Saldırılar (Fuzzing attacks):* Saldırganlar, rastgele veri alanı ve sahte kimliklere sahip rastgele CAN mesajları oluşturarak bu saldırıyı gerçekleştirir. Araştırmacılar, bulanık saldırıların araçların arızalanmasına ve istenmeyen davranışlar sergilemesine neden olabileceğini ve bu durum karşısında yolcuların hayatlarını tehlikeye atabileceğini belirtmiştir (Khatri vd., 2021).
- *Tekrar Saldırıları (Replay attacks):* Saldırgan, CAN veri yolu üzerinden iletilen mesajları toplayabilir ve bu mesajları daha sonra tekrar iletebilir. CAN protokolünde kimlik doğrulaması yapılmadığından ECU'lar, bu mesajların kaynağının sahte olup olmadığını belirleyemez. Dolayısıyla bu tür saldırıların algılanması zordur. Saldırgan, önceden iletilen mesajları saklayıp, daha sonra tekrar CAN'e ileterek duran bir aracın motorunu çalıştırabilir, kapıyı açabilir veya aracı uzaklaştırabilir (Khatri vd., 2021; Liu vd., 2017).
- *Sahtecilik Saldırıları (Spoofing attacks):* Saldırgan, değiştirilmiş mesajları veri yolundan iletmek için belirli CAN ID'lerini hedef alır. Sahte mesajları tanımlamak zor olduğu için bu saldırı türü, araç sisteminin arızalanmasına sebep olabilir (Khatri vd., 2021; Hossain vd., 2020).

3. Araştırma Yöntemi

İncelenen derleme çalışmalarında sistematik bir kapsam üzerinden hareket edilmemiştir. Başka bir ifadeyle, incelenecek çalışmaların nasıl belirlendiği detaylandırılmamıştır. Bu derleme çalışmasında ise öncelikle belirlenen hedefe yönelik olarak araştırma sorularının neler olduğu belirlenmiştir. Ardından bu araştırma sorularına cevap arayacak çalışmaların seçilmesi üzerine veritabanı taramaları için sorgu cümlelerinin nasıl belirlendiği detaylandırılmıştır. Son olarak, veritabanı taramalarının ardından elde edilen çalışmalar için elemelerin nasıl gerçekleştirildiğinden bahsedilmiştir.

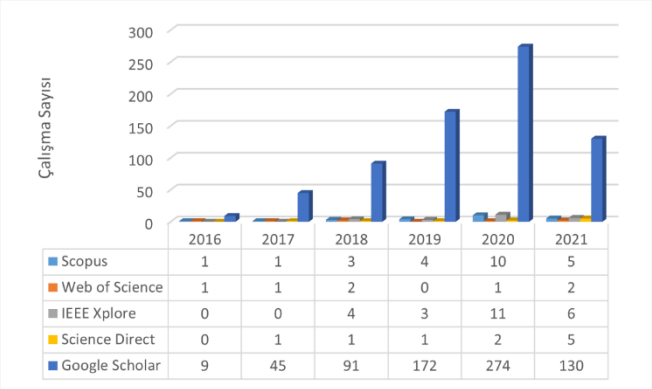
3.1. Araştırma Stratejisi

Bu sistematik derleme çalışması için belirlenen hedefe ulaşmaya yönelik olarak öncelikle aşağıdaki araştırma soruları oluşturulmuştur:

- *S1:* Araç içi CAN için önerilen saldırı tespit sistemlerinde derin öğrenme yöntemlerinden hangisi tercih edilmektedir?
- *S2:* Bu IDS'ler hangi saldırı türlerine odaklanmıştır, CAN verileri nasıl toplanmıştır ve hangi öznitelikler seçilmiştir?
- *S3:* Önerilen saldırı tespit modellerinin performansı hangi metrikler kullanarak değerlendirilmiştir ve literatürdeki diğer çalışmalara bir üstünlük sağlamakta mıdır?

Araştırma sorularının belirlenmesinin ardından bu sorulara cevap aramak için IEEE Xplore, Scopus, Web of Science, Science Direct ve Google Scholar olmak üzere beş veritabanı üzerinde literatür taraması gerçekleştirilmiştir. Belirlenen farklı anahtar kelimeler için "AND", anahtar kelimelerin eş anlamlıları için "OR" anlamsal operatörleri Tablo 3'te özetlendiği gibi kullanarak arama uzayı genişletilmiştir.

Beş veritabanı için kullanılan sorgu cümleleri ve hangi alanlarda tarandığı hakkındaki bilgiler Tablo 3'te verilmektedir. Tabloda yer alan bilgiler doğrultusunda beş veritabanı üzerinde sorgular gerçekleştirilmiş ve bu sorgular sonucunda 2016 yılından günümüze kadar olan çalışmaların sayısı Şekil 3'te özetlenmiştir. Google Scholar sorgularında hedefe yönelik çalışmaların yanı sıra çok genel sonuçlara da ulaşıldığı için bu veritabanı üzerinde etkili bir filtrelemenin gerçekleştirilmediği görülmüştür. Bu sebeple Google Scholar sorguları gözardı edilmiştir. Sonuç olarak dört veritabanında 2016-2021 yılları arasında yayınlanan toplam 65 çalışma listelenmiştir.



	2016	2017	2018	2019	2020	2021
Scopus	1	1	3	4	10	5
Web of Science	1	1	2	0	1	2
IEEE Xplore	0	0	4	3	11	6
Science Direct	0	1	1	1	2	5
Google Scholar	9	45	91	172	274	130

Şekil 3. Sorgu Cümleleri ile Veritabanlarında Filtrelenen Çalışmalar

3.2. Çalışmaların Seçimi

2016-2021 yılları arasında yapılan sorgulamalar sonucunda yakın geçmişe ağırlık verilmesi düşünülüp bu aralık 2019-2021 olarak güncellenmiş ve yayımlanan çalışma sayısı 65'ten 50'ye düşürülerek 50 çalışma üzerinden elemeler gerçekleştirilmiştir. Yapılan sorgulamalar sonucunda elde edilen 50 çalışmadan bazılarının birden fazla veritabanında tarandığı görülmüştür. Bu yüzden, veritabanlarında ortak taranan çalışmaların bir kez listelenmesi sağlanmıştır. Listelenen çalışmaların, derleme çalışması kapsamında incelenmeye değer olup olmadığının belirlenmesi için eleme ve seçme kriterleri aşağıdaki gibi tanımlanmıştır:

Seçme kriterleri:

- 2019-2021 yılları arasında Q1 veya Q2 sınıflı dergilerde yayımlanan çalışmalar
- Araç içi CAN güvenliği için derin öğrenme yöntemlerinin kullanıldığı çalışmalar

Eleme kriterleri:

- Yayımlanan çalışmaların derleme veya konferansta sunulmuş bildiri olması
- Araç içi CAN güvenliği için derin öğrenme yöntemlerine odaklanmayan çalışmalar

Çalışmaların başlıkları, özetleri okunmuş ve belirlenen bu kriterler doğrultusunda 50 çalışmadan incelenmek üzere 9 çalışma seçilmiştir. Çalışmalar incelenirken 2016 yılında yayımlanan Kang ve Kang'ın (2016) yapmış olduğu çalışmasına yapılan atıf sayısının 370 olduğu görülmüştür. Bu sebeple

belirlenen 9 çalışmaya bu çalışma da eklenmiş olup toplam 10 çalışma detaylı bir şekilde incelenmek üzere seçilmiştir.

Tablo 3. Veritabanlarında Gerçekleştirilen Sorguların Detayları

Veritabanı	Sorgu Cümlesi	Tarandığı Alan
IEEE Xplore	("controller area network" OR "CAN bus") AND ("deep learning" OR "DL") AND ("intrusion detection" OR "anomaly detection" OR "attack detection")	Tüm alanlar
Scopus	(TITLE-ABS-KEY (("controller AND area AND network" OR "CAN bus")) AND TITLE-ABS-KEY (("deep AND learning" OR "dl")) AND TITLE-ABS-KEY (("intrusion AND detection" OR "anomaly AND detection" OR "attack AND detection")))	Başlık, özet, anahtar kelimeler
Web of Science	AB = (("controller area network" OR "CAN bus") AND ("deep learning" OR "DL") AND ("intrusion detection" OR "anomaly detection" OR "attack detection"))	Özet
Science Direct	(("controller area network" OR "CAN bus") AND ("deep learning" OR "DL") AND ("intrusion detection" OR "anomaly detection" OR "attack detection"))	Başlık, özet, anahtar kelimeler
Google Scholar	(("controller area network" OR "CAN bus") AND ("deep learning" OR "DL") AND ("intrusion detection" OR "anomaly detection" OR "attack detection"))	Tüm alanlar

4. Literatür Taraması ve Analizi

Bu bölümde, her bir araştırma sorusu için 10 çalışmanın ayrı ayrı analizi verilmiştir.

4.1. S1: CAN-IDS'lerde Kullanılan Derin Öğrenme Yöntemleri

Song ve arkadaşları (2020), araç içi haberleşmeyi sağlayan CAN'i siber saldırılardan korumak için derin evrişimli sinir ağına (Deep Convolutional Neural Network-DCNN) dayalı bir saldırı tespit sistemi önermiş ve bu yöntemle CAN veriyolu üzerinden iletilen mesajların saldırı mı yoksa normal mi olduğunun tespitini gerçekleştirmiştir. Önerilen IDS için DCNN'nin bir türü olan ve büyük ölçekli görüntülerin sınıflandırılması için tasarlanan Inseption-Resnet modeli kullanılmıştır. Girdi-çıktı boyutundaki farklılıklar ve veri yapısının karmaşıklığı nedeniyle mimarideki bileşenler azaltılarak ve parametreler ayarlanarak orijinal Inception-Resnet modeli yeniden tasarlanmıştır. Tasarlanan bu model, Song ve Kim (2021) tarafından gerçekleştirilen çalışmada da kullanmıştır. Elde ettikleri CAN verileri ile bu modeli eğittiklerinde patlayan gradyan problemi ile karşılaşmışlar. Bu sorunun üstesinden gelmek için hesaplanan gradyanın belirledikleri eşik değerinden daha büyük olması durumunda gradyan kırpma işleminin uygulanmasını önermişlerdir.

Tariq vd. yapmış oldukları çalışmada CAN veri yolu için anomalilik oluşturma, algılama ve değerlendirme sistemi olan CAN-ADF'i (CAN Bus Message Attack Detection Framework) önermiştir. Önerdikleri bu sistemde saldırıların tespiti için kural tabanlı sezgisel yaklaşımdan ve tekrarlayan sinir ağlarının bir türü olan Uzun-Kısa Dönemli Bellek Ağı (Long-Short Term Memory-LSTM) yönteminden yararlanılmıştır. Kural tabanlı sezgisel yaklaşım için öncelikle CAN trafiği analiz edilmiş ve ardından çalışmada belirlenen saldırıların her biri için kurallar tanımlanmıştır. Bu iki yöntem hem ayrı ayrı hem de beraber uygulanarak CAN veri yolundaki saldırılar tespit edilmeye çalışılmıştır (Tariq vd., 2020).

Hossain ve arkadaşları tarafından araç içi CAN veri yoluna yapılan ağ saldırılarını tespit etmek ve saldırıları azaltmak için LSTM yöntemine dayanan IDS modeli geliştirilmiştir. İncelediklerı çalışmalar doğrultusunda, CAN'e yapılan saldırıların tespitinde derin öğrenme yöntemlerinden özellikle LSTM'in istatistiksel analiz, Hidden Markov modeli ve frekans tabanlı analiz gibi yöntemlere oranla daha iyi performans gösterdiğini ve bu sebeple de LSTM yöntemini tercih ettiklerini belirtmişlerdir. Belirlenen bu yöntemin öğrenme oranı, aktivasyon fonksiyonu, gizli katman sayısı, optimizasyon algoritması ve kayıp fonksiyonu hiperparametreleri için çeşitli denemeler yapılarak en iyi parametreler seçilmeye çalışılmıştır. Hiperparametre ayarlamalarının yapılmasının ardından önerilen LSTM modeli ile hem ikili sınıflandırma (saldırı/normal) hem de saldırı türünün tespit edilmesi için çoklu sınıflandırma gerçekleştirilmiştir (Hossain vd., 2020). Başka bir çalışmada, Qin ve arkadaşları da CAN veri yolundaki saldırıların tespiti için LSTM yöntemini kullanmıştır. Çalışmalarında önerdikleri LSTM modelinin mimarisi hakkında çok fazla detaya yer vermeyip sadece optimizasyon algoritması ve öğrenme oranı hiperparametrelerinin seçimine değinilmiştir (Qin vd., 2021).

Hanselmann ve arkadaşları (2020) ise CAN veri yolundan gelen büyük boyutlu CAN mesaj akışından bilinen ve bilinmeyen saldırı türlerini tespit etmek için derin öğrenmeye dayalı CANet isimli bir saldırı tespit modeli önermiştir. Bu modelde LSTM ve otokodlayıcı (Autoencoder-AE) yöntemlerinden yararlanılmış olup denetimsiz öğrenme yaklaşımı esas alınmıştır. Ayrıca önerilen modelin dezavantajı olarak sistemin karmaşık olması, sinir ağının eğitimi için büyük boyutlu eğitim verisinin gerektiği ve hesaplama maliyetinin yüksek olduğu belirtilmiştir.

Kang ve Kang yapmış oldukları çalışmada araç içi CAN veri yoluna yerleştirilen kötü amaçlı veri paketlerini tespit etmek için Derin Sinir Ağları (Deep Neural Network-DNN) tabanlı IDS önermiştir. Önerdikleri bu yöntem ile ağ üzerinden iletilen paketlerin normal mi yoksa kötü amaçlı mı olduğunu belirlemek için ikili sınıflandırma yapılmıştır (Kang ve Kang, 2016). DNN yöntemini kullanan başka bir çalışmada (Zhang vd., 2019) ise araç içindeki anormal davranışların tespitinin doğruluğunu ve verimliliğini arttırmak için 2 farklı optimizasyon algoritması önerilmiştir. Bunlar momentumlu gradyan iniş (Gradient Descent with Momentum-GDM) ve uyarlanabilir kazançlı GDM (Gradient Descent with Momentum and Adaptive Gain-GDM/AG) algoritmalarıdır. Zhang vd. (2019), GDM ve GDM/AG algoritmalarının kullanılmasının asıl hedefinin önerilen IDS modelinin daha hızlı yakınsamasını sağlayarak daha kısa sürede saldırıların tespit edilmesi olduğunu belirtmiştir.

Gao ve arkadaşları (2019) araç içi saldırı tespiti ile ilgili yapılan geçmiş çalışmaları incelemiş ve bu çalışmalarda önerilen IDS modellerinin büyük bir kısmının belirli bir araca veya belirli saldırılara yönelik olduğunu başka bir deyişle IDS'lerin evrensel olmadığını belirtmiştir. Bu kapsamda, evrensel bir IDS modeli oluşturmak için derin öğrenmeye ve bilgi temsil yapısı olan SOEKS'e (Set of Experience Knowledge Structure) dayalı yeni bir araç içi saldırı tespit modeli önerilmiştir. Bu çalışmada, derin öğrenme yönteminin öznitelik çıkarımı için kullanıldığı yüzeysel olarak ifade edilmiş olup evrensel IDS modelinin temelini oluşturan SOEKS yapısına daha fazla değinilmiştir.

Amato ve diğerleri (2021), CAN veri yoluna yönelik saldırıların tespit edilmesi için derin öğrenmeye dayalı iki farklı sınıflandırma algortiması kullanmıştır: Sinir Ağları (Neural Networks-NN) ve Çok Katmanlı Algılayıcı (Multi Layer Perceptron-MLP). Bu iki algoritma ile hem ikili hem de çoklu sınıflandırma gerçekleştirilmiştir. Ayrıca MLP mimarisinin gizli katman sayısındaki değişikliğin saldırı tespit modelinin performansı üzerindeki etkisi araştırılmıştır.

4.2. S2: CAN-IDS'lerde Kullanılan Veri Kümesi ve Odaklanılan Saldırı Türleri

Hossain ve arkadaşları (2020), önerdikleri LSTM tabanlı CAN-IDS modeli için hem kendi veri kümelerini oluşturmuş hem de (Han vd., 2018) çalışmasındaki üç farklı araçtan (Sonata, Soul ve Spark) toplanan ve üç saldırı türünü içeren veri kümesini kullanmıştır. Oluşturdukları veri kümesi için Vehicle Spy analiz aracı ile Toyota Hybrid otomobilinden saldırısız CAN mesajları toplanmıştır. Toplanan gerçek CAN mesajlarına, tasarlanan DoS, bulanık ve sahtecilik saldırı senaryoları uygulanarak saldırı veri kümesi oluşturulmuştur. Veri kümesindeki her bir kayıt 11 öznitelik ve etiket bilgisine (saldırı/iyi huylu) sahip olmakla birlikte önerilen IDS modeli için zaman damgası dışındaki 10 öznitelik seçilmiştir:

- CAN- ID: CAN mesajlarının kimlik bilgisi.
- DLC: İletilen verinin kaç bayt olduğu bilgisi (maksimum 8 bayt olabilir).
- Veri alanı (D0-D7): İletilen verideki her bir baytta tutulan bilgi.

Kang ve Kang (2016) yapmış oldukları çalışma için araç içi ağı simüle ederek yaklaşık 200.000 CAN paketi üretmiştir. Bu çalışmada genel bir saldırı senaryosu tasarlanarak bazı CAN paketleri manipüle edilmiştir. Önermiş oldukları saldırı tespit modeli için CAN paketlerinin sadece 64 bitlik veri alanıyla ilgilenilmiştir. Bu paketlerden ağın istatistiksel davranışını temsil eden özelliklerin çıkarılması için DNN yöntemini kullanarak kötü amaçlı bir saldırının olup olmadığını tespit etmeye çalışmışlardır.

Zhang vd. (2019), çalışmalarında kullanılacak veri kümesi için gerçek bir araçtan KvaserCAN Leaf Light V2 aracılığıyla CAN paketlerini toplamıştır. Toplanan CAN paketleri üzerinde tekrar ve sahtecilik saldırılarının oluşturulması için bilgisayar aracılığıyla saldırganlar simüle edilmiştir. Ayrıca CAN paketlerinin zaman damgası, mesaj kimliği (CAN-ID), veri alanı ve aracın durum bilgisini içeren açıklamaların yer aldığı belirtilmiştir.

Araç içi evrensel IDS modeli için SOEKS bilgi temsil yapısını öneren Gao ve arkadaşları (2019), öncelikle araç içi ağı simüle ederek yaklaşık 100.000 CAN mesajını toplamıştır. Saldırı verilerinin oluşturulması için de entropiye bağlı deneyler gerçekleştirilmiştir. Ardından CAN verilerinin standartlaştırılması için SOEKS bilgi temsil yapısının bileşenleri olan değişkenler, kısıtlamalar, fonksiyonlar ve kurallar tanımlanmıştır. Ayrıca yapmış oldukları çalışmada belirli bir saldırı türüne odaklanmadıkları ve genel olarak kötü amaçlı saldırıları tespit etmeyi hedefledikleri belirtilmiştir.

Tariq vd. (2020) yapmış oldukları çalışma için KIA Soul ve Hyndai Sonata araçlarından iki farklı sürücüyle 24 saatten fazla sürüş gerçekleştirerek toplam 7.875.792 CAN paketi toplamıştır. Ayrıca belirlenen DoS, bulanık ve tekrar saldırıları için senaryolar tasarlanmış ve saldırı verileri oluşturulmuştur. Ardından önerilen IDS modeli için 11 öznitelik belirlenmiştir: Zaman farkı, CAN-ID, DLC ve veri alanındaki her bir baytın içerdiği bilgi. Seçilen zaman farkı özniteliği, ağ üzerinden iletilen iki CAN paketi arasındaki zaman aralığını ifade edecek şekilde hesaplanmıştır. Ayrıca sekiz bayttan daha az veri içeren CAN paketleri için 0 ile doldurma (zero-padding) işlemi gerçekleştirilmiştir.

Song ve arkadaşları (2020) önerdikleri DCNN modeli için kendi veri kümelerini oluşturmuştur. Bunun için aracın OBD-II portu üzerinden araç içi ağa bağlanarak saldırısız CAN verileri toplanmıştır. Ardından saldırganın CAN veri yoluna erişimi ve mesaj yerleştirme saldırısı için bir veya daha fazla CAN düğümü üzerinde yetkiye sahip olduğu varsayımıyla hareket etmişler. Böylece belirlenen DoS, bulanık, RPM ve vites sahtecilik saldırıları için veri kümeleri oluşturulmuştur. Oluşturulan CAN verilerinin CAN 2.0B genişletilmiş veri çerçeve formatında olduğu ve dolayısıyla her CAN mesajının 29 bitlik CAN-ID bilgisi içerdiği belirtilmiştir. Önerilen DCNN tabanlı saldırı tespit modeli için sadece CAN-ID bilgisi öznitelik olarak seçilmiştir. Sıralı 29 CAN mesajından 29 bit ID bilgisi çıkarılarak oluşturulan 29x29'luk çerçeve DCNN sınıflandırıcısına girdi olarak verilmiştir.

Hanselmann vd. (2020), çalışmalarında diğer saldırı tespit sistemlerinden farklı olarak CAN paketlerini sinyal uzayında değerlendirmiş ve önerdikleri CANet'in aynı anda birden fazla CAN-ID sinyalleri üzerinde çalışabilme yeteneğine sahip olduğunu belirtmiştir. Bu kapsamda CAN paketlerinin sadece CAN-ID ve veri alanı ile ilgilenilmiştir. CANet saldırı tespit modeli beş farklı saldırı türünü içeren (Plato, sel, oynatma, sürekli değişim ve baskılama saldırıları) hem gerçek hem de sentetik veriler üzerinde değerlendirilmiştir.

Qin ve arkadaşları (2021), CAN veri yolundaki anormal davranışları tespit etmek için ikili ve onaltılı olmak üzere iki veri formatına (64-bit binary, 16-set hexadecimal) dayalı LSTM tabanlı IDS sistemi önermiştir. Önerilen model için CAN-ID ve veri alanları dikkate alınmış olup CAN veri yolunun mesaj akışındaki üç CAN-ID için ayrı ayrı saldırı tespiti gerçekleştirilmiştir. Çalışmada kullanılan veriler gerçek bir araçtan elde edilmiş ve kurcalama saldırıları oluşturmak için kurallar (paket düşürme, tekrar etme ve içerik değiştirme) tanımlanmıştır.

Amato vd. (2021), NN ve MLP tabanlı IDS modelleri için herkesin erişimine açık olan ve dört farklı saldırı türünü (DoS, bulanık, vites ve RPM sahtecilik saldırıları) içeren veri kümelerini kullanmıştır. Önerilen yaklaşım için seçilen öznitelik vektörünün farklı saldırıları sınıflandırmak için yeterli bilgiye sahip olup olmadığını doğrulamaya yönelik deneyler oluşturulmuş ve bunun için tanımlayıcı analiz ve hipotez testi gibi istatistiksel yöntemlerden yararlanılmıştır. Yapılan deneyler sonucunda CAN paketlerinin sekiz bayt olan veri alanlarının saldırı tespiti için

önemli olduğunu ve bu alanların baytlar şeklinde (F1-F8) ele alınması gerektiği belirtilmiştir.

Song ve Kim (2021), genellikle denetimli öğrenme tabanlı IDS modellerinin eğitim veri kümesine bağlı olduğunu ve bu sebeple de modelin bilinmeyen saldırı türlerini tespit edemediğini belirtmiştir. Bu problemin üstesinden gelmek için LSTM yöntemi ile gürültülü sözde normal veriler üretilmiştir. Bunlar, gerçek CAN verilerini taklit eden ancak eklenen gürültü ile normal verilerden sapmasını sağlayan veriler olarak tanımlanmıştır. Oluşturulan bu veriler saldırı olarak etiketlenmiş ve normal CAN verileri ile birlikte DCNN tabanlı IDS modelinin eğitim veri kümesini oluşturmaktadır. Eğitilen modelin saldırılar üzerindeki performansını değerlendirmek için ise (Amato vd., 2021) çalışmasında kullanılan ve dört farklı saldırı türünü içeren veri kümesi tercih edilmiştir.

4.3. S3: CAN-IDS'lerin Performans Değerlendirmesi ve Literatürdeki Diğer Çalışmalarla Karşılaştırılması

Hossain ve arkadaşları (2020), önermiş oldukları LSTM tabanlı CAN-IDS modelinin hem ikili hemde çoklu sınıflandırma performansını iki veri kümesi üzerinde değerlendirmiştir. Bunun için doğruluk (accuracy), F1 skor, duyarlılık (recall), yanlış pozitif oranı (False Positive Rate-FPR) ve yanlış negatif oranı (False Negative Rate-FNR) metriklerinden yararlanmıştır. Oluşturmuş oldukları veri kümesi üzerinde önerdikleri model ile ikili sınıflandırma gerçekleştirdiklerinde DoS ve sahtecilik saldırıları için %100, bulanık saldırılar için ise %99,98 doğruluk değeri elde edilmiştir. (Han vd., 2018) çalışmasındaki veri kümesi kullanıldığında ise her bir otomobil verisindeki üç saldırı türü için çoklu sınıflandırmada %99,7'nin ve ikili sınıflandırma da ortalama %99,87'nin üzerinde doğruluk değeri elde edilmiştir. Bunun yanı sıra her iki sınıflandırmada da bulanık saldırılar için %100 doğruluk değerine ulaşıldığı görülmüştür. Ardından önerilen modelin performansı, bu veri kümesi üzerinde gerçekleştirilen (Han vd., 2018) çalışmasındaki yöntem ile saldırı tespit oranı (detection rate) bakımından karşılaştırılmıştır. Yapılan karşılaştırma sonucunda önerilen LSTM tabanlı modelin daha yüksek saldırı tespit oranına ulaştığı görülmüştür.

Kang ve Kang (2016), saldırı tespiti için geliştirdikleri DNN tabanlı IDS modelinin performansını FNR, FPR ve doğruluk metrikleri ile değerlendirmiştir. Ayrıca modelin performansı, Yapay Sinir Ağları (Artificial Neural Networks-ANN) ve Destek Vektör Makinesi (Support Vector Machine-SVM) yöntemlerininkiyle kıyaslanmıştır. Yapılan değerlendirmeler sonucunda önerilen modelin %97,8 doğruluk, %1,6 FPR ve %2,8 FNR değeri ile diğer yöntemlerden daha iyi performans gösterdiği görülmüştür.

Zhang vd. (2019), önermiş oldukları IDS modelinin performansını ortalama işlem zamanı, ROC eğrisi, FPR, doğru pozitif oranı (True Positive Rate-TPR) metrikleri bakımından literatürde yer alan (Bo vd., 2013) ve (Yan vd., 2014) çalışmaları ile karşılaştırmıştır. Belirlenen bu dört metrik için de diğer iki çalışmaya üstünlük sağladığı ve TPR değerinin %98'e ulaşırken FPR'nin ise yaklaşık %1-2 civarında olduğu belirtilmiştir. Ayrıca önerdikleri GDM/AG algoritmasının GDM'ye göre daha hızlı yakınsama sağladığı ve milisaniye düzeyinde saldırıları tespit edebildiği ifade edilmiştir.

Gao ve arkadaşları yapmış oldukları çalışmada (2019), önerdikleri araç içi CAN-IDS modelinin performansını TPR, FPR, doğruluk ve ROC eğrisi metrikleri ile değerlendirmiştir. Ayrıca modelin performansı, saldırıları tespit etmek için pozitif ve negatif sapmaların ortalama değerini hesaplayan Naive yöntemininki ile karşılaştırılmıştır. Önerilen yöntemin %98'in üzerinde TPR ve yaklaşık %1-2 civarında FPR değeri ile Naive yönteminden daha üstün performans gösterdiği görülmüştür.

Tariq vd. (2020), CAN-ADF modelinin performansını değerlendirmek için F1 skor, doğruluk, duyarlılık ve kesinlik (precision) metriklerini kullanmıştır. Değerlendirmeyi gerçekleştirirken her bir araç için kural ve RNN tabanlı yaklaşımı hem ayrı ayrı hem de birlikte uygulamıştır. İki yöntemin birlikte uygulandığı durumda her iki araç için en yüksek F1 skor değerine (%99-%99,9) ulaşıldığı görülmüştür. Ayrıca önerilen kural+RNN tabanlı saldırı tespit yaklaşımının (Lee vd., 2017) çalışmasındaki OTIDS yöntemi ile karşılaştırılması yapılmış ve her iki araç için de OTIDS yönteminden oldukça başarılı olduğu görülmüştür.

Song ve arkadaşları (2020), CAN'e yapılan saldırıların tespiti için önerdikleri Inception-Resnet modelinin performansını FNR, hata oranı (Error Rate-ER), kesinlik, duyarlılık ve F1 skor metrikleri ile değerlendirmiştir. Modelin sınıflandırma sonuçları incelendiğinde her bir saldırı veri kümesi için %99'un üzerinde F1 skor, kesinlik, duyarlılık değerlerinin elde edildiği görülmüştür. Bulanık saldırıların daha karmaşık olmasından dolayı bu saldırı veri kümesindeki başarının diğerlerine oranla daha düşük olduğu belirtilmiştir. Ayrıca önerilen modelin performansı LSTM, ANN, SVM, k-en yakın komşu (KNN), Naive Bayes (NB), karar ağacı (DT) yöntemleri ile karşılaştırılmış ve DCNN modelinin bu yöntemlerin hepsinden daha başarılı olduğu görülmüştür.

Hanselmann vd. (2020), CANet modelinin performans açısından diğer yöntemlerle doğrudan karşılaştırma yapmanın mümkün olmadığını belirtmiş. Bu sebeple tahmine ve oto kodlayıcıya dayalı (predictive-autoencoder baseline) iki temel yaklaşımla ROC eğrisi altında kalan alan (AUC), doğruluk, TPR, TNR metrikleri aracılığıyla kıyaslama yapılmıştır. Modelin performansı değerlendirildiğinde %99'un üzerinde algılama doğruluğu elde edilmiş ve hem gerçek hem de sentetik veriler üzerinde diğer iki yaklaşımı da önemli bir farkla geride bıraktığı görülmüştür.

Qin ve arkadaşları (2021), önerdikleri modelin performansını F1 skor, duyarlılık, kesinlik, doğruluk ve AUC metrikleri ile değerlendirmiş fakat başka bir yöntemle karşılaştırma yapmayıp farklı araç üzerinde denemeler gerçekleştirmiştir. Belirlenen üç tipik saldırı senaryosu için %90'ın üzerinde doğruluk değeri elde edilmiştir. Önerilen model iki farklı araç üzerinde uygulandığında ise her iki araç için de %85'in üzerinde F1 skor değerinin elde edildiği belirtilmiştir.

Amato vd. (2021), CAN veri yoluna yönelik saldırıları tespit etmeye yönelik önerdikleri NN ve MLP yöntemleri ile hem ikili hem de çoklu sınıflandırma gerçekleştirmiştir. Bu sınıflandırmaların performansını değerlendirmek için ise duyarlılık, kesinlik, F skor ve ROC alanı metriklerinden yararlanılmıştır. İkili sınıflandırma sonuçları incelendiğinde her iki yöntemin de çok başarılı olduğu fakat MLP'nin NN'ye kıyasla daha başarılı sonuçlar verdiği görülmüştür. MLP'nin ikili sınıflandırmadaki bu başarısından dolayı çoklu sınıflandırmada, gizli katman sayısı 0-5 arasında değişen altı farklı MLP mimarisi ele alınmıştır. 1 ve 3 gizli katmana sahip MLP mimarisinin daha başarılı olduğu ve her iki durum için %96,5'ten daha yüksek kesinlik ile duyarlılık değerinin elde edildiği belirtilmiştir.

Song ve Kim (2021) önerdikleri IDS modelinin bilinmeyen saldırı türlerini sınıflandırmadaki başarısını ölçmek için eğitim veri kümesine ipucu verisi olarak ifade edilen RPM sahtecilik saldırı verilerini eklemiştir. Modelin eğitilmesinde ipucu verileri ile birlikte gürültülü sözde normal verilerin kullanılmasının modelin performansını önemli ölçüde arttırdığı belirtilmiştir. Önerilen model SVM, derin otokodlayıcı (Deep autoencoder-DAE) ve denetimsiz öğrenmeye dayalı SOMK-D yöntemleri ile duyarlılık, kesinlik, F1 skor ve doğruluk metrikleri üzerinden karşılaştırılmıştır. Önerilen yöntem ile eğitilen DCNN modelinin 0,9537 doğruluk ve 0,9451 F1 skor değerleri ile en iyi algılama performansı gösterdiği belirtilmiştir. Ayrıca bu modelin hem bilinen hem de bilinmeyen saldırı türleri için oldukça başarılı olduğu ve diğer yarı denetimli öğrenme tabanlı modellerden daha üstün performans gösterdiği belirtilmiştir. Buna ek olarak, patlayan gradyan probleminin üstesinden gelmek için sunulan gradyan kırpma işleminin de model performansı üzerinde olumlu bir etki gösterdiği ifade edilmiştir.

İncelenen çalışmalar, araştırma soruları kapsamında, kullanılan derin öğrenme yöntemi, seçilen öznitelik, odaklanılan saldırı türleri, performans metrikleri ve başka bir yöntemle performans karşılaştırmasının yapılıp yapılmadığı bakımından Tablo 4'te özetlenmiştir. Ayrıca çalışmalarda belirlenen performans metrikleri için elde edilen değerler Tablo 5'te verilmiştir. Hanselmann vd. (2020), önerdikleri saldırı tespit modeli ile baskılama saldırılarında düşük TPR değeri elde ettiklerinden tabloya eklenmemiştir.

5. Sonuç ve Öneriler

Araç içi ağların güvenliği arttırmak için araştırmacılar tarafından şifreleme, kimlik denetimi ve saldırı tespit sistemlerine yönelik çalışmalar gerçekleştirilmiştir. Bu çalışmada araç içi ağ iletişim protokollerinden en yaygın kullanılan CAN'in güvenliğinin sağlanması için derin öğrenme tabanlı IDS'ler üzerine odaklanılmıştır. Bunun için IEEE Xplore, Scopus, Web of Science, Science Direct ve Google Scholar olmak üzere beş veritabanı üzerinde literatür taraması gerçekleştirilerek bu sistematik derleme kapsamında incelenmiş 10 çalışma belirlenmiştir. Seçilen çalışmalar kullanılan yöntem, veri kümesi, öznitelik seçimi, performans metrikleri ve karşılaştırılan yöntem bakımından detaylı bir şekilde incelenmiştir. Bu incelemeler sonucunda:

- Araç içi CAN-IDS modellerinde derin öğrenme yöntemlerinden LSTM'in sıklıkla tercih edildiği görülmüştür. Bunun sebebi olarak ise CAN'den toplanan verilerin zaman serisi olarak ele alınabildiği ve LSTM'in de zaman serisi verilerinde başarılı bir şekilde uygulandığı gösterilebilir.
- Çalışmalarda genellikle gerçek bir araç üzerinden CAN verileri toplanarak veri kümesi oluşturulmakla birlikte sentetik veri kümelerinin de kullanıldığı görülmüştür.
- Önerilen IDS modelleri için öznitelik olarak CAN-ID ve veri alanlarının sıklıkla tercih edildiği dikkat çekmiştir. Bunun sebebi olarak ise bu alanların saldırı tespiti için belirleyiciliğin daha yüksek olduğu ifade edilebilir.
- İncelenen çalışmaların çoğu DoS, sahtecilik, bulanık gibi belirli saldırı türleri üzerine odaklanırken bazıları ise genel saldırı türlerine yoğunlaşmıştır.
- Çalışmalarda önerilen IDS modellerinin performansının değerlendirilmesinde ise sınıflandırma problemlerinde sıklıkla kullanılan doğruluk, duyarlılık, kesinlik, ROC eğrisi, TPR ve FPR metriklerinden yararlanılmıştır.
- İncelenen çalışmaların çoğunda önerilen yöntemler başka yöntemler ile kıyaslanmış olup karşılaştıran yönteme oranla saldırı tespitinde daha üstün performans sergiledikleri belirtilmiştir.

Ayrıca, incelenen çalışmalar doğrultusunda, önerilen CAN-IDS sistemlerinin genellikle iki alanda farklılaştığı görülmüştür:

- Veri önişleme: Genellikle gerçek araçlar üzerinden toplanan CAN verilerinin saldırı tespit sistemi için uygun formata getirilmesi ve saldırıların tespitinde hangi özniteliklerin seçileceğinin belirlenmesi konusunda farklılaşma sağlanmıştır. Bu kapsamda, CAN verilerinin sinyal uzayında değerlendirilmesi, verilerin standartlaştırılmasını sağlamak için SOEKS bilgi temsil yapısının kullanılması, özniteliklerin belirlenmesi için veriler üzerinde istatistiksel analizlerin gerçekleştirilmesi gibi konular üzerine odaklanılmıştır.
- Saldırı tespiti: Buradaki farklılaşma, saldırıların tespit edilmesi için yöntemin doğrudan uygulanması yerine bu yöntem üzerinde çeşitli hiperparametre denemeleri ile daha başarılı bir modelin oluşturulması veya diğer çalışmalardan farklı bir yöntemin önerilmesi gibi durumları içermektedir.

Bu kapsamda derleme için seçilen çalışmaların bu alanlardan hangisine odaklanarak diğerlerinden farklılaşmanın sağlandığı Tablo 6'da verilmiştir.

Yapılan değerlendirmeler ışığında aşağıda belirtilen konularda açık problemlerin olduğu belirlenmiştir:

- Açık veri kümelerinin eksikliği
- Öznitelik seçiminin farklılaştırılması
- Gerçek zamanlı ve açık kaynak kodlu saldırı tespit sistemlerinin eksikliği
- Kriptografik protokollerin güvenlik analizi ve bunu iyileştirmeye yönelik çalışmalar
- Önerilen IDS'lerin bilinmeyen saldırı türlerini tespit edememesi
- Çalışmalarda simülasyon ortamının sıklıkla kullanılması
- Derin öğrenme yöntemlerinin farklılaştırılması

Tablo 4. İncelenen Araç İçi CAN-IDS Çalışmalarının Özetlenmesi

Çalışma	Yöntem	Öznitelik	Saldırı Türü	Performans Metriği	Karşılaştırılan Yöntem
Song ve Kim (2021)	DCNN	CAN-ID	DoS Bulanık Sahtecilik	Doğruluk F1 skor Duyarlılık Kesinlik	SVM DAE SOMK-D
Hossain vd. (2020)	LSTM	CAN-ID DLC Veri alanı	DoS Bulanık Sahtecilik	Doğruluk F1 skor FPR, FNR Duyarlılık	[30]
Kang ve Kang (2016)	DNN	Veri alanı	Genel	Doğruluk FPR, FNR	SVM ANN
Zhang vd. (2019)	DNN	Zaman damgası CAN-ID Veri alanı	Sahtecilik Tekrar	TPR, FPR Doğruluk ROC eğrisi	[31] [32]
Gao vd. (2019)	Net belirtilmemiş	Net belirtilmemiş	Genel	Doğruluk TPR, FPR ROC eğrisi	Naive
Tariq vd. (2020)	LSTM ve kural tabanlı yaklaşım	Zaman farkı CAN-ID DLC Veri alanı	DoS Bulanık Tekrar	Doğruluk F1 skor Duyarlılık Kesinlik	OTIDS [33]
Song vd. (2020)	DCNN	CAN-ID	DoS Bulanık Sahtecilik	F1 skor FNR, ER Duyarlılık Kesinlik	LSTM SVM ANN KNN DT Naive Bayes
Hanselmann vd. (2020)	LSTM ve AE	CAN-ID Veri alanı	Plato Sel Oynatma Sürekli değişim Baskılama	Doğruluk AUC TPR, TNR	Tahmine ve otokodlayıcıya dayalı yöntemler
Qin vd. (2021)	LSTM	CAN-ID Veri alanı	DoS Bulanık Sahtecilik	F skor AUC Duyarlılık Kesinlik	Karşılaştırma yapılmamış
Amato vd. (2021)	NN ve MLP	Veri alanı	DoS Bulanık Sahtecilik	F skor AUC Duyarlılık Kesinlik	Karşılaştırma yapılmamış

Tablo 5. İncelenen Araç İçi CAN-IDS Çalışmalarının Performans Metrikleri

Performans Metrikleri	Song ve Kim (2021)	Hossain vd. (2020)	Kang ve Kang (2016)	Zhang vd. (2019)	Gao vd. (2019)	Tariq vd. (2020)	Song vd. (2020)	Hanselmann vd. (2020)	Qin vd. (2021)	Amato vd. (2021)
Doğruluk	%95,37	≥%99,7	≅%97,8	≅%98	%98	%99,45	-	≥ %99	≥ %99	-
Kesinlik	0,9671	-	-	-	-	≥ 0,97	≥ 0,99	-	≥ 0,994	≥ 0,819
Duyarlılık	0,9262	≥ 0,9792	-	-	-	≥ 0,93	≥ 0,99	-	≥ 0,791	≥ 0,902
F1 skor	0,9451	≥ 0,9696	-	-	-	≥ 0,95	≥ 0,99		≥ 0,881	-
F skor	-	-	-	-	-	-	-	-	-	≥ 0,858
AUC	-	-	-	-	-	-	-	≥ 0,743	≥ 0,868	≥ 0,984
FNR	-	≤0,0208	≅%2,8	-	-	-	≤%0,35	-	-	-
TNR	-	-	-	-	-	-	-	≥ 0,911	-	-
FPR	-	≤0,0034	≅%1,6	≅%1-2	≅%1-2	-	-	-	-	-
TPR	-	-	-	≅%98	>%98	-	-	-	-	-
ER	-	-	-	-	-	-	≤%0,18	-	-	-

Tablo 6. Çalışmaların Odaklandığı Alanlar

Çalışma	Veri Önişleme	Saldırı Tespiti
Song ve Kim (2021)	✓	
Hossain vd. (2020)		✓
Kang ve Kang (2016)	✓	
Zhang vd. (2019)		✓
Gao vd. (2019)	✓	
Tariq vd. (2020)		✓
Song vd. (2020)		✓
Hanselmann vd. (2020)		✓
Qin vd. (2021)	✓	
Amato vd. (2021)	✓	

Kaynakça

Al-Jarrah, O. Y., Maple, C., Dianati, M., Oxtoby, D., & Mouzakitis, A. (2019). Intrusion detection systems for intra-vehicle networks: A review. IEEE Access, 7, 21266-21289.

Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. ACM Computing Surveys (CSUR), 54(1), 1-37.

Amato, F., Coppolino, L., Mercaldo, F., Moscato, F., Nardone, R., & Santone, A. (2021). CAN-Bus Attack Detection With Deep Learning. IEEE Transactions on Intelligent Transportation Systems.

Baki, S., & Tutkun, N. (2021). Otomotiv haberleşmesinde denetleyici alan ağı için hibrit bir saldırı savuşturma uygulaması. Anadolu Bil Meslek Yüksekokulu Dergisi, 16(61), 51-72.

Bosch, R. (Ed.). (2014). Bosch automotive electrics and automotive electronics: systems and components, networking and hybrid drive. Springer Vieweg.

Bozdal, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of can bus security challenges. Sensors, 20(8), 2364.

Çalışır, S., Atay, R., Pehlivanoğlu, M. K., & Duru, N. (2019). Intrusion detection using machine learning and deep learning techniques. In 2019 4th International Conference on Computer Science and Engineering (UBMK), 656-660. IEEE.

Gao, L., Li, F., Xu, X., & Liu, Y. (2019). Intrusion detection system using SOEKS and deep learning for in-vehicle security. Cluster Computing, 22(6), 14721-14729.

Han, M. L., Kwak, B. I., & Kim, H. K. (2018). Anomaly intrusion detection method for vehicular networks based on survival analysis. Vehicular communications, 14, 52-63.

Hanselmann, M., Strauss, T., Dormann, K., & Ulmer, H. (2020). CANet: An unsupervised intrusion detection system for high dimensional CAN bus data. IEEE Access, 8, 58194-58205.

Hira, E. (2017). Automotive Electronic Control Unit (ECU) Market Size Share, Allied Market Research. Available online: https://www.alliedmarketresearch.com/automotive-electronic-control-unit-ecu-market (accessed on 24 May 2021).

Hossain, M. D., Inoue, H., Ochiai, H., Fall, D., & Kadobayashi, Y. (2020). LSTM-based intrusion detection system for in-vehicle can bus communications. IEEE Access, 8, 185489-185502.

Hu, Q., & Luo, F. (2018). Review of secure communication approaches for in-vehicle network. International Journal of Automotive Technology, 19(5), 879-894.

Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE Access, 4, 5356-5373.

Kalkan, S. C., & Sahingoz, O. K. (2020). In-Vehicle Intrusion Detection System on Controller Area Network with Machine Learning Models. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1-6. IEEE.

Kang, M. J., & Kang, J. W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. PloS one, 11(6), e0155781.

Khatri, N., Shrestha, R., & Nam, S. Y. (2021). Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain. Electronics, 10(8), 893.

Lee, H., Jeong, S. H., & Kim, H. K. (2017, August). OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame. In 2017 15th Annual Conference on Privacy, Security and Trust (PST) (pp. 57-5709). IEEE.

Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. IEEE Network, 31(5), 50-58.

Lokman, S. F., Othman, A. T., & Abu-Bakar, M. H. (2019). Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-17.

Miller, C. (2019). Lessons learned from hacking a car. IEEE Design & Test, 36(6), 7-9.

Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. Journal of information security and applications, 36, 90-100.

Qin, H., Yan, M., & Ji, H. (2021). Application of Controller Area Network (CAN) bus anomaly detection based on time series prediction. Vehicular Communications, 27, 100291.

Sharma, N., Chauhan, N., & Chand, N. (2018, December). Security challenges in Internet of Vehicles (IoV) environment. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 203-207). IEEE.

Song, H. M., & Kim, H. K. (2021). Self-Supervised Anomaly Detection for In-Vehicle Network Using Noised Pseudo Normal Data. IEEE Transactions on Vehicular Technology, 70(2), 1098-1108.

Song, H. M., Woo, J., & Kim, H. K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications, 21, 100198.

Sun, J., Iqbal, S., Arabi, N. S., & Zulkernine, M. (2020). A classification of attacks to in-vehicle components (IVCs). Vehicular Communications, 25, 100253.

Tariq, S., Lee, S., Kim, H. K., & Woo, S. S. (2020). CAN-ADF: The controller area network attack detection framework. Computers & Security, 94, 101857.

Wang, L., & Liu, X. (2018). NOTSA: Novel OBU with three-level security architecture for internet of vehicles. IEEE Internet of Things Journal, 5(5), 3548-3558.

Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2019). A survey of intrusion detection for in-vehicle networks. IEEE Transactions on Intelligent Transportation Systems, 21(3), 919-933.

Yan, S., Malaney, R., Nevat, I., & Peters, G. W. (2014). Optimal information-theoretic wireless location verification. IEEE Transactions on Vehicular Technology, 63(7), 3410-3422.

Young, C., Zambreno, J., Olufowobi, H., & Bloom, G. (2019). Survey of automotive controller area network intrusion detection systems. IEEE Design & Test, 36(6), 48-55.

Yu, B., Xu, C. Z., & Xiao, B. (2013). Detecting sybil attacks in VANETs. Journal of Parallel and Distributed Computing, 73(6), 746-756.

Zhang, J., Li, F., Zhang, H., Li, R., & Li, Y. (2019). Intrusion detection system using deep learning for in-vehicle security. Ad Hoc Networks, 95, 101974.