T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DOKTORA TEZİ

AKILLI ARAÇ AĞLARINDA HİBRİT SALDIRI TESPİT SİSTEMİ MODELİ ÖNERİSİ

Mehmet Fatih YÜCE

Akıllı Ulaşım Sistemleri Anabilim Dalı

Akıllı Ulaşım Sistemleri Programı

DANIŞMAN
Dr.Öğr.Üyesi Mehmet Ali ERTÜRK

II. DANIŞMAN
Doç.Dr. Muhammed Ali AYDIN

Nisan, 2024

İSTANBUL

Bu çalışma 22.04.2024 tarihinde aşağıdaki jüri tarafından Akıllı Ulaşım Sistemleri Anabilim Dalı Akıllı Ulaşım Sistemleri Programında Doktora Tezi olarak kabul edilmiştir.

Tez Jürisi

Dr.Öğr.Üyesi Mehmet Ali ERTÜRK (Danışman)
İstanbul Üniversitesi
Bilgisayar ve Bilişim Teknolojileri Fakültesi

Doç. Dr. Erkan ÇELIK
İstanbul Üniversitesi
Ulaştırma ve Lojistik Fakültesi

Dr.Öğr. Ali BOYACI
İstanbul Ticaret Üniversitesi
Mühendislik Fakültesi

Prof. Dr. Mehmet ADAK
İstanbul Üniversitesi
Ulaştırma ve Lojistik Fakültesi

Prof. Dr. Selim AKYOKUŞ
İstanbul Medipol Üniversitesi
Mühendislik ve Doğa Bilimleri Fakültesi

- **İntihal Programı Beyanı**

20.04.2016 tarihli resmi gazetede yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

- **Proje Destekleri**

Bu tez, "2021-02107" referans ve "SEK 10 589 723" hibe numaralı EUREKA CELTIC Next IMMINENCE projesi tarafından, ayrıca Ulak Haberleşme A.Ş. Yeni Nesil Yazılım Tabanlı Ağlar Projesi kapsamında desteklenmiştir.

- **Tezden Üretilmiş Yayınların Künye Bilgileri**

[Yuce, M. F., Erturk, M. A., & Aydin, M. A. (2024). Misbehavior detection with spatio-temporal graph neural networks. Computers and Electrical Engineering, 116, 109198.,
Yuce, M. F. (2024), "BurST-ADMA Dataset For Spatio-Temporal GNNs", Mendeley Data, V1, doi: 10.17632/m92r72fv23.1,
"EvolveGCNO_improved", https://github.com/mfyuce/EvolveGCNO_improved", last accessed: 2024-03-25,
Patent (Beklemede) 2021/017991 Özel Blok Zinciri Tabanlı Güvenli Eternet ve Local Ağlar,
Patent (Beklemede) 2021/021908 Bir Sertifika Oluşturma ve Dağıtma Sistemi]

ÖNSÖZ

Bu tezi görmeyi çok isteyen, ancak tembelliğim nedeni ile onun vaktine yetiştiremediğim rahmetli babam Galip YÜCE'ye, annem Saide YÜCE'ye, ayrıca geceli gündüzlü çalışmalar sırasında bana en büyük desteği veren kıymetli eşim Mediha KÜFREVİ YÜCE'ye ve gözümün nuru iki evladıma ithaf ediyorum.

Bununla birlikte, tezimin bu hale gelmesinde en üst yardımlarını gördüğüm ve beni yetiştiren hocalarım Doç. Dr. Muhammed Ali AYDIN ve Dr. Öğr. Üyesi Mehmet Ali ERTÜRK'e sonsuz saygılarımı sunarım.

Tez izleme komitemde çalışmama fikirleri ile katkıda bulunan Dr.Öğr.Üyesi Ali BOYACI'ya ve Doç.Dr. Erkan ÇELİK'e teşekkürlerimi sunmayı bir borç bilirim.

Ayrıca son olarak değil, belki en başta belirtmem gereken ve en kötü zamanımda elimden tutup benim devam edebilmemi sağlayan Prof.Dr. Abdullah OKUMUŞ hocam; iyi ki varsınız.

Nisan, 2024 Mehmet Fatih YÜCE

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

$\subseteq$: Alt Küme veya Eşit
$\sum$: Toplam
\# : Adet

Kısaltmalar **Açıklama**

3GPP : The 3rd Generation Partnership Project, 3. Nesil Mobil İletişim Ortaklık Projesi
5G : The Fifth-Generation mobile Telecommunication Technology, 5. Nesil Mobil Telekomünikasyon Teknolojisi
5GAA : The 5G Automotive Association, 5G Otomotiv Derneği
AD : Autonomous Driving, Otonom Sürüş
ADMM : Alternating Direction Method of Multipliers, Çarpanların Yön Değiştirme Yöntemi
AGL : Automotive Grade Linux, Otomotiv Sınıfı Linux
AGNN : Attention-based Graph Neural Network, Dikkat Tabanlı Grafik Sinir Ağı
AHN : Add-Hoc Network, Geçici Ağ
AHP : Analytic Hierarchy Process, Analitik Hiyerarşi Süreci
AI : Artificial Intelligence, Yapay Zekâ
ASAM : Association for Standardisation of Automation and Measuring Systems, Otomasyon ve Ölçüm Sistemlerinin Standardizasyonu Derneği
ANN, NN : Artificial Neural Networks, Yapay Sinir Ağları
ASIC : Application Specific Integrated Circuit, Uygulamaya Özel Tümleşik Devre
AV : Autonomous Vehicle, Otonom Araç
BC : Blockchain, Blok Zinciri
BSM : Base Security Message, Temel Güvenlik Mesajları
BTP : Base Transport Protocol, Temel Aktarım Protokolü
C-ITS : Cooperative Intelligent Transport Systems, Kooperatif Akıllı Ulaşım Sistemleri ve Hizmetleri

C-V2X : Cellular V2X, Hücresel V2X

C2C-CC : CAR 2 CAR Communication Consortium, Araçtan Araca İletişim Konsorsiyumu

CA : Cooperative Awareness, İşbirlikçi Farkındalık

CAM : Cooperative Awareness Message, İşbirlikçi Farkındalık Mesajı

CAMP : Crash Avoidance Metrics Partners, Kazalardan Kaçınma Metrikleri İş Ortakları

CAN : Controller Area Network, Denetleyici Alanı Ağı

CEN : European Committee for Standardization, Avrupa Standartlar Komitesi

CGNN, GCN : Graph Convolutional (/Convolutional Graph) Neural Networks, Evrişimli GNN

CIDS : Cooperative IDS, İşbirlikçi IDS

CNN : Convolutional Neural Networks, Evrişimli Yapay Sinir Ağları

CP : Collective Perception, Kolektif Algı

CPM : Collective Perception Message, Kolektif Algı Mesajı

DARPA : Defense Advanced Research Projects Agency, ABD Savunma İleri Araştırma Projeleri İdaresi

dBm, dBmW : Decibel Miliwatt

DCC : Decentralized Congestion Control, Merkezi Olmayan Tıkanıklık Kontrolü

DENM : Decentralized Environment Notification Message, Merkezi Olmayan Çevresel Bildirim Mesajları

DL : Deep Learning, Derin Öğrenme

DM : Distance Measure, Uzaklık Birimi

DML : Distributed Machine Learning, Dağıtık Makine Öğrenmesi

DoS : Denial Of Service, Hizmet Reddi

DP : Differential Privacy, Diferansiyel Gizlilik/Mahremiyet

DSRC : Dedicated Short-Range Communications, Özel Kısa Menzilli İletişim

DT : Decision Tree, Karar Ağacı

ECC : Elliptic Curve Encryption, Eliptik Eğri Şifreleme

eDRX : Extended Discontinuous Reception, Uzatılmış Kesintili Alım

eMTC : Enhanced Machine Type Communication, Geliştirilmiş Makine Tipi İletişim

ETSI : European Telecommunications Standard Institute, Avrupa Telekomünikasyon Standartlar Komitesi

EV : Electric Vehicle, Elektrikli Araç

FANET : Flying Ad-hoc Network, Uçan Geçici Ağ

FCC : Federal Communications Commission, ABD Federal İletişim Komisyonu

FDMA : Frequency Division Multiple Access, Frekans Bölmeli Çoklu Erişim

FFANN : Feed Forward Artificial Neural Network, Basit İleri Doğru Giden Yapay Sinir Ağ

FDD : Frequency Division Duplex, Frekans Bölmeli Çift Yönlü

FFS : For Further Study, Daha Fazla Araştırma İçin

FL : Federated Learning, Fedele Öğrenme

FNTP : Fast Networking & Transport Protocol, Hızlı Ağ ve Aktarım Protokolü

GAN : Generative Adversarial Network, Çekişmeli Üretici Ağ

GDM : Global Dynamic Map, Küresel Dinamik Harita

GEM : Global Environment Model, Küresel Çevre Modeli

GHz : Gigahertz

GL : Geometric Learning, Geometrik Öğrenme

GNN : Graph Neural Networks, Çizelge Sinir Ağları

GNNS : Global Navigation Satellite Systems, Küresel Uydu Seyrüsefer Sistemi

GPS : Global Positioning System, Küresel Konumlandırma Sistemi

GRU : Gated Recurrent Unit, Kapılı Tekrarlama Ünitesi

ICE : Internal Combustion Engine, İçten Yanmalı Motor

IDS : Intrusion Detection System, İzinsiz Saldırı Tespit Sistemleri

INS : Inertial Navigation System, Atalet Seyrüsefer Sistemi

IEEE : Institute of Electrical and Electronics Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü

IEEE-SA : The IEEE Standards Association, IEEE Standartları Birliği

IoT : Internet of Things, Nesnelerin İnterneti

IoV : Internet of Vehicle, Araçların İnterneti

IPS : Intrusion Prevention System, İzinsiz Giriş Önleme

IR : Infrared Radio, Kızılötesi Radyo

IrDA : Infrared Data Association, Kızılötesi Veri Birliği

ISO : International Organization for Standardization, Uluslararası Standardizasyon Örgütü

ITS : Intelligent Transportation Systems, Akıllı Ulaşım Sistemleri

KNN : K-Nearest Neighbors, K-En Yakın Komşu Algoritması

LA : Learning Automata, Öğrenen Otomat

LDM : Local Dynamic Map, Yerel Dinamik Harita

LEM : Local Environment Model, Yerel Çevre Modeli

LiDAR : Light Detection and Ranging, Işık Algılama ve Uzaklık Belirleme

LIN : Local Interconnect Network, Yerel Ara Bağlantı Ağı

LLC : Low Latency Cellular Communication, Düşük Gecikmeli Hücresel İletişim

LoRa : Long Range, Uzun Menzil

LOS : Line-of-sight, Görüş Hattı

LPWAN : Low Power Wide Area Network, Düşük Güçlü Geniş Alan Ağı

LSTM : Long Short-Term Memory, Uzun Kısa Vadeli Bellek

LTE : Long Term Evolution, Uzun Dönem Geliştirme

MA/MBA : Misbehaviour Detection Authority, Uygunsuz Davranış Tespit Otoritesi

MANET : Mobile AHN, Mobil AHN

MCC : The Matthews Correlation Coefficient, Matthews Korelasyon Katsayısı

MB : Misbehaviour, Uygunsuz Davranış

MBD, MD : Misbehaviour Detection, Uygunsuz Davranış Tespiti

MBR : Misbehaviour Report, Misbehaviour Raporları

MHz : Megahertz

MSE : Mean Squared Error, Ortalama Kare Hata

ML : Machine Learning, Makine Öğrenimi

mmWave : Millimeter Wave, Milimetre Dalga

MOST : Media Oriented System Transport, Medya Odaklı Sistem Taşıma

MP : Max Pooling, En Büyük Havuzlama

MPGNN : Message Passing GNN, Mesaj İleten GNN

N/A : Not Available, Ulaşılabilir Değil

NB-IoT : Narrowband IoT, Dar Bant Nesnelerin İnterneti

NFV : Network Function Virtualization, Ağ İşlevi Sanallaştırması

NGSDN : New Generation SDN, Yeni Nesil SDN

NGV : New Generation VANET, Yeni Nesil VANET

NHTSA : National Highway Traffic Safety Administration, ABD Ulusal Kara Yolu Trafik Güvenliği İdaresi

NIDS : Network IDS, Ağ IDS'si

NLOS : Non-Line-of-Sight, Görüş Hattı Dışı

NN, ANN : Artificial Neural Networks, Yapay Sinir Ağları

NR : New Radio, Yeni Radyo

OBU : On-Board Unit, Yerleşik Ünite

OFDMA : Orthogonal Frequency Division Multiple Access, Dikey FDMA

PAN : Personal area network, Kişisel Alan Ağı

PC5 : LTE-V2X

PCA : Principle Component Analysis, Temel Bileşenler Analizi

PCM : Powertrain Control Module, Güç Aktarma Sistemi Kontrol Modülü

PER : Probabilistic Entity-Relationship Model, Olasılıklı Varlık-İlişki Modeli

PKI : Public Key Infrastructure, Açık Anahtar Altyapısı

POS : Proportional Overlap Score, Orantılı Örtüşme Puanı

PyG : PyTorch Geometric

ReLU : Rectified Linear Unit, Düzeltilmiş Lineer Ünite

RF : Random Forest, Rastgele Orman

RFID : Radio Frequency Identification, Radyo Frekansı ile Tanımlama

RL : Representational Learning, Temsili Öğrenme

RNN : Recurrent ANN, Tekrarlayan Yapay Sinir Ağı

RSU : Road Side Unit, Yol Kenarı Birimi

RSSI : Received Signal Strength Indicator, Alınan Sinyal Gücü Göstergesi

Rx : Reception, Alım

SAE : Society of Automotive Engineers, Otomotiv Mühendisleri Derneği

SAT : Self Attention Network, Kişisel Dikkat Ağı

SB : Standard Bodies, Standart Kuruluşlar

SC-FDMA : Single-Carrier FDMA, Tek Taşıyıcılı FDMA

SDN : Software Defined Network, Yazılım Tanımlı Ağ

SDR : Software Defined Radio, Yazılım Tanımlı Radyo

SLE : Self Loop Edge, Kendi Kendine Döngü Kenarı

SOC : System on a Chip, Çip Üzerinde Sistem

SPoF : Single Point of Failure, Tek Bir Arıza Noktası

SCMS : Security Credential Management System, Güvenlik Kimlik Bilgisi Yönetimi Sistemi

SVM : Support Vector Machines, Destek Vektörü Makineleri

TA : Threat Analysis, Tehdit Analizi/Değerlendirmesi

TDD : Time Division Duplex, Zaman Bölmeli Çift Yönlü

USDOT : United States Department of Transportation, ABD Ulaştırma Bakanlığı

UNII-3 : Unlicensed National Information Infrastructure, Lisanssız Ulusal Bilgi Altyapısı 3

Uu : 5G Uu Interface, 5G Uu Arayüzü

V2X : Vehicles to Everything, Araçlardan Her Şeye

VANET : Vehicle Ad-Hoc Networks, Araç Geçici Ağları

WAVE : Wireless Access in Vehicular Environments, Araç Ortamlarında Kablosuz Erişim

Wi-Fi : Wireless Fidelity, Kablosuz Bağlantı Alanı

WSMP : WAVE Short Message Protocol, WAVE Kısa Mesaj Protokolü

Tx : Transmission, İletim

TVRA : Threat Vulnerability and Risk Analysis, Tehdit Zafiyet ve Risk Analizi

ÖZET

DOKTORA TEZİ

AKILLI ARAÇ AĞLARINDA HİBRİT SALDIRI TESPİT SİSTEMİ MODELİ ÖNERİSİ

Mehmet Fatih YÜCE

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Akıllı Ulaşım Sistemleri Anabilim Dalı

Danışman: Dr.Öğr.Üyesi Mehmet Ali ERTÜRK

II. Danışman: Doç.Dr. Muhammed Ali AYDIN

Gelişen teknolojinin amacı, sahip oldukları otonomi seviyelerine bağlı olarak, araçların az veya hiç insan müdahalesi olmadan, otonom çalışabilmesini sağlamaktır. Tam otonom sürüşü (AD) mümkün kılan çeşitli faktörler vardır. Bunlar, düşük gecikmeli hücresel iletişim (LLC), Araçlardan Her Şeye (V2X) ve Yapay Zekâ (AI) olarak öne çıkmaktadır. Ancak, bilgisayar algoritmalarına dayanmak siber güvenlik endişelerini de beraberinde getirmektedir. Herhangi bir Otonom Araçtaki (AV) bir güvenlik ihlali, ciddi yaralanmalara, hatta ölümlere sebep olabilir. Bu nedenle, yeni nesil AV'ler kötü niyetli saldırıları önlemek için iyi güvenlik çözümlerine ihtiyaç duyar. Bu tez, en yeni güvenlik teknolojilerini, protokolleri, organizasyonları ve AD'nin diğer yönlerini irdeleyecektir. Başlangıçta, V2X, İzinsiz Saldırı Tespit Sistemleri (IDS), iş birliğine dayalı güvenlik yaklaşımları ve standartları gibi kavramlara odaklanılacaktır. Ardından, yanlış davranış tespiti (MBD), kolektif algı (CP) ve AI gözünden, bugüne kadar AD üzerine yapılmış en son güvenlik çalışmaları belirtilecektir. Bununla birlikte, bu çalışma, MBD, CP, AI ve ilgili teknolojiler hakkında kapsamlı bir V2X güvenlik kılavuzudur. Öte yandan, MBD, bir V2X ağ öğesinin, araç geçici ağlarında (VANET) işlemler gerçekleştirirken, öğenin amacını veya itibarını değerlendirme sürecidir. V2X ağında bulunan Yanlış Davranış Yetkilisi (MBA), bir ağ öğesinin itibarını farklı kaynaklarla ilişkilendirilen veriler ve ölçümlerle değerlendirir. Bu kaynaklar uygunsuz davranış raporları (MBR), işbirlikçi farkındalık mesajları (CAM), merkezi olmayan çevresel mesajlar (DENM) veya kolektif algı (CP) mesajları (CPM) olabilmektedir. MBR'ler diğer kaynaklar arasında en faydalı katkıyı sunar. MBR, bir V2X ağ öğesinin diğer V2X ağ öğeleri tarafından algılanmış durumudur. MBA tüm raporları alır ve zararlı davranışları

değerlendirir. Değerlendirmenin olumsuz sonuçlanması halinde, hatalı davranışta bulunan tarafın ağa bağlanmak için kullandığı sertifikası geçersiz veya kısıtlı hale getirilir. Böylece düğüm ağa katılamayacak veya en azından aynı kötü amaçlı işlemleri yapamayacak durumda olacaktır. Belirtildiği gibi MBD, sertifika tabanlı bir siber güvenlik mekanizmasıdır. Bu nedenle MBD'ler, Saldırı Tespit Sistemi (IDS) olarak sınıflandırılamazlar. Klasik IDS'ler öncelikle (OSI seviye 3 ve üst katmanlar) veri paketleri üzerinde çalışırken, MBD raporlar veya mesajlar üzerinde çalışmaktadırlar. Literatürde MBA tarafından sağlanan tek karşı önlem bir V2X öğesinin itibarını değerlendirmek ve buna dayanarak da bu öğeyi kısıtlamak veya ağa giriş yapmasını engelleyerek yasaklamaktır. Bununla birlikte, bu çalışmada, MBA içerisinde karşılaşılan güvenlik sorunlarına uzay-zamansal (spatio-temporal, ST) çizelge yapay sinir ağları (GNN) tabanlı bir çözüm önerisi sunulmuştur. GNN'ler, Temsili Öğrenmedeki gelişmelerin ardından araştırmacıların dikkatini çekmeye başlamıştır. Klasik makine öğrenimi (ML) yöntemlerinden farklı olarak, veri yapısında daha fazla kavramı temsil etme yeteneği, GNN'ye açık bir avantaj sağlamaktadır. Öte yandan, MBD, yetkili araçların V2X Ağlarındaki kötü niyetli faaliyetlere karşı korunmasını sağlayan bir güvenlik çözümü haline gelmiştir. Yetkililer MBD'yi standart durumuna getirmektelerse de, ML çalışmaları için gereken yeterli sayıda MBD veri seti bulunmamaktadır. Var olan veri setleri de GNN'ler için uygun durumda değillerdir. Bu çalışmada, klasik MBD veri kümelerini GNN uyumlu hale dönüştürmek için bir algoritma sağlayarak bu konuyu da ele almaktayız. Ardından, V2X ağlarındaki hatalı davranış aktivitelerini tespit etmek için yeni bir GNN modeli önerilmiştir. Elde edilen sonuçlar, önerilen GNN modelinin %99,92 doğruluk, %99,9196 geri çağırma, %41 daha iyi çalışma zamanı verimliliği ve %97,35 Matthews Korelasyon Katsayısı (MCC) ile mevcut yöntemlerden daha iyi performans göstermektedir.

Nisan 2024, 198 sayfa.

Anahtar kelimeler: Araçlardan Her Şeye, Araçların İnterneti, Saldırı Tespiti, Hatalı Davranış Tespiti, Yapay Zekâ, Kolektif Algı.

SUMMARY

Ph.D. THESIS

HYBRID INTRUSION DETECTION SYSTEM MODEL PROPOSAL IN AUTONOMOUS VEHICLE NETWORKS

Mehmet Fatih YÜCE

İstanbul University

Institute of Graduate Studies in Sciences

Intelligent Transportation Systems

Supervisor: Asst. Prof. Mehmet Ali ERTÜRK

Co-Supervisor: Assoc. Prof. Muhammed Ali AYDIN

The aim of developing technology is to enable vehicles to operate autonomously, with little or no human intervention, depending on their level of autonomy. There are several factors that make fully autonomous driving (AD) possible. These stand out as low latency cellular communications (LLC), Vehicles to Everything (V2X) and Artificial Intelligence (AI). However, relying on computer algorithms also raises cybersecurity concerns. A security breach in any Autonomous Vehicle (AV) can cause serious injuries or even death. Therefore, next-generation AVs need good security solutions to prevent malicious attacks. This thesis will examine the latest security technologies, protocols, organizations, and other aspects of AD. Initially, the focus will be on concepts such as V2X, Intrusion Detection Systems (IDS), collaborative security approaches and standards. Then, the latest security studies on AD from the perspective of misbehavior detection (MBD), collective perception (CP) and AI will be highlighted. However, this study is a comprehensive V2X security guide on MBD, CP, AI, and related technologies. On the other hand, MBD is the process by which a V2X network element evaluates the purpose or reputation of the element while performing transactions on vehicle ad hoc networks (VANET). The Misbehavior Authority (MBA) in the V2X network evaluates the reputation of a network element with data and metrics associated with various sources. These sources can be misbehavior reports (MBR), collaborative awareness messages (CAM), decentralized environmental messages (DENM), or collective perception (CP) messages (CPM). MBRs offer the most useful contribution among other resources. MBR is the state of a V2X network element as detected by another V2X network elements. MBA receives all reports and evaluates harmful behavior. If the evaluation

is negative, the certificate used by the offending party to connect to the network will be invalidated or restricted. Thus, the node will be unable to participate in the network or at least will not perform the same malicious actions. As mentioned, MBD is a certificate-based cybersecurity mechanism. Therefore, MBDs cannot be classified as Intrusion Detection Systems (IDS). While classical IDSs primarily work on data packets (OSI level 3 and upper layers), MBDs work on reports or messages. For MBAs, The only countermeasure provided in the literature is evaluating the reputation of a V2X element and based on that, restrict or ban it by preventing it from entering the network. In this work, our method, provided as a solution to indicated security concerns, created with graph artificial neural networks (GNN), has found the best results in the literature. Moreover, GNNs have begun attracting the attention of researchers following advances in Representation Learning. Unlike classical machine learning (ML) methods, the ability to represent more concepts in the data structure gives GNN a clear advantage. On the other hand, MBD has become a security solution that ensures the protection of authorized vehicles against malicious activities in V2X Networks. Although authorities are standardizing MBD, there are not enough MBD datasets needed for ML studies. Existing data sets are also not suitable for GNNs. In this work, we also address this issue by providing an algorithm to convert classical MBD datasets into GNN compatible ones. Additionally, a new GNN model is proposed to detect misbehavior activities in V2X networks. The results obtained show that the proposed GNN model outperforms existing methods with %99.92 accuracy, %99.9196 recall, %41 better runtime efficiency and %97.35 Matthews Correlation Coefficient (MCC).

April 2024, 198 pages.

Keywords: Vehicles to Everything, Internet of Vehicles, Intrusion Detection, Misbehavior Detection, Artificial Intelligence, Collective Perception.

1. GİRİŞ

Araçlardan Her Şeye (V2X) ve otonom araçlar (AV) son yılların üzerinde en çok çalışılan teknolojilerinden olmuşlardır [1]. Bunda elektrikli araçların görece olarak hızlı bir şekilde piyasaya çıkmaları, ayrıca daha az karmaşık bir yapıya sahip olmalarının etkili olduğu düşünülebilir. Her ne kadar AV teknolojisinde elektrikli araçlar önde görünüyor olsa da, tüm araç çeşitlerinde bu teknolojiye yatırım katlanarak ilerlemektedir [1]. Araçlardaki programlanabilirlik artıkça, yazılım karmaşıklığı da bununla birlikte artmaktadır. Yazılımdaki karmaşıklık ise beraberinde araçların siber saldırı yüzeylerini arttırmaktadır [2]. Bu nedenle de bir V2X ağında saldırı tespit (IDS) ve engelleme (IPS) alt yapıları çok daha önemli hale gelmişlerdir. Ancak bir V2X ağı, yerel ağlardan farklı olarak kötü davranış tespiti (MBD) ile korunmaya çalışılır. Bunu yaparken ise araçlardan veya V2X ağında bulunan her ögeden toplanan veriler çok önemli olmaktadır. Bütün bunlarla birlikte, bu tez V2X, AV ve siber güvenlik konularının son durumlarını irdelemeye ve buna bir çözüm olarak da yeni bir model belirtecektir.

Ad-Hoc ağlardaki (AHN) her bir öğe, iletişim kuran bağımsız (eşit) düğümlerdir. Bu öğeler merkezi bir kontrol olmaksızın kablosuz bağlantılar aracılığıyla birbirleriyle veya bağlantı noktası ile iletişim kurarlar [3]. Bununla beraber, Mobil AHN (MANET), düğümlerin çoklu atlama (hop-by-hop) tabanlı bir yöntemle iletişim kurduğu AHN türüdür. Anca bu ağlarda, kablosuz donanımın yetersizliği veya merkezi bir denetleyicinin bulunmaması diğer düğümlerle iletişimi zorlaştırmaktadır. Uçan AHN (FANET) ve VANET, her ikisi de birer MANET türüdür.

Kablosuz Doğruluk (Wireless Fidelity, Wi-Fi) ve Eternet yerel ağ (LAN) alt yapılarıdır. Wi-Fi'da merkezi bir erişim noktası vardır. Ağa kaydolmayı yönetir ve kontrol eder. Böylelikle bu tür ağlarda, ağa kabul, merkezi düğümden geçer. Özel Kısa Menzilli İletişim (Direct Short Range Communication, DSRC) omurgası ile VANET, Wi-Fi [4] teknolojisinden geliştirilmiştir. Burada IEEE (IEEE 802 ve IEEE 1609 ailesi) alt katmanları tanımlarken, Otomotiv Mühendisleri Derneği (SAE) (J2735 ve J2945) uygulama katmanlarını tanımlamaktadır.

DSRC geliştirilmelerine 1990'ların başında başlanmış, ilk araştırma Birleşik Devletler (ABD) Kongresi tarafından üstlenilmiş ve ABD Ulaştırma Bakanlığı'nın (USDOT) akıllı araç-otoyol sistemleri [5] projesi için düşünülmüştür. Bu projenin başarısı ardından, 1999'da Federal İletişim Komisyonu (FCC), Akıllı Ulaşım Sistemleri (ITS) [6] için 5.9 gigahertz (GHz) bandından, spektrumun 75 megahertz'ini (MHz) tahsis etmiştir. Bu 75MHz'lik aralık, 5850MHz ile 5925MHz arasındaydı. 2012'de, Wi-Fi'ya yönelik DSRC değiştirmeleri, IEEE 802.11p olarak IEEE 802.11 standardına eklenmiştir. Avrupa'da ise, spektrumun 30MHz'i, 5875MHz'den 5905MHz'e [7] olarak ayarlanmıştır. Daha sonra 2020'de bu, raylı sistemler için 5915MHz'den 5935MHz'e kadar olan spektrum dahil olmak üzere, 5875MHz ile 5935MHz olmuştur [8]. 2021'de ise, FCC, ITS operasyonlarında C-V2X teknolojilerini kullanmaya çağırmış, spektrumu da lisanssız kullanım için, 5850MHz'den 5895MHz'e (alt 45MHz) tahsis etmiştir. C-ITS için ise frekans spektrumunu, 5895MHz'den 5925MHz'e (üst 30 MHz) almıştır [9].

Yeni nesil V2X (NGV) için olmak üzere, 3. Nesil Ortaklık Projesi (3GPP) ise, yeni radyo (NR) ve 4G/5G Hücresel V2X (C-V2X) önermektedir. IEEE ise, yine yeni nesil olması düşünülerek, bir IEEE 802.11bd değişikliği üzerinde çalışmaktadır. Bununla birlikte, Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) de, CP Mesajları (CPM) üzerinde çalışmaktadır.

Geleceğin araçları işbirlikçi ve otonom olacaktır. Bu tanımın işbirlikçi tarafı V2X ile ilgili standartlardan gelmektedir. Özerklik tarafı ise SAE tarafından tanımlanmaktadır. Otonom araçlarda bulunacak özerklik, sürücüye, yolcuya veya yüke zarar vermeden AV'nin kendisinin karar verme süreci olarak tanımlanabilir. Bu süreç, protokollerle, AI eğitimleri ve öğrenmesi sırasında sistem tarafından sağlanan ve ağ aracılığıyla toplanan metrikler veya durum bilgileri ile desteklenir. Süreç analitiktir; açıklanabilir ve bir dereceye kadar da kanıtlanabilir. Öte yandan, insan kararları hislere bağlıdır ve bu da kişinin içinde bulunduğu duygusal durumdan etkilenebilir. Buna ek olarak, bazı DL algoritmalarının nasıl çalıştıklarını hala açıklayamayabiliyoruz [10]. AI algoritmalarındaki açıklanabilirlik, bu tezin kapsamı dışındadır. Ancak bu karar verme süreci, sürücünün daha iyi bir sonuca varması için araç (veya VANET) tarafından yapılabilir.

Araçların dış ortamla yapılan iletişimine V2X denmektedir. Trafik alt yapısı ve yayalar gibi öğeler arasında iletişim de dahil olmak üzere çok çeşitli teknolojiler içermektedir. Araçların

kendi iç iletişimleri için de yerel ağları Bulunmaktadır. Bu tezin konusu V2X ile ilgili olduğundan iç ağ yapılarından çok bahsedilmeyecektir.

Harici iletişim için, VANET kablosuz iletişim olanaklarını sağlamaktadır. Bu iletişim katmanı Avrupa'da G5, ISO'da M5 ve ABD/SAE'de WAVE (DSRC) olarak tanımlanır. IEEE 802.11p, ağ ve taşıma katmanlarını tek bir katmanda birleştirerek OSI katmanlama ana akımından ayrılmaktadır.

Siber güvenlik, herhangi bir iletişimin temel direklerinden biridir. VANET, standartlarda görüldüğü kadarı ile, ağırlıklı olarak sertifika tabanlı bir güvenlik mekanizması [11] sunmaktadır. İletişim bu sertifikalar ile şifrelenir. Bu yapıda, türetilmiş (sahte/psödo) sertifikalar adı verilen bir yapı bulunmaktadır. Kullanılma sebebi ise süreçte gerçek sertifikaların kullanılmasını engellemektir. Bunun için bir iletişim öncesi sahte bir sertifika üretilir. Üretilen her sertifikanın yenilenen bir ömrü vardır [12]. Bununla birlikte, MBD mekanizması ise, kötü davranışlı araçları VANET'den sınır dışı etmeye, kısıtlamaya veya yasaklamaya çalışır. MBD hizmetinin içerikleri ise standartlarda çok net değildir. Ancak raporlama mekanizmaları iyi bir şekilde anlatılmıştır.

Araştırmaların yaptığı tavsiyeler dışında, şu anda AV'lerde siber güvenliğinin temellerini değiştirilmiş X.509 sertifikalar [11, 12] ve MBD sağlamaktadır.

Çizelge (graph) Sinir Ağları (GNN) ise aktif bir araştırma alanıdır. Başlangıçları önceki bin yıldaki araştırmalara dayansa da, temsili öğrenme (RL) ilkelerinin ivme kazanmasıyla sıcak bir konu haline gelmiştir. Veri yapısındaki ilişkileri ve diğer kavramları temsil etme yeteneği, klasik makine öğrenimi (ML) ve derin öğrenme (DL) yöntemlerinin aksine, GNN'ye net bir avantaj sağlamaktadır. Bunun dışındaki özellikleri (dik öğrenme eğrisi, geniş uygulanabilirlik alanı, hatta neredeyse özellik mühendisliğinin hiç bulunmaması) onu başlangıç için en iyi yöntemlerden biri haline getirmektedir. Öte yandan, araçlardan her şeye ağlar (V2X) da son teknoloji ürünü bir konudur. Bir V2X ağı birbiriyle etkileşim halinde olan birçok sabit ve hareketli öğeden oluşur ve bir çizelge yapısında çok iyi bir şekilde temsil edilebilir. Ancak siber güvenlik açısından sertifikalar, güvenli bir V2X ağına katılmanın tek yoludur. Bunun dışında V2X protokolleri mesaj tabanlıdır. Bu durumda, klasik ağ paketi tabanlı izinsiz giriş tespit (IDS) veya izinsiz giriş önleme (IPS) mekanizmaları kullanılamamaktadır. Bunun için güvenli bir V2X'e bağlandıktan sonra hatalı davranış tespiti (MBD) önerilmektedir. MBD'den şu anda yalnızca standartlarda ve en son makalelerde

bahsedilmektedir. Buna ek olarak, literatürde ML operasyonlarında kullanılacak çok fazla MBD veri kümesi de bulunmamaktadır. Ancak mevcut veri kümeleri de GNN için uygun değildir. Bu çalışmada, mevcut bir klasik (MBD) veri kümesinin GNN veri kümesine dönüştürülebileceğini ve bu dönüşümden, yeni bir modelle mevcut araştırmalardan daha iyi sonuçların kolayca elde edilebileceği görülecektir.

Bu tezdeki başlıca katkılar şu şekilde özetlenebilir;

1. VANET ve V2X üzerine ve buna ek olarak MBD altyapıları üzerine oldukça geniş bir literatür taraması
2. Mevcut tablosal veri kümelerinden uzay-zamansal GNN veri kümeleri oluşturmanın genel bir yöntemi,
3. Bu veri kümelerini mevcut yapay zekâ araçlarına yüklemek ve işlemek için bir GNN yükleyici,
4. Bu veri kümelerini değerlendirmek ve denemek için özelleştirilmiş bir GNN yöntemi,
5. Uzay-zamansal GNN modellerinin performansını değerlendirmek için yeni bir performans metriği oluşturma yöntemi.

Bu Tezin geri kalan yapısı şu şekilde organize edilmiştir; Bölüm 2., VANET, V2X, MBD ve GNN konuları ile ilgili geniş bir literatür taramasıdır. Bölüm 3. de tez sonucu olan yöntem geliştirilirken kullanılan altyapılar hakkında bilgi verilecektir. Bölüm 4. de ise tez çalışmaları ile gerçekleştirilen modelin sonuçları hakkında bilgi verilmiştir. Bölüm 5. de tezin gerçekleştirdikleri ardından çıkan sonuçlar ve gelecek ile ilgili araştırma yönleri belirtilmiştir.

2. GENEL KISIMLAR

Teknolojik yatırım yapan firmaların ve standart kuruluşlarının (SB) yoğun çalışmaları sayesinde, son on yıl, Otonom Araçların (AV) gerçeğe dönüşmesine tanık oldu [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 7, 8, 24, 25, 26]. Bununla birlikte hava limanları gibi, tam otonomi sağlayan altyapılar gelişmeye başladığı gibi, Niğde-Ankara otoyolu gibi, üçüncü seviye otonomiye sahip araç sürüş olanakları da bulunmaktadır [1] . Bu olurken V2X'in önünü açan temel teknolojiler şunlar olmuştur;

- Hücresel ağlar [27],
- Kablosuz Radyo/Işık/Kızılötesi (IR) İletişimi [28],
- Nesnelerin İnterneti (IoT) [29]
- Araçların İnterneti (IoV) [27],
- Yazılım Tanımlı Ağ Oluşturma (SDN) [30]
- Ağ İşlevi Sanallaştırması (NFV) [31]
- AI/Derin Öğrenme (DL) [26]

Araçların, otonom olabilmesi için heterojen ortamlarda "sosyal" [24] olması gerektiği öngörülüyor. "Sosyal" sözcüğünün altı çizilmek gerekirse, çevrelerinin durumu hakkında diğer düğümleri bilgilendirmeleri ve başkalarının da aynı konudaki algılarını almaları gerekmektedir. Önceden, bu amaçla yalnızca işbirlikçi farkındalık (CA) yayın (broadcast) mesajları kullanılıyordu. Her türlü ağ öğesi (yaya, bisiklet, çeşitli araç tipleri vb.) yola çıktığında ise CA yetersiz hale gelebilmektedir. Bununla birlikte, son zamanlarda kolektif algının (CP) [32] bu yönde bir ilerleme olduğu düşünülmektedir. Tezin hazırlandığı tarih itibarı ile de, bu mesajı siber güvenlik şemsiyesi altına almak standartların kapsamı dışında kalmıştır. Yalnızca IEEE belgelerinde yanlış davranış tespiti (MBD, standartlarda MD olarak kısaltılır) ile ilgili "bahsetmeler" diyebileceğimiz kısımlar bulunmaktadır. ETSI'den de yayın

[1] https://www.ankaranigdeotoyolu.com/akilli-ulasim-sistemleri

öncesi bir rapor ve bir fizibilite çalışması (TVRA yöntemi) olarak yoldadır [33, 34]. Ancak bu raporlar sadece CA ile MBD üzerindedir. Aynı zamanda sadece sertifika tabanlı bir güvenlik sistemi tanımlar (SCMS sistemi). MBD standartlarında CP ile ilgili herhangi bir ifade yoktur. Ayrıca, her iki konuyu araştıran ve birleştiren çalışmalar, bu tezin yazıldığı tarihte bulunamadı. Bu tezin yardımcı olacağı konulardan bir tanesi "Daha iyi yanlış davranış tespiti ile sonuçlanmak için MBD'yi CP ile entegre etme olasılığı nedir?" sorusu olacaktır.

MBD omurgası, yol kenarı biriminin (RSU) ötesinde (uç/sis veya bulut) VANET dışında barındırılır. MBD, özel amaçlı bir saldırı tespit sistemidir (IDS). CA mesajlarının farkındadır, ancak CP mesajı (CPM) ile ilgili çalışmalar hala standartlarda yoktur ve araştırma çalışmaları devam etmektedir. Bu anlamda, bu çalışma, saldırı tespiti, MBD ve CP'yi göz önünde bulundurarak, V2X'te siber güvenlik konusunda son beş yılda kaydedilen gelişmeleri de sunacaktır. En yeni ağ teknolojilerini, organizasyonları ve protokolleri de içerecektir. Her bölüm kendi başına bir çıkarım olsa da, gelecekteki çalışmalar için çıkarımlar da belirtilecektir. Başlangıçta, genel bir V2X bilgisi ve ilgili teknolojiler gösterilecektir. Bu tez, V2X ve IDS'den, MBD ve CP'ye kadar kapsamlı ayrıntıları nedeniyle literatürden oldukça fazla bilgiyi bir araya getirmiştir. Bu tez, güvenlik açısından, bu alanlara ışık tutmaya çalışacaktır. Ayrıca bu tez, bu teknolojileri ve geleceklerini MBD ve CP'nin gözünden de irdelemeye çalışacaktır.

2.1. OTONOM ARAÇLAR

Otonom araçlar elektrikli araçların çıkması ile daha popüler olmuştur [1]. Yaklaşık iki yüz yıl sonra bile, içten yanma motorlu (ICE) otomobillerin otonom sürüş teknolojisinde çok da ileri gidemediği görülmektedir. Ancak bu ICE araçların otonom olamayacağı anlamına gelmemektedir. Sadece daha büyük sorunlara sahip oldukları anlaşılabilir. Bunun nedenlerinden birisi çok karmaşık olan motor yapısı ve kapladığı alan gösterilebilir. Öte yandan, geleceğin arabasının elektrikli olması öngörülüyor. Bunun bir nedeni CO2 emisyonu ile ilgili kaygılardır [35]. Araçlar elektrikli olacağı için de, beraberinde gelen sadelik, başka bir özellik için değerlendirilebilecek bir alan sağlamaktadır. İlk elektrikli arabalara verimli bir şekilde güç sağlanamadığından, uzun menzilli sürüş için uygun olamadılar. Pil ve elektrikli kontrol üniteleri (ECU) teknolojisindeki gelişmeler, klasik arabaların yerini alabilecek modern elektrikli araçların (EV) ortaya çıkmasına sebep oldu [36]. Ayrıca modern

EV'ler, otonom şanzıman, otonom park etme ve A noktasından B noktasına insan müdahalesi olmadan sürüş gibi otonom görevleri gerçekleştirebilmektedir. Kısaca AD, aracın çevresini algıladığı, ayrıca verilen bir amaca göre gerekli eylemlerin gerçekleştirildiği sürekli bir görevdir.

AD'de birimler, çevreyi algılayabilen, çevre ile iletişim kurabilen birimlerle belirtilebilir. Bunlardan çeşitli sensörler (radar, LiDAR, video kameralar, gece görüş kameraları vb.), ağ yapıları (Wi-Fi, V2X, SDN, NFV/VNF), araç tipleri (otomobil, tren, bisiklet vb.), yayalar ve alt yapı (yol kenarı birimleri/RSU, trafik ışıkları, köprüler vb.) sayılabilir. Bu ağ, büyük hareketliliği ve hızlı topoloji değişikliklerini işlemeli ve minimum gecikmeye sahip olmalıdır. Araç Doğaçlama (Geçici, Ad-hoc) Ağı (VANET), günlük olarak kullandığımız Wi-Fi teknolojisin, AV'ler için gereken değişikliklerin eklenmesi ile meydana gelen bir sistemdir [25]. Bütün bu bileşimlerin nihayetteki hedefi ise otonom araçlara sahip olmaktır. Ancak yine de, VANET'lerin Seviye 5 özerkliğini (tam otonomi, bkz. 2.2.2.) desteklemek için hala iyileştirmelere ihtiyacı olacaktır. Bunlar kısaca şunlar olabilir (veya daha sonraki gelişmeler aşağıdakilerin üzerinde olabilecektir);

- İletişim için 5G [37] ve ötesi (6G),
- Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) tarafından geliştirilmiş VANET 2.0 (IEEE 802.11bd),
- Altyapı için SDN [38],
- Hat hızıyla (line-speed) programlanabilen yeni ağ donanımları [30].

(Son iki kısım kolay dağıtım ve kolay yeniden yapılandırma için gerekmektedir)

Otonom araçlardaki yoğun geliştirme çalışmalarının farklı sâikleri bulunmakla birlikte, en önemlisinin emniyet olduğu söylenebilir. 2015 Ulusal Kara Yolu Trafik Güvenliği İdaresi (NHTSA) raporuna göre, trafik kazalarının %94'ü insan hatasından kaynaklanmaktadır [39]. Buradan yola çıkarak, tam otonomiye ulaşılıncaya kadar, zamanla insan faktörünün azaltılması öngörülmektedir [40]. Başka bir nokta ise, otonom araç olduğu belirtilen EV'lerin son zamanlarda karıştığı kazalardır. Bu da teknolojinin geldiği durumda tam otonomi ile ilgili emniyet kaygılarını ortaya çıkarmaktadır. Emniyet alanında ise en önemli alt başlığın siber güvenlik olarak karşımıza çıktığı görülmektedir [25].

Uzay çalışmalarında, örneğin Mars gezicisindeki teknoloji, uzun süren sinyal alıp verme nedeni ile belirli bir dereceye kadar otonomiye sahiptir. Hava alanları gibi özel kurulumlar da tam otonomiye sahip olmuşlardır. Ancak otonom araçlarını elektrikli araçlarla eşleştirdiğimiz için, ilk arabanın, elektrikli bir araç olduğu şaşırtıcı olabilir. Ancak, aradan geçen 150 yıl boyunca otonom araç teknolojisinin her yere yayılmasının ve ilerlemesinin genel olarak yavaş geliştiği söylenebilir. Örneğin, DSRC ancak 90'lı yıllarda geliştirilmeye başlanmıştır [5]. Bununla birlikte, Mars gezicisinden farklı olarak, otonom arabalar, kırılgan ve ihtilaflı insanlardan birkaç santim ötede, şehir sokaklarının karmaşık dünyasında gezinmek durumundadır. Ayrıca emniyet, hız, erişim, yolu paylaşan başka arabalar, akıllı kavşaklar ve tıkanıklığı azaltmak gibi konular, ilerlemesi uzun zaman alan problemlerdir.

2.1.1. Otonom Araç Teknolojisi İçin Gerekli Altyapılar

Genel olarak belirtmek gerekirse, tez itibarı ile, AV teknolojisini basamakları aşağıdaki gibi belirtilebilir [1];

1. Algılama/Sensörler
2. Dış dünyayı Modelleme,
3. Karar verme
4. Tepki

İlk, ikinci ve son adımlar bilinen teknoloji ile uygulanabilir, ancak bilinmeyen parça arada ihtiyaç duyulan makine zekâsıdır.

İlk AV altyapılarını daha önce Avrupalı araştırmacılar başlatmış (CAN) [41], ardından ABD ciddi bir ekler yapmıştır. Böylece geliştirilen yol takip ve çarpışmadan kaçınma yazılımları, geliştirilmiş radar, lazer sensörleri ve iyi haritalama sistemleri yukarıdakileri problemleri çözmeyi amaçlamıştır.

2.1.1.1. Algılama ve Sensörler

Sensörler, otonom araçların gerçekleşebilmesi için anahtar konumundadır. Belirli bir özelliği ölçen herhangi bir cihaz otonom araçlarda kullanılabilir. Bunlar basınç, konum, hızlanma

sensörleri vb. olarak sayılabilir. Üç ana sensör tipi bulunmaktadır [42]; Kamera, radar ve LiDAR. Antifriz sıcaklık sensörü veya emme havası sıcaklık sensörü gibi diğerleri de bulunmaktadır.

Kamera

Kameralar, sürücülerin göremediği dünyanın görsel bir temsili olabilirler. AV'ler önde, arkada, sol ve sağda kameralara sahip olabilmektedir. Özelliklerine göre 360 derece veya balık gözü kamera (daha geniş, panoramik görüntü) bulundurabilirler. Özellikle yeni araçlarda bulunan otomatik park etme özelliği kameraları oldukça fazla kullanır.

Radar

1904 yılında Alman mucit Christian Huelsmeyer, "telemobiloskop" adlı bir patent aldı [43]. Bu patentte gemilerin üç kilometre kadar uzaktan geldikleri fark edebiliyordu. Böylece hız, geliş açısı gibi önemli özellikler hava, deniz ve karada hesaplanabilir oldu. Ayrıca kalman filtreleri de denen bir alt yapı ile daha doğru bir bildirim yapmak da mümkün oldu [44]. Radarın yaptığı ana işlem ise, radyo dalgalarını kısa aralıklarla iletmektir. İletilen dalga bir nesneye çarpar, ardından tekrar geldiği yönde bir sensöre yansır. Böylece fark edilen nesnenin hızı ve yönelimi belirlenebilir. Radar kötü şartlarda kamera görüşünü de destekleyebilir, ancak, farklı nesne türlerini fark edemez. Bunun için kamera vardır daha iyi bir sonuç vermektedir.

Kamera türlerinden uzak kızılötesi (far-infrared, uzak kızılötesi) ve ısı kameraları (termal) nesnelerin çıplak gözle görülemeyecek, belli belirsiz resimlerini ortaya çıkarabilir. Özellikle yaşayan nesnelerin fark edilmesi için kullanılırlar. Gece görüşü kameraları bu türdendir. Yere nüfuz eden kameralar da yer altındaki özellikleri algılar.

Kamera ile ilgili ilerideki olacak gelişmeler daha çok askeri türevli sistemlerin sivil alana yayılması ile ilerleyecek gibi görünmektedir [45].

LiDAR

LiDAR kısaltma olarak "Işık Algılama ve Menzil" (Light Detection and Ranging) den türetilmiştir. Kameralar nesne tanıma için, radarlar nesne tespiti için kullanılmakta ve bu ikisi ile sadece bir veya iki seviye algılama mümkün olmaktadır. LiDAR, bunlara ek olarak ışık ile algılamayı getirmiştir. Aracın etrafında, 360 derece, üç boyut bir görüntü sağlamaktadır. Çok az ışığın olduğu ortamlarda iyi çalışır. Bir şekilde kameraya ulaşım olmadığında da ona yakın bir görev icra eder. Ancak fazladan olarak sağladığı şekil ve derinliktir. Daha çok radarlarla birlikte kullanılır (veya kullanılmalıdır). LiDAR, saniyede bir milyon ışık (lazer) atımı yapabilmektedir. Yansımaları harmanlayıp, üç boyut nokta bulutu (3D point cloud) denen bir altyapıya çevirir. Bu üç boyutlu altyapı ile araç çok rahat hareket etme imkanına sahip olur [46].

LiDAR cihazlarının pahalı olması, üzerine konduğu araçlara kötü bir görüntü eklemesi ve kameralarda üç boyut teknolojisinin ilerlemesi [47], LiDAR'a yönelik eleştirileri de beraberinde getirmiştir. Örneğin, Tesla daha önce LiDAR yerine kullandığı ultrason sensörünü de 2021 yılından itibaren kullanmamayı kararlaştırmış[2] . Yeni modellerinde, radarın bile olmayacağını belirtmiştir. Neden olarak da, bir sonraki bölümde anlatılacak olan "sensör bileşimi"'nin (sensor fusion) zorluğunu göstermiştir.

Sensör Bileşimi

Sensör bileşimi, aracın otonom hareketini sağlamak üzere, tüm sensörlerden gelen verilerin merkezi, yüksek performanslı bir sistemde toplanması ve kararların alınmasına yardımcı olmasını sağlamaktır [48]. Bu merkez, NVIDIA DRIVE AGX veya Jetson TX2 gibi yapay zekâ makineleri de olabilmektedir. Sensör bileşimi, literatürde oldukça çok araştırılan [49] ve tartışılan bir alandır. Konu ile ilgili [50, 45, 48, 51] araştırmaları incelenebilir.

Sensör bileşiminin ilgili olduğu önemli bir nokta, yerel dinamik harita (Local Dynamic Map, LDM) [52, 53, 54] veya küresel dinamik harita (Global Dynamik Map, GDM) [55] de denen, standartlarda [56] ve araştırmalarda ayrıca yer bulan durum, temsil veya gösterim (representation) dediğimiz altyapıdır. Bu altyapı, MBD'nin de ilgi alanındadır. Tezin hazırlandığı an itibarı ile, daha iyi bir MBD, bu sistem üzerinde çalışmalıdır gibi

[2] https://www.tesla.com/support/transitioning-tesla-vision

görünmektedir. Sistemde bulunan nesnelerin durumlarını, hem araçlardan gelen bilgilerle, hem de merkezde tutulan küresel haritadan alıp, son karar buna göre verilebilir. Buna ek olarak, CP, bu konunun önemini belirtmiş ve yine standartlarda yer bulmuştur [57].

Sensörler - Tartışma

Kameralar parlamalardan etkilenebilirler, radar ise bir nesnenin hızını bulabilir ancak görme yetisi iyi değildir. Ultrason sensörleri, yalnızca yakın nesneleri çok iyi biçimde olmayacak şekilde fark edebilirler. LiDAR'ın da uzaklık problemi bulunmakta ve yağmur altında iyi performans gösterememektedir. En iyi yapay zekâ ile bile, doğru veri olmadan iyi bir sonuç veremez. Ancak, alınması gereken çok yol olsa da, otonom araçlar zamanımızda şehir sokaklarında gezmeye başlamıştır bile.

2.1.1.2. Dış Dünyayı Modelleme

Dış dünyayı modelleme, otonom araçların önündeki en önemli konulardan birisidir [54]. Araçlar etraflarını çok iyi irdeleyip, bu duruma göre tavır almalıdır. MBD ise, merkezde toplanan (fusion) bu model ile gerekli kararları verebilmelidir. Sensörlerden gelen veri, bu modeli oluşturmada en büyük yardımı sağlar. Ancak, çoğu zaman olduğu gibi, araştırmalar, ilk önce benzetim (simülasyon) uygulamalarından başlar. Bunun için de gerekli birçok veriyi sahadan toplamak zorundadırlar. Bu nedenle, sürüş veri kümeleri bu konuda çok yardımcı olacaklardır. Sürüş veri kümeleri yoksa bile, Carla [58] gibi üç boyutlu, gerçeğe yakın benzetim sunan sistemler de bulunmaktadır. Bununla birlikte, dış dünya modellemesi yaparken aşağıdaki gibi bazı durumların hesaba katılması gerekmektedir [59];

- Hava durumu (bulut opaklığı ve yaygınlığı, ışık şiddeti, güneş sıcaklığı),
- Günün saati (ışık, parlaklık, mercek parlaması veya yansıması, gündüz veya gece olması),
- Reklam tabelaları, duvarlar, diğer araçlar (bisikletler, yayalar),
- Frenleme mesafesi, hız,
- Kara yolu ağı (nadiren optimum durumdadır, çizgiler solabilir, belirsiz sapmalar vardır) [60],

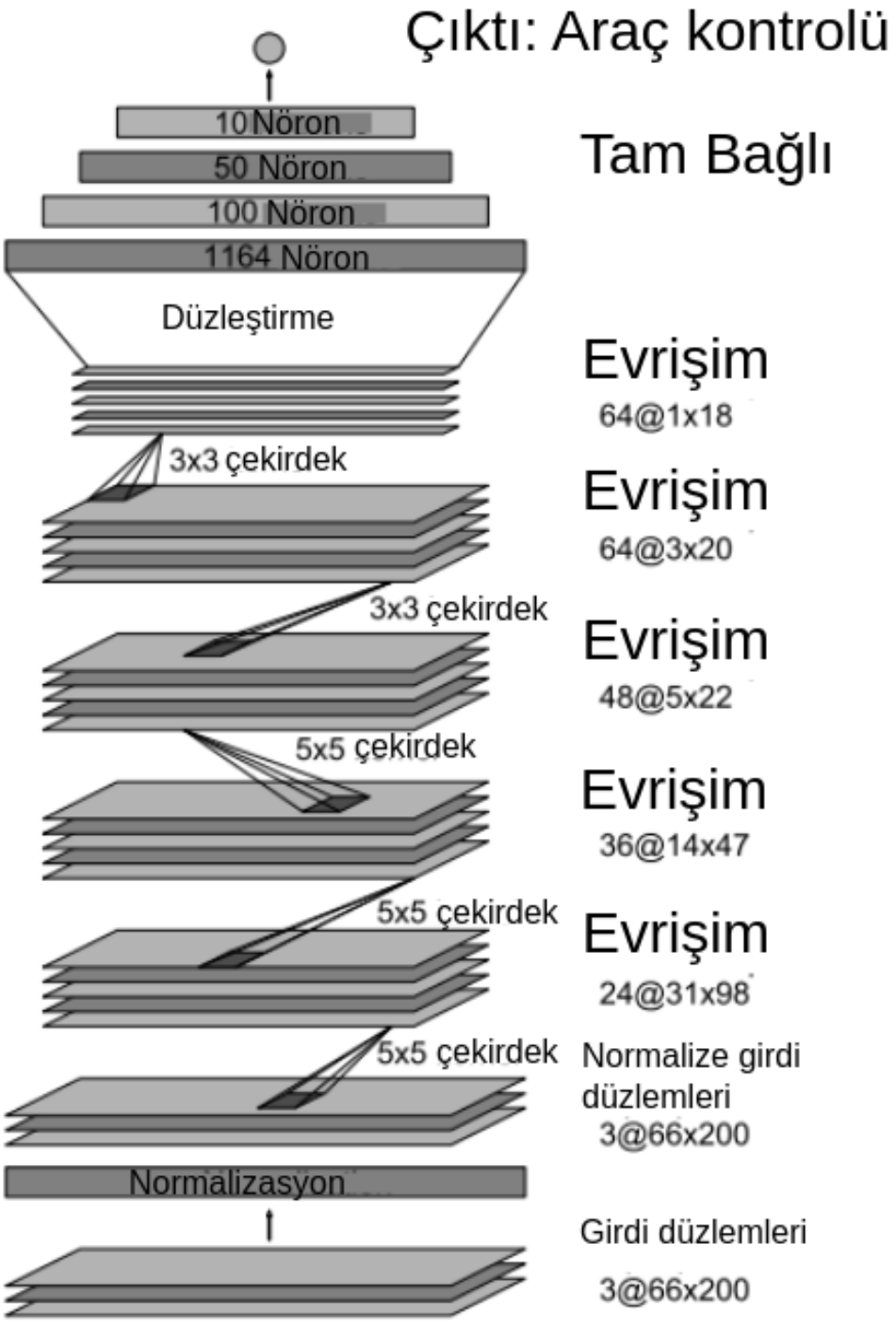
- Sürüş türü,
  - Normatif: yolun orta çizgisine yakın durmak,
  - Yoldan sapmış: Yolun bir kenarından diğerine sürekli keskin dönüş,
- Bilgisayarlar, donanımlar (düşük güç kısıtlamaları, gerçek zamanlı sistemler),
- Direksiyon kullanımı (+daha önce kaydedilmiş direksiyon kullanımları),
- Konum farkındalığı,
  - AV'nin kendi konumunun farkında olma,
  - Harita ile yer bulma (kaçırılan robot sorunu, Kidnapped robot problem [61]),
  - Odyometri [62],
    - Zaman içinde konum değişikliğini tahmin etmek için, hareket sensörlerinden gelen verilerin kullanılması,
    - Video kameraları, yol haritaları,
  - Küresel Konumlandırma Sistemi (GPS),
    - Sinyal her zaman mevcut değildir,
    - Kesin olmayan, örneğin gökdelenlerin, tünellerin veya sıkışmış sinyallerin bulunduğu ortamlar,
    - Sürücüsüz arabalar gibi otonom cihazlar için feci sonuçlar olabilir,
    - GPS'nin tamamen kullanılamadığı yer altı veya iç mekân ortamları.

PilotNet Modeli

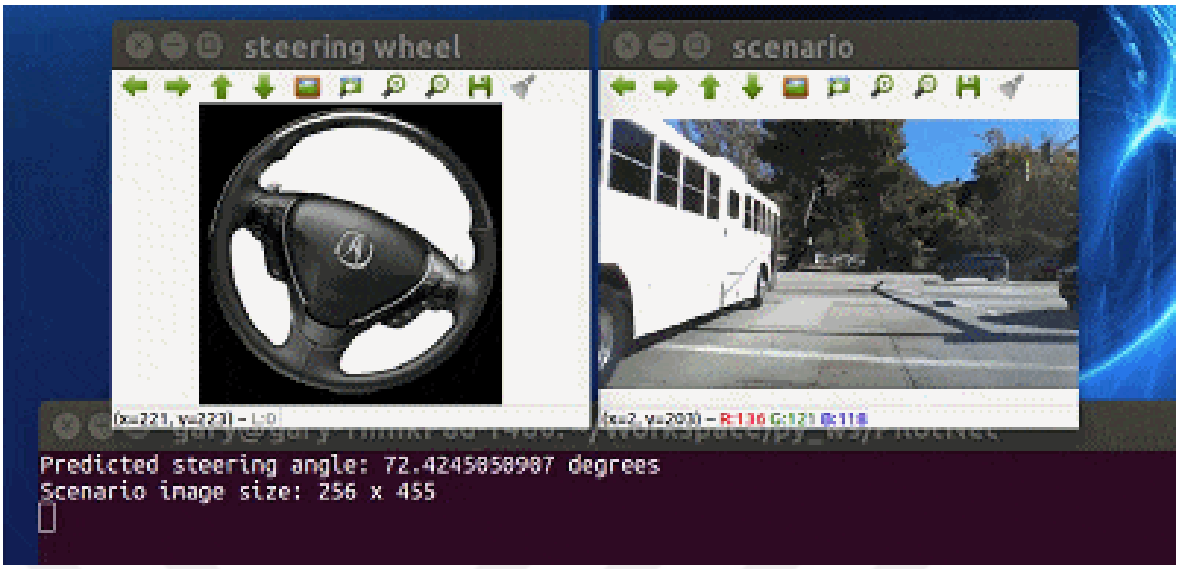
PilotNet, Nvidia'nın, AV'ler için yönlendirme konusunda uçtan uca öğrenimi yakalanan tek bir görüntüye (kamera) dayalı olan AI yapısıdır. Otonom araçlar için direksiyon değerlerini tahmin etmek üzere tasarlanmış uçtan uca bir ANN mimarisidir [64]. 250M bağlantısı 250T parametresi bulunmaktadır.

2.1.1.3. Karar ve Tepki Verme

Toplan tüm verilerden ve oluşturulan modelden sonra, bir araç için karar verme bölümü gelmektedir. Ancak bu anda çeşitli parametreler ortaya çıkmaktadır. İlk parametre, kararın



Şekil 2.1: Pilotnet Yapay Sinir Ağı Yapısı [63]



Şekil 2.2: Pilotnet Direksiyon Ekranı [64]

kim tarafından verileceğidir. İkinci parametre de emniyettir [65]. Alınan karardan sonra, aracın tepki vermesi en son uygulamadır.

2.1.2. Otonom Araçların Genel Tarihi

1500'lü yıllar, Da-Vinci'nin kendinden tahrikli arabasına[3] şahit olmuştur [66]. 1860'lara gelindiğinde ise, Robert Whitehead ilk etkili kendinden tahrikli deniz torpidosunu icat etmiştir [67]. 1939'da ise, Futurama adında bir sergi New York Dünya Fuarında yapılmıştır. Bu sergide yirmi yıl sonra dünyanın nasıl bir yer olabileceği anlatılmış, kendi kendine giden arabalarla otonom bir otoyol hayal edilmiştir. Daha sonraları ise, Norman Bel Gedde ilk sürücüsüz arabayı tanıtmıştır [68]. Elektrikli araç, kara yoluna gömülü manyetize metal çivilerle üretilen radyo kontrollü elektromanyetik alanların rehberliğinde hareket etmekte idi. 1958 de General Motors, AV konseptini gerçeğe dönüştürmüştür. Ön uç, yola gömülü bir telden akan akımı algılayabilen, alıcı bobinler adı verilen sensörlerle sarıldı. Akım, araca, direksiyon simidini sola veya sağa hareket ettirmesini söylemek için manipüle edilebilirdi [69]. 1960'lar da ise, SRI ve Stanford, deneysel robotlar üretmeye başladı. Yeni ortamlarda gezinmek, yeni AI tekniklerini test etmek için tasarlanmışlardı [70]. 1971 yılı ise, yarı otonom uzay sondalarına (Voyager uzay sondası) şahit oldu. 1980'ler, Almanya'da, kameralarla donatılmış Ernst Dickmanns'ın bir Mercedes minibüsü ile 56 mil gitmesini konuşuyordu (**Tablo 2.1:**).

[3] https://www.wired.com/brandlab/2016/03/a-brief-history-of-autonomous-vehicle-technology/

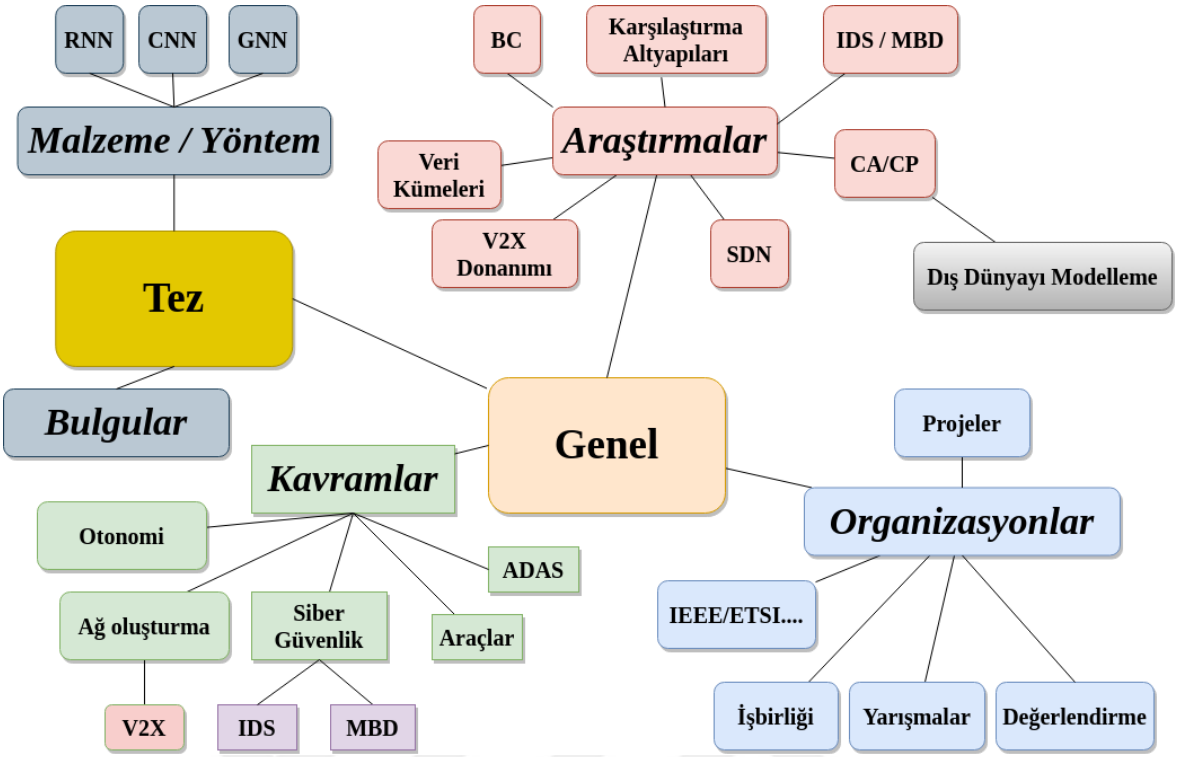
Tablo 2.1: Elektirikli Araç Tarihi [3]

Yüzyıl	Yıl	Açıklama
1500	Yaklaşık 1500	da Vinci'nin Kendinden Tahrikli Arabası
1800	1868	Whitehead Torpidosu
1900	1933	Mechanical Mike uçak otopilotu
1900	1945	Teetor Hız Sabitleyici
1900	1961	Stanford Arabası
1900	1977	Tsukuba Makine Mühendisliği
1900	1987	Ernst Dickmanns'ın VaMoRs'u
1900	1995	General Atomic'in MQ-1 Predatorü
2000	2004-2013	DARPA Yarışmaları
2000	2015	Tesla Otopilot
2000	2015	Michigan Üniversitesi'nin MCity'si

DARPA yarışmaları [71], otonom araçların tarihinde önemli bir yere sahiptir. İlk 2004'te, ABD İleri Savunma Araştırma Projeleri İdaresi (DARPA) tarafından başlatılmıştır. Amaç, 2015 yılına kadar askeri araçların üçte birinin kendi kendine gitmesini sağlamaktı. Birinci olacak araca 1 milyon dolarlık ödül verileceği belirtilmiş ancak 2004 yılındaki yarışmada tüm araçlar başarısız olmuşlardır. 2005 yılındaki yarışmada ise, başarılı olan takımlar büyük firmalar tarafından kapışılmış ve bugünkü elektrikli otomobil firmalarının otonom altyapılarının başlangıcını oluşturmuştur. Yarışmaya 2007 yılında, sahte bir şehir altyapısı da eklenmiştir.

Bugünlerde ise, uygun donanımlı arabaları güvenli bir şekilde yönlendirmek için özel otoyollara odaklanan, erken kendi kendine sürüş planlarına sahip bulunmaktayız. Her ne kadar teknoloji, 1939 Futurama'da projelendirildi ve 1950'lerde sergilendi ise de, kamu altyapısını inşa etmek için gereken büyük fikir birliğine varmak gerekmekte idi. Zamanımızda çoğunlukla yarı özerk araçlarımız bulunmaktadır. Yardımlı park etme ve otonom fren sistemleri yaygın hale gelmiştir. Tam otonom araçların varlığı ise çoğunlukla özel ortamlarda bulunmaktadır. Örneğin, Londra'nın Heathrow hava alanındaki veya Avustralya maden ocaklarındaki devasa araçlar insan müdahalesi olmadan çalışabilmektedir.

Gelecek için ise, her ne kadar erken gibi gözükse de, 2025'e kadar sekiz milyon yarı otonom araç olması beklenmektedir [70]. Yelkenliler, örneğin, muhtemelen ilk kendinden tahrikli ve bir tür otomatik direksiyona sahip (auto-tiller) ilk araçlar olacaklardır.



Şekil 2.3: Tezin Yapısı

2.2. V2X'E GİRİŞ

V2X teknolojisi hızla gelişmekte ve erişimi her geçen gün artmaktadır. Bu bölüm, güvenlik konularına girmeden önce temel AV teknolojilerini tanıtacaktır. Ardından, ağ oluşturma, özerklik seviyeleri ve güvenliği gibi gerekli kavramlar ele alınacaktır.

2.2.1. Genel Kısımlar

V2X'e kısa bir giriş olarak, çok kullanılan bazı terimleri açıklayan bir listenin iyi bir başlangıç noktası olacağı düşünülmüştür. **Tablo 2.2:**'deki tüm öğeler, çoğunlukla [72]'ten alınmıştır. Bu tabloda bulunan "IEEE", "802.11", "1609", "PC5", "WAVE", "C-V2X" gibi terimler bu tezde oldukça tekrar edilmektedir.

Kullanım durumları veya V2X üzerindeki uygulamalar "gün"lere bölünmüştür. Teknoloji bugün "1. gün"dedir. Yani, farkındalığı artırmak ve akıllı altyapı oluşturma kısımları şu anda yürürlüktedir. Ardından, "2. gün"de, AV'lerin sensör bilgilerini diğer arabalarla ve altyapıyla paylaşabilmesi için işbirlikçi algı (CP) (bu tezin araştırma alanlarından biri) uygulanmalıdır. Öte yandan, "fazlar", çoğunlukla benzer yapıyı tanımlamanın CAR 2 CAR İletişim Konsorsiyumu (C2C-CC) yoludur.

Tablo 2.2: V2X terminolojisi

Ad	**Alan**	**Açıklama**
IEEE 802.11 Standart Ailesi	Kablosuz iletişim	VANET'i etkinleştiren teknolojinin dayanağı
IEEE 802.11p değişikliği	Kablosuz iletişim	VANET için IEEE 802.11 eklemeleri
IEEE 1609 standart ailesi	VANET	PHY katmanının üzerinde dahili çalışmalar (ulaşım, güvenlik, uygulamalar vb.) [73]
ETSI ITS PC5[a,b,c]	V2V, C-V2X	Doğrudan iletişim: C-V2X Yan Bağlantısı (Sidelink)
ETSI Uu[a,b]	V2N, C-V2X	C-V2X Uu arayüz
ETSI ITS G5	ETSI, CEN (TC278), IEEE 802.11p	ETSI'nin, IEEE 802.11p ve CEN'in VANET'i ile
WAVE	IEEE, IEEE 802.11p	IEEE'nin DSRC'li VANET'i
C-V2X	3GPP	G5 veya WAVE ile rekabet eden 3GPP teknoloji terminolojisi
DSRC	IEEE 802.11p	VANET teknolojisi
IEEE 802.11bd	IEEE TGbd [74]	IEEE çalışma grubu [75], Yeni Nesil V2X için taslak oluşturur (NGV) [76]
"Günler" [77]	Day0, Day1 (bugün)	Uygulama sınıfları için zamanlama
"Aşamalar"	C2CC aşamaları	Aşama 1 (Phase 1), Aşama 2, Aşama 3, Aşama 4 [14]

- a: Uzun Süreli Gelişim V2X (LTE-V2X): 3GPP Rel. 14 veya 15
- b: 5G-V2X (NR-V2X): 3GPP Rel. 16 ve sonrası
- c: Buradaki "5" sayısı, frekans bandından (5.9GHz) türetilmiştir.

Baştan başlamak için, öncelikle bir Ad-Hoc ağ (AHN) tanımının yapılması gerekebilir. AHN'ler, iletişim kuran bağımsız (eşit) düğümlerdir. Merkezi kontrol olmaksızın kablosuz bağlantılar aracılığıyla birbirleriyle iletişim kurarlar [3]. Dahası, Mobil AHN (MANET), mobil düğümlerin çoklu atlama (hop-by-hop) tabanlı bir düzenleme yoluyla iletişim kurduğu AHN türüdür. Kablosuz donanımın yetersizliği veya merkezi bir denetleyicinin bulunmaması diğer düğümlerle iletişimi zorlaştırır. Uçan AHN (FANET) ve VANET, her ikisi de birer MANET türüdür.

Kablosuz Doğruluk (Wireless Fidelity, Wi-Fi) ve Eternet oldukça benzer teknolojilerdir. Her ikisi de yerel ağlara (LAN) karşılık gelmektedir. Wi-Fi'da merkezi bir yönlendirici veya bir erişim noktası vardır. İnternet bağlantısını veya ağa kaydolmayı yönetir ve kontrol eder. Böylece bu tür ağlarda, ağa kabul, merkezi düğümden geçer. Özel Kısa

Menzilli İletişim (Direct Short Range Communication, DSRC) omurgası ile VANET, Wi-Fi [4] teknolojisinden geliştirilmiştir. Burada IEEE (IEEE 802 ve IEEE 1609 ailesi) alt katmanları tanımlarken, Otomotiv Mühendisleri Derneği (SAE) (J2735 ve J2945) uygulama katmanlarını tanımlamıştır.

DSRC geliştirilmelerinin 1990'ların başında başladığı söylenebilir. İlk araştırma, Birleşik Devletler (ABD) Kongresi tarafından üstlenildi. ABD Ulaştırma Bakanlığı'nı (USDOT) araştırmaya başlamak zorunda bırakan akıllı araç veya akıllı otoyol sistemleri [5] idi. Başarısından sonra, 1999'da Federal İletişim Komisyonu (FCC), Akıllı Ulaşım Sistemleri (ITS) [6] için 5.9GHz bandından, spektrumun 75MHz'ini tahsis etmiştir. Aralık, 5850MHz ile 5925MHz (75 MHz) arasındaydı. 2012'de, Wi-Fi'ya yönelik DSRC modifikasyonu, IEEE 802.11p olarak IEEE 802.11'e entegre edilmiştir. Avrupa'da, spektrumun 30MHz'i, 5875MHz'den 5905MHz'e [7] ayrılmıştır. Daha sonra 2020'de bu, raylı sistemler için 5915MHz'den 5935MHz'e kadar olan spektrum dahil olmak üzere, 5875MHz ile 5935MHz oldu [8]. 2021'de FCC, ITS operasyonlarında C-V2X teknolojilerini kullanmaya çağırdı, spektrumu da lisanssız kullanım için, 5850MHz'den 5895MHz'e (alt 45MHz) tahsis etti ve C-ITS için de frekans spektrumunu, 5895MHz'den 5925MHz'e (üst 30 MHz) aldı [9]. AV'lerin ve V2X'in geçmişi hakkında ayrıca daha fazla bilgi almak için, özellikle [78] adresindeki güzel tanıtım incelenebilir.

Gün olarak birinci gün, aşama olarak da birinci aşamadayız. Ancak, daha sonra gelecek olan aşamalar ve günler için, ayrı birimler ayrı gelecek tasavvurları çizmektedirler. Yeni nesil V2X (NGV) (**Tablo 2.2:**) için olmak üzere, 3. Nesil Ortaklık Projesi (3GPP), yeni radyo (NR) ve 4G/5G Hücresel V2X (C-V2X) önermektedir. IEEE ise, bir IEEE 802.11bd değişikliği üzerinde çalışmaktadır. Artı, Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) CP Mesajları (CPM) üzerinde çalışmaktadır.

Aşağıdaki bölümlerde, kuruluşlar, teknolojiler ve toplulukların bu geliştirmelere yaptıkları katkılara ilişkin kısa bilgiler verilecektir. V2X için saldırı tespiti olan MBD ve siber güvenlikle ilgili diğer kuruluşlar hakkında daha fazla bilgi için [79] araştırması kontrol edilebilir. İlerdeki bölümlerde ise, V2X'te temel siber güvenlik ve IDS/IPS hakkında bilgiler verilmiştir. AV'lerde ve V2X'te siber güvenlik hakkında daha fazla bilgi için özellikle [80] araştırması kontrol edilebilir. Son olarak, 2.4. bölümünde, en son teknoloji araştırmaları belirtilecek, bireysel değerlendirmeleri ve eleştirisi de yer alacaktır.

Tablo 2.3: SAE'nin Ünlü Otomasyon Düzeyleri [40]

Seviye	Sürücü Rolü	Özellikler	Tür
SEVİYE 0	a, b	1	Sürücü desteği
SEVİYE 1	a, b	1	Sürücü desteği
SEVİYE 2	a, b	2	Sürücü desteği
SEVİYE 3	c, d	3	Otonom sürüş
SEVİYE 4	c, e	3	Otonom sürüş
SEVİYE 5	c, e	4	Otonom sürüş

2.2.2. Özerklik

Bu bölüm, EV'ler veya AV'ler için tanımlanan otonomiyi ve bunun neden gerekli bir özellik olduğunu kısaca açıklayacaktır. Bu anlamda bir AV'nin ne kadar özerklik kazanabileceği ve bilimsel ölçütlerin bu süreci tanımlayıp tanımlayamayacağı anlatılacaktır.

Özerklik, sürücüye, yolcuya veya uçaktaki yüke zarar vermeden AV'nin kendisinin karar verme sürecidir. Bu karar verme süreci, protokollerde, eğitimde ve öğrenme geçmişinde alt yapı tarafından sağlanan, ağ aracılığıyla toplanan metrikler veya durum bilgileri aracılığıyla yapılır. Bu süreç analitik, açıklanabilir ve bir dereceye kadar kanıtlanabilirdir. Öte yandan, insan kararları her zaman gerçeklerin sunduğunu takip etmez ve bu da kişinin içinde bulunduğu duygusal durumdan etkilenir. Ek olarak, bazı DL algoritmalarının neden çalıştıkları şekilde çalıştığını hala anlayamıyor veya açıklayamıyoruz [10]. AI algoritmalarındaki açıklanabilirlik, bu tezin kapsamı dışındadır. Ancak bu karar verme süreci, sürücünün daha iyi bir sonuca varması için araç (veya VANET) tarafından yapılır.

Geleceğin araçları işbirlikçi ve otonom olacaktır. Tanımın kooperatif kısmı V2X ile ilgili standartlardan gelmektedir. Özerklik ise SAE Seviyeleri tarafından tanımlanır [4] [40] (**Tablo 2.3:**);

- Seviye 0: Sürüş Otomasyonu Yok (otomatik acil frenleme, kör nokta uyarısı, şeritten ayrılma uyarısı)
- Seviye 1: Sürücü Yardımı (şerit merkezleme VEYA uyarlanabilir hız sabitleyici)

[4] https://www.sae.org/standards/content/j3016_202104

Tablo 2.4: Tablo 2.3: İçin Bilgiler

Sürücü Rolü
• **a**: Sürücü destek özellikleri devreye girdiğinde, ayaklar pedallardan çekilse ve direksiyon çevrilmiyor olsa bile, sürücüye ihtiyaç vardır. • **b**: Bu destek özellikleri sürekli denetlenmelidir; Güvenliği sağlamak için gerektiğinde yönlendirilmeli, fren yapılmalı veya hızlanılmalıdır. • **c**: "Sürücü koltuğunda" oturuluyor olunsa bile, bu AD özellikleri devredeyken, araba sürücü gerektirmeyecektir • **d**: Özellik talep gerektirdiğinde, sürücü devreye girmelidir • **e**: Bu AD özellikleri, sürüşün devralınmasını gerektirmeyecektir
Özellikler
• **1**: Bu özellikler, uyarı ve anlık yardım sağlamakla sınırlıdır. • **2**: Bu özellikler, sürücüye direksiyon VE fren/hızlanma desteği sağlar • **3**: Bu özellikler, aracı sınırlı koşullar altında kullanabilir ve gerekli tüm koşullar sağlanmadıkça çalışmaz. • **4**: Bu özellik, aracı her koşulda sürebilir.

- Seviye 2: Kısmi Sürüş Otomasyonu (aynı anda şerit merkezleme VE uyarlanabilir hız sabitleyici)
- Seviye 3: Koşullu Sürüş Otomasyonu (trafik sıkışıklığında yol alma)
- Seviye 4: Yüksek Sürüş Otomasyonu (yerel sürücüsüz taksi, pedallar/direksiyon takılı olabilir veya olmayabilir)
- Seviye 5: Tam Sürüş Otomasyonu (4. seviye ile aynı, ancak özellik her koşulda her yere gidebilir)

Özerkliğe sahip olmak için AV'ler ortamın durumu hakkında birbirleriyle iletişim kurmalıdır. Bu iletişim, mobil teknolojilerle ABD'de DSRC veya Araç Ortamlarında Kablosuz Erişim (WAVE), Avrupa'da G5, Uluslararası Standardizasyon Örgütü'nde (ISO) M5 veya 3GPP C-V2X ile sağlanabilir.

Kaynakları daha iyi kullanmak için AV'ler kendi aralarında kümeler oluşturabilir. Bu, kendi içlerinde küme başı (cluster head) seçimini zorunlu hale getirir. **Tablo 2.5:** Kümeleme sürecini açıklayan çalışmaların listesine bir örnektir.

Tablo 2.5: Küme Başı Seçim Yöntemleri

Araştırma	Yöntem
[83]	Analitik Hiyerarşi Süreci (AHP)
[84]	Çizelge ANN'ler
[85]	Hibrit Bulanık Çok Kriterli Karar Verme

Tablo 2.6: V2X İletişim Türleri

Kısa Ad	Uzun Ad
V2V	Araçtan Araca
V2I	Araçtan Altyapıya
V2P	Araçtan Yayaya
V2B[88]	Araçtan Bisiklete
V2N	Araçtan Ağa
V2C	Araçtan Buluta
V2G	Araçtan Şebekeye
V2H	Araçtan Eve
X2X	VANET'te herhangi bir paydaş arasındaki iletişim

Araç kümelemesi, standartlarda çok fazla yer almamakla birlikte çok geniş bir literatür kapsamı vardır [81]. Öte yandan, müfreze (platooning) araçların aynı yolda, aynı işi yapmak için iş birliği yaptığı özel bir tür kümelenme şeklidir [82].

2.2.3. Ağ Kurulumu

Bu bölümde, bir VANET sistemindeki temel ağ özellikleri tartışılacaktır. Temel V2X bilgisi ile başlayacak, ardından ISO katmanlarına kıyasla katman yapısını tanımlayacaktır. AV'lerin dahili ve harici ağ bağlantısı olmasına rağmen, bu çalışma harici, dışarıya doğru olan iletişim ile ilgilidir. Bir diğer yön ise iletişim ortamıdır. Örneğin, C-V2X hücresel radyo teknolojisini kullanırken, IEEE 1609 standartları Wi-Fi ile ilgili teknolojileri kullanmaktadır.

2.2.3.1. Araçlardan Her Şeye

Aracın dış ortama olan iletişim şekline V2X denir. Trafik ışığı, yayalar ve altyapı gibi öğeler arasında iletişimle ilgili çok çeşitli teknolojiler içerir [86, 87].

C-V2X ve IEEE 802.11p gibi harici fiziksel katmanlar standartlarda bulunmakla birlikte, **Şekil 2.7:**'de tanımlandığı gibi, uzun menzil (LoRa) altyapısı başka bir araştırma öğesidir [89, 28]. LoRa kullanımı, yalnızca altyapı olarak eksiklikler bulunuyorsa (RSU'ların

uzak olması gibi), olası görülmektedir. Bununla birlikte, Yazılım Tanımlı Radyo (SDR) iletişiminin bu alanda IR benzeri seçenekler sunduğu düşünülmektedir [90].

Araştırmaların yaptığı tavsiyeler dışında, şu anda AV'lerde şu anda AV'lerde siber güvenliğinin temellerini değiştirilmiş X.509 sertifikalardır [11, 12].

Her aracın kendi iç iletişimi için ayrıca kendi içinde yerel bir ağı bulunmaktadır. Bu iç ağda da ilerlemeler ve farklılaşmalar olmakla birlikte, en eski alt yapı Bosch tarafından icat edilen kontrolcü tarafı alan (Controller Area Network, CAN) olmuştur. Daha sonra gelen Local Interconnect Network (LIN), Medya Odaklı Sistem Taşıma (MOST), Otomotiv Eternet, FlexRay gibi yapılar da bulunmaktadır. Daha önce belirtildiği gibi, bu tezin konusu V2X ile ilgili olduğundan iç ağ yapılarından çok bahsedilmeyecektir.

Harici iletişim için, VANET kablosuz iletişim olanakları sağlar. Bu iletişim katmanı Avrupa'da G5, ISO'da M5 ve ABD/SAE'de WAVE (DSRC) olarak adlandırılır. IEEE 802.11p, ağ ve taşıma katmanlarını tek bir katmanda birleştirerek OSI katmanlama ana akımından ayrılır. Transport (taşıma) katmanı üzerinde aşağıdaki yapılar eklenir;

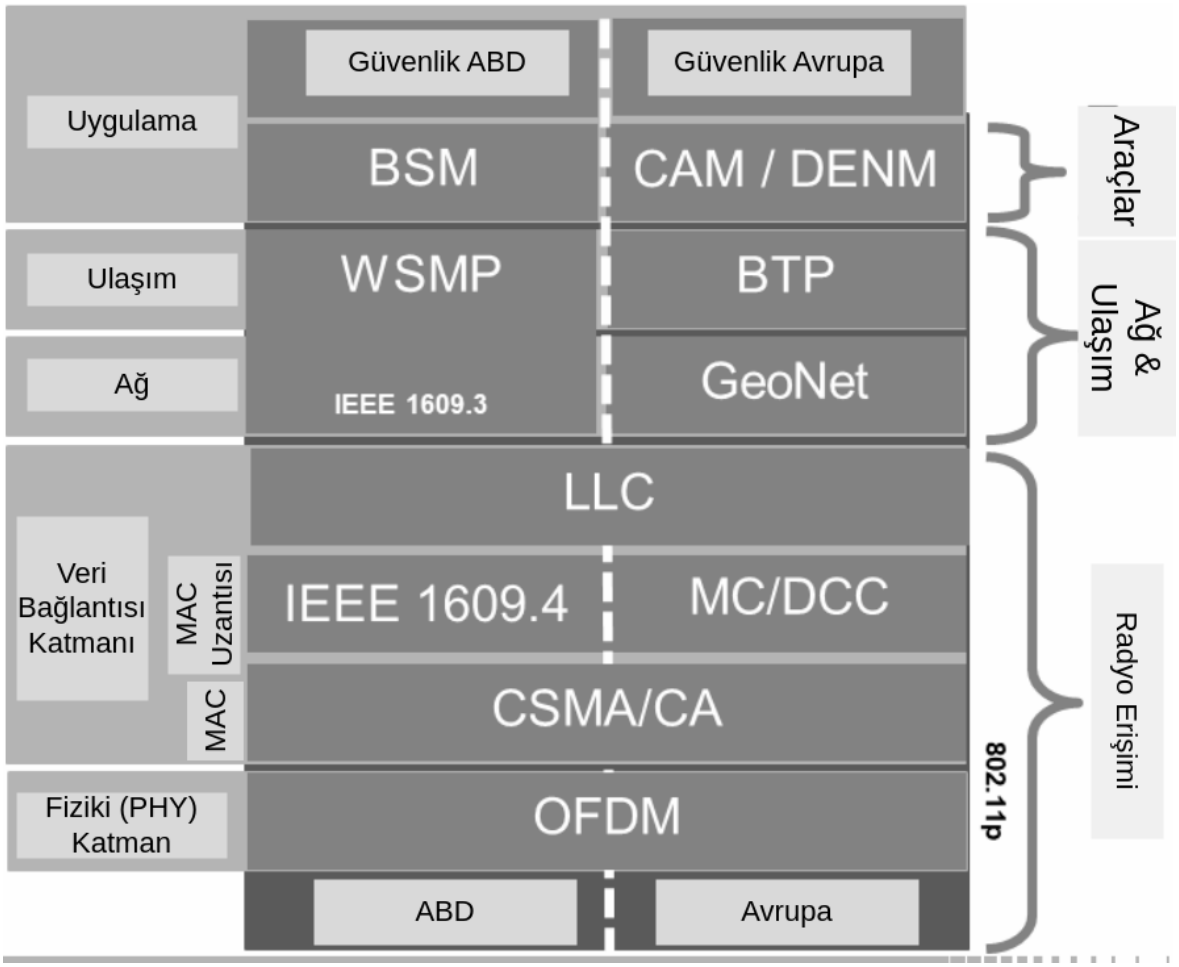
- ABD/SAE: WAVE kısa mesaj protokolünü (WSMP) [91],
- Avrupa ülkeleri: Temel Aktarımı Protokolünü (BTP),
- ISO: Hızlı Ağ & Aktarım Protokolünü (Fast Networking & Transport Protocol, FNTP).

Uygulama katmanında aşağıdaki yapılar bulunur;

- İşbirlikçi Farkındalık Mesajları (CAM),
- Merkezi Olmayan Çevresel Bildirim Mesajları (DENM) (AB),
- Temel Güvenlik Mesajları (BSM) (US/SAE).

Veri bağlantı (data link) katmanı, karşılaştırıldığında daha fazla dikkat gerektirir. IEEE 1609.4 öncelikle çoğu paydaşın kullandığı veri bağlantı katmanını tanımlar.

Daha önce açıklandığı gibi, M5, G5 ve WAVE, iletişim için tek seçenek değildir. Uzun mesafeli iletişim için aşağıdaki seçenekler düşünülebilir [28].



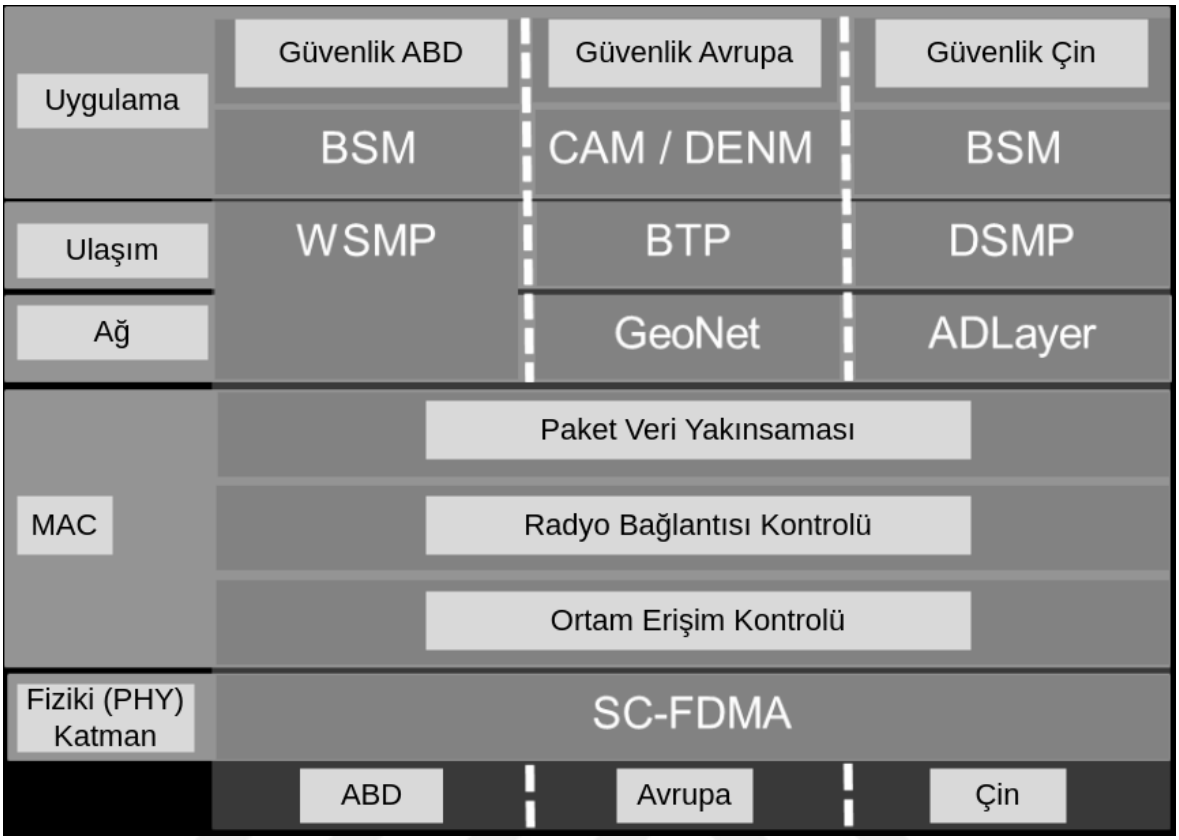
Şekil 2.4: IEEE 802.11p Protokol Yığıtı [91]

- Düşük Güçlü Geniş Alan Ağı (LPWAN),
- Gelişmiş Makine Tipi İletişim (eMTC),
- Dar Bant Nesnelerin İnterneti (NB-IoT) (**Tablo 2.10:**).

Kısa mesafe için (**Tablo 2.8:**), Nesnelerin İnterneti (IoT) ve Araçların İnterneti (IoV) gibi diğer kullanım durumları için de olsa (**Tablo 2.9:**) birçok başka iletişim türü mevcuttur.

İletişim türlerinin detaylı bir karşılaştırması **Tablo 2.7:**'da özetlenmiştir.

Paket anahtarlama (packet switching), doğrudan V2X ile ilgili olmayan başka bir alandır. Daha sonra, bu tezde, anahtarlamanın V2X'e dokunabileceği donanım yapılarından bahsedilecektir.



Şekil 2.5: C-V2X Protokol Yığıtı [91]

2.2.4. Güvenlik

VANET, standartlarda olduğu gibi, ağırlıklı olarak sertifika tabanlı güvenlik mekanizmaları [11] sunar. Şifrelenen iletişim sırasında sertifikalar kullanılır. Türetilmiş sertifikalarla (sahte sertifikalar) da denilen bir yapı bulunmaktadır. Nedeni ise süreçte gerçek sertifikaların kullanılmaması ama onların yaptığı işi yapabilen türemiş sertifikaların kullanılabilmesidir. Bunun için herhangi bir iletişimden önce sahte bir sertifika oluşturulur. Üretilen her sertifikanın, bitimi ile yeni bir sertifika ile yenilenen, bir ömrü vardır [12]. Bunun dışında, MBD mekanizması, kötü davranışlı araçları VANET'den sınır dışı etmeye veya yasaklamaya çalışır (bir süreliğine veya tamamen). MBD servis içerikleri standartlarda net değildir. Öte yandan, raporlama mekanizmaları iyi bir şekilde anlatılmıştır.

2.2.4.1. Giriş

ETSI belgesinde [34] ITS için güvenlik amaçları şu şekilde açıklanmaktadır;

Tablo 2.7: V2X ve Uzun Menzilli Protokoller [28]

Teknoloji	**Çalışma Frekansı**	**Veri Hızı**	**Gecikme**	**Kapsam Aralığı**	**Mobilite Desteği**
Hücresel Ağlar	0,8-3,6 GHz	20 Mbps	50 ms	10 km	✓
DSRC	5.8-5.9 GHz	3-27 Mbps	200 mikro saniye	1 km	✓
Bluetooth	2,4 GHz	24 Mbps	3 ms	10 m	Sınırlı
ZigBee	2,4 GHz	250 Kbps	100 ms	20 m	✓
IR	2,6 GHz	1 Mbps	Çok Düşük	100 m	
RFID	125 KHz-2,45 GHz	106 kbps (13,56 MHz), 424 kbps (27,12 MHz)	Düşük	10 m	✓
WiMAX	5,8 GHz	75 Mbps	50 ms	50 km	✓
mmWave	30-300 GHz	1 Gbps	150 mikro saniye	10m	Sınırlı
LoRa	868-915-433 MHz	0,3-50 Kbps	<2s	3-8 km (kent içi), 15-22 km (kırsal), 15-45 km (düz)	✓
NB-IoT	900-1800MHz	Uplink: <250 Kbps, Downlink: < 230 Kbps	1,4-10 s	35 km	
eMTC	DL: 729-2170 MHz, UL: 699-1980 MHz	1 Mbps	10-15 ms	10 km	✓

- Gizlilik (Confidentiality),
- Bütünlük (Integrity),
- Ulaşılabilirlik (Availability),
- İnkâr Edilemezlik/Sorumluluk (Non-Repudiation),
- Özgünlük (Authenticity).

Her hedef için saldırı türleri **Tablo 2.11:**'da belirtilmiştir.

Bu saldırı türleri arasında korunması en zor olanı DoS saldırılarıdır. Konuyla ilgili literatürde, ayrıca [92, 93, 94] oldukça çok çalışma bulunmaktadır. Yine çok iyi bir standart belge

Tablo 2.8: Kısa Mesafe V2X Adayları

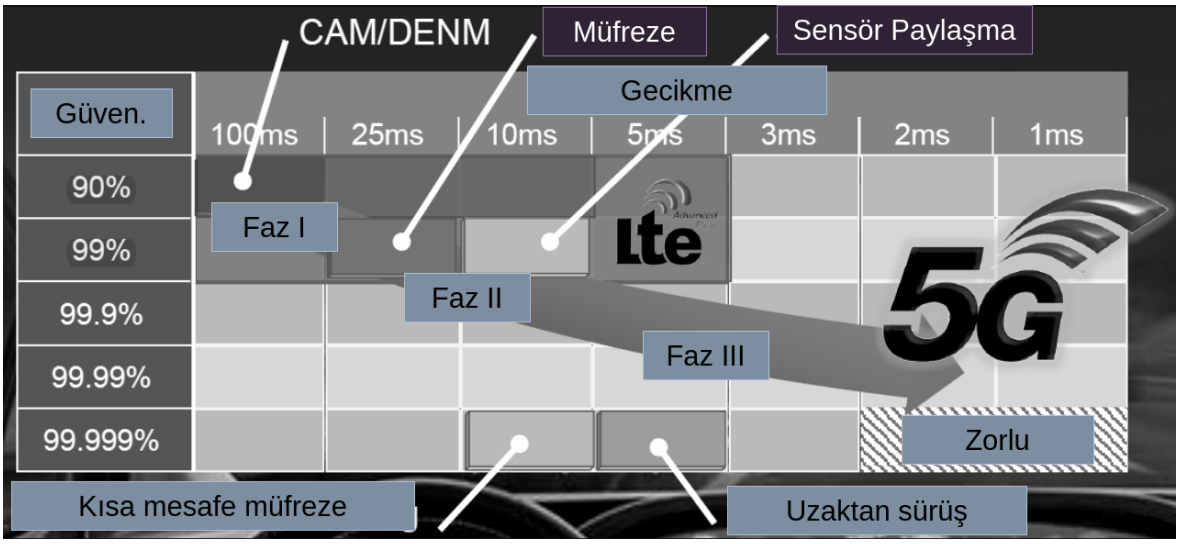
Ad	**Açıklama**
RFID	10 metre
IR	1. 100 m'nin altındaki mesafede 1-128 Mbps, 2. Çok düşük gecikme (birkaç mili saniye).
Milimetre dalga (mmWave)	1. Kısa iletişim mesafesi, 2. Yakın araçlar arasında yüksek hacimli veri iletimi.

Tablo 2.9: Kişisel Alan (PAN/WPAN/IEEE 802.15) V2X Adayları

Ad	**Açıklama**
Kızılötesi Veri Birliği (IrDA)	TV uzaktan kumandası vb.
Kablosuz USB	Kısa menzilli, yüksek bant genişliği
Bluetooth	IEEE 802.15.1
Düşük Oranlı PAN	IEEE 802.15.4, ZigBee

Tablo 2.10: eMTC ile NB-IoT [28]

	eMTC (LTE Cat M1)	**NB-IoT (Cat NB1)**
Dağıtım	Bant İçi LTE	Bant İçi LTE, Koruma Bandı, Tek Başına LTE
Downlink	OFDMA (15 kHz)	OFDMA (15 kHz)
Yukarı bağlantı	SC-FDMA (15 kHz)	Tek tonlu (15/3,75 kHz), SC-FDMA (15 kHz)
Tepe Hızı	DL: 1 Mbps, UL: 1 Mbps	DL: 250 kbps, UL: 20 kbps (ST)
Gecikme	10-15 ms	1,4-10s
UE alıcı BW	1,4 MHz	200kHz
Çift yönlü mod	Tam/Yarım Çift Yönlü, FDD, TDD	Yarı Çift Yönlü, FDD
UE iletim gücü	23 veya 20 dBm	23 veya 20 dBm
Güç tasarrufu	PCM, eDRX	PCM, eDRX
Kapsam	155,7 dB	Tek başına 164 dB, diğerleri için de, daha sonraki araştırmalar için (For Further Study, FFS))



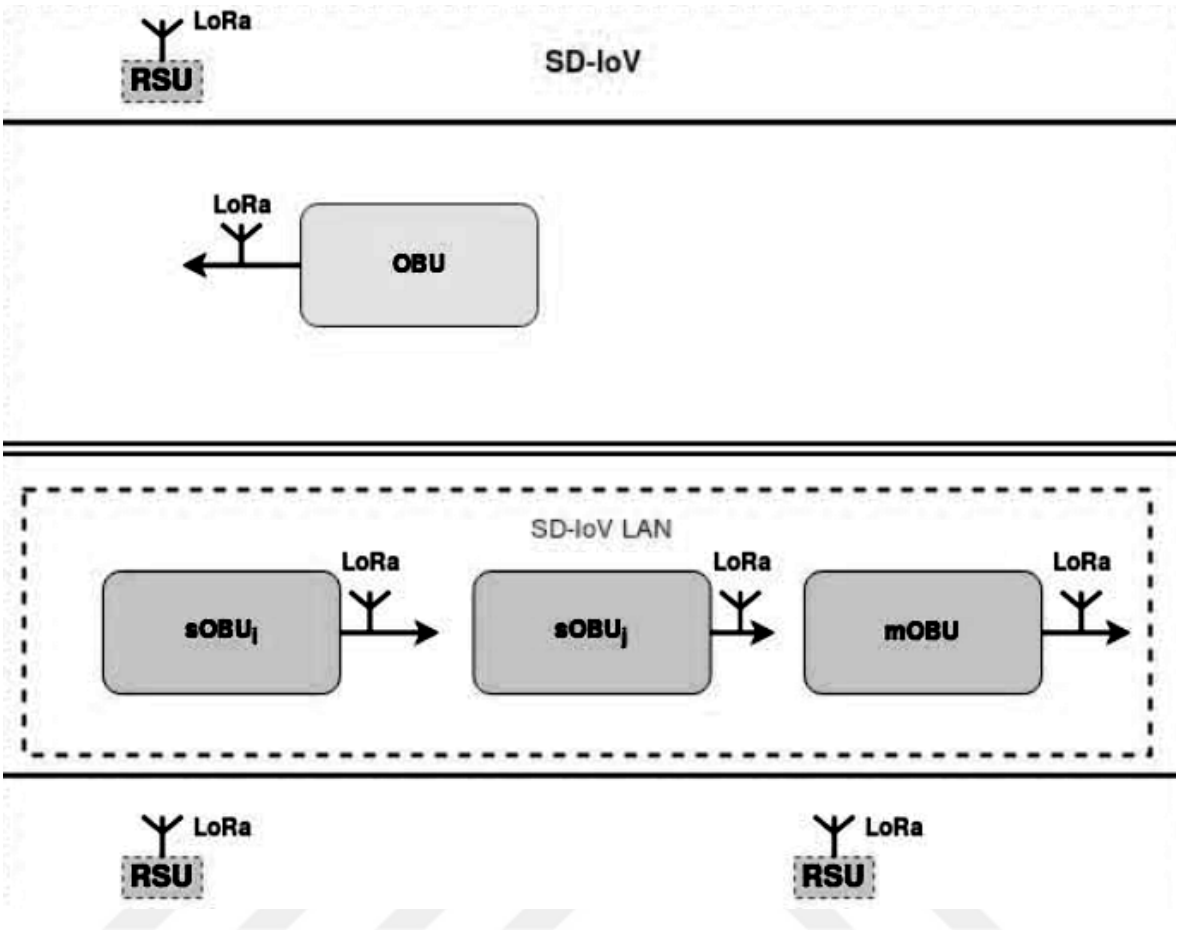
Şekil 2.6: C-V2X Teknolojisinde Son Durum [91]

olan [34]'e göre saldırılara karşı alınabilecek önlemler **Tablo 2.12:**'de belirtilmiştir. Bu önlemlerden; 2, 4, 6, 7, 9, 13 ve 15 sertifikasyon ile [95, 11, 12, 96, 97, 98] çözülür. Bu, VANET sertifikasyon altyapısı [23, 99], öncesinde devlet destekli bir çalışma iken, daha sonra IEEE tarafından, IEEE 1609 ailesi olarak V2X altyapısına entegre edilmiştir.

2.2.4.2. Saldırı Tespit Sistemleri

En çok kullanılan siber güvenlik mekanizmalarından ikisi, IDS'lerdir (Bu belgede IDS veya IPS ifadesi kullanıldığında, genellikle hem IDS, hem de IPS anlamına gelir) ve Saldırı Önleme Sistemleridir (IPS). IDS saldırıyı algılar ve ardından rapor eder veya bazı ağ ekipmanlarına yönlendirir. Öte yandan, IPS saldırıyı fark ettikten sonra rapor eder ve saldırı ile ne yapılacağına karar verir. Genellikle, bu IPS eylemi, engellemedir. Bir akış başlatıldığında, IPS müdahale edecek ve akış özelliklerinin (five-tuples) kontrol ettikten sonra akış paketleriyle ne yapılacağına karar verecektir.

Geleneksel olarak, IDS'ler çalışmak için kapsamlı kaynaklar gerektirir. Yani, genellikle kendi ekipmanına sahip olurlar. Uçta (edge) veya yerel ağlarının çevresinde bulunurlar. VANET durumunda ise, Yol Tarafı Birimi (RSU) üzerinde veya bir üst düğümde konumlanabilirler. Artık Araçlar, örneğin Tesla'lar, bir dahili sinir ağı (ANN) işlemcisi ile gelmektedirler. Böylece, bir IDS mekanizması (eğer ANN tabanlıysa) kolayca üzerine kurulabilir durumdadır. MBD ise, dağıtılmış bir IDS olarak görülebilir. Burada, MBD hizmeti, RSU'nun ötesindeki ağda kurulmuş olabilir.



Şekil 2.7: LoRa ve VANET [89]

IDS SINIFLANDIRILMASI

IDS'ler, türlerine, yerleşimlerine ve topolojilerine göre sınıflandırılabilirler. Türlerine göre, geleneksel ve modern olarak ikiye ayrılabilirler. Bu tezin gözünde, geleneksel IDS'ler, tehdidi kural tabanlı [5] bir şekilde tespit eden eski sistemlerdir. Halihazırda, bilinen saldırılar için bekçi (watchdog) olarak kabul edilebilirler [100]. Modern IDS tarafında ise, AI veya istatistiksel yöntemlerle trafik örüntüleri (pattern) ile veya anormallik (anomali) tabanlı sistemler ile problemleri fark etme ivme kazanmaktadır [101, 29]. Bunun yaygınlaşması için daha fazla zamana ihtiyaç olmakla birlikte, bazı şirketler [6] yılların deneyimiyle bunu zorlamaktadırlar. Geleneksel IDS'lerin sahip olduğu önemli bir özellik, şimdiye kadar meydana gelen tüm saldırıları kaydetmeleridir; bu, AI ve istatistiksel yöntemler için hayati bir kaynak olarak durmaktadır. Bu yöntemlerden bazıları, önceki saldırılar için eğitime ve yeni saldırıları görmek için bunun üzerine inşa etmeye ihtiyaç duyar. Bu, geleneksel ve

[5] https://suricata.io/
[6] https://www.xcitium.com/

Tablo 2.11: ITS Amaçları ve Saldırı Türleri [34]

	Saldırılar
Ulaşılabilirlik	• Hizmet Reddi (DoS).
Bütünlük	• Manipülasyon, • Maskeli Saldırgan, • Tekrarlama, • Bilgi Ekleme.
Özgünlük	• Manipülasyon, • Maskeli Saldırgan.
Gizlilik	• Dinleme, • Trafik analizi.
İnkâr Edilemezlik	• Reddetme.

modern IDS'lerin en iyi sonuç için birlikte çalışması gerekliliğini göstermektedir.

Geleneksel IDS'ler ise, Ana bilgisayar (host) veya ağ tabanlı olarak [102, 85] iki türe ayrılabilir. Ana bilgisayar tabanlı IDS, günlük (log) denetleyicileri, dosya yazma denetimleri, işlem yürütme müdahalesi vb. içerebilir. Müdahale, genellikle işletim sistemi tarafından sağlanan özellikler aracılığıyla yapılır. Tüm işlemler ana bilgisayar için yapılır ve IDS ana bilgisayarda bulunur. Öte yandan, ağ tabanlı IDS, ağ trafiği verileri üzerinde çalışır. Ana bilgisayara veya ağ ucuna gelen paketlerle ne yapılacağına karar veren güvenlik duvarları ile entegre olarak düşünülür.

IDS türleri üzerinde, aşağıdaki gibi bir ayrım da yapabiliriz;

- Bekçi (watchdog) IDS [103],
- Kural Tabanlı (rule based) IDS [7] ,
- Anomali Tabanlı IDS [85],

[7] https://suricata.io/

Tablo 2.12: ITS'nin Amaçları ve Önerilen Karşı Önlemler [34] (Devamı **Tablo 2.13:**'de)

	Karşı Koyma	**Saldırı**
1	Azalan sinyal frekansı	• DoS/doyma (saturation).
2	Kaynak IP benzeri yapı	• DoS/doyma.
3	V2I/I2V mesaj sınırlama	• DoS/doyma, • Hatalı mesaj ekleme, • Yoldaki mesajları değiştirme, • Sahte Tavır (Masquerade), • Eski mesajları tekrar gönderme, • GNSS sahteciliği, • Kara delik (Black hole), • Solucan deliği (Worm hole).
4	Frekans çevikliği	• Karıştırma (Jamming).
5	C-V2X kullanımı	• Karıştırma (Jamming).
6	PKI sistemi	• Hatalı mesaj ekleme.
7	CRC	• Yoldaki mesajları değiştirme.
8	Mesaj geçişi için gereksinimleri kaldırma	• Yoldaki mesajları değiştirme.
9	Kaynak ve hedef kimliği ekleme	• PKI sistemi ile.
10	Yayın zaman damgası ekleme	• Solucan deliği • Eski mesajları yeniden gönderme.
11	Her mesaja, mesaj sıra numarası ekleme	• Eski mesajları yeniden gönderme.
12	Diferansiyel Küresel Uydu Seyrüsefer Sistemi (GNSS) (Atalet Seyrüsefer Sistemi/INS, Parakete ile Seyrüsefer Hesabı/Dead Reckoning)	• Solucan deliği, • GNSS sahteciliği.

Tablo 2.13: ITS'nin Amaçları ve Önerilen Karşı Önlemler (Devam)

	Karşı Koyma	**Saldırı**
13	Şifreleme	• Kulak misafiri olmak (Eavesdropping).
14	Yazılım kurulum güvenliği (PMI, yazılım sertifikası)	• Kötü Amaçlı Yazılım (Malware).
15	Takma ad sertifikası	• Trafik koklama (Traffic sniffing), • Konum izleme.
16	Her mesaj için günlük kaydı	• Reddetme (Repudiation).
17	Her mesaj için olasılık kontrolleri ekleme	• Bozuk mesaj ekleme, • Yoldaki mesajları değiştirme, • Sahte Tavır (Masquerade), • Solucan deliği.
18	Yazılım için donanım tabanlı koruma	• Kötü Amaçlı Yazılım, • Reddetme.

- Eşik Tabanlı (threshold) IDS [104].

Watchdog IDS'ler, potansiyel olarak kötü amaçlı kodları izlemek için donanıma entegre edilmiş watchdog zamanlayıcılarını kullanabilir. Öte yandan, eşik tabanlı IDS'ler, işlemlere bir normallik sınırı koyar.

[105] gibi bazı çalışmalarda, IDS'ler aktif veya pasif olarak etiketlenmiştir. Ancak aktif IDS'ler, IPS'lerdir. Ayrıca, çoğu IDS sınıflandırma şeması, her yinelemenin sonunda bir "melez" tip içerir. Bu "hibrit" tür, genellikle IDS'nin birçok türden özellikler içerdiği anlamına gelir. Dolayısıyla burada her sınıflandırmadan sonra bir "melez" tip de kastedildiği düşünülebilir.

Modern IDS fikri değişmektedir. Örneğin, ana bilgisayar tabanlı IDS "Sessiz Veri Bozulmasına" (silent data corruption) karşı [106] savunabilmelidir. Ayrıca, "Sıfır Güven Güvenlik Koruması" (zero trust security protection, ZTSP) veya Tespit Etmeden

Önleme/Koruma, tehdidi önceden temizleme ve ardından ağın içine alma yöntemleri ivme kazanmaktadır [107].

Ağdaki yerleşimlerine göre ise, IDS sınıflandırması şu şekilde olabilir;

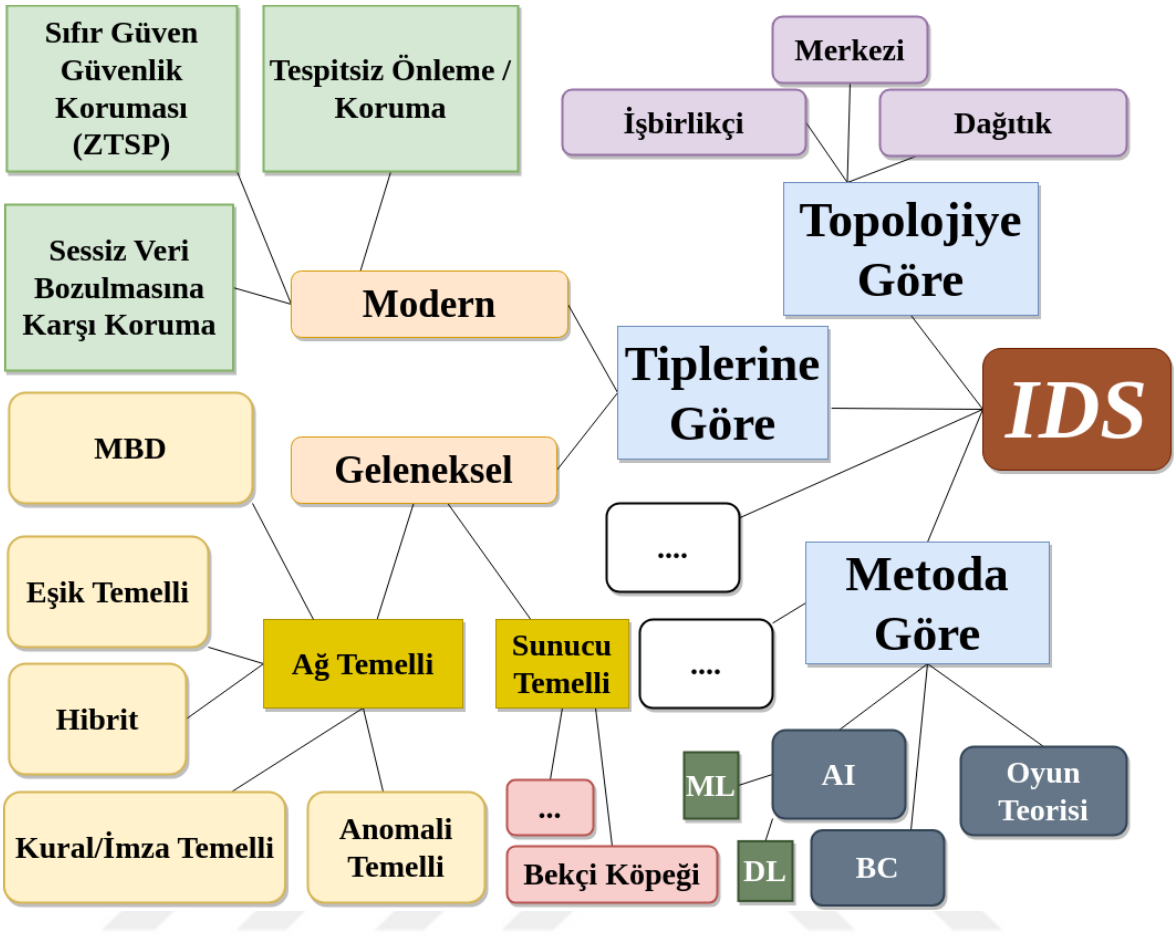
- Araç İçi IDS
  - CAN için IDS [108, 109],
  - Otomotiv eternet için IDS [110, 108],
  - Merkezi Ağ Geçidi İçin IDS,
  - ANN Tabanlı IDS (hem araç içi hem de V2X için kullanılabilir).
- V2X IDS (büyük olasılıkla RSU'da veya üst katmanlarda) [104].

Araç içi ağlar basittir ve harici bağlantı ağlarının aksine genel olarak gerçek zamanlıdırlar. Bu nedenle, bunun için IDS gereksinimi de hafif olmaktadır. Sonuç olarak, araç içi IDS'ler basit olmalı ve kısıtlı araç kaynaklarından çok fazla şey gerektirmemelidir.

Topolojilerine göre ise IDS'leri de merkezi IDS, işbirlikçi ve dağıtılmış şeklinde sınıflandırma mümkündür. Buradaki ayrım, merkezi IDS'de, kontrolün merkezi bir konumda olması ve sistemin tek bir arıza noktası (SPoF) problemine eğilimli olmasıdır. Dağıtılmış IDS'de ise, bu kontrol dağıtılır ve SPoF'un bir önemi yoktur. Dağıtılmış bir IDS, ayrıca işbirlikçi olabilir, yani birlikte çalışıp, kötü niyetli araçlar hakkında birbirlerine bilgi verir veya onlar hakkında karar verirler. Mevcut durumunda, MBD işbirlikçidir ancak uygulamaya bağlı olarak SPoF sorunları olabilir.

IDS'ler yöntemlerine göre de sınıflandırılabilir. AI çok kullanılan bir yöntemdir ve yeni tehditleri, bu tehditlerle ile eğitilmeden de tespit edebilir yapılar sunar. AI tabanlı yöntemler, ML, DL, BC (veri tarafı) ve oyun teorisi (game theory) [111] şeklinde belirtilebilir. ML tabanlı yöntemler, Öğrenme Otomatları (learning automata, LA), Markov Zinciri Modeli, Yapay Bağışıklık Sistemleri (Artificial Immune Systems) içerebilir.

ML tabanlı yöntemlerde, verilerdeki boyut küçültme işlemi, önemli aşamalardandır. Bu şekilde, veriler daha yönetilebilir hale getirilir. Her bir yöntemin, artı ve eksileri bulunabilir (örneğin, PCA ile, bazı boyut bilgileri kaybolacaktır). Boyut küçültme için bazı yöntemler aşağıdaki şekilde belirtilebilir;



Şekil 2.8: IDS Tipleri

- Otomatik Kodlayıcı (auto encoder) [112],
- Temel Bileşen Analizi (Principle Component Analysis, PCA),
- Coreset'ler [113],
- Orantılı Örtüşen Puan (Proportional Overlap Score, POS) [114],
- UMAP [115] (burada, makalenin kendi yazarı, orjinal makaleye gitmemeyi önerir),
- Aykırı Değer Algılama (Outlier Detection) [115].

DL tabanlı yöntemler, Üretken Karşıt Ağlar (generative adversarial networks, GAN) [113, 116] veya Çizelge Tabanlı ANN [84], gibi birkaç yöntem olarak listelenebilir.

IDS için araştırmalar, genellikle yöntemlerin bir kombinasyonunu kullanır. Örneğin, halihazırda var olan tehditler için (veri kümeleri, imza dosyaları vb.) ML kullanılıyor (karar

ağaçları vb.) ve yeni tehditler için DL (özel veya gelişmiş DL yöntemleri) kullanıyor olabilirler.

2.2.4.3. Yanlış Davranış Tespiti

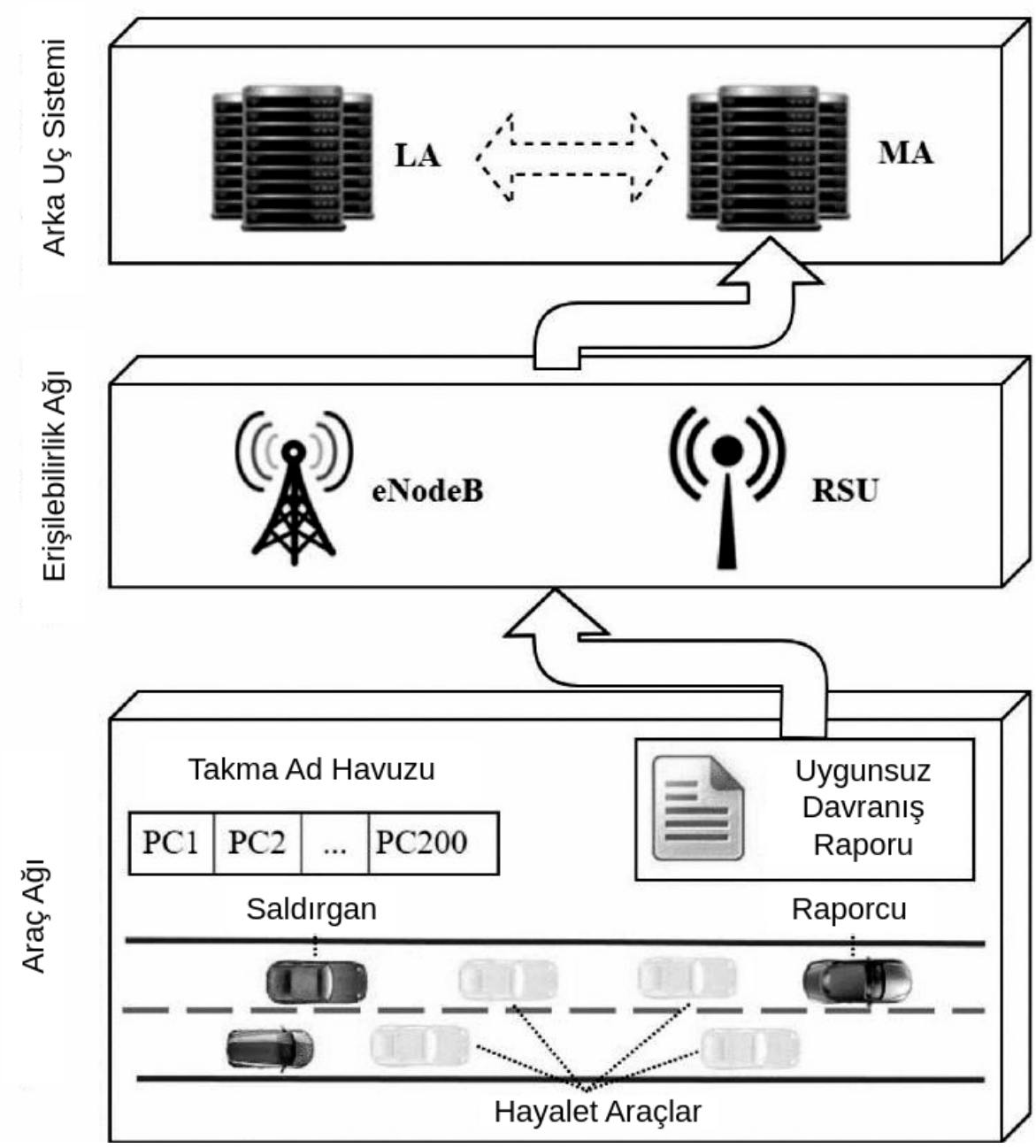
Daha önce belirtilen PKI (ortak anahtar altyapısı) tabanlı sistem [12], mesaj güvenilirliğini, gizliliğini ve reddedilmemesini sağlasa da, bir V2X ağındaki saldırıları tamamen engelleyemeyecektir. Bazı araçlar yasal bir yapıya sahip olmalarına rağmen, yine de kötü davranış sergileyebileceklerdir. Araştırmacılar ve standartlar, uygunsuz davranış tespit sistemini bu durumlarda bir önlem olarak kabul etmişlerdir (standartlarda MD olarak anılır, ancak bu tezde MBD olarak anılmıştır) [33, 117, 118, 119, 42, 50, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130]. Bir MBD sisteminde, merkezi bir MBD Otoritesi (MA) vardır. MA, tüm üyelerden MB raporlarını toplar ve analiz eder ve ardından analiz sonuçlarını, gerektiğinde sertifika yetkilisine (CA) gönderir. CA, ayrıca gerektiğinde sorunlu araçların sertifikalarını bloke eder ve böylece V2X iletişiminde aktif olmalarını yasaklar. MBD sisteminin, standartlarda henüz bu kadar detaylı olarak belirtilmemişse de, bu tezin de aynı şekilde düşünmesi ile, genel bir modeli **Şekil 2.9:**'da gösterilmektedir.

Bu modelde süreç, üç aşamada işlemektedir [118];

- Yerel algılama: AV, yerel işlemlerle şüpheli bir durum algılar,
- Raporlama: AV, ardından bu belirlemeyi MBD raporlaması ile MA'ya gönderir,
- Global Tespit: MA, diğer yerlerden gelen raporları birleştirir ve bir karar verir,
- Cevap (Response): MA, CA'yı bilgilendirir.

MBD, VANET ekosistemine, görece olarak, yeni bir eklenti olup, AV'lerden (veya VANET ekosistemindeki herhangi bir paydaştan) MB raporlarının alındığı dağıtılmış bir IDS sistemidir.

Rapor biçimi, yanlış davranış raporları (MBR) olarak adlandırılır. MBR'ler uygunsuz davranış yetkilisine (MBA) gönderilir. Söz konusu düğümler hakkında raporlar alındıktan sonra, MBA sertifikanın kaderine karar vermelidir. Bunun için de MBA, rapor gönderen AV düğümü hakkında, mümkünse başka kaynaklardan gelebilecek daha fazla bilgiye



Şekil 2.9: MBD Sistem Modeli[118]

sahip olmalıdır. Bu nedenle çoğu araştırma ve standart, CA mesajları (CAM/DENM) kullanımından bahsetmektedir. CA mesajları ise yalnızca genel sübjektif çevresel bilgiler sunmakta, MBA'nın ihtiyacını tam olarak karşılayamamaktadır. Öte yandan, CP, MBA'nın daha iyi bir değerlendirme için ihtiyaç duyduğu verilere mükemmel bir çerçeve sunmaktadır. Ancak CP ile MBD yapabilme veya CPM mesajlarının güvenliği, tezin yazılmaya başlandığı sıralarda, standartlarda bulunamamıştır[120, 131].

Gelişmekte olan diğer tüm AV teknolojilerinde olduğu gibi [32, 57], CP'li MBD, önemli bir konudur [65, 42, 132, 121]. MBD, [33] standartlarında bulunduğu şekliyle, kötü amaçlı düğümlere karşı sertifika tabanlı bir korumadır. Bunu genişletmek ve MBD'yi gerçek bir IDS sistemi haline getirmek için, daha fazlasını getiren standart belgeler [34] tamamlanmak üzeredir. Fakat standart kuruluşların tavsiyelerinin gerçekleşmesi zaman alacaktır. Bunun dışında, bu tez de son zamanlarda CP ilaveleri ile MBD olasılığı üzerine bir araştırma olarak başlamış, ancak CP veri kümelerinin henüz simülasyon araçları ile henüz yapılamadığından diğer veri kümeleri ile çalışmaya devam etmiştir.

2.2.5. İletişim ve Eğlence Sistemleri

Bilgi-Eğlence Sistemleri, araç içinde, ayrıca kurulu olan sistemlerdir. Şu anda AV'lere kurulabilecek birçok aday var bulunmaktadır;

- BMW aiDrive [133],
- Audi Multimedya Arayüzü (MMI) [134],
- Ford Sync 4 Bilgi-Eğlence Sistemi [135].

Teoride, bu sistemler OBU ile entegre olabilirler, ancak bu işlem araç içi ağlara aittir.

Genellikle internet bağlantısı bir hücresel bağlantıdan veya RSU'dan alınabilir. Bu sistemlerde bir IDS de bulunabilir, ancak bu, tezin kapsamı dışındadır. **Tablo 2.14:** içerisinden bu sistemler için kullanılabilecek işletim sistemleri belirtilmiştir.

Bununla birlikte, özellikle SDN altyapılarında, çok daha fazla kullanılabilecek bir AV altyapısı olan Otomotiv Sınıfı Linux'ten (AGL) bu bölüm içerisinde yerine almaktadır.

Tablo 2.14: İletişim ve Eğlence İşletim Sistemleri

Ad	**Açıklama**
JASPAR	Japonya Otomotiv Yazılım Platformu ve Mimarisi
AUTOSAR	Otomotiv Açık Sistem Mimarisi
OSEK/VDX	Açık Sistemler ve Otomotiv Elektroniği için İlgili Arayüzler / Dağıtılmış Araç Yöneticisi (Vehicle Distributed eXecutive)
AGL	Otomotiv Sınıfı Linux

2.2.5.1. Otomotiv Sınıfı Linux

AGL, özellikle otonom araçlar (AV) için tasarlanmış bir Linux dağıtımıdır. Bu bakımdan, Linux çekirdeğinin sahip olduğu tüm yeteneklere artı olarak AV çalışmaları için ek özelliklere de sahiptir.

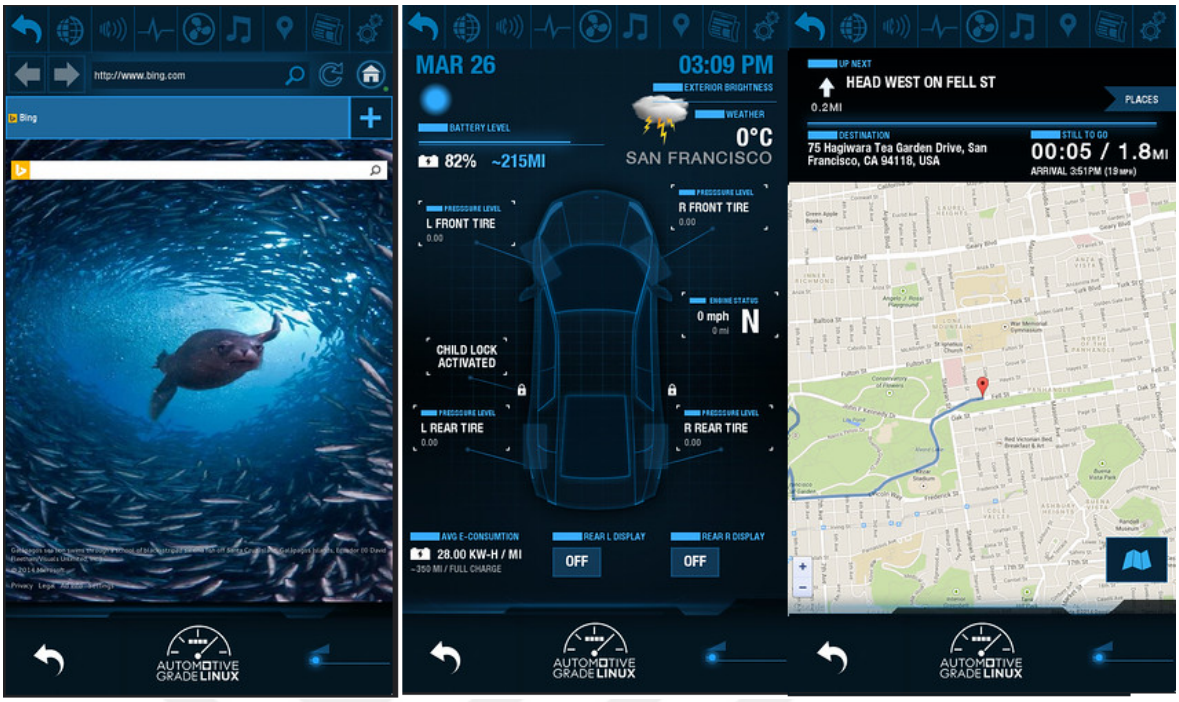
AGL, bağlantılı araçlar için tamamen açık bir yazılım yığıtı geliştirmeyi amaçlamaktadır [22]. Güvenlik varsayılanları olarak, izin verilmeyen her şey yasaktır. AGL, tanımlı donanım yerine (ki çoğu altyapı böyledir), yazılım tanımlı bir mimari uygulamaya çalışır.

Linux Vakfı

Linux Vakfı, kendini Linux'un büyümesini desteklemeye adamış, kâr amacı gütmeyen bir konsorsiyumdur. 2000 yılında kurulmuştur ve Linux mucitti Linus Torvalds'ın çalışmalarına sponsorluk yapmaktadır. Üyelerinin ve açık yazılım geliştirme topluluğunun kaynaklarını sıralayarak, Linux işletim sistemini (OS) desteklemekte, korumakta ve ilerletmektedir. Linux Vakfı, LinuxCon dahil olmak üzere Linux konferanslarına ev sahipliği yapmaktadır. Orjinal Linux araştırmaları, Linux videoları ve Linux platformunun anlaşılmasını, içerikler üreterek desteklemektedir. İş birliği ve eğitim için tarafsız bir forumu sağlamaktadır. Linux.com da dahil olmak üzere web mülkleri ayda yaklaşık iki milyon kişiye ulaşmaktadır. Kuruluş ayrıca, Linux çekirdek topluluğunun önde gelen uzmanlarını eğitmen olarak öne çıkaran kapsamlı Linux eğitim fırsatları da sunmaktadır. Jaguar Land Rover, Nissan, Toyota, DENSO Corporation, Fujitsu, HARMAN, NVIDIA, Renesas, Samsung ve Texas Instruments (TI) tarafından 2010 yılında kurulan AGL, Linux Foundation tarafından önerilmiş ve 146 üye tarafından desteklenmiştir[8] [9] .

[8] https://www.automotivelinux.org/about/members/

[9] https://www.flickr.com/photos/linuxfoundation/14508094434/in/album-72157644957457710/



Şekil 2.10: Bilgi-Eğlence Biriminden Örnek Ekran Görüntüsü[9]

2.2.6. Benzetimciler, Öykünücüler ve Yazılım Sistemleri

AV ile ilgili herhangi bir yazılım geliştirmeden önce, iyi bir simülatör (benzetimci) veya varsa iyi bir emülatör (öykünücü) şarttır. Mevcut araştırma kullanımlarının çoğu SUMO, OMNET ve son zamanlarda VEINS ve CARLA kullanmıştır. Ancak aynı zamanda diğerleri de literatürde bolca bulunabilir. **Tablo 2.15:**, açık kaynaklı bir simülatör listesidir. Karşılaştırma için VANET simülatörleri üzerine olan [136] araştırmasını ve "Ağ Simülasyon Araçları"[10] kaynağı incelenebilir.

Simülatör seçiminden sonra sıra kullanılacak olan yazılımlara gelmektedir. Araştırma için çalışmanın türüne göre birçok açık kaynak kütüphaneler ve çerçeveler bulunmaktadır. **Tablo 2.16:** ve github sayfası [11] içinde yer almayanlardan bazılarını listelemektedir.

[10] https://networksimulationtools.com/
[11] https://github.com/daohu527/awesome-self-driving-car

Tablo 2.15: Simülatörler

Ad	Açıklama	Tür
SUMO	Son derece taşınabilir; Mikroskobik; Büyük ağları yönetebilir; TraCI uzantısı	Trafik
OMNET++	Ayrık (Discrete) olay; VSimRTI uzantısı; INET Framework uzantısı (SimuLTE ile) [137]	Ağ
VEINS [138]	Araç ağı simülasyonu çerçevesi; Zümre (platooning) uzantısı (PLEXE)	VANET
Artery [139]	ITS-G5 yığıtı (WLAN V2X) [140, 141, 142] [a]	VANET
Artery-C [143]	OMNET tabanlı C-V2X; Veins kullanmakta	VANET
Qualnet	Araştırmacılar için	Ağ
NS-3	Araştırma ve öğretim odaklı; LENA [144] uzantı (LTE/EPC Ağı)	Ağ
WiLabV2Xsim [145]	C-V2X (5G) etkin	VANET
CARLA [58]	Otonom sürüş için 3D simülatör [146]	VANET
AirSIM	AI ile ilgili araştırmalar için Microsoft'tan 3D simülatörü [147]	MANET
LGSVL [148]	LG'den ROS/ROS2 AV'ler çoklu robot için simülatörü (artık LG tarafından desteklenmemektedir)	VANET
GNS3 [149]	Graphical Network Simulator-3	Network
EVE-NG [150]	Benzetim + sanallaştırma hizmeti [151]	Ağ
[152]	CARLA; Veri kümesi oluşturma	VANET
OPENC2X [153]	Açık Kaynak ETSI ITS-G5 Destekleyen Deneysel Prototipleme Platformu	VANET
F^2MD [122]	OMNET++ ve Veins tabanlı Açık Kaynak MBD çerçevesi	VANET
OpenCV2X [154]	Açık Kaynak 3GPP uyumlu C-V2X (Rel 14) Mod 4 Uygulaması (Artery & Veins uyumlu)	VANET

- a: https://github.com/anupama1990/Artery-C/issues/1#issuecomment-1167322181

Tablo 2.16: VANET Yazılım Listesi

Ad	Açıklama	Tür
Talkycars [155]	Cellular-V2X iletişimi (standartlara dayalı değil); CP/CA'ya benzer dağıtılmış platform yaklaşımı	CP
Valhalla [156]	Açık kaynak yönlendirme motoru (OpenStreetMap); Gezgin satıcı sorunu; Mesafe matrisi; Tesla [26]	Araç
TEPLITS [157]	Akıllı ulaşım sistemleri için kapsamlı bir test platformu	Araç
VANETZA [158]	ETSI C-ITS protokol paketi uygulama	Uygulama Çerçevesi ve kütüphanesi
CarMaker [159]	Araç dinamik simülatörü[157]	Fizik
Akraino [160]	Bağlantılı Araç Planı (CVB) ile Linux Foundation Edge	AV, Edge

2.3. ORGANİZASYONLAR

Bu bölümde, paydaşlarının daha iyi bir resmini çizmeye yardımcı olması adına, V2X teknolojileri ve standartlarının arkasındaki kuruluşlar belirtilecektir. Ayrıca, son teknolojiye katkıları, ayrıca iş birliği yapma biçimleri de yer bulacaktır.

V2X ve AV'ler bağlamında birçok kuruluş vardır. Her birisi V2X teknolojisinin gelişimine birçok katkı sağlamıştır. Kurumlar, otomotiv endüstrisi, hükumetler ve akademilerden olabildiği gibi, SB'ler veya sınıflandıramadığımız diğer bazı alanlardan da olabilmektedirler.

Burada açıklanan her kuruluş, AV'ler ve VANET'lerin sürecini önce ülkelerinde yapmışlar, ardından da dünya ile standartlar veya raporlar şeklinde paylaşmışlardır. Her ne kadar kurumlar çok çeşitli olsa da, 3GPP tabanlı bir teknoloji olan C-V2X dışında, tüm standartların temeli, yani AV ağlarının (VANET'ler) teknik omurgası aynı görünmektedir. Hepsi, IEEE 802.11 ve IEEE 1609 standart ailesinden başlamışlardır. Tüm bunları ABD başlatmış gibi görünmekte ise de, dünyanın diğer bölgelerindeki kurumlar da bunu almış, geliştirmiş, yerelleştirmiş ve yaymışlardır. Burada, bu tezin düşündüğü şekilde, en önemli kuruluşlar belirtilmeye çalışılacaktır. Daha fazla bilgi için [95] içerisindeki "Related standards and organizations" bölümü incelenebilir. Bundan başka, bu tez en son teknoloji ile ilgili en son standartları da belirtmeye çalışacaktır.

Unutulmaması gereken, her ülke orjinalinden uzağa gitmemeye çalışarak kendi AV, V2X ve

Tablo 2.17: V2X'te MBD ve CP ile İlgili Organizasyonlar (Devamı **Tablo 2.18:**'de)

Ad	**Kısaltma**	**Katkılar**	**Ülke**
Elektrik ve Elektronik Mühendisleri Enstitüsü	IEEE	IEEE 802.11[13], IEEE 1609 [95], TC (Technical Committee) ITS çalışma grubu	ABD
Avrupa Telekomünikasyon Standartları Enstitüsü	ETSI	Akıllı Ulaşım Sistemleri ve Hizmetleri (ITS) standartları ve ilgili faaliyetler	Avrupa
Üçüncü Nesil Ortaklık Projesi	3GPP	C-V2X [17]	Avrupa
Uluslararası Telekomünikasyon Birliği	ITU	İlgili siber güvenlik ve C-V2X küresel standardizasyonu	Dünya
Offene Systeme und deren Schnittstellen für die Elektronik in	OSEK	Otomotiv Açık Sistem Mimarisi (AUTOSAR)	ABD
Otomotiv Mühendisleri Derneği (SAE) International	SAE	SAE J2735 (BSM)	USA
Çin Otomotiv Mühendisleri Derneği	Çin SAE	İlgili yerel standartlar	Çin
Uluslararası Standardizasyon Organizasyonu	ISO	ISO uluslararası bir kuruluştur. Her üye, standardını ISO belgelerine dayalı olarak yeniden tanımlayabilir. AV'ler durumunda ISO, IEEE, SAE, IETF tarafından geliştirilen standartları alır ve dünya kabulleri için belgeler ve referanslar (ISO 204 çalışma grubu).	Dünya
Otomotiv hizmetlerini (MEC4AUTO) desteklemek için 5G Otomotiv Derneği	5GAA	MEC teknolojisi	Dünya
Otomotiv Uç (Edge) Bilişim Konsorsiyumu	AECC	AV'ler, 5G ve Edge bilgi işlem [161, 162]	Dünya
ABD Ulaştırma Bakanlığı	USDOT	İşbirliğine Dayalı ve Akıllı Ulaşım için Mimari Referansı (ARC-IT). USA için bazı ekipmanlar gibi ABD'deki ITS'deki birçok CP projesinin temelini oluşturmaktadır. [163]	ABD
iMOVE Avustralya	iMOVE	İlgili Projeler	Avustralya

Tablo 2.18: V2X'te MBD ve CP ile İlgili Organizasyonlar (Devam)

Ad	Kısaltma	Katkılar	Ülke
Florida Ulaştırma Bakanlığı	FDOT	Florida'nın Bağlantılı ve Otomatik Araç (CAV) Girişimi	ABD
Alman Federal Otoyol Araştırma Enstitüsü	BAST	Mobilite Veri Pazarı (MDM)	Almanya
Avrupa Standardizasyon Komitesi	CEN	TC 278 - Akıllı ulaşım sistemleri	Avrupa
Avrupa Elektroteknik Standardizasyon Komitesi	CENELEC	Avrupa'da ITU eşdeğeri	Avrupa
5G Altyapısı Kamu Özel Ortaklığı	5G PPP	5GROWTH	Avrupa
Avrupa Komisyonu	AT	Mevzuatı ile teknolojinin ilerlemesine yardımcı olmaktadır	Avrupa
Çarpışma Güvenliği ve Analiz Merkezi	CCSA	İlgili araştırma raporları	ABD
Siber Güvenlik Üretim İnovasyonu Enstitüsü	CYMANII	San Antonio'daki Teksas Üniversitesi liderliğindeki Konsorsiyum	ABD
CAR2CAR İletişim Konsorsiyumu	C2C-CC	Kara yolu güvenliği ve trafik verimliliği ile ilgili araştırma raporu	Dünya
Motor Endüstrisi Yazılım Güvenilirliği Derneği	MISRA	Programlama dili standartları, Otomotiv sektörü yazılımlarında yönergeler MISRA C/C++	Dünya
Uluslararası Elektroteknik Komisyonu	IEC	İlgili standartlar	Dünya
Amerikan Ulusal Standart Enstitüsü	ANSI	İlgili Standart	ABD
Alman Otomotiv Endüstrisi Birliği'nde Kalite Yönetim Merkezi	VDA QMC	Automotive SPICE (ASPICE): Otomotiv endüstrisi ve Avrupa'da Kalite Yönetimi ile ilgili standartlar	Avrupa
C-Roads Platformu	C-ROADS	ITS dağıtımları	Avrupa
Çin Bilgi ve İletişim Teknolojileri Akademisi	CAICT	Çin resmi kurumu	Çin
Akıllı ve Bağlantılı Araçlar için Çin Endüstri İnovasyon Birliği	CAICV	Çin resmi kurumu	Çin
Kore Akıllı Ulaşım Sistemleri	ITSKOREA	Kore resmi kurumu	Kore

Tablo 2.19: V2X'te MBD ve CP ile İlgili Organizasyonlar (Devam)

Ad	**Kısaltma**	**Katkılar**	**Ülke**
OMNIAIR Konsorsiyumu	OMNIAIRCON	ITS için Birlikte Çalışabilirlik ve Sertifikasyon	Dünya
Crash Avoidance Metrics Partners LLC	CAMP	İlgili projeler ve yazılım	ABD
Çin Otomobil Üreticileri Birliği	CAAM	Kâr amacı gütmeyen sosyal araçla ilgili endüstriler	Çin
İnternet Mühendisliği Görev Gücü	IETF	İletişim için standartlar kuruluşudur. Bu tezde belirtilen birçok standart (IP [4], TCP/UDP vb.) IETF'de kendilerine yer bulur	Dünya
Federal İletişim Komisyonu	FCC	Gerekli radyo frekansları [4]	ABD

VANET standartlarını oluşturmak için çabalamışlardır. Bu nedenle, farklı ülkelerde, farklı isimlerdeki standartların çoğu, neredeyse aynı temele dayanmaktadır. Örneğin, Türk "TS EN 61508" standardı, "IEC 61508" standardını baz almıştır. Yerel ihtiyaçlara göre zaman zaman da güncellenmektedir. Daha fazlası ve kurumların her biri hakkında daha fazla bilgi için ilgili kendi çevrim içi kaynaklarını kontrol edebilirsiniz.

2.3.1. IEEE

AV'ler bağlamında, IEEE istisnai bir yere sahiptir. AV, V2X ve VANET'in altyapısını oluşturan IEEE 802.11 ve IEEE 1609 standart ailesi, hepsi IEEE ile ilgili teknolojilerdir. Diğer kuruluşların çoğu kendi tabanlarını bu standartlar üstünden alıp üzerine inşa etmişlerdir. IEEE Standartları Derneği (IEEE-SA, Basit olması için, bu tezde "IEEE" şeklinde adlandırır) bu raporlar ve standartlardan sorumlu organdır. Ayrıca, IEEE'nin AV'ler ile ilgili görüşü hakkında daha fazla bilgi için [95] kaynağı kontrol edilebilir.

2.3.1.1. IEEE 1609.2

Bu standart, daha önce yapılan ünlü bir USDOT çalışmasından (daha sonra [23, 99] olarak yeniden yayınlanan) büyük ölçüde etkilenmiştir [164]. Bu standart, önceleri, IEEE P1556 (taslak) olarak da biliniyordu. Ancak daha sonraları, IEEE 1609.2 olarak yeniden markalandı [11]. İlk olarak 2006 yılında yayınlanmıştır. En son sürümü 2016 yılında bitirilmiştir. Standart, V2X güvenlik işlemlerinin nasıl gerçekleştirileceği hakkında, genel standartlar ailesi adına bilgi vermeyi amaçlamaktadır. Bu bilgiler aşağıdaki gibi sıralanabilir;

Tablo 2.20: IEEE'nin MBD ve CP ile İlgili Katkıları

Kod	Sürümler	Ad	Açıklama
IEEE 1609.2	2006, 2013, 2016, 2017 (A1), 2019 (A2)	Araç Ortamlarında Kablosuz Erişim için IEEE Standardı--Güvenlik Uygulamalar ve Yönetim Mesajları için Hizmetler	Genel bir güvenlik çerçevesi tanımlar [11]
IEEE 1609.2.1	2020, 2022 (D6)	Araç Ortamlarında Kablosuz Erişim için IEEE Standardı (WAVE)--Son Kuruluşlar için Sertifika Yönetim Arayüzleri	Sertifika işlemleri ayrıntılı olarak anlatılmıştır [12].
IEEE 802.11bd [74]	(D7)	NGV [76]	IEEE çalışma grubu [75]

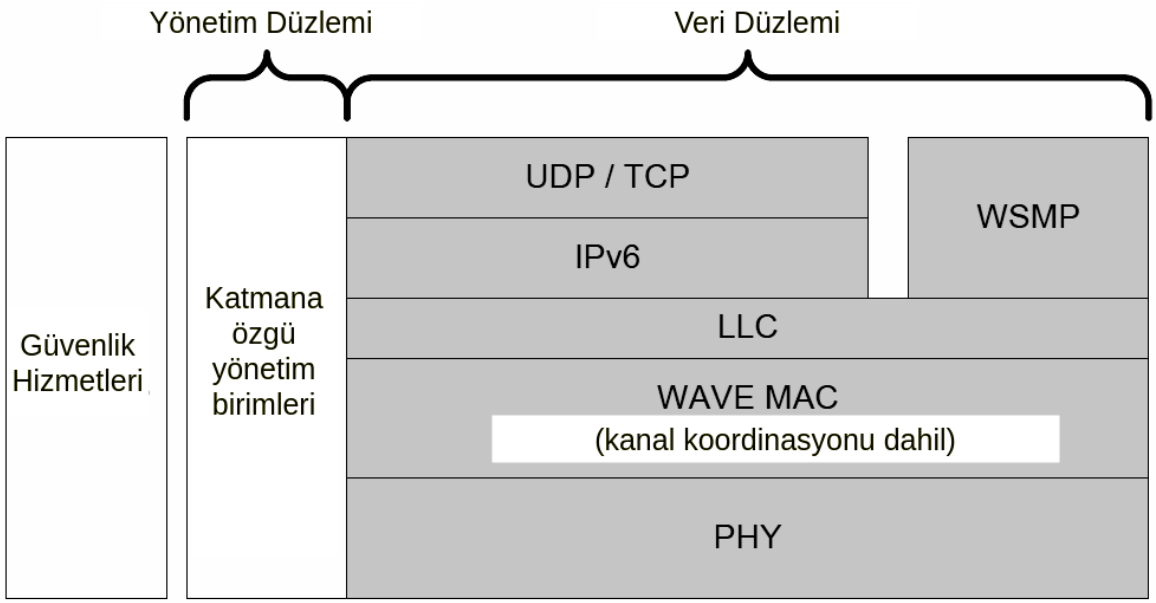
- A1: 1609.2a-2017 Değişiklik 1
- A2: 1609.2b-2019 Değişiklik 2--PDU Fonksiyonel Tipler ve Şifreleme Anahtarı Yönetimi
- D6: P1609.2.1/D6 (Taslak)
- D7: Aralık 2022'de RevCom ve SASB onayı (Taslak [75])

- Zaman açısından kritik işlemleri etkinleştirme,
- Güvenliği ihlal edilmiş aracın sistemden (yani MBD sisteminden) çıkarılması (bu durum standartlarda genel bilgi olarak vardır, ayrıntılar çok açık değildir),
- Gerçek zamanlı işlemler olması gerektiğinden siber güvenlik için daha az ek yük,
- Mahremiyet mümkün olduğu ölçüde nasıl korunur? Anonim (takma ad, psödo) sertifikalar (hem kişiyi açık etmez hem de yasayı korur).

Kapsamında aşağıdaki güvenlik sistemi bileşenlerini içerir;

- Mesaj biçimleri,
- Güvenli yönetim ve uygulama mesajları,
- Yönetim işlevselliği.

Burada, VANET ve V2X'te, MBD ve CP standardının en önemli kısımlarını detaylandırılacaktır. Standardın en önemli olanaklarından biri "Sağlayıcı Tanımlayıcı Hizmetidir" (Provider Service Identifier, PSID). PSID'ler, çalışan uygulamayı belirtirler.



Şekil 2.11: WAVE Modelinde Güvenlik Hizmetleri [11]

Bu iletim kontrol (TCP) veya kullanıcı datagram (UDP) protokollerindeki “port" yapısına benzerdir. “İş birliği" bölümünde de anlatılacağı gibi, IEEE, WAVE/WSMP’deki bağlantı noktası numaraları için PSID önermiştir (WAVE, DSRC sisteminin ABD’deki VANET’e uygulanmasıdır). Ancak ISO, ilgili standart belgelerinde numaralar, yalnızca bağlantı noktasını (portlar), kullandı. IEEE 1609 kılavuzu uyum çalışmaları sonrasında, 2016 yılı itibarı ile, “port” kullanılabileceğini, ancak bunun tavsiye edilmediğini belirtmektedir. Aynı durum, ISO’nun ilgili standartları [95] için de geçerlidir. “IEEE 1609.2.1” bölümünde PSID’ler daha fazla bilgi verilecektir.

Standart, bir VANET’te bulunması gereken güvenlik servislerini ikiye ayırır;

1. WAVE İç Güvenlik Hizmetleri (WAVE Internal Security Services),
    i. Güvenli Veri Hizmeti (Secure Data Service, SDS),
    ii. Güvenlik Yönetimi (Security Management, SM),
2. WAVE Üst Katmanı Güvenlik Hizmetleri,
    i. Sertifika İptal Listesi (Certificate Revocation List, CRL) Doğrulama Varlığı (CRL Verification Entity, CRLVE),
    ii. Eşler Arası Sertifika Dağıtımı (Peer-to-Peer Certificate Distribution, P2PCD) Varlığı (P2PCD Entity, P2PCDE).

Burada, SDS, Protokol Veri Birimlerini (PDU'lar) güvenli hale getirmekten sorumludur (Güvenli PDU'lar, SPDU). SPDU'lar ise, bir sertifika ile imzalanabilir veya ayrıca güvenli teslimat için şifrelenebilir. SM ise sertifika yönetiminden sorumludur. Ayrıca CRLVE, sertifikaları devre dışı bırakma işlemlerini yönetir. Bunula birlikte P2PCDE ise, AV'lerin veya altyapının sertifikaları, arasında dağıtmasını sağlar (P2PCD).

Aşağıda, standartta, MBD ve CP'ye dokunan kısımlar belirtilmiştir;

- MBD,
- Eşler arası sertifika dağıtımı,
- Takma ad sertifikaları.

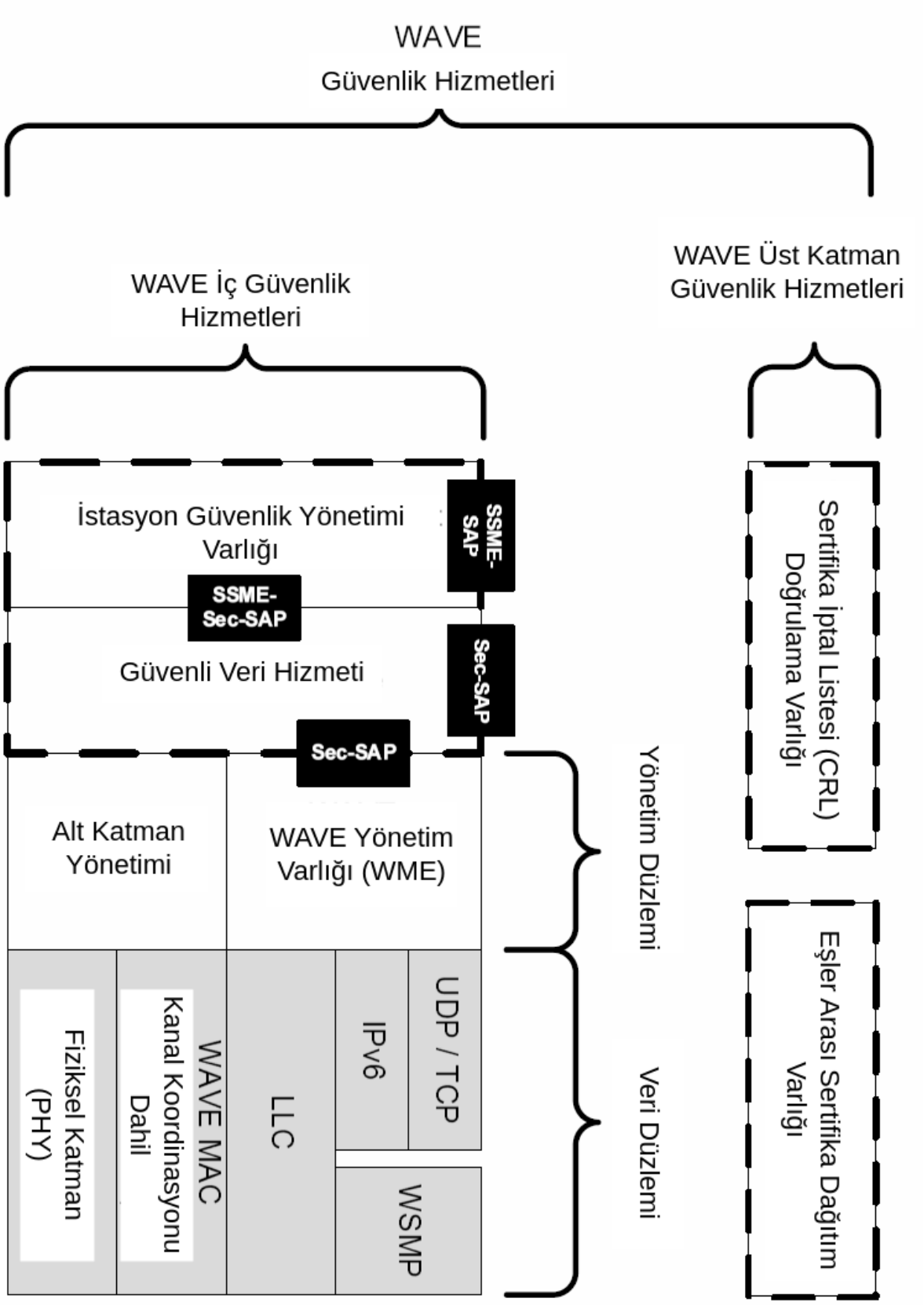
Bunlardan bazıları sonraki bölümlerde anlatılmıştır. Bir ek not, bu standart, güvenlik işlemlerinin kullanılmasını "zorunlu" olarak belirtmez (yani bir VANET'i, güvenlik "açık" olarak çalıştırmaya zorlamaz), sadece önerir.

2.3.1.2. IEEE 1609.2.1

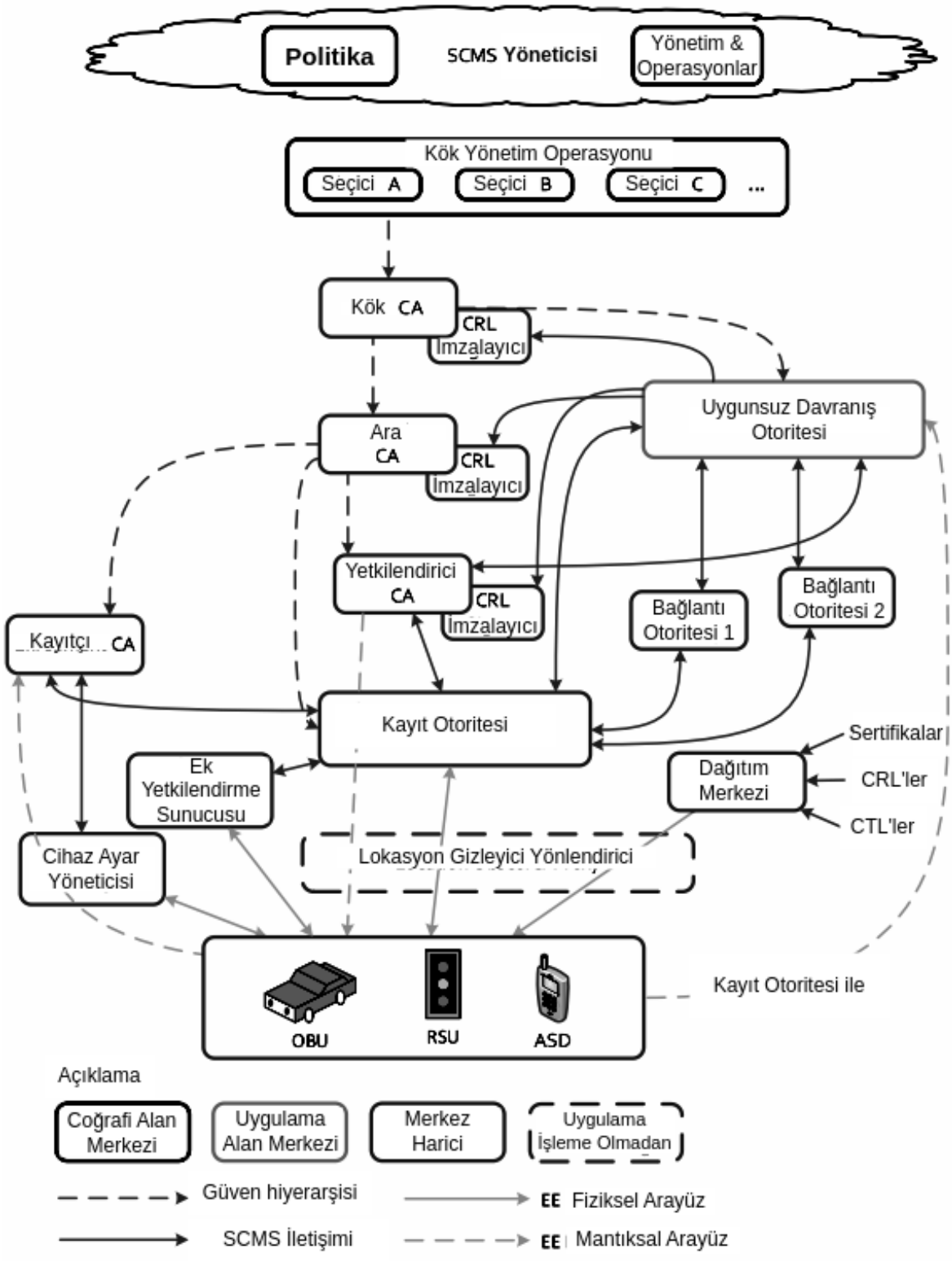
Bu standart, Ortak Anahtar Altyapısına (PKI) sahip olan Güvenlik Kimlik Bilgisi Yönetimi Sistemi (Security Credential Management System, SCMS) için ara birimleri tanımlar. Bir varlığın ağda sahip olduğu her bir sertifika, bir PSID içerir ve sertifika sahibinin izni olan uygulamayı belirtir. Ek olarak, yetkilendirmeler ve roller, hizmete özel izinlerde (service-specific permissions, SSP) kodlanmıştır. Bu da, sertifikaların aslında bir izin belgesi yığını olduğu anlamına gelir. Bu işleme şekli, Uluslararası Telekomünikasyon Birliği (ITU) sertifika sistemi tavsiyesi olan, X.509'un bir uzantısıdır. V2X içerisindeki herhangi bir varlık, birden çok sertifikaya sahip olabilir. Ayrıca, takma ad sertifikaları da birden çok olabilir ve birçok uygulama için ait olduğu kimliği koruyabilir. Kimlik ve başvuru sertifikaları (Identification and Application Certificates) ise sadece tek bir nesne için mevcuttur.

SCMS sisteminde kullanılan iki tür sertifika vardır;

1. Kayıt Sertifikaları (Enrollment Certificates),
2. Yetki Sertifikaları (Authorization Certificates).



Şekil 2.12: WAVE Güvenlik Hizmetleri ile WAVE Protokol Yığıtı [11]



Şekil 2.13: Kavramsal SCMS Mimarisi [12]

Kayıt sertifikaları, AV'nin, bir VANET'e katılma amacı ile, Kayıt Sertifikası Yetkilisine (ECA) başvurması ile gönderilir. Bu operasyondan sonra, ECA sistemde kullanılması amacı ile iki tür geçici sertifika sunabilir;

1. Kimlik Sertifikaları (Identification Certificates),
2. Takma Ad Certifikaları (Pseudonym Certificates).

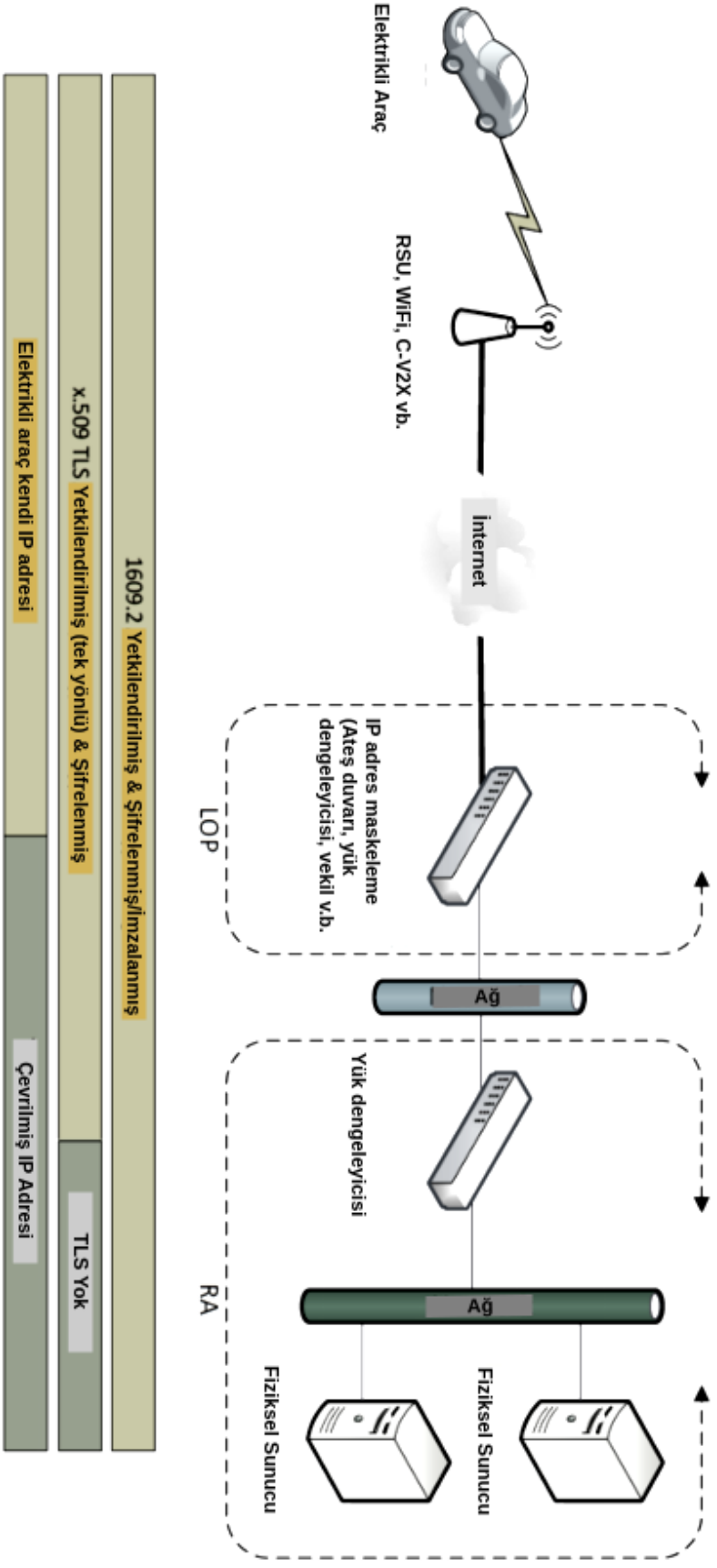
Takma ad sertifikaları, doğrudan kişiye özel bilgiler içermez. Bu nedenle, AV kulak misafirlerinden (eaves dropper) korunur. Ancak bunlar, kimlik sertifikalarından üretilmiş olmaları nedeni ile de, sistem tarafından izlenebilir. Takma ad sertifikaları, aynı zamanda ABD'de BSM, Avrupa'da ise ETSI terminolojisinde CAM ve DENM ile de kullanılır.

Bir V2X elemanın (örneğin bir AV) bir sertifika almak için kendini nasıl tanımlayacağı standartlarda bilerek boş bırakılmış bir alan gibi görünmektedir. Ancak, burada OAUTH2 sunucusu gibi sistemler kullanma referansları vardır. Bu durumda, OAUTH2 sunucusuna Kayıt Yetkilisi (RA) adı verilmiş olur.

2.3.2. ETSI

AV'ler bağlamında ETSI, IEEE'ye uyumlu gitmektedir, ayrıca V2X'e katkısı da oldukça fazladır. ETSI, her yeni işlem veya standardizasyon için bir görev grubu oluşturmaktadır. AV'lerin ve VANET'lerin (veya ITS) teknolojisi veya iyileştirilmesi için ETSI tarafından birçok belge sunulmaktadır. Bunlar, uzun araştırmalar ve toplantılar ardından, konusunda uzman kişiler tarafından doldurulmuştur. Sunulan belge tipleri aşağıda belirtilmiştir;

1. Teknik Rapor (TR),
2. Teknik Şartname (Technical Specification, TS),
3. Avrupa Normu/Standart (EN),
4. ETSI Standardı (ES),
5. Özel Görev Gücü (STF),
6. Grup Raporu (GR),



Şekil 2.14: IEEE Tarafından Açıklanan Güvenli İletişim Mimarisi [12]

7. Özel Rapor (SR),
8. Grup Spesifikasyonu (GS),
9. ETSI Kılavuzu (EG)

Belgenin kısa başlığı, örneğin “ETSI **EN** 302 637-2 V1.4.1 (2019-04)” yukarıdaki tipleri de içerir. Bu tez hazırlanırken, bilindiği kadarıyla ve güvenlik söz konusu olduğunda, ETSI daha çalışkan ve hızlı görünmektedir. CP (bu tezin en önemli çıkarımlarından biri) MBD referansları zaten ETSI belgelerinde [32] bulunmakta idi. Buna ek olarak, [165] ve [166] çalışmaları da, 5G’de V2X ihtiyaçlarını daha iyi düzenlemek için, ilgili MEC çabalarıdır. ETSI belgelerinde, V2X, gerçekten de en çok talep gören uygulamalardan biri olarak belli bir yere sahiptir.

2.3.2.1. ETSI TS 102 940 / 41 / 42 / 43

MBD ve CP bakış açısından, bu standartlar IEEE 1609.2 standart ailesine dayanmaktadır. Bu tez ile ilgili olan kısımlarından, savunma katmanı da bu standartlarda açıklanmıştır.

Belgelerde belirtilen dört savunma hizmeti vardır;

1. Olabilirlik (plausibility) doğrulaması
2. Log MBD bilgisi
3. Yerel MBD için Güvenlik ilkesi kurallarının yönetimi ve saldırılara tepkiler
4. Hatalı ITS İstasyonlarının (ITS-S) Bildirimi

Bu hizmetlerin her biri, ETSI’nin birçok diğer dökümanlarında açıklanmıştır.

2.3.2.2. ETSI TR 103 460

Bu tezin ana konusu olan MBD ve standartlarının geliştirilmesi, bu ETSI belgesinde açıklanmıştır. İlginç olan nokta ise, tez yazımı sırasında bilindiği kadarı ile, (IEEE belgelerindeki “bahsetmeler" dışında) MBD üzerindeki tek standardizasyon çabasıdır. Bu belgeden, IDS’lerin ve ilgili teknolojilerin ITS’de hala çok önemli bir yere sahip olduğu görülür. Her AV’deki yerel tehdit algılama yöntemlerinin her zaman en yeterli bir yöntem

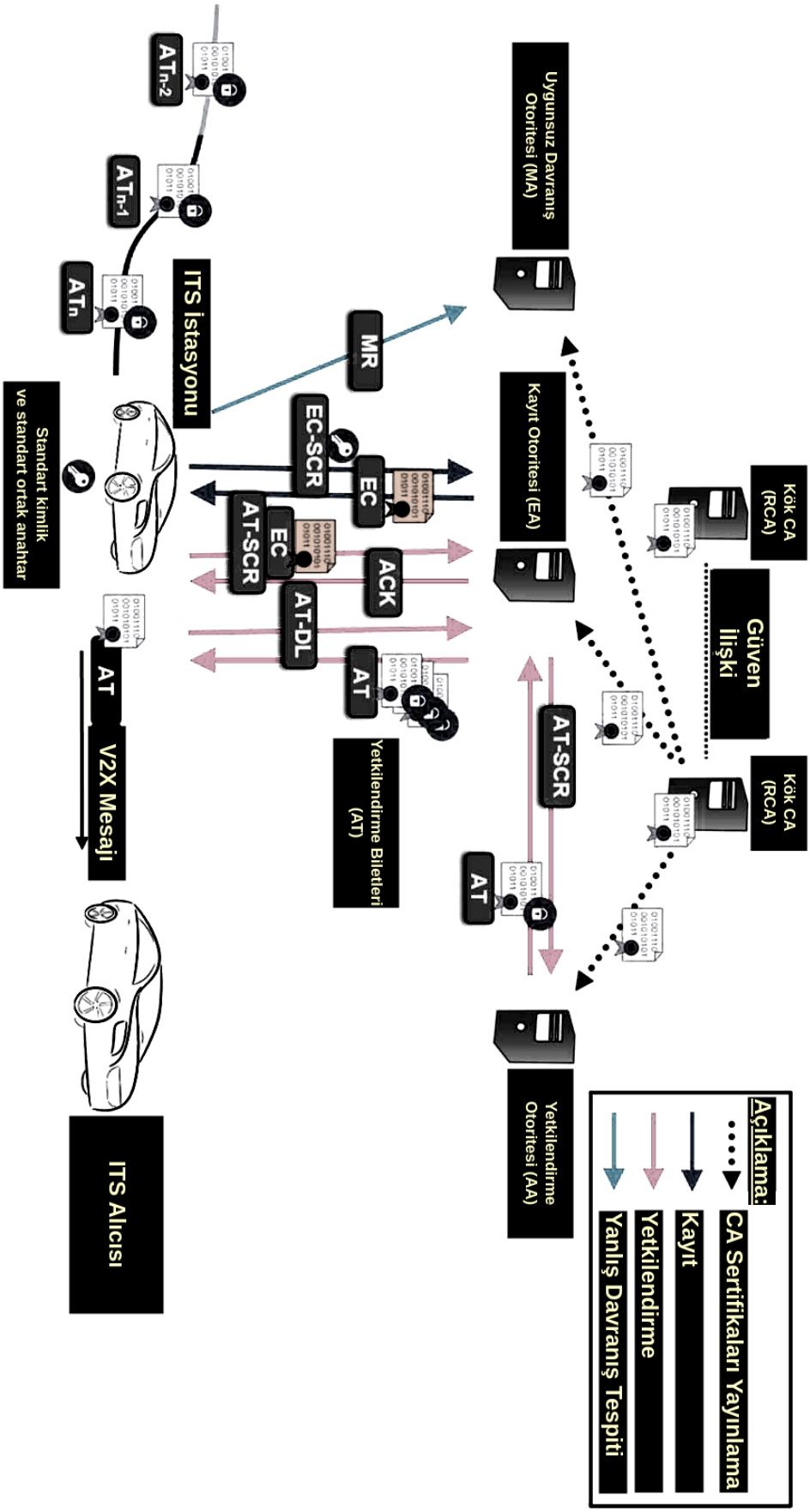
Tablo 2.21: ETSI'nin V2X'e MBD ve CP ile İlgili Katkıları (Devamı **Tablo 2.22:**'de)

Kod	Sürümler	Ad	Açıklama
ETSI EN 302 637-2	V1.1.1 (2010-04), V1.2.1 (2011-03), V1.3.2 (2014-11), V1.4.0 (2018-8), V1.4.1 (2019-04))	Akıllı Ulaşım Sistemleri (ITS); Araç İletişimi; Temel Uygulamalar Kümesi; Bölüm 2: İşbirlikçi Farkındalık Temel Hizmetinin Belirtimi	CAM mesajı açıklaması [167]
ETSI EN 302 637-3	V1.1.1 (2010-09), V1.2.2 (2014-11), V1.3.0 (2018-08), V1.3.1 (2019-04)	Akıllı Ulaşım Sistemleri (ITS); Araç İletişimi; Temel Set Uygulamalar; Bölüm 3: Merkezi Olmayan Çevre Bildirimi Temel Hizmetinin Özellikleri	DENM mesajı açıklaması [168]
ETSI TS 103 324	V2.1.1 (2023-06)	Akıllı Ulaşım Sistemi (ITS); Araç İletişimi; Temel Uygulama Seti; Toplu Algı Hizmeti, Sürüm 2	CP Hizmetinin Belirtimi [32]
ETSI TS 102 731	V1.1.1 (2010-09)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Güvenlik Hizmetleri Mimari	Güvenlik mimarisi
ETSI TS 102 860	V1.1.1 (2011-05)	Akıllı Ulaşım Sistemleri (ITS); ITS uygulama nesnelerinin sınıflandırılması ve yönetimi	Nesne sınıflandırması [16]
ETSI TR 102 893	V1.1.1 (2010-03), V1.2.1 (2017-03), V1.3.3D (2020-08), V 2.1.1E (2022-12)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Tehdit, Güvenlik Açığı ve Risk Analizi (TVRA)	Yöntem değerlendirmesi [34]
ETSI TS 102 940	V1.1.1 (2012-05), V1.2.1 (2016-11), V1.3.1 (2018-04), V2.1.1 (2021-07)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; ITS iletişimleri güvenlik mimarisi ve güvenlik yönetimi; Sürüm 2	Güvenli bir ITS sisteminin temel direklerini ve gereksinimlerini tanımlar [97].

- **D**: Taslak
- **E:** Beklenen

Tablo 2.22: ETSI'nin V2X'e MBD ve CP ile İlgili Katkıları (Devam)

Kod	Sürümler	Ad	Açıklama
ETSI TS 102 941	V1.1.1 (2012-06), V1.2.1 (2018-05), V1.3.1 (2019-02),V1.4.1 (2021-01),V2.1.1 (2021-01), V2.1.1 (2021-10)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Güven ve Gizlilik Yönetimi; Sürüm 2	Güven ve gizlilik yönetimi için [97]'den ayrıntılı açıklamalar: Ayrıntılı bölümler [98]
ETSI TS 102 942	V1.1.1 (2012-06)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Erişim Kontrolü	[15]
ETSI TS 102 943	V1.1.1 (2012-06)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Gizlilik hizmetleri	Gizlilik hizmetleri için [97]'den ayrıntılı açıklamalar: ayrıntılardaki kısımlar[96]
ETSI TS 103 097	V1.1.1 (2013-04), V1.2.1 (2015-06), V1.3.1 (2017), V1.4.1 (2020-10), V2.1.1 (2021-10)	Akıllı Ulaşım Sistemler (ITS); Güvenlik; Güvenlik başlığı ve sertifika biçimleri; Sürüm 2	Sertifika biçimleri
ETSI TR 103 460	V2.1.1 (2020-10)	Akıllı Ulaşım Sistemleri (ITS); Güvenlik; Yanlış Davranış Tespiti ile ilgili ön standardizasyon çalışması; Sürüm 2	MBD [33]
ETSI TR 103 562	V2.1.1 (2019-12)	Akıllı Ulaşım Sistemleri (ITS); Araç İletişimi; Temel Set Uygulamalar; Kolektif Algı Hizmetinin (CPS) Analizi; Sürüm 2	Kolektif algı (CP) hakkında teknik rapor, ortamın durumu [57]
ETSI GR MEC 022	V2.1.1 (2018-09)	Çoklu Erişim Uç Bilgi İşlem (MEC); V2X Kullanım Örnekleri için MEC Desteği Çalışması	MEC'de V2X ile ilgili Grup raporu, dolaylı olarak CP ile ilgili [165]
ETSI GS MEC 030	V2.1.1 (2020-04), V2.2.1 (2022-05)	Çoklu Erişim Uç Bilgi İşlem (MEC); V2X Bilgi Hizmeti API'si (VIS)	ETSI Endüstri Spesifikasyon Grubu (ISG) MEC ile V2X birlikte çalışabilirliği hakkında MEC raporu [166]



Şekil 2.15: Sertifikalarla Güvenli İletişim [97, 98]

olmayabildiğini belirtir. Bu nedenle, küresel bir algılama oluşturulması gerektiğini anlatır. Cooperative-ITS Credential Management System (CCMS) olarak da adlandırılan PKI altyapısı, MBD ile ilgili özellikler içermektedir. Burada, araçlar görünüşte kötü niyetli olarak gördükleri diğer araçlar için MBR'ler gönderir.

Bu işlem hali hazırda yalnızca CAM/DENM IDS olarak sınıflandırılabilir. Dökümanda MBD süreci şu şekilde belirtilmektedir;

1. Yerel uygunsuz davranış tespiti,
2. Uygunsuz davranış bildirimi,
3. Küresel yanlış davranış tespiti,
4. Hatalı ITS istasyonlarının (ITS-S) bildirimi.

ABD altyapıları ve standartlarında tüm bu sistem takma ad sertifikaları kullanır. AB'de ise bu takma ad sertifikaları yetkilendirme biletleri (AT) olarak isimlendirilir.

2.3.2.3. ETSI TR 102 893

Bu döküman, ETSI tarafından kullanılan "Tehdit, Güvenlik Açığı ve Risk Analizi" (TVRA) [169] yöntemini açıklamaktadır. ITS sisteminde olası güvenlik açıklarının her birini tanımlayıp, ortadan kaldırmak adına yapılabilecekleri belirtir, ayrıca savunma mekanizmalarını anlatır. Bunların nasıl yapılması gerektiğini de, son teknoloji araştırma çıktılarını kullanarak belirtir. Öneriler de her izinsiz girişe ve uygulamaya puanlama yöntemi ile anlatılır. Bu puanlama sistemi çok büyük bir kolaylık sağlar veya mevcut altyapı göz önüne alındığında uygulanmasının önemi veya kolaylığını belirtir. Karşı ataklar ve TRVA için 2.4. bölümünü kontrol edebilirsiniz.

2.3.2.4. ETSI TR 103 562

Bu tezden çıkarılabilecek bir başka çıkarım da CP'dir. Daha çok rapor gönderen araca ve onun anlık durumuna göre mesajları barındıran kolektif farkındalığın (CA) aksine, CP daha çok çevrede bulunan nesneler ve ortamla ilgilidir. CP ile araçların çevreye ilişkin bilgileri, daha iyi bir operasyon için merkezi bir yere (MA) gönderilir.

Tablo 2.23: MBD ve CP ile İlgili Diğer Katkılar

Kod	Sürümler	Ad	Açıklama
ISO/AWI TS 5083	Yalnızca yeni taslağı olan sürüm	Kara yolu araçları - Otonom sürüş sistemleri için güvenlik - Tasarım, doğrulama ve doğrulama	Güvenlik
3GPP TR 22.886	v.16.2.0 (2018)	5G V2X Hizmetleri için 3GPP Desteğinin İyileştirilmesi Çalışması (Sürüm 16)	3GPP V2X desteği
RFC6830bis	2017'den 2022'ye kadar 38 sürüm	Konum Belirleyici/Kimlik Ayırma Protokolü (LISP)	Bağlı araçlar için dağıtılmış yer paylaşımlı ağ oluşturma

Burada, CP (veya bu konuda MBR) için bir temsil (representation, tasarım) modeli seçmek çok önemlidir. ETSI TR 103 562 [57] (Yerel Dinamik Harita /LDM), [56] içerisinde ve diğer araştırma maddelerinde birçok temsili model önerilmiştir. Daha fazla bilgi için 2.4.4.1. bölümüne bakılabilir. LDM, Yerel Çevre Modeli (LEM) olarak da bilinir. Yine Küresel Çevre Modeli (GEM) de Küresel Dinamik Haritayı (GDM) kapsar.

2.3.3. SAE

SAE'nin AV'lere ve VANET'lere farklı katkıları bulunmaktadır. Ünlü özerklik seviyeleri, DSRC'deki mesaj yapıları ve hatta bazı ekipman standartları SAE'den gelmektedir.

SAE ile ilgili tüm standartlar (bazıları burada belirtilmektedir), öyle ya da böyle, CP yükünü taşıyacak uygulama katmanı omurgalarıdır. Bir CP uygulaması, mesaj yapılarının ve biçimlerinin üzerinden gelmelidir. Burada, CAM ve BSM'ye özel dikkat gösterilmelidir.

2.3.4. İş Birliği ve Uyum

2000'lerde Avrupa ile yeni dünya arasında geçen teknolojik bir savaş olmuştu [171]. Bir tarafta, Dünya Çapında Birlikte Çalışabilirlik (Worldwide Interoperability for Microwave Access, WiMAX) bulunmaktaydı. WiMAX, IEEE'nin 802.16 standart ailesini temel alıyordu. Öbür tarafta, Avrupa'da, 3GPP Uzun Dönem Geliştirme (Long Term Evolution, LTE) geliştiriliyordu. Sonunda, LTE kazandı ancak WiMAX hala etrafta, özel kurulumlarda

Tablo 2.24: SAE'nin MBD ve CP'ye Katkıları

Kod	Sürümler	Ad	Açıklama
SAE J2735	2006-12-19: DSRC, 2009-11-19, 2015-09-02, 2016-01-19, 2016-03-30, 2020-07-23: V2X, 2023-09-22: V2X	V2X İletişim Mesaj Seti Sözlüğü (Ayrıca BSM olarak bilinir)	Güvenlik [170]
SAE J2945/1	2016-03-30, 2020-04-30	V2V Emniyet Haberleşmesi	Emniyet için Araç Üstü Sistem Gereksinimleri [25]
SAE J2945/2	2018-10-30	Özel Kısa Menzilli İletişim (DSRC) V2V Güvenlik Farkındalığı	Güvenlik için Performans Gereksinimleri
SAE J2945/5	2020-02-05	İşbirliğine Dayalı Uyarlanabilir Hız Sabitleyici ve Müfreze İçin Performans Gereksinimleri	Güvenlik Yönergeleri
SAE J2945/6	(Şu anda devam eden çalışma / 2022-07 itibarıyla WIP)	İşbirliğine Dayalı Uyarlanabilir Hız Sabitleyici ve Takım Oluşturma	ADAS
SAE J2945/8	(Şu anda devam eden çalışma / 2022-07 itibariyle WIP)	İşbirlikçi Algı Sistemi	CP
SAE J2945/2S	2019-07-01	Özel Kısa Menzilli İletişim (DSRC) V2V Güvenlik Farkındalık Seti	Güvenlik için Performans Gereksinimleri
SAE J2945/9	2017-03-21	Hassas Yol Kullanıcısı Güvenlik Mesajı Minimum Performans Gereksinimleri	Güvenlik
SAE J3161/1	2022-03-21	LTE V2X V2V Emniyet Haberleşmesi	Emniyet için Araç Üstü Sistem Gereksinimleri
SAE J3224	2022-08	V2X İşbirlikçi ve Otomatik Sürüş için Sensör Paylaşımı	CP ile ilgili sensör paylaşımı [24]

veya belirli bölgelerde, görülmektedir.

İki rakip standart geliştirmek zordur. Harcanan zaman nedeni ile ekonomi için hiç iyi olmamaktadır. AV'lerin geldiğinde ise, zaman iş birliği zamanı gibi görünmektedir. Önceki savaşlardan alınan dersler, teknolojiyi daha da geliştirmek için, çoğu kuruluş birbirine yardımcı olmaya başlamış görünmektedir. Örneğin, IEEE'nin ISO ve ETSI ile olan bu "uyum" (harmonization) durumu ("AB-ABD standart uyumlaştırma görev grubu", "EU-US standards harmonization task group") ilgili belgelerinde görülebilmektedir [95]. Ortak bir görev gücü oluşturduktan sonra ve geliştirilen raporlar ve öneriler, IEEE standartlarına entegre da edilmiştir. ITS Koordinasyon Grubu (ITS Coordination Group, ITS-CG) ise ETSI ve CEN arasında koordinasyon için kurulmuştur. Bundan başka, "ETSI TS 102 860 Akıllı Ulaşım Sistemleri (ITS); ITS uygulama nesnelerinin sınıflandırılması ve yönetimi" [16], ITS uygulama tanımlayıcısı (ITS-AID) ve yapısı ve uyumlaştırma çabalarını ele almaktadır. Yalnızca bir sürümü vardır, V1.1.1 (2011-05). ISO, IEEE ve ETSI arasındaki benzer bir çaba ise, ISO'nun "bağlantı noktası" (port) alt yapısında mevcuttur. IEEE buna PSID[12] adını verir. ETSI'de ITS-AID[13] olarak tanımlanır.

Uyumlaştırma hakkında daha fazla bilgi için Norveç Kamu Yollarının (Norwegian Public Roads Administration) 2019 raporu incelenebilir [172]. Ayrıca, **Tablo 2.25:**'de iş birliği çabaları özetlenmiştir.

Eğer bir iş birliği matrisi yapabilse idik, satır ve sütunlar aynı olmak üzere tüm kurumları listelese idi, IEEE tüm diğer ilgili teknolojilerin temeli olduğundan, değerleri çoğunlukla matris boyunca köşegen olacaktı.

ETSI'de ise, uyumlaştırma çabaları özel görev birimleri (special task force, STF) tarafından yürütülmektedir. Daha fazla bilgi için [16] kaynağı incelenebilir. Teknik Standartlar için Uyumlaştırılmış Mimari Referansı (Harmonized Architecture Reference for Technical Standards) [14] web sitesi de bu konuda ayrıntılı bilgiler içermektedir.

Bir diğer iş birliği öğesi olarak yarışmalara ve projelere de değinilebilir. Bu ikisinden ilki, teknolojinin hangi aşamada olduğunu anlamanın güzel bir yoludur. Ayrıca, kazananlar gelecek yıla daha iyi hazırlanmaları için teşvikler de alabilmektedir. Bundan başka,

[12] https://standards.ieee.org/products-services/regauth/psid/public/
[13] http://its-standards.info/ITS%20Registries/ISO17419/ITSaidRegistry.html
[14] http://htg7.org/html/triples/s11d27f170.html

Tablo 2.25: İş Birliği Grupları

Kod	**Sürümler**	**Ad**	**Açıklama**
CEN, ETSI	CEN TC 278, ETSI TC ITS	ITS Koordinasyon Grubu (ITS-CG)	Çalışma grubu
CEN, ISO	CEN 278, ISO 204	Toplantılar	Yılda iki kez ortak toplantılar
ETSI, IEEE	IEEE, ETSI TC ITS	Uyum gurubu	ETSI TS 102 860
IEEE/SAE, ISO	Birçok	İş birliği standartları	Birbirleriyle uyumlu, birbirini takip
ETSI, ISO	ISO 18750:2018, ETSI EN 302 895	LDM	Yerel dinamik harita[56]
ISO, ITU	N/A	telekomünikasyon konularında birlikte çalışmak üzere anlaşma [173]	Anlaşma
ISO, ITU, IEC	Birçok	Dünya Standartları İş Birliği (World Standards Cooperation, WSC)	İş grubu (Work group)
CEN, CENELEC, ITU	Birçok	Anlaşma[173]	Birbirleriyle uyumlu, birbirini takip
5GAA, AECC	Birçok [161]	Raporlar	5G ve Çoklu Erişimli Uç Bilgi İşlemden (Multi-access Edge Computing, MEC) yararlanma
5GAA, 3GPP, ETSI	İş birliği [174]	Raporlar	ETSI ve ITS ile uyumlu Standardizasyon
FCC, Avrupa Komisyonu	Uyum [8, 9]	AB ile uyumlu Kurallar	Standardizasyon

Tablo 2.26: Yarışmalar

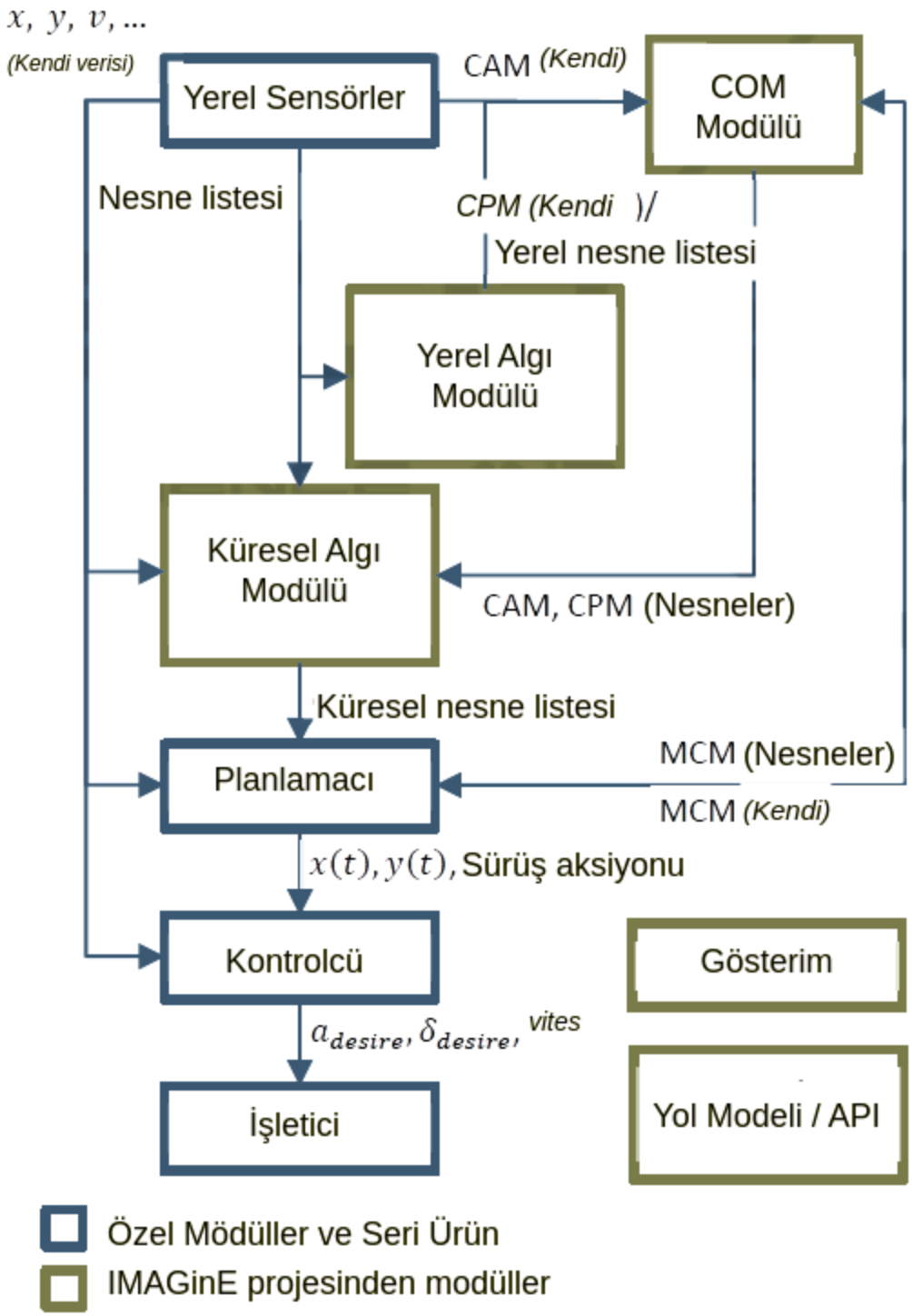
Ad	**Açıklama**
carhackingvillage [175]	Genel etkinlikler ve yarışmalar hakkında bilgiler
Car Hacking: Attack & Defence Challenge	Bilgi güvenliği ar-ge veri yarışması (2019 [176])
Pwn2Own [177] ve Zero Day Initiative	2019'dan beri araç yazılım korsanlığı
SINCON [178]	Yıllık araç güvenlik atölyeleri
Ipswich Bağlantılı Araç Pilotu [179]	Bağlantılı araçların en büyük yol testi denemesi ve Avustralya'da kamu yollarında üstlenilecek altyapı
Tesla Bug Ödül Programı [180]	Güvenlik açığı başına $100 – $15.000
DARPA 2016 Cyber Grand Challenge	AV'lerdeki ilk [71] yarışmalarından biri
Beşinci Uluslararası Bilgi Keşfi ve Veri Madenciliği Konferansı [181]	KDD-99 [182] ile düzenlenen, üçüncü Uluslararası Bilgi Keşfi ve Veri Madenciliği Araçları Yarışması
f1tenth [183]	Otonom robot/araç yarışı
IAC [184]	Indy Autonomous Challenge

yarışmaların kendilerinde bile birçok teknolojik gelişmenin başlangıcını görebilmekteyiz. Örneğin, ünlü DARPA Grand Challenge, birçok şirketi sahada çalışmaya teşvik etmiştir. Ünlü AV şirketleri ise, yarışma sonraları kazananları işe almıştır. **Tablo 2.26:** ise sektörü büyük ölçüde etkileyen bazı yarışmaları listelemektedir.

Öte yandan, projeler, teknolojinin mevcut durumunu kullanarak, V2X hizmetlerini geliştirmeyi denemektedir. Bunu yapmak, teknolojinin dar boğazlarını ve inceliklerini daha iyi fark etmeye yardımcı olur. Bununla birlikte, birçok standardın (hükumetler veya SB'ler tarafından desteklenen) çıktıları, ana akım standartlarla bütünleşmeden çok önceleri, projeler olarak başladığını görmek gerekir. Örneğin, V2X sertifikasyon altyapısı henüz standartlarda yerini bulmadan hayata geçirilmiş bir projeydi [164]. **Tablo 2.27:** dünya çapında şu anda devam eden bazı V2X ile ilgili projeleri listelemektedir.

Bunlardan IMAGinE projesinde detaylı olarak işbirlikçi sürüş işlevleri, ön koordinatlarda yol modeli, çarpışma kontrollerini işleme, izleme, iletişim birimi arayüzü (COM), planlama modülü tarafından istenen sürüş eylemi (seyir tavsiyesi ve hesaplanmış bir yörünge) bulunur.

Resimdeki (**Şekil 2.16:**) MCM, "Manevra Koordinasyon Servisi"'nin "Manevra Koordinasyonu" içindir. Bu mesaj türü ise, [32] taslağında yeni tanımlanmaktadır.



Şekil 2.16: IMAGinE Sistemine Genel Bakış [185].

Tablo 2.27: Projeler

Ad	Tür	Ülke	Açıklama
TransAID	CP	Avrupa	Trafik yönetimi prosedürleri ve protokolleri [186, 187, 188]
AutoNet2030	CP	Avrupa	2030'a Kadar Ağ Bağlantılı Otomatik Sürüş[189]
IMAGinE	CP	Avrupa	Akıllı Manevra Otomasyonu – gerçek zamanlı işbirlikçi tehlikeden kaçınma [157, 65, 185]
Autoware / Apollo	AVs	Dünya	Hepsi bir arada otonom sürüş kıyafeti [190]
MAVEN	CP	Avrupa	AV'lerin akışını düzenlemek için algoritmalar [191]
InSecTT	AI, IoT	Avrupa	Nesnelerin İnterneti ve Yapay Zekâ [192, 193]
Openc2x	AV'ler	Avrupa	iletişim teknolojileri ve ortak yardım sistemleri[153]
iMove	AVs	Avustralya	Avustralya'nın ulaşım ve mobilitede önde gelen uygulamalı araştırma merkezi [88]
5G-CORAL	SDR	Avrupa	Uç (Edge) Sanal radyo erişimi[174, 194]
5G-Miedge	SDR	Avrupa	5G uçta milimetrik dalgalar ile [174, 195]

2.3.5. Organizasyonlar Değerlendirmesi

Standartların ve genel olarak V2X'in kısa bir değerlendirmesinin yapmak gerekirse, V2X ve VANET teknolojisi için en çok yapılan eleştirilerden birinin, 5.9 GHz'in neredeyse kullanılmamış olması ve 30 MHz'in, CP daha fazlasını gerektirse de, kritik oto güvenlik hizmetleri [5] için yeterli olduğunun anlaşılmasıdır. Hücresel gelişmeler göz önüne alındığında ise, yeni düşünme biçimleri teşvik edilmektedir [8, 9].

DSRC'nin (standartlara ve dağıtımlara rağmen) "modasının geçmiş olması" başka bir eleştiridir. Ana itici güç, uygulamanın maliyetli olmasıdır ve bu noktada, ITS için yirmi yıl önce tahsis edilen spektrum kullanılamamaktadır.

Başka bir konu, standartlar güvenliği zorlamamakta [11] ancak önermektedir. Böylelikle, bir şekilde güvensiz ve kötü niyetli VANET'lerin inşa edilmesini ve işletilmesini sağlayabileceği öne sürülebilir. Bu da sürücülerin bilgilerini ve hayatını tehlikeye atabilecektir.

V2X tarafında, IDS/IPS çoğunlukla MBD [117] olarak ele alınmaktadır. Her ne kadar, ilk

araştırma maddeleri, en azından MANET'ler için, son yirmi yılda bulunmakta idi ise de, MBD, standartlara yeni eklenen bir yapıdır. Bu tür saldırı tespitinde her araç kablosuz ağa [23] sertifikaları ile bağlanır. Bu durumda, araç göz atmalara (eves-dropping) karşı yeterince güvenlidir, ancak ihtiyaç duyulduğunda şebeke operatörü için de aracın tam olarak hangisi olduğu yeterince açık olacaktır. Bu da, çoğunlukla sorumlu ağ otoritesi düğümlerinden alınan takma ad sertifikaları (IEEE) veya AT (ETSI) sertifikaları ile başarılır. Burada sertifikaların dağıtılması ve iptali, standartların pek üzerinde durmadığı çok önemli bir konu haline gelmektedir. Buna gibi durumlar, V2X iletişimini tanımlarken veya gerçekleştirirken farklı uygulamalara dönüşme ihtimallerini barındırır. Sadece bu değil, Resim **Şekil 2.15:**'da sunulan düğümlerin çoğu aynı dezavantajlara sahiptir.

Tüm bunların dışında, mobil teknolojilerin eski WiMAX ve 3GPP savaşını dikkate alarak, standart kuruluşları, diğer kuruluşlar, ülkeler ve pazar arasındaki iş birliğinin oldukça tatmin edici göründüğü kesinlikle söylenebilir. Endüstri, WAVE veya C-V2X'i geniş çapta kabul ediyor gibi görünmektedir. Elbette, her kurum tarafından tanımlanan standartlarda farklılıklar olabilecektir. Ancak bu farklılıklar, birbirini tamamlar ve eldeki ihtiyaç için küçük düzeltmeler şeklinde olabilirler.

2.4. V2X ARAŞTIRMALARI

V2X araştırmaları oldukça fazla çalışılan bir konu olarak gösterilebilir. Bu bölümde, bu çalışmalar; veri kümeleri, donanım, IDS & MBD, SDN, CA & CP, AI, BC ve kıyaslamalar şeklinde gruplandırılmaya çalışılacak, ayrıca birçok yönden en son araştırma öğeleri listelenecektir.

2.4.1. Veri Kümeleri

Bu kısımda, literatürdeki veri kümeleri, MBD bakış açısıyla ve CP gözüyle değerlendirilecektir. Bir çalışmanın altyapısı için, iyi veri kümeleri bulmak her zaman zordur. Aşağıda belirtilen birkaç veri kümesi oluşturma yöntemi yardımcı olabilir, ancak MBD/CP'nin yakın zamanda ortaya çıkması nedeniyle, konu için en uygun veri kümesini bulmak yine de kolay olmayacaktır. Bu tezde verilen ipuçları ve açıklamalar gelecekteki araştırmalar için de yardımcı olabilir. Bunun dışında, yalnızca CP veri kümeleriyle ilgili, eksiksiz bir araştırma [142] içerisinde bulunabilir.

Tablo 2.28: Autoware Yol Haritası [190]

Yıl	Gelişmeler
2015 - 2019	• 2015'teki ilk sürüm, • Birçok özel kampüse ve halka açık kara yolu servis/otobüs uygulamasına uyarlanmıştır.
2020	• v1.0'da Otonom Vale Park Etme (AVP)
2021	• v2.0'da Kargo Teslimatı, • Otonom yarış (F1TENTH ve IAC).
2022	• Autoware Core/Universe mimarisi tanıtıldı, • Otobüs genel yol desteği v3.0 için Core'da planlanmıştır, • Robo-taksi işlevi "Universe"'e eklendi.
Gelecek	• Mobility as a Service (Maas)/Robo-Taxi Autoware Core, yoğun kentsel ortamlarda L4 AD'yi desteklemeyi hedefliyor

Buradaki tüm veri kümeleri açık kaynak veri kümeleri olacaktır. Kapalı kaynak veya var olduğu belirtilen ama paylaşılmayan veri kümeleri belirtilmeyecektir. Ayrıca bu çalışmada, çoğu botnet'lerle ilgili olan veri kümeleri veya 2017 ve öncesi eski veri kümeleri de yoktur. Son olarak da, CAN veri kümeleri, bu tez ile ilgili değildir, ancak bazı önemli olanları V2X ile çalışabilirlikleri [196] nedeniyle dahil edilmiştir. Kapsamlı araştırma geçmişi olan hizmet reddi (DoS) [92] veya ilgili saldırı veri kümelerinden de bahsedilmemeye çalışılacaktır.

Lisans bilgileri belirtilmemişse, veri kümesi olağan bir araştırma olarak alınabilir. Bu nedenle, kullanım hakları ile ilgili olarak, herhangi bir araştırma öğesi gibi kullanılabilir.

[218]'da 1998 ile 2016 yılları arasında üretilen veri kümeleri dikkate alınmıştır. Geçmiş veri kümeleri ve metrikleri üzerinde faydalı olabilecek bir araştırmadır.

[102] adresindeki araştırma, 2019 yılına kadar olan veri kümeleri için faydalı olabilecek ipuçları sağlamaktadır. Birçok veri kümesini aşağıdaki gibi sınıflandırmıştır;

1. Akış tabanlı olup olmadığına

Tablo 2.29: Veri Kümeleri Listesi (Açıklamaları **Tablo 2.33:**'dedir) (Devamı **Tablo 2.30:**'da)

Ad	Alıntı	Yıl	Tür	Açıklama	Kurum	Lisans
CSE-CIC-IDS-2018, CIDDS-001, CIDDS-002	[197, 198, 199]	2018	1, 3, 8	Coburg İzinsiz Giriş Tespiti; Veri Kümelerini temel alan dokuz saldırı türüne sahip yeni bir akış veri kümesi	2, 3, 25	1
ISCX IDS 2012	[200]	2012	1, 8	IDS kıyaslama veri kümesi	2	1
NSL KDD	[201]	2009	1	IDS, KDD'99	1, 4	1
KDD KUPASI 99 Veri Kümesi	[202]	1999	1	5. Uluslararası Bilgi Keşfi & Veri Madenciliği Konf.	5	1
UNSW-NB15	[203, 204, 205]	2015	1	Yalın ağ paketleri	8	1
DARPA99	[206]	1999	1	IDS değerlendirme veri kümesi	9	4
DARPA2000	[207]	2000	1	Üç veri kümesi daha, belirli senaryolar	9	4
DARPA Cyber Grand Challenge - Veri kümeleri	[208]	2016	1	DARPA Deneysel Siber Araştırma Değerlendirme Ortamı (DECREE) için yeni nesil otonom siber savunma yeteneklerini "tehlikeye atmak" için veri kümeleri	9	4
ADFA LD12 / ADFA13 / ADFA 2013	[209]	2013	1	IDS veri kümesi, KDD	7	1
HogZilla	[210]	2019	1	Open Source IDS (NIDS), ISCX 2012 ve CTU-13 Botnet	29	1, 5
InSDN	[211]	2020	1, 4	Yeni Bir SDN Saldırı Veri Kümesi	30	1
Kyoto kıyaslama veri kümesi	[212]	2015	1	Kyoto Üniversitesi Bal küpleri	31	1

Tablo 2.30: Veri Kümeleri Listesi (Devam)

Ad	Alıntı	Yıl	Tür	Açıklama	Kurum	Lisans
VeReMi	[117]	2018	1, 5	MBD, CAM DENM ile ve yalnızca işaretleme	32	4
F^2MD	[122]	2020	1, 5	MBD	34	1
VeReMi-Extension	[118]	2020	1, 5	VeReMi eklemeleri (F^2MD kullanılarak), yeni saldırı türleri	34	1 ile
CalTrans (PeMS)	[213, 214]	2014	1, 6	39.000 ayrı detektör, Kaliforniya Eyaleti	33	6
COnGRATS veri kümesi	[215]	2016	5, 6	KITTI	34	4
TUDataset	[216]	2020	1, 6, 7	Graph Temelli ANN	34	4
Ogb-lsc	[217]	2021	1, 7	Büyük Ölçekli Çizelge ML Veri Kümeleri	34	4
CAIDA	[218]	2002 / 2016	1	Kapsamlı veri kümeleri listesi	11	4
CDX	[219]	2009	1	NSA ile ilgili yarışmalar veri kümesi	14	4
Twente	[197]	2009	1, 8	Gerçekçi, nispeten küçük veri kümesi	26	4
gureKddcup	[220]	2016	1	kddcup99 bağlantılarını (UCI deposunun veri tabanı) içerir, ancak yükünü (ağ paketlerinin içeriği) bağlantıların her birine ekler	15	4
UGR'16	[221]	2018	1, 3, 8	Birkaç netflow v9 toplayıcısından, stratejik olarak bir İspanyol ISP'nin ağına yerleştirilmiş	34	1

Tablo 2.31: Veri Kümeleri Listesi (Devam)

Ad	Alıntı	Yıl	Tür	Açıklama	Kurum	Lisans
TRAbID	[222]	2017	1	Kolayca güncellenebilen veri tabanları üretmeyi amaçlayan yeni araç tabanlı izinsiz giriş veri tabanı oluşturma yöntemi	34	4
Birleşik Sunucu ve Ağ	[223]	2018	8	Los Alamos Ulusal Laboratuvarı'ndan toplanan loglar (event)	34	4
V2X-Sim	[224]	2022	6	A Kapsamlı Sentetik Çok Aracılı Algı Veri Kümesi	17, 18	1
highD veri kümesi	[225]	2018	5, 6, 7	Almanya otoyollarında	19	1
5RoutingMetrics	[226, 227]	2021	6	Kentsel senaryolarda VANET simülasyonlarından farklı trafik ölçümlerinin toplanması	20	1
Ngsim	[119]	2017	6	Gerçek trafik veri kümesi	35	1
Wyoming CV Pilotu Bir Günlük BSM, UMTRI	[228, 229]	2021	5	Wyoming CV Pilot Temel Güvenlik Mesajı Bir Günlük Örnek	22, 23, 35	1
Pekin taksi GPS yörünge veri kümesi	[181]	2018	6	GPS taksi yörüngeleri	34	1
USDOT C2SMART	[163]	2021	6, 7	CP veri kümesi oluşturuluyor	24, 35	1
IDS İmza Dosyaları	[31, 230]	Çeşitli	Çeşitli	Snort veya Suricata topluluğunun ve çeşitli zaten var olan kural ve imza koleksiyonu	Çeşitli	Çeşitli

Tablo 2.32: Veri Kümeleri Listesi (Devam)

Ad	Alıntı	Yıl	Tür	Açıklama	Kurum	Lisans
Waymo Açık Kaynak Veri Kümesi	[163]	2022	6	CP, 1.950 sahne için sensör verileri ve etiketler, nesne yörüngelerini içeren hareket veri kümesi; 103.354 sahne	28	3
KITTI Veri Kümesi	[163]	2021	6	Görüntü kıyaslama paketi kayıtları	36, 37	4
MARS Veri Seti	[231]	2016	6	Hareket Analizi ve Yeniden Tanımlama Seti, Market-1501 veri kümesi	34	4
BurST-ADMA	[232]	2022	1,5	VeReMi ilham alan Avustralya MBD veri kümesi	34	1

2. Türlerine ve özelliklerine (ör. Netflow, OpenFlow)

3. Paket tabanlı (ör. TCP/UDP) olup olmadığına

4. "diğer" (ne paket tipi, ne de akış tipi)

Araştırmanın sonunda CICIDS 2017, CIDDS-001, UGR'16 veya UNSW-NB15 veri kümelerinden birini seçmeyi önerir.

[233]'de makine öğrenimi ve veri madenciliği ile ilgili yöntemler dikkate alınmıştır. Veri kümeleri, özellikle CIC-IDS-2017 ve CSE-CIC-IDS-2018'i tanıtmış ve o zamana kadarki saldırılar için güncel olan bu veri kümelerine ihtiyaç olduğunu belirtmiştir.

[112]'de, DL ile ilgili bir metodoloji, otuz beş adet mevcut veri kümelerine uygulanmıştır. Ayrıca CSE-CIC-IDS2018 veri kümesini ve başka bir IoT tabanlı veri kümesini de tanıtmıştır. Bu çalışma 2019'a kadar, DL'deki veri kümelerini anlamak için kullanılabilir.

[234]'de, en çok kullanılan sekiz veri kümesi analiz edilmiş, sınıflarına göre ayrılmıştır. Bunların nasıl kullanılacağına ilişkin genel bir öneri de en sonda belirtilmiştir. Bu çalışma içinde belirtilen veri kümeleri için bir ölçüt olarak kullanılabilir.

Trafik ile ilgili veri kümeleri hakkında daha fazla bilgi de [235] çalışmasında bulunabilir. Bu

Tablo 2.33: Tablo 2.29: İçin Açıklamalar

Kurumlar

1. New Brunswick Üniversitesi (UNB), Kanada
2. UNB Kanada Siber Güvenlik Enstitüsü (CIC), Kanada
3. İletişim Güvenliği Kuruluşu (CSE), Kanada
4. Bilgi Teknolojisi Enstitüsü (IIT), Ulusal Araştırma Konseyi (NRC), Kanada
5. Veri tabanlarında Bilgi Keşfi (KDD), Bilgi ve Bilgisayar Kaliforniya Bilim Üniversitesi, Irvine
6. Hacking ve Karşı Tedbir Araştırma Laboratuvarı, Kore Üniversitesi
7. Yeni Güney Galler Üniversitesi (UNSW)
8. Akıllı Güvenlik Grubu, UNSW Canberra
9. MIT Lincoln Laboratuvarı
10. C2SMART
11. Uygulamalı İnternet Veri Analizi Merkezi
12. Lawrence Berkeley Ulusal Laboratuvarı
13. ICSI
14. ABD Askeri Akademisi
15. Universidad del Pais Vasco
16. Massachusetts Üniversitesi
17. AI4CE Laboratuvarı
18. MediaBrain Grubu
19. Otomatik Sürüş Departmanı, Otomotiv Mühendisliği Enstitüsü RWTH Aachen Üniversitesi
20. Universitat Politècnica de Catalunya. Departament d'Enginyeria Telemàtica
21. Araçla Hizmet Reddi Ağları, Sistem Laboratuvarı
22. Caocsar
23. Michigan Üniversitesi Ulaştırma Araştırma Enstitüsü
24. Çeşitli üniversiteler ve devlet kurumları arasında iş birliği
25. Coburg Üniversitesi
26. Twente Üniversitesi
27. Shmoo Grubu
28. Waymo
29. Hogzilla kimlikleri
30. University College, Dublin, İrlanda
31. Kyoto Üniversitesi
32. Dağıtık Sistemler Enstitüsü, Ulm Üniversitesi
33. Kaliforniya Ulaştırma Bakanlığı
34. Araştırma Raporu öğe USDOT
35. Karlsruhe Teknoloji Enstitüsü
36. Chicago'daki Toyota Teknoloji Enstitüsü

Lisans

1. Yok, ancak belirtilmesi veya alıntı yapılması gerekiyor
2. İndirmek için e-posta adresi gerekiyor
3. Apache 2.0
4. Yok
5. GPL
6. Yok, ancak kayıt gerekiyor

Türler

1. kimlikleri/MBD
2. CAN kimlikleri
3. Botnet
4. SDN IDS/MBD
5. İşbirlikçi Farkındalık (CA) IDS/MBD
6. CP IDS/MBD
7. Çizelge Tabanlı ML IDS/MBD
8. Akış Tabanlı IDS/MBD
9. DoS

kümeler, MBD ve CP işlemleri için de kullanılabilir.

2.4.1.1. IDS İmza Dosyaları

[31, 230]'in önerdiği gibi, topluluk (ensemble) yöntemleri veya IDS yazılımı kullanılarak toplanan imza ve kural dosyaları, veri kümeleri için iyi bir adaydır. Bunlar, P4 [236] programlanabilir ağ anahtarlarında (veya başka alanlarda) bile kullanılmak üzere, orjinal biçimlerinden öğelere (five-tuples, 5 öğe veya daha fazla) çıkarılabilir.

2.4.1.2. Veri Kümeleri Değerlendirme

Literatürdeki çoğu veri kümelerinin, özellikle V2X ile ilgili olmadığı söylenebilir ve özellikle CAN trafiği ile ilgili olanlar çoktur. Mevcut veri kümeleri, V2X veri kümelerine dönüştürülebilir, ancak pratikliği ve performansı gelecekteki bir araştırma öğesi olarak düşünülebilir. Ayrıca, bazı araştırma öğeleri, V2X'e atıfta bulundukları halde yalnızca V2X'in CAN [196] üzerindeki etkisi ile çalışmışlardır.

Bir yan not olarak, bu çalışma diğer veri kümesi türlerinden CA & CP ile ilgili çizelge veri kümelerini de içermektedir. Daha fazla bilgi için **Tablo 2.29:**'a bakılabilir.

V2X ile İlgili Veri Kümeleri

V2X veri kümeleri listesinden çıkarabildiğimiz kadarıyla, tüm veri kümeleri sentetik veri kümeleridir. [237, 238] içinde açıklandığı gibi, kullanılan benzetim yapıları ile VANET sentetik veri kümeleri oluşturulabilir. Öte yandan, highD veri kümesi araç kimliği barındırmamakta, ancak dron ile kuş bakışı görüntüleri tutmaktadır. V2x veri kümeleriyle ilgili daha fazla bilgi, V2X için VereMi ve VDDD'yi öneren [239] çalışmasında bulunabilir. BurST-ADMA, VeReMi ve VeReMi-Extension arasındaki farklar için **Tablo 2.35:** incelenebilir. VeReMi uzantısı veri kümesi, F^2MD (Framework For MBD, Yanlış Davranış Tespiti Çerçevesi) [122] ile oluşturulmuştur. F^2MD araştırmacıların yeni özellikler ve yöntemler kullanarak MBD'yi kolayca geliştirmelerine olanak tanır.

Tablo 2.34: MBD ile İlgili Veri Kümeleri

Veri Kümesi	Simülatör	Açık Kaynak	Yeniden Üretim	CPM	Çizelge	Bölge
VeReMi (2018) [117]	Veins	✓	✓			ABD
Dynamic (F^2MD) (2020) [122]	Veins	✓	✓			ABD
VeReMi-Uzantısı (F^2MD) (2020) [118]	Veins	✓	✓			ABD
MISO- V (2021) [121]	CARLA			✓		AB
(+F^2MD) (2022) [120]	ARTERY			✓		AB
BurST-ADMA (2022)[232]	SUMO	✓				AU
iLDM (2022) [52]	SUMO			✓	✓	AB
S-LDB (2022) [55]	ms-van3t	✓		✓	✓	AB

MBD ile İlgili Veri Kümeleri

Bu tezde VeReMi[117] ve BurST-ADMA[232] veri kümelerinin, MBD ile ilgili çalışmalarda kullanılmaya en uygun açık kaynak veri kümeleri olduğu görülmüştür. VeReMi, bir veri kümesini yeniden oluşturmak için gereken hem veri kümesini hem de altyapıyı sağlar. Öte yandan BurST-ADMA, VeReMi'den esinlenerek Avustralya V2X sistemi için uyarlanmış bir veri kümesidir. Ancak, özelleştirilmesi için hiçbir açık kaynaklı yazılım sağlanmamıştır. **Tablo 2.34:** içinde MBD için veri kümeleri ile ilgili ulaşılabilen son durum incelenebilir.

Toplu Algı Mesajı (CPM), standartlarda yerini yeni almış ve geliştirme çalışmaları devam eden bir sistem olarak kabul edilebilir [32, 57]. Bu mesajlar CAM/DENM mesajlarıyla veya kendi mesaj yapılarıyla (CPM) iletilip ve AV'nin ortamdaki tüm nesneler hakkındaki kendi düşüncesini veya hissini belirtecektir.

2.4.2. Donanım

2011 yılında Marc Andreessen, "Yazılım dünyayı yiyor" demişti [240]. Demek istediği programlanabilirlik olduğu açıktır. Bir kutudaki bir yazılımı yeniden programladıktan, derledikten ve aynı yere kurduktan sonra, bu yeni sürüm çalışmaya devam eder. DevOps işlemlerinin çoğu bu basit fikir üzerine kuruludur; yazılım sürüm döngülerini iyileştirmeyi nasıl yapabiliriz? Bu döngüyü nasıl daha az zaman ve kaynak harcayacak hale getirebiliriz? Daha az hataya açık ve daha az tehlikeli duruma nasıl gelebiliriz? Yazılımı nasıl geliştirebiliriz ve sonra nasıl kolayca kullanmaya başlarız? Yazılım dünyasında, bu hep böyle

Tablo 2.35: BurST-ADMA, VeReMi ve VeReMi-Extension [232]

Tür	**Öğe**	**BurST-ADMA**	**VeReMi**	**VeReMi-Ext.**
C-ITS Öğeleri	Bisiklet	✓	✓	✓
C-ITS Öğeleri	Veri Yolu	✓	✓	✓
C-ITS Elemanları	Motosiklet	✓		
C-ITS Öğeleri	Yaya	✓		
C-ITS Elements	Toplu Taşıma Otobüsü	✓	✓	✓
C-ITS Elements	Toplu Taşıma Tramvay	✓		
C-ITS Öğeleri	Kamyon	✓		
C-ITS Unsurları	Binek Araç	✓	✓	✓
Saldırılar	Sabit Rastgele Konum	✓	✓	✓
Saldırılar	Pozitif Konum Ofseti	✓	✓	✓
Saldırılar	Negatif Konum Ofseti	✓	✓	✓
Saldırılar	Sabit Rastgele Hız	✓		✓
Saldırılar	Pozitif Hız Dengesi	✓		✓
Saldırılar	Negatif Hız Dengesi	✓		✓
Saldırılar	Tersine Yönlendirme	✓		
Trafik Türü	Sol Trafik	✓		
Trafik Türü	Sol Trafik		✓	✓

olmuştur. Kurulan bir yazılımın, yeni sürümü aynı makineye rahatlık kurulabilir. Donanım dünyasında ise, donanım geliştirmek için en iyi seçenek Uygulamaya Özel Entegre Devreler (ASIC) geliştirmektir. Bunun için, öncelikle bir prototip oluşturulur. Bu prototip, yavaş bir benzetim de olabilir. Böylece donanımlar yazılımdaki yetenekleri taklit ederdi. Bu prototip, benzetimlerden daha hızlı ancak ASIC'den daha yavaş olan Sahada Programlanabilir Kapı Dizileri (Field Programmable Gateway Array, FPGA) de olabilir. FPGA, donanıma daha yakındır ancak talep üzerine yeniden programlanma özellikleri bulunur. FPGA veya emülatör sürümü, her testi geçtikten sonra, en performanslı durum için son halini bir ASIC'e dönüştürmek gerekmektedir. Genel kabul donanımın hızlı ve yazılımın yavaş olduğudur. Bir alt yapıda ne zaman programlama yetenekleri artar, ilginç bir şekilde performans düşer. Bu birlikte yaşamamız gereken bir fenomen gibi görünmektedir. Bunun istisnası, çizelge işlemci birimleri (GPU) [241] ve P4 programlanabilir ağ ekipmanları olmuştur [19]. GPU'lar, hızlı matriks işlemlerinin genel amaçlı kullanımının yolunu açtı [18] ve genel amaçlı GPU'lar (GPGPU) oldular. Yapay zekâ işlemlerini hızlandırdılar. P4 programlanabilir ekipmanlar da ağ üzerinde benzer bir etkiye sahip oldular. Artık IPSec bile P4 [30] ile uygulanabilir bir haldedir. Artık bu iki gelişme ile donanım programlanabilirliği dünyayı, Marc Andreessen'in deyişi ile, "yiyebilir" durumdadır. Bütün bunlar, sırayla SDN'nin çalışma şeklini değiştirdi.

Şimdi, Yeni Nesil SDN (NGSDN) [242, 243] ile karşı karşıyayız. Ağ ekipmanları, daha iyi programlanabilirlik ile daha hızlı hale gelmiştir. Bu, SDN'yi daha iyi yönde etkileyecek ve doğrudan ileride açıklayacağımız gibi 6G [27] ve V2X'i etkileyecektir.

2.4.2.1. FPGA

FPGA, birçok araştırmanın yapı taşıdır. ASIC'e yakın performansının olması, daha fazla enerji verimliliğine sahip olması [244] kullanım için inisiyatif sağlar. FPGA üzerinde, araç içi ve V2X ortamlarında, IDS ve MBD'nin AI ile çalışması konusu literatürde aktif bir araştırma konusudur.

[244]'de daha fazla enerji tüketen CPU'lar veya GPU'lar yerine FPGA'nın kullanılabileceği belirtilmiştir. Doğrudan V2X ile ilgili olmasa bile, bizim durumumuzda, AV'ler gibi kısıtlı bir ortamda iyi bir seçim olabilirler. Ancak, GPU ortamlarında dağıtık işlemleme yapısı olan TensorFlow gibi bir geliştirme çerçevesinin mevcut olmaması [18], bir dezavantajdır.

[101], V2X'teki olayların sayısını gerçek zamanlı işlemeye odaklanan bir SAE makalesidir. IDS amaçları için donanım teknolojilerinin, FPGA veya benzerini kullanılmasını önerir.

[29]'daki araştırma, V2X'te uygulanabilir FPGA tabanlı bir NIDS IoT ekipmanında tasarımın nasıl yapılacağına dair öneriler ve örnekler vermektedir.

[245]'de yazarlar FPGA ile, DSRC'de bulunan radyo frekansları yerine ışık temelli teknolojilerin kullanımı olasılığını araştırmaktadırlar. Ücretsiz bant genişliğinin olmaması ve araçlarda LED ışıkların mevcut olması gibi durumların bunu bir olasılık haline getirebildiği belirtilmiştir.

[246] içerisinde, performanslı bir V2X-IoT platformu açıklanmaktadır. Hem bir sinyal işlemcisi, hem de bir hızlandırıcı olarak FPGA'yı kullanmaktadır. Cihazlarının RF sinyallerini, FPGA modülü dinlemekte ve sistemi güçlendirmektedir.

2.4.2.2. P4

P4 doğrudan AV'lerle ilgili olmamakla birlikte, dolaylı olarak VANET'te bir etkinleştirici olabileceği düşünülmektedir. Temel V2X ağlarına, öngörülebilir performans için C-ITS sistemlerine [NG]SDN yetenekleri sağlanabilir [247]. P4 ile, ağ içi (data plane, veri düzleminde) makine öğrenimi algoritmalarını çalıştırmanın da mümkün olduğu belirtilmiştir

Tablo 2.36: V2X için FPGA ile İlgili Araştırmalar

Araştırma	Alan	İsim
[244]	ANN	FPGA ANN Araştırması
[101]	V2X	FPGA ve IDS için önerilen benzer sistemler
[29]	IoT	NIDS için FPGA önerisi
[245]	V2X	FPGA tabanlı SDR VLC
[253]	V2H, V2G	FPGA'da Araç şarj aktarım denetleyicisi
[254]	V2X	Müfreze (platooning) senkronizasyonu
[255]	C-V2X	FPGA tabanlı fiziksel yan bağlantı kontrol kanalı (PSCCH) kör nokta algılama
[256]	V2X, C-V2X	FPGA tabanlı [C-]V2X tasarımı
[257]	V2X	Birden Çok FPGA Sistemi Bazlı AV Ekipmanları
[258]	V2X	FPGA üzerinde kriptografi işlemleri
[246]	V2X, IoT	Sinyal işlemci ve hızlandırıcı olarak FPGA

[248, 249].

Programlanabilir veri düzlemleri ile AI ve IDS hakkında daha fazla bilgi için [250] araştırması incelenebilir.

2.4.2.3. ASIC

Tesla, araçlarında ANN ASIC'leri içeren bir bilgisayar konumlandırmıştır [251]. Böylece, AV'lere CP ve CA için büyük güç verilmiş olur. Benzer şekilde, NVidia Jetson [60] ve DRIVE [252] bulunan birkaç başka sistem de vardır.

2.4.2.4. OBU ve RSU

OBU'lar ve RSU'lar, kişisel bilgisayarlar (PC) benzeri tümleşik sistemlerdir. Genellikle, önceden tanımlanmış, otomobillerdeki sunucu/bilgisayar birimleri veya işletim sistemli bilgisayarlar olarak düşünülebilir[15] . Ülkemizde ise Ulak Haberleşme A.Ş. ve Netaş'ta üretilen RSU ve OBU'larımız bulunmaktadır[16] [17] .

Çoğu standart OBU veya RSU, Linux yazılımına sahip kutularıdır. Buradaki soru, piyasadaki arabaların çoğunun akıllı olmaması, görece az miktarda olmalarıdır. Akıllı ulaşımın veya en azından CAM/DENM mesajlarını almanın çaresi ise [259, 260, 261]'da tartışılmaktadır.

[15] https://www.commsignia.com/products/obu/
[16] https://www.netas.com.tr/documents/annual-reports/2020/annual-report_Q1_2020-05-15.pdf
[17] https://www.ulakhaberlesme.com.tr/tr/cozumlerimiz/akilli-ulasim-sistemleri

Tablo 2.37: V2X için P4 ile İlgili Araştırmalar

Araştırma	Alan	Açıklama
[93]	MBD, IDS, AI	ANN ile DDoS tespiti
[262]	IDS, SDN	ANN ile IDS
[263]	IDS, SDN	İki seviyeli IDS
[264]	IDS, SDN	SDN tabanlı IDS ve SYN paketlerini kullanan IPS
[265]	IDS, SDN	Federe/İşbirlikçi Öğrenme (Federated/Collaborative Learning, FCL) tabanlı, hat hızında, IDS
[266]	IDS SDN	IDS için yüksek performanslı (100 Gb/sn) meta veri çıkarıcı
[31]	IDS, SDN	Trafik işlemede azalmayı belirtmek için vitrin

2.4.2.5. Değerlendirme

Donanımda programlanabilirlik, yalnızca yazılım temelli çözümlerden daha az enerji ve daha fazla performans sağlar. Ağ teknolojileri çok hızlı ilerlemektedir. Buna karşılık, donanım teknolojilerindeki ilerlemeler, bunlar üzerine inşa edilen V2X ağlarını ve çevre birimlerini etkileyebilir. AV'lerde donanım çözümlerinin kullanılmasına yönelik çalışmalar oldukça çoktur. Bu, ister ML veya [N]IDS için olsun, ister hızlandırma amaçlı olsun, oldukça güncel ve aktif bir araştırma alanıdır. V2X'in geleceği ise SDN çözümlerinde görünmektedir.

2.4.3. Yazılım Tanımlı Ağlar

5G ve 6G'de, SDN ve NFV'nin temel teknolojilerden bazıları olduğu görülmektedir [267]. Ağ için özel yapılmış ekipmanlar yerine, yerinde veya tesis yakınında, uç (edge) veya sis (fog) alt yapıları, tüm hizmet işlevselliğini verebilmektedir. V2X durumunda ise, SDN, performans sağlayıcı olarak hizmet edebilir görünmektedir. Bundan sonra tartışılacağı gibi, asıl soru bunun mümkün olup olmadığıdır. Bu tezde, AV'lerin programlanabilir veri düzlemleri olup olamayacağı da tartışılacaktır.

[248]'de, bir V2X yapısına benzeyen bir ağ yapılandırılmıştır. Burada, AV'lerin, yolun ve çizgilerinin bir resmini programlanabilir bir anahtara (switch) gönderen kameraları bulunmaktadır. Bu anahtar, bir görüntü paketi geldiğinde, bir DL işlemi çalıştırır. Yolun çizgi konumunu tanınır ve AV'lere geri gönderilir. Bu uygulama, sıkı gecikme kısıtlamaları adına "ağ içi hesaplama" olarak adlandırılan sistemlerde kullanılmak üzere iyi bir fikir gibi görünmektedir. Ayrıca V2X iletişim performansını arttırabileceği görülmektedir. Bu çalışma,

Tablo 2.38: SDN & V2X ile İlgili Araştırmalar

Araştırma	Alan	Açıklama
[248]	Bilgisayar görüşü, (computer vision, CV), V2X	CV için veri düzlemi kullanımına ilişkin bir araştırma
[268]	CV, Görüntü Sınıflandırması, CP, CA	NetPixel, P4 anahtarlarında (switch) gerçek zamanlı dağıtılmış görüntü sınıflandırması
[94]	Ağ içi literatür taraması	Kendi kendine sürüş yetenekleri için ağ içinde nelerin programlanabileceğine bir yanıt
[269]	CP, CPM	VANET “Faz 2" gereksinimleri üzerine bir literatür taraması
[270]	C-V2X, IoV, Edge, MEC	Dinamik SDN Denetleyicisi
[271]	Literatür Taraması	SDN ile VANET’lerin hem güvenliği hem de geleceği üzerine bir literatür taraması

aynı zamanda ağ içi hesaplamanın güzel bir literatür incelemesini de sunmaktadır.

[94] aynı zamanda ağ içi bilgi işlemleme ile ilgili bir çalışmadır. Cihazlar üzerinde neler işlenebileceğine dair dair örnekler vermektedir. DDoS tespiti gibi algoritmaların bu durumda güzel adaylar olabileceğini belirtilmiştir. Algoritmaların, işledikleri verilerle olabildiğince yakın olması gerektiğini savunulur.

[269], SDN’in araç veri iletişimi için önemli olduğunu belirtir. SDN’lerin ağ heterojenliğini soyutlama yeteneğinde ileri olmasını, onların araç ağları için iyi bir yapı olduğunu gösterdiği belirtilmiştir. Ayrıca IoT veri toplama tekniklerinin, CP[M] sinyallerini de kolayca uygulanabileceğini belirtilmiştir [272].

[270], dinamik SDN denetleyici atamasının daha önce olmayan bir yolunun (DSDVMEC), yeni bir “aSDNalloc" algoritması ile, 5G’deki NFV yapılarına uygulanabilirliği hakkında bir makaledir. Atama için yapay zekâ kullanılmakta, kapsamlı ve değerli olan bir SDN denetleyicileri literatür taraması da sağlanmaktadır. Ayrıca, SDN ağından toplanan ölçümler için bir izleme bileşeni de içerir.

[271] ise, SDN tabanlı VANET’ler ve gerekli güvenlik altyapıları için bir literatür taramasıdır. VANET’in geleceğinin neden SDN teknolojilerine bağlı olduğunu açıklamaktadır.

Tablo 2.39: SDR & V2X ile İlgili Araştırmalar

Araştırma	Alan	Açıklama
[273]	5G, merkezi/bulut (C-RAN)	5G OpenAirInterface test yatağı üzerine bir araştırma
[245]	Görünür Işık İletişimi (Visible Light Communication, VLC), FPGA	VLC ile SDR
[90]	Literatür Taraması, MANET, SDN, SDR	MANET, SDN ve SDR hakkında kapsamlı bir literatür taraması

2.4.3.1. V2X Programlanabilir Veri Düzlemleri

VANET'te, bir ağ elemanından diğer ağ elamanına yönlendirme işlemi bulunmaktadır [38]. Bu yönlendirmeyi DSRC, IPv4 veya IPv6 (veya başka herhangi uygun bir protokol) gerçekleştirebilir. Genel olarak, araç ortamı kısıtlı bir sistemdir. Böylece, bir araçta anahtarlama (switching) yeteneklerini beklemek uzak görünebilir. Ancak, [mobil] RSU'lar (mRSU), sabit RSU'ların (fRSU) aksine, farklı bir kullanım alanı sunarlar. mRSU'lar, bu tür anahtarlama yeteneklerini çok iyi içerebilir gibi görünmektedirler. Bu durumda, mRSU'nun kendisi de bir AV olacaktır.

2.4.3.2. Yazılım Tanımlı Radyo

Yazılım tanımlı radyo (SDR), yazılım tanımlı mobil ağlar (SDMN) iletişiminin bir etkinleştiricisidir. 5G ve 6G'de, radyo erişim ağı (RAN), en yeni SDR teknolojilerini tamamıyla yazılım ile [273] çalıştıran bir alt yapı olarak tasarlanmaktadır. "Radyo" terimi kullanıldığında, sadece radyo dalgalarını değil, aynı zamanda iletişim kurulabilen herhangi bir ortam altyapı aracı [245] da düşünülebilir. Bu nedenle, daha iyi bir isimlendirme, Yazılım Tanımlı Sinyalleşme (SDS) olabilir.

[273]'de uygulama, OpenAirInterface (OAI) ile C-RAN için bir test ortamı gerçekleştirmiştir. OAI, açık kaynaklı bir mobil ağ sistemidir. Daha önce donanım tarafından işlemlenen durumlar için kodlama yeteneği sağlar. Böylelikle herkes, 5G sistemlerini gerçek yazılımlarla, güncel standartlarla uygulamaya başlayabilir.

[90]'da MANET için SDN ve SDR'nin birleştirilmiş bir görünümü ve katmanlar arası optimizasyon anlatılmıştır. Bu literatür taraması, V2X için mutlaka bakılması gereken çalışma ve aynı zamanda tezin bu bölümü ile de çok ilgili görünmektedir. Göze çarpan

SDN tabanlı bir MANET özeti ve iyi çıkarımlar içermektedir. Çalışmanın çıktısı, benzer özelliklere sahip herhangi bir V2X senaryosuna da kolayca uygulanabilir.

SDR, V2V senaryolarında, diğer ortamlarla birlikte, V2X için önemli görünmektedir. Örneğin, iki araç C-V2X'te VLC kullanabilir [245]. Bu, başka türlü kapsama alanı bulmak mümkün olmayan bir alanda, mükemmel iletişimin oluşmasını sağlayabilir.

2.4.3.3. V2X-SDN'de Güvenli İletişim için Wireguard Kullanımı

WireGuard, en iyi performans gösteren Sanal Özel Ağ (VPN) çözümlerinden biridir [2]. Linux çekirdeğinde (LK) uygulanır ve çoğu ortamda çoğu VPN teknolojisinden daha hızlıdır. WireGuard'ın şifreleme yapı taşlarını içeren mimarisi diğer VPN protokollerine göre daha kolaydır [2, 274] çünkü güvenlik seçeneklerine yönelik yapıların pek çok tak ve çalıştır parçasını kapsaması gerekmez. Her adımda [274, 275, 276] ChaCha20, SipHash24 veya Curve25519 gibi bir şifreleme ilkelini aynı anda kullanır. Gürültü protokolü çerçevesi (NoiseIK) [277], WireGuard aracılığıyla güvenli mesaj alışverişi için modern bir çerçeve olarak kullanılmıştır. Ayrıca WireGuard, OpenVPN gibi diğer VPN uygulamalarındaki milyonlarca koda karşılık bin satırdan daha az kod içerir. Bu basitlik, çeşitli güvenlik sorunlarının analizinde büyük kolaylık sağlar. Öte yandan WireGuard bir sunucu olduğunda performans dar boğazı yaşayabilmektedir. Aynı WireGuard sunucusuna daha fazla istemcinin bağlanmasıyla daha az verim elde edilebilecektir. Bu da WireGuard'ın VPN sunucuları için uygun olmadığını gösterir. WireGuard ve IPSec ile ilgili VPN protokollerinin ayrıntılı bir analizi [278, 279] adresinde bulunabilir. Öte yandan, diğer araştırmalardan da görülebileceği gibi [280], WireGuard'ı yavaşlatan şey şifreleme değildir. Bu, tüm işlem tarafından harcanan toplam sürenin yalnızca %7'sidir.

Yeni nesil mobil ağlar IP tabanlı olduğundan, güçlü çekirdek ağ güvenliği için WireGuard, basitliği nedeniyle mobil ağlarda birçok kullanıma sahip olacak [281]; V2X senaryolarında, standartlar birçok iletişim ayrıntısına dokunulmadığı için [96, 34, 97, 98], WireGuard'ın orada bir yeri var gibi görünüyor. Ancak yaygın olarak kullanılabilir olması için tek bir sunucuda Tb/s ölçeğinde hizmet vermesi gerekmektedir.

2.4.3.4. Değerlendirme

SDN ve SDR, IDS & MBD'nin nasıl yapılabileceğini tanımlayacak iki farklı teknik olabilir. Buna karşılık, IDS & MBD, bileşenlerini daha iyi tanımlamak için bu yapıları

kullanabilir. Yazılım tanımlı olmak her zaman yavaş işleme anlamına gelmeyecektir. Aksine, programlanabilir donanımlar, hat hızında operasyonların önünü açmaktadır. Daha önceki SDN tasarılarının sorunları (örneğin OpenFlow eleştirileri), SDN'yi uygulamak için yeni yöntemlerin yolunu açmaktadır. Aynı zamanda, P4 ve ilgili ortam araçlarının NGSDN [242] olduğu savunulmaktadır. Bu yeni P4/SDN ortamı şu yapılardan oluşmaktadır;

1. P4Runtime
2. gRPC Ağ İşlemleri Arayüzü (gNOI)
3. gRPC Ağ Yönetim Arayüzü (gNMI)
4. gRPC Yönlendirme Bilgi Tabanı Arayüzü (gRIBI)

P4Runtime, ağ öğesinde bulunur ve P4 dili denetleyicisiyle iletişime aracılık etmektedir. Diğer öğeler, denetleyicinin ve P4Runtime'ın iletişim kurduğu gRPC protokolleridir.

V2X ağlarında Wireguard'ın kolay kullanımı nedeni ile bir geleceği bulunmaktadır. Ancak daha iyi performans için çekirdek (kernel) ve yapılarından kaçınmak en iyisi gibi görünmektedir. İleride görülebilecek terabayt ölçeğinde WireGuard ile ilgili olarak, şifreleme performansı daha önemli bir rol oynayacaktır. Böylece gelecekteki araştırmaların WireGuard'ı daha iyi optimize etmesine tanık olunacaktır.

2.4.4. CA ve CP

CA, CAM/DENM/BSM mesajlarıyla ilişkilidir. AV, sık sık veya eyleme ihtiyaç duyduğunda, bu mesajlarla kendi durumunu veya etrafındaki bazı durumları diğer AV'lere veya RSU'lara göndermektedir. Tüm VANET düğümlerinde V2X etkin olmayabilir veya bir VANET iletişim katmanı da olmayabilir. Buna, VANET'in etrafındaki yayalar, bisikletler veya diğer nesneler de katılabilir. Pek çok düğüm bu tür özelliklerle donatılabilse de, bunları VANET özelinde (LDM veya GDM'de) temsil etmenin bazı yolları olmalıdır. Buna ek olarak, AV'lerin topladığı sensör verileri, CA mesajlarına dahil edilmemektedir [186]. CP'nin aynı ortam üzerinden gönderilen CPM mesajlarıyla bu sorunu çözeceği düşünülmektedir. [42]'de CPM'in MBD için cazip bir veri kaynağı olarak adlandırılması, bu tezin de doğru yolda olduğunu göstermektedir.

CP etkinleştirildiğinde, AV'lerin "görüş hattı dışı" (non-line-of-sight) sorunları çözülmelidir. Ne yazık ki, CP şu anda ve çoğunlukla henüz geliştirilme aşamasındadır ve tek tamamlanmış standart, halka açık olmayan Çin [20] standardıdır.

CP, aşağıdaki standartlarla, ilgili ülkelerde tanımlanmıştır;

- Avrupa'da [32, 57] (çok yeni veya yayın öncesi durumdadır)
- ABD'de [24] (yayınlandı, ancak ücretlidir)
- [20] Çin'de (yayınlandı, ancak herkese açık kaynak değildir)

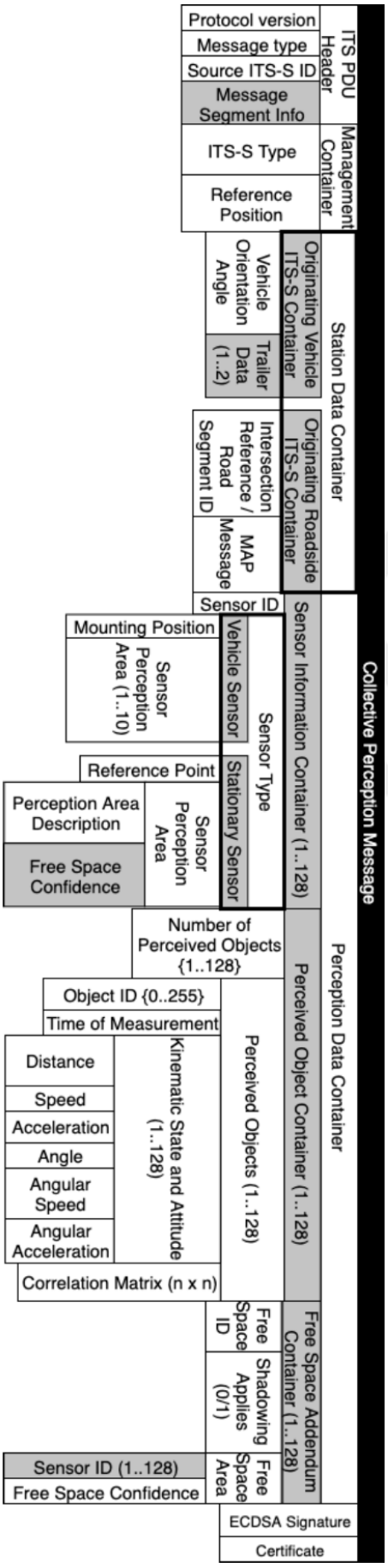
CP mimarisinin en önemli bileşenlerinden olan "sensör veri füzyonu" üzerinde de çalışılmaktadır. Kapsamlı bir literatür vermek gerekirse [163, 65, 50, 45, 282, 48, 51] çalışmaları ve [57] standardı incelenebilir. Bunun için bahsetmeye değer başka bir bileşen iletişim kanallarını daya uygun tutmak için tıkanıklık kontrolüdür ve daha az veri göndermekle ilgilidir [186].

CP nispeten yeni bir konudur. Bu nedenle, bu konudaki eski makaleler standartlara referans veremiyorlar. Bu nedenle, bu bölümde anlatılan makaleler daha çok 2020'den sonrası yazılmış olanlarıdır.

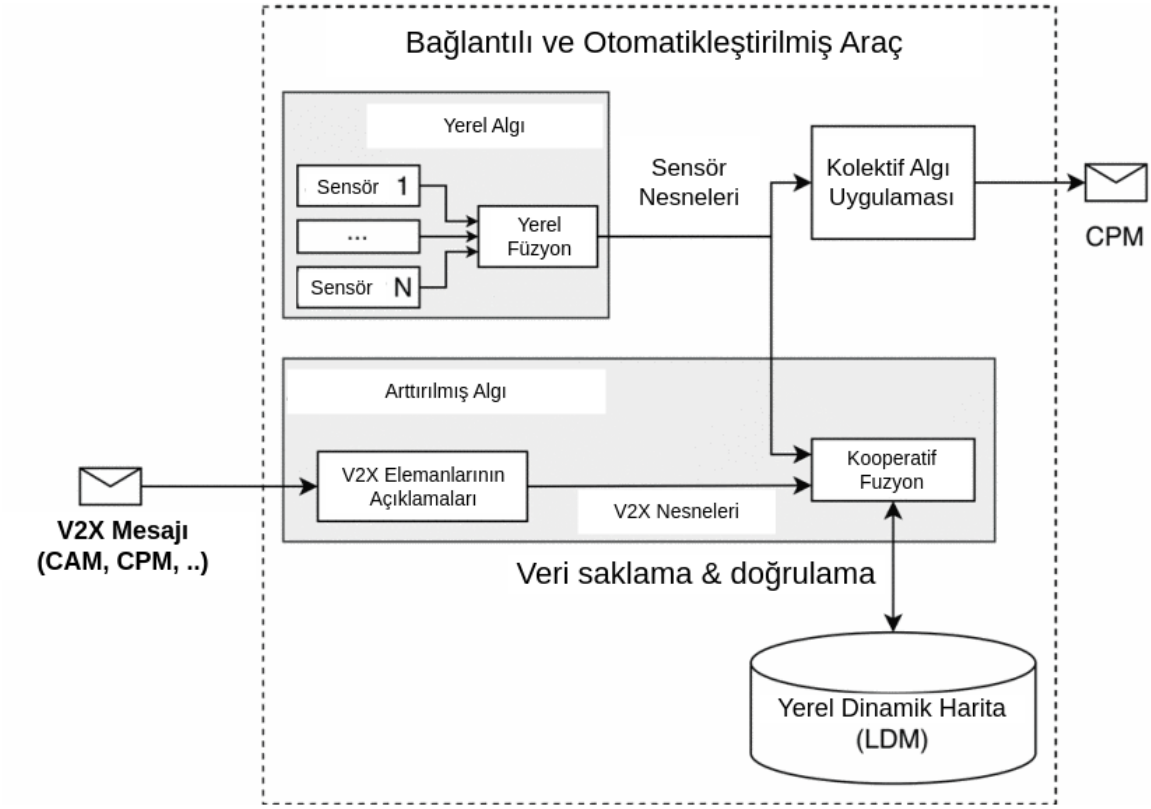
[120], Kalman Filtre durumlarına dayalı yeni model bir MBD yapısı kullanan CA+CP çalışmasıdır. Bazen, uzak olan veya takma ad kimliklerini değiştiren zararsız araçlardan gelen bazı CAM mesajlarını kabul etmeme durumu olabilmekte ve bu sonuçlar da felakete yol açabilmektedir. Çalışmada, son teknoloji bir simülasyon yapmanın iyi bir yöntemi de sunulmaktadır. Önerilen sistemin sağlam ve kullanışlı olması için de, ilk bir 500 saniyeye ihtiyaç olduğu belirtilmektedir.

[269]'deki çalışma, teknolojinin mevcut durumu hakkında hızlı bir giriş sağlamaktadır. V2X ve ardından NGV gelişmeleri hakkında bilgi vermekte, ayrıca "2. Gün", "2. Aşama" ve sonrası için de gelişmeleri anlatmaktadır. Sonuçta V2X'teki son teknolojiye basit ve bir kısa giriş olarak görünmektedir.

[42]'de standartlar ve çözmeye çalıştıkları ihtiyaç göz önüne alındığında, CP ve MBD'ye çok değerli bir giriş bulunabilir. Araştırma [57] üzerinde çalışmaktadır ve CPM mesajları



Şekil 2.17: ETSI CPM Formatı [42]



Şekil 2.18: CP Sistemi [42]

güvenliği hakkında bir TA oluşturmaktadır. Çalışmanın önemli bir sonucu, saldırıları azaltmanın bir yönteminin CPM mesajlarında çoklama gerektirmesi olduğunu belirtir. Diğer iyi davranışlı araçların, CPM verilerini göndermesi ile halihazırda alınan veriler ile çapraz referans yapmaktadır. Ancak, CP için sahip olduğumuz veya devam eden standartlar, buradaki çoklamayı azaltmaya çalışmaktadırlar. Bu nedenle, bu çalışmadaki saldırıları karşılama yöntemlerini, tam olarak uygulamak için, standartlar yeterince izin vermelidirler. Standartlar, kendi TA yöntemlerini önerse de ([169] genel kullanım, [34] ITS durumu için), çalışmanın TA yöntemi [131]'dan alınmıştır.

[163]'deki araştırma, 3D algılama teknolojisini kullanıp AV'lere CP özellikleri sağlayan, ayrıca USDOT tarafından finanse edilen bir projedir. İyi bir IDS/MBD, çevre hakkında doğru bilgiye ihtiyaç duymaktadır. 3D algılama, çevredeki nesneler, kilit noktalar (keypoint) ve derinlik hakkında daha iyi sonuçlar sağlar. Çalışmanın çıktısı, (derinlik bilgisi) tek bir görüntüden, önemli noktalar (bir nesnenin hareket veya önemli ortak noktalarından) doğru bir 3D araç yerelleştirme algoritmasıdır. Bu çalışma, aynı zamanda CP ile ilgili teknolojiler (ranging, radar vb.) anlatır ve literatür taraması çok kapsamlı ve tatmin edicidir.

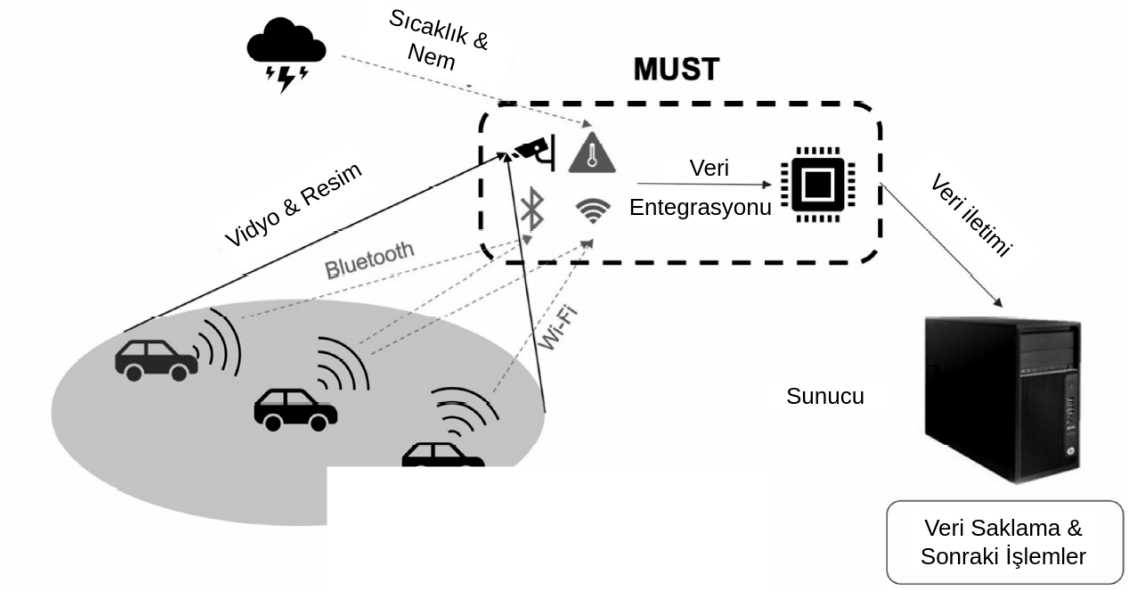
Tablo 2.40: CA & CP Araştırmaları

Araştırma	Alan	Açıklama
[120]	CP, MBD, Gösterim	Yerel Dinamik harita (LDM) ile hareket tahmini algoritması (Kalman Filtresi durumları)
[269]	CP	VANET aşama 1(CAM/BSM/DENM) ve aşama 2 (CP/CPM) gereksinimleri üzerine bir literatür taraması
[42]	CP, MBD	A tehdit analizi/değerlendirmesi (TA) CPM mesajlarında
[163]	CP, Prototip Geliştirme	CP yetenekleri 2D algılama yerine 3D algılama teknolojisini kullanır
[283, 132]	CP, Prototip Geliştirme	Amaçlar ve çıktılar açısından [163]'e çok benzer
[65]	CP, Güvenlik	Güvenlik hususları için CP üzerine bir değerlendirme çalışması
[157]	CP, V2X, Test	(Açık kaynak değil) test çerçevesini basit CP mesajlarıyla açıklayan bir çalışma
[185]	CP	(IMAGinE proje çıktısı) CP, MCM ile yakıt tüketimi
[186, 284]	CP, Merkezi Olmayan Tıkanıklık Kontrolü (DCC)	ETSI'nin DCC'sinin ve konfigürasyonunun değerlendirilmesi, ayrıca DCC için yeni bir algoritma
[155]	CP	Dağıtılmış bir CP sistemi geliştirmenin standart olmayan bir yolu
[285]	CP, Değerlendirme	CP performansı ve AV'lerin geleceği hakkında performans ölçümleri veren nispeten eski bir makale
[286]	CP	AutoC2X

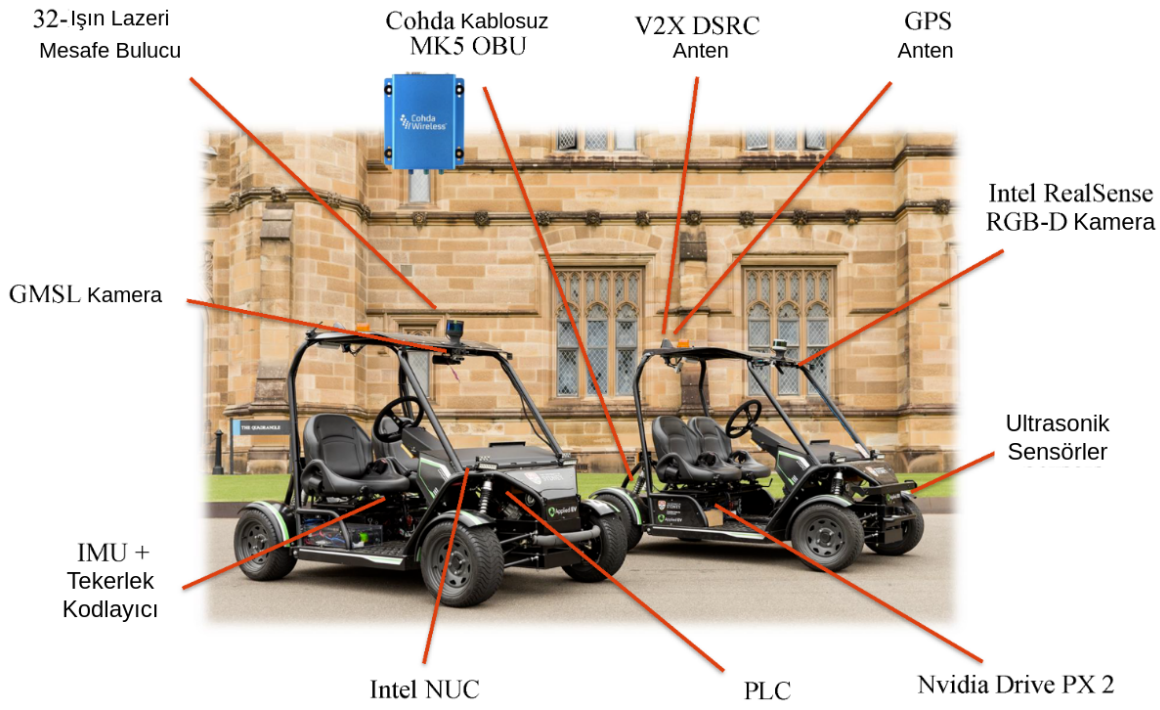
Geliştirdikleri MUST sensörü RSU'da bulunur. OBU'da (Raspberry Pi veya NVIDIA Jetson) bir monoküler kamera mevcuttur. Çalışma aynı zamanda çok çeşitli kendi kendine sürüş ve nesne algılama veri kümelerini de araştırmıştır. Bu veri kümeleri, daha başka amaçlar için de kullanılabilir. Bir not olarak da, bu çalışmada diğer araştırma çalışmaları ile karşılaştırma yapılmamaktadır.

[283, 132] çalışması bir Avustralya projesi (iMove) hakkındadır. İlk olarak, CP için, 2000'li yıllardan başlayarak, iyi bir literatür taramasını sunmaktadır. Burada, CPM'nin önceki çalışmalardan nasıl ortaya çıktığı görülmektedir. Ortaya çıkan sonuç, doğal bir ortamdan ve birden çok simülatörden geçer.

[65]'deki çalışma da (yazarın daha önce yayımladığı birkaç eski araştırmada olduğu



Şekil 2.19: [163] İçin Veri İşleme Ardışık Düzeni



Şekil 2.20: [60]'da Kullanılan CAV Platformu

Şekil 2.21: [163] İçindeki RSU'lara Bağlı Sensörler

gibi) CP'ye bir güvenlik yaklaşımını benimsemektedir. Belirtildiği gibi, çalışmada CP hakkında farklı açılardan pek çok değerlendirme yapılmıştır. Ancak, CP kullanan bir aracın çarpışma oranları bugüne kadar elimizde bulunmamaktadır. Gösterilen bir başka sonuç ise, birçok iletişim teknolojilerinin gelecek için yarıştığıdır; DSRC'den IEEE 802.11bd'ye (IEEE 802.11p'den türetilmiştir) ve 3GPP'nin C-V2X'inden 5G-NR C-V2X'e kadar. Tüm bunları bilerek, hangi iletişim teknolojisinin dünyayı şekillendireceği ve gelecekte nasıl bir manzara olacağı hala tartışılmaktadır. Kullanılan simülasyon çerçevesi (TEPLITS) ve test altyapısı açık kaynak değildir ve bu tez bunun çalışma için bir eksi olduğunu düşünmektedir (muhtemelen AB projesi IMAGinE'nin resmi final gösteriminde duyurulacak gibi görünmektedir[18]). Çalışmada, CP ile ilgili işlemler için, aşağıdaki metrikler kabul edilmiştir:

1. Çevresel Farkındalık Oranı (Environmental Awareness Ratio)
2. Algılanan Nesne Fazlalığı (Detected Object Redundancy)
3. Güncelleme Peryodu (Update Period)
4. Bilginin Yaşı (Age of Information)
5. Nesne İzleme Doğruluğu (Hassas Algılama Durumu, Object Tracking Accuracy/Detecting Precise State)

[18] https://www.imagine-online.de/en/news-events/final-event-agenda

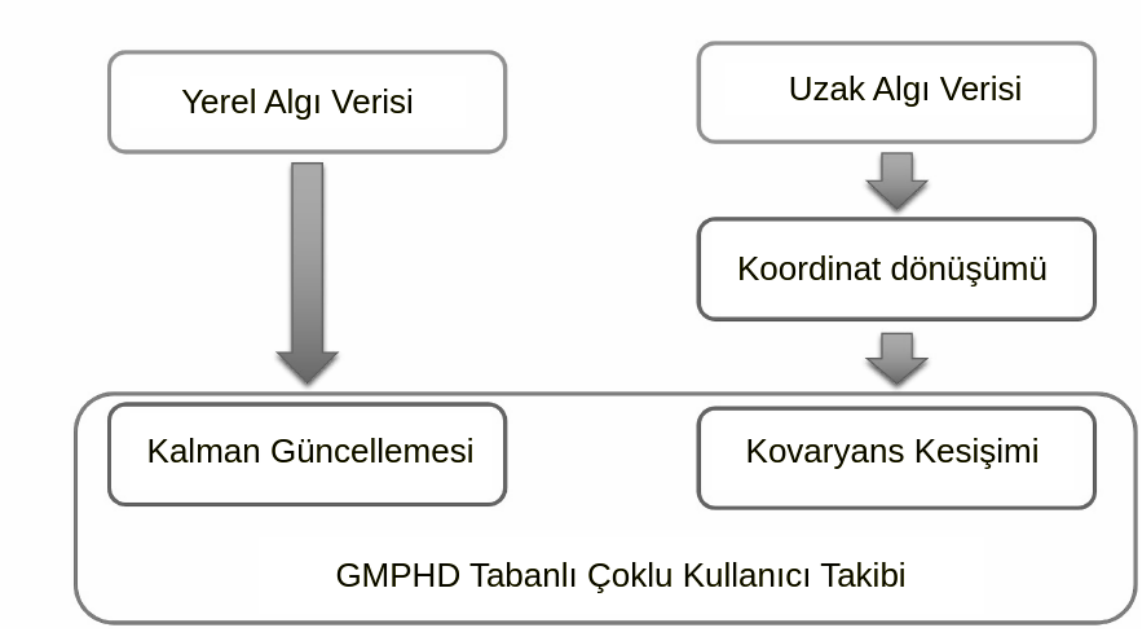
[185], CP ’yi yakıt tüketimine uygulamıştır. Olumlu bir sonuçla, CPM ile iyi bir manevra planlayıcısı meydana getirmişlerdir. Başka bir makalenin alıntısı olarak; AV’lerin V2X ile veya V2X’siz aynı anda çalışabilmelerini gerektirdiğini belirtmişlerdir. Bunun için de tek yolun CP olduğunu belirtmektedirler. Makalenin önerdiği bir başka ilgi çekici terim ise, sürme düzleminin yörüngeler olarak düşünüldüğü “işbirlikçi tahmin"dir (“cooperative prediction”). LEM ve GEM arasında kıyaslama da yapılmıştır. Yine bu çalışmada da başka herhangi bir çalışma ile karşılaştırma yapılmamıştır.

[186], ETSI’de bulunan standartlarda, Merkezi Olmayan Tıkanıklık Kontrolü (DCC) ve yapılandırmasında ince ayar yapmanın önemini vurgulamaktadır. CPM’nin, %40 nüfuz oranında bile ve iyi bir konfigürasyonla, çok yüksek bir algılama oranı elde edilebildiğini belirtmektedir. Bu durum, [285] tarafından da onaylanmaktadır.

[155] çalışması (gelişmekte olan) CP standartlarına uymamakla birlikte bunu, tezin yazıldığı sırada, standartların yokluğu olduğunu belirtmektedir. Ancak sıfırdan ve standartsız başlangıç aşamasında nasıl bir tasarım olabileceğine dair iyi bir örnek olduğu görünmektedir. Çalışma QuadKeys ile Olasılıklı Varlık-İlişki Modelleri (Probabilistic Entity-Relationship Models, PER) kullanmaktadır. Sahne temsili içinse Doluluk Izgaraları (Occupancy Grids) kullanılmaktadır. Önerilen modelde, DSRC kaynaklarının daha iyi kullanımı için, C-V2X üzerinde çalışıldığı belirtilmiştir. ‘Metcalfe"’nin kanunu ile C-V2X’in daha iyi olduğunu belirtmektedir. C-V2X ile olası bağlantı sayısı hesaplanmak gerekirse, bunun “n^2" olduğu, DSRC ile hesaplamak gerekirse de, bunun “n” bağlantı olduğunu belirtmektedir. PER modeline duyulan güven de, [32]’deki gelişen standarda eklenmektedir.

2.4.4.1. Nesne Temsili veya Modeli

Nesnelerin dahili veya harici temsili veya modelleri, genel MBD performansını etkileyeceği görülmektedir. Model veya temsil dış dünyanın sistem içerisinde nasıl bir yöntem ile yönetildiğidir. Nesne temsili veya model terimi ”temsil” veya "gösterim" olarak da kısaltılabilir. CP’de (veya bu konuda CA’da) temsil genellikle ikiye ayrılmaktadır; LEM ve GEM. LEM’de, rapor gönderen araç, yakındaki nesneleri takip eder ve tahmin edilebileceği gibi (veya ihtiyaç duyma anında), GEM ile birleştirilmek veya eşleştirilmek (synchronization) üzere CPM mesajları gönderir [65]. Bu birleştirme “artırılmış algı" (“augmented perception”) veya “kaynaştırma" (“fusing”) olarak da adlandırılır. ETSI, bu gösterimi LDM/GDM içinde tutar [56]. Çoğu çalışma, iç veya dış gösterim amaçları için



Şekil 2.22: [60, 252] İçindeki Gösterim/Temsil Modeli

standartları takip etmektedirler. Başkaları da (aşağıdaki **Tablo 2.41:**'de belirtildiği gibi) özel yapılar [121] ile gösterimi ele alabilmektedir. Özel bir gösterim uygulaması şu iki anlama gelebilir:

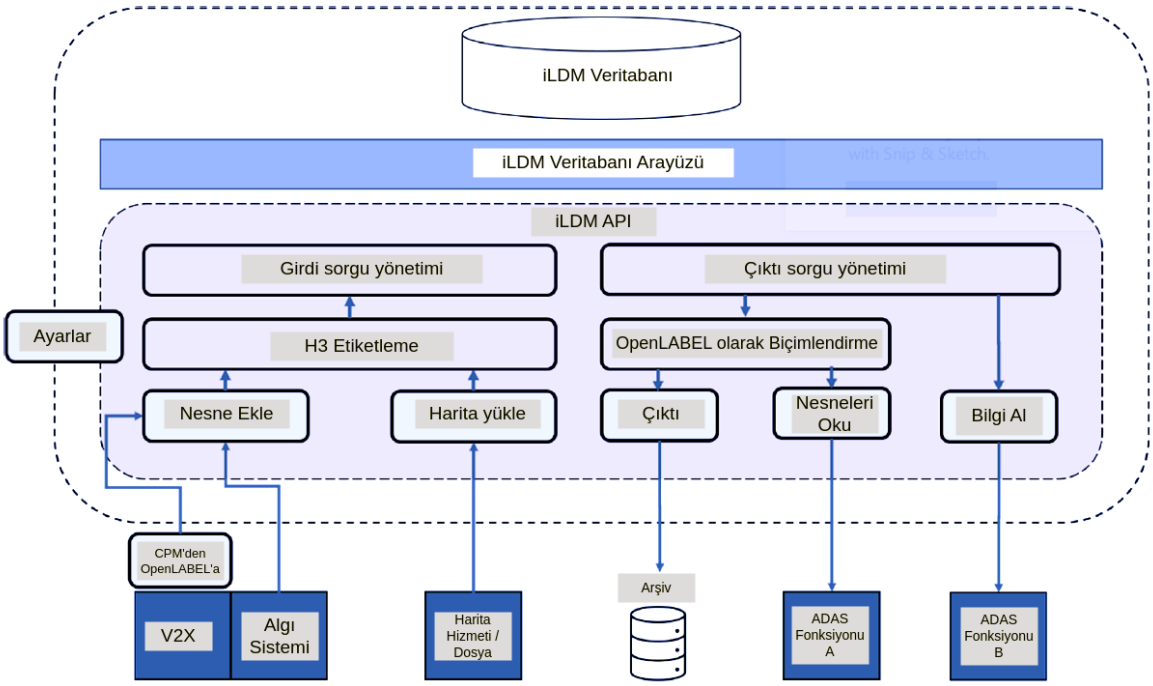
- Çalışma eski bir araştırma olabilir, yazarların henüz standartları duymamış olma olasılığı da bulunmaktadır.
- Veya çalışma farklı bir yapıya ihtiyaç duymaktadır.

Her durumda, CP henüz tam olarak standardize edilmediğinden, bu çalışmalar gelecekteki araştırmalar veya standartlar için hala önemli olabilmektedir. Diğer taraftan, LDM farklı kullanım durumları için farklı geliştirme seçeneklerine de sahiptir. Örneğin, neo4j'yi DB [52] olarak kullanmak veya bir 3D LDM [54] yapmak gibi seçenekler de vardır.

[52] çalışması, çizelge tabanlı, gerçek zamanlı duyarlı bir temsil modeli uygulamaktadır. Bu modeli depolamak için de, bir çizelge veri tabanı olan neo4j kullanmaktadır. Bunun üzerine, nesnelerin etiketlenmesi için OpenLabel standardı kullanılmıştır. ASAM, bu standardı çok sensörlü verilere ve senaryolara açıklama eklemek için oluşturmuştur. Çalışma, diğer LDM yöntemlerinin (literatüre göre küçük bir sayı) karşılaştırmalı bir analizini de eklemiş ve yöntemin birçok durumda üstün olduğunu belirtmiştir. Bu çalışma aynı

Tablo 2.41: CP Temsili Model Araştırmaları

Araştırma	Alan	Açıklama	Veri Kümesi
[52]	Çizelge LDM, Çizelge DB, İndeksleme, Araç Ontolojisi	DB olarak Neo4j, Veri yapısı olarak OpenLABEL, İndeksleme için H3, test için RTMaps	KITTI
[51]	Füzyon, FL, Nesne Algılama, DBSCAN	FL, SECOND (CNN), DBSCAN'ı nesneleri etiketlemek ve LDM 'le birleştirmek için kullanır	KITTI
[121]	LDM, Maliyet Haritası, Doluluk Izgaraları	Birleştirilmiş Maliyet Haritası	N/A
[120]	Kalman Filtreleri	Hareket Tahmin Algoritmalı LDM (Kalman Filtre durumları)	VeReMi
[54]	3D LDM, UAV, Doluluk Haritası, Parçacık Filtresi, Dairesel Tampon	Konum bilgisi, doluluk haritasından (ızgara) ve parçacık filtresi ile hesaplanır	N/A
[53]	Doğrusal Zamansal Mantık (LTL)	İlişkisel DB (RDB) veya Kaynak Açıklama Çerçevesi (RDF) ve Web Ontoloji Dili (OWL) yerine LDM'nin LTL yolu.	Yok
[49]	LEM, 3D Nokta Bulutu, Dempster-Shafer Kanıt Akıl Yürütme, Maliyet Haritası	LIDAR tabanlı CP üretimi, şeritler için kamera (çok kanallı eşik bariyeri sınır füzyonu, uyarlanabilir kayan pencere algoritması)	N/A
[155]	PER, LEM, GEOID	Temsil modeli için olasılıksal varlık-ilişki modellerini kullanır.	Çalışmanın topladığı
[283, 132]	Gauss karışımı (Gaussian mixture) olasılık hipotez yoğunluğu (probability hypothesis density, PHD) Filtresi	GMPHD	MARS (yalnızca CNN'de)
[287]	PetriNet'ler	PetriNet'te tüm ağ durumu	N/A
[104]	Kendi Kendini Düzenleyen Harita (SOM)	Durum (state), gelişmiş, büyüyen bir hiyerarşik SOM (I- GHSOM) içinde tutulur	N/A



Şekil 2.23: [52]'deki LDM Yapısı

zamanda çizelge tabanlı veriler de önermektedir ve standart uyumluluğuna sahip olmayan LDM uygulamalarının çoğunlukla topluluk tarafından reddedildiğini belirtmektedir. Yazarlar ayrıca küresel otomotiv ontolojisi (global automotive ontology) için başka bir araştırmayı temel almışlar. Bu araştırma ayrıca LDM ile ilgili geçmiş için iyi bir başlangıçtır. CAM/DENM/BSM/CPM'den OpenLabel formatına dönüşüm için adımlar da belirtilmiştir. Ayrıca, Uber'in altıgen hiyerarşik jeo-uzaysal hızlı sorgulama için indeksleme sistemini de (hexagonal hierarchical geospatial indexing system, H3) kullanmaktadırlar. Bu indeksleme sistemi, metrekare çözünürlüğe kadar indeksleme desteği, ayrıca bu alana yerleşen nesnenin kimliğini de barındırmaktadır. Son olarak, KITI veri kümesi de test için kullanılmıştır. Nihayetinde, bu çalışma, LDM araştırmaları için ileriye doğru giden yolu işaret etmektedir.

[51], nesne algılama ve veri birleştirme sorunlarına, aşağıda belirtildiği gibi işaret etmektedir;

- Algılama
- Model (LDM)
- Çevrim içi öğrenme için eksik etiketlerdeki belirsizlikler (çünkü nesne algılama çoğunlukla yapay zekâdadır)

Bunlara karşı koymak için de, çalışma üç aşamada bir çözüm önermektedir;

1. Üç aşamalı harita (LDM içerisindeki map/harita tabiri) birleştirme (fusion)
2. Nokta bulutu tabanlı FL
3. Yeni bir bilgi damıtma (distillation) ve etiketleme yöntemi

Araştırmanın sonucu, açık kaynak olarak, Github'da yayınlanmıştır. Bu çerçevede, bulut sunucuları bir AI modeli oluştururken, uç sunucular FL, etiketleme ve füzyon işlemlerini yapmaktadırlar. Çalışmada, benzer araştırmalar için bir karşılaştırma da bulunmaktadır. En son, araştırma, oldukça özet ve başından sonuna kadar okuması keyifli bir çalışmadır.

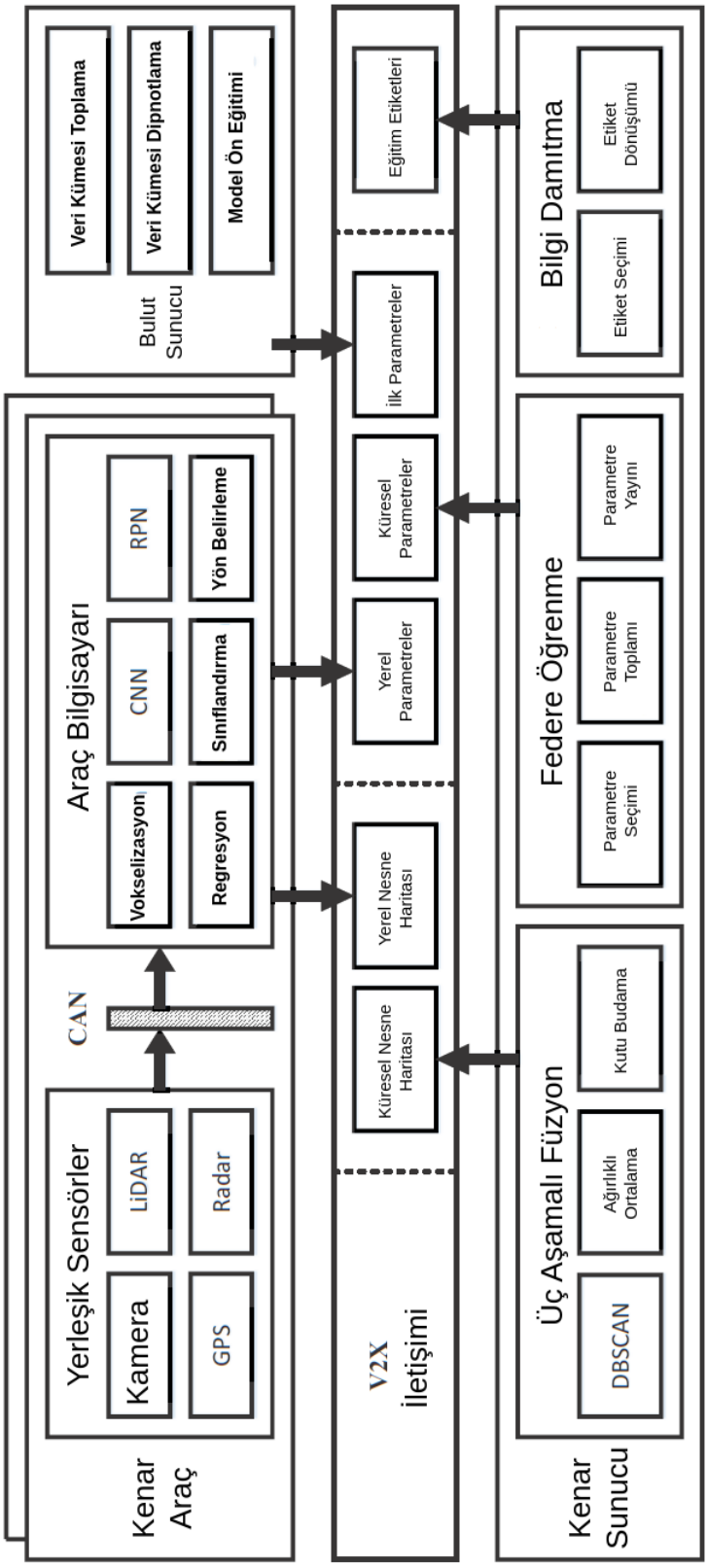
[54], kümelemeyi doluluk ızgarası (occupancy grid) ile sunmaktadır. İlk algılamanın ardından, otomatik hesaplanan konum bilgisine sahip (ızgara voksel kümeleme/grid voxel clustering, ayrıca parçacık filtresi hız tahmini/particle filter velocity estimation) bir 3D LDM yönetmektedir. Kaynak kullanımını daha uygun hale getirme adına da, çemberimsi tampon (circular buffer) tabanlı kaynak doluluk ızgarası kullanımı da belirtilmiştir.

[288, 289, 290] çalışmaları ise CP ile doğrudan ilgili olmamakla birlikte, modeller, makine öğrenimi tabanlı CP çalışmalarında kullanılabilmektedir. Örneğin [288] araştırması, veri tabanı ile çalışan ilişkisel modeller için teoremi tanımlamıştır. Ayrıca [289, 291, 290] çalışmaları da CP'de çizelge tabanlı makine öğrenimi için önerilebilir. [287] ise CP ile PetriNet'lerin nasıl kullanılacağı hakkında güzel bir araştırma gibi görünmektedir.

[155]'de, çalışma, CP ile ilgili yeniliklerle doludur. Ancak o zaman henüz standartlar yayınlanmadığı düşünülürse, çalışmada standartların neden takip edilemediği anlaşılabilir. Her durumda, örnek bir dağıtılmış platform yaklaşımı olarak görünmektedir. Bu araştırmada CP, C-V2X İletişimine dayalı tasarlanmıştır. PER modellerini, QuadKeys kullanarak jeo-döşemeyi (geo-tiling) ve doluluk ızgaralarını kullanmakta ve durum temsili için de zamansal bozulma (temporal distortion) ile yüksek seviyeli füzyon kullanır. Uygulama, CARLA simülatörü kullanılarak gerçekleştirilmiştir.

Aşağıdaki araştırmalar da dikkat çekmektedir;

1. [121]: Maliyet haritalarını (cost map) kullanmakta ve bir MBD uygulaması içermektedir.



Şekil 2.24: [51]'deki Çerçeve

2. [53]: Yüksek çözünürlüklü yol haritası için Lanenet2 [292]'yi kullanır. Lanelet'in kendisi bir CP bileşeni olarak da düşünülebilir.

3. [283, 132]: (Kalman filtresinden ilham alan) GMPHD filtresi kullanmaktadır. Bu çalışma açıklama adına daha fazlasını hak emektedir. Ancak bunlar IDS bölümünde daha detaylı incelenecektir. Ayrıca çalışma, doğrudan CP ile de ilgili değildir, ancak model olarak gelecek araştırmalara faydalı olabileceği düşünülmüştür. .

2.4.4.2. Değerlendirme

AV'nin tam özerkliği uygulayabilmesi için, çevresini görmesi gerekmektedir. AV, ortamı ve içeriğini algıladıktan sonra, daha iyi kararlar verebilecektir. 5G ve ötesinin gelişiyle de performans, neredeyse gerçek zamanlı iletişim yeteneğine sahip olabilecektir. Bu aşamada, CA ile CP, eksiksiz bir ortam görünümü için gerekli olan tüm verileri toplayabilecektir. MBD'ler ve IDS'ler ayrıca, aracı veya VANET sistemini daha iyi korumak için bu bilgileri kullanabileceklerdir.

2.4.5. IDS VE MBD

Bu tezde, V2X bağlamında, IDS'nin ve MBD'nin benzer oldukları düşünülmektedir. Diğer taraftan, IDS, MBD'nin bir alt sistemi olabilmektedir. Bu bölümde, ilgili araştırmaları daha iyi anlama adına, bir MBD/IDS ayrımını yapılması gerektiği düşünülmüştür.

2.4.5.1. IDS

IDS literatürü oldukça fazladır. Araştırma geçmişi, ve aynı zamanda VANET üzerindeki kullanımı, yoğun bir şekilde çalışılmıştır. IDS veya MBD'nin, önemli ölçüde CP'den [33] yararlanacağı düşünüldüğünden, yapılabilecek olan, bu araştırmalara bir CA & CP ve MBD perspektifi verebilmek, ayrıca biraz da son teknolojideki durumlarını anlayabilmektir. 2019'a kadar uzanan literatür için [293] çalışması incelenebilir. Aşağıda, MBD içermeyen bazı ilginç araştırmalar, **Tablo 2.42:** içinde listelenecektir.

[294], Dağıtılmış Makine Öğrenimi (DML) kullanan bir CIDS çalışmasıdır. Diferansiyelli Çarpanların Yön Değiştirme Yöntemi (Alternating Direction Method of Multipliers, ADMM) ve diferansiyel gizlilik (Differential Privacy, DP) üzerine çalışılmıştır. Kullanılan makine öğrenimi yöntemleri aşağıdaki gibi belirtilmiştir;

Tablo 2.42: MBD'siz V2X için IDS ile İlgili Araştırmalar

Araştırma	**Alan**	**Açıklama**	**Veri Kümesi**
[294]	CIDS, AI	Dağıtılmış Makine Öğrenimi (DML) kullanan bir CIDS (SP-CIDS) üzerine bir çalışma	NSL-KDD
[295]	SDN, Enerji Verimliliği, CIDS	p-CIDS adlı SDN tabanlı bir VANET çalışması	NSL-KDD
[104]	IDS, ML, DL	Gelişmiş, büyüyen ve kendi kendini organize eden haritalar (I-GSOM)	Kendi kendine toplanan
[287]	IDS	PetriNet tabanlı çok basit ve etkili IDS	N/A
[116]	Oyun Teorisi, IDS, Araç İçi	IDS ve saldırganlar Nash dengesini arıyor	Car Hacking Veri Kümesi
[105]	AI, ML, IDS	Rastgele Ormanlar ve Coreset'ler ile bir IDS çalışması	CICIDS2017

- Lojistik Regresyon
- Naïve Bayes
- Topluluk (ensemble) Sınıflandırıcıları

Çalışma yalnızca, daha önceden tanımlanmış yöntemlerini bu araştırma ile karşılaştırmıştır. Ayrıca, F1 gibi diğer metrikler de metin biçiminde verilmediğinden, resimlerden tahmin edilmesi gerekmektedir (aynısı [295] için de geçerlidir).

[295]'de yazarlar Eliptik Eğri Şifreleme (ECC) işlemlerini V2X için tanıtmışlardır. Ancak, tanımlar gerekli işlemler standartlarda zaten bulunmaktadır [11] ("5.3.1 İmza algoritmalar"ında). Çalışmada ayrıca "enerji verimliliği"nin sadece kimlik doğrulama işlemlerinde olduğu görülmüştür. Araştırma, enerji verimliliğine dayalı olarak Homomorfik Şifreleme, grup kimlik doğrulaması ve DP üzerine de dikkat çekmektedir. İleri düzey gizlilik ile sonuçlanan bu son iki teknoloji, üçüncü şahıslarla hiçbir özel bilgiyi paylaşmaması ile bilinmektedir. Bununla birlikte, standartlarda [11] grup tabanlı kimlik doğrulama gibi benzer yapılar görülebilmektedir. DP ile de ilgili olarak, IEEE 1609.2'de tanımlanan hizmetlerle, herhangi bir dinleyici, ağdaki bir öğenin kimliğini belirleyemez. Her ne kadar, şu anda

kısıtlı araç ekipmanlarındaki performans nedeniyle ile çok geçerli olmayabilecekse de, homomorfik şifreleme her zaman ilginç bir fikirdir. Araştırmada karşılaştırmalı analiz de bulunmaktadır. Makine öğrenimi tarafında doğruluk, kesinlik, hatırlama ve F1 puanı verilmekte, ancak kesin oranların resimlerden çıkarılmak zorunluluğu bulunmaktadır.

[104] bir performans hafifletme (performance mitigation) yöntemi kullanmaktadır. Bu yöntem, trafik akışına ve araç konumuna dayalı çıkarma yöntemini de önermektedir. Ayrıca, I-GSOM modifikasyonları olan bir sınıflandırıcı da uygulanmıştır. Çalışma, mesaj boyutunu ve ölçeğini küçülttüğünü, böylece performans arttırımı yaptığını belirtmektedir. Bunun, mesajı küçülttüğünden, bir yayın fırtınası (broadcast storm) gibi tıkanıklık senaryolarını hafiflettiği anlatılmıştır. Ancak, tıkanıklık sorunları, ağdaki düğümlerin sayısı ile ilgilidir. Performans ve mesaj büyüklüğü küçülse de, yüzde yüz bir sonuç almak mümkün olmayabilir görünmektedir. Herhangi bir açık veri kümesi kullanılmadığından diğer eserlerle karşılaştırma bölümü bulunmamaktadır. Diğer bir konu ise, IDS'nin yerleştirildiği ağ bölgesidir. Açıkça belirtilmese de, algoritmalar kısıtlı AV'lerde çalışacak görünmektedir. Ancak DL işlemlerinin kısıtlı AV ortamında nasıl çalışacağı belirtilmemiştir.

[287] PetriNet tabanlı bir durum/temsil (representation) çalışmasıdır. Çok basit ve VANET için uygulaması kolay bir IDS önerilmektedir. Çalışmada, araçlar arasındaki güven sorununun nasıl çözüleceği belirtilmemiştir. Bu durumda, blok zinciri çok iyi bir aday gibi görünmektedir. Çalışma, araç tanımlamaları için bir kümeleme algoritması uygulamıştır. Ancak araç tanımlaması zordur ve uygulamanın bunu nasıl yaptığını açıklığa kavuşturması gerekmektedir. Buradaki itibar (reputation) ölçütleri, doğrudan siber güvenlikle ilgili olmayan bazı performans ölçütleridir.

[113]'in yazarının daha sonra yayınlanmış bir çalışması olan [296], bu tezin de üzerinde durduğu yapay zekâ ile hibrit bir IDS sisteminin nasıl uygulanacağına dair bir referans çalışmasıdır. Makale, iyi bilinen bir veri kümesini rastgele bir orman (random forest) ile kullanmaktadır. Daha sonraki bir aşamada, ML operasyonlarında boyut küçültme için "coreset"'ler kullanılmaktadır. Boyut küçültme nedeniyle de, çalışma meydana gelen performans kazanımlarını irdelemektedir.

[31, 93, 262, 263, 264, 265, 266] çalışmaları, doğrudan VANET ile ilgili olmamakla beraber, bir VANET arka planının (backend) nasıl yapılacağına dair aşağıdaki fikirleri vermektedir;

Tablo 2.43: V2X için MBD ile İlgili Araştırmalar

Araştırma	Açıklama	Veri Kümesi
[124]	MBD ile pekiştirmeli öğrenme	VeReMi
[125]	RSSI tabanlı AI yöntemi	VeReMi [19]
[126]	BC, FL	N/A [erişilemedi]
[117, 118]	VeReMi veri kümesi araştırması	Araştırma ile Oluşturulan
[127]	CNN, LSTM, SVM	VeReMi
[128]	Pearson Korelasyon Analizi	[228, 229], UMTRI
[129]	İşbirlikçi ve dağıtık topluluk (ensemble) öğrenimi	NSL-KDD
[42]	CPM güvenlik değerlendirmeleri ve önermeleri	N/A
[122]	MBD Çerçevesi (F^2MD)	Simülasyon Çerçeveleri

- VANET içerisinde SDN teknolojilerini kullanabilmek
- Ağ içi işlemleme (in-network processing) adına bazı işlemleri SDN ağına yükleme (offloading) teknolojisi (P4 ile programlanabilir ağ cihazları vb. ile)

Bu sayede IDS işlemlerinin bir kısmı verilerin olduğu yere boşaltılabileceğini (offload) belirtir. AI operasyonlarının bile programlanabilir donanım sistemlerinde uygulanabileceğini anlatır. Bu şekil çalışma biçimi, bu tezin düşündüğü şekli ile, VANET ağları ile ilgili yeni bir sınırda olacaktır.

2.4.5.2. MBD

Siber güvenlik standartları, öncelikle dijital sertifika tabanlı bir VANET güvenlik sistemi tanımlamaktadır. Özel bir sertifika türü kullanılır ve bu sertifikalar yetkilendirmenin amacını kendi içerisinde barındırır. Bu sistem, MBR'leri toplamakta ve bunları bir MBD hizmetine göndermektedir. Bu da, davetsiz misafirleri ve kötü davranış sergileyen (misbehavior) düğümleri sistemden uzak tutmaya çalışmaktadır. MBD araştırma literatürü büyümektedir. **Tablo 2.43:** içerisinde, ilgi çekici çalışmaların bir listesi bulunabilir. 5G ve makine öğrenimi çalışmaları üzerinde daha fazla bilgi için ise, [123] çalışması incelenebilir.

[124], önceki bir anormallik (anomaly) algılama yöntemine dayanmaktadır. Bu yöntem de pekiştirmeli (reinforcement) öğrenmeye dayalıdır. Ancak, yalnızca araçların hareketlilik

[19] https://github.com/stevenso8/WiSec_DataModifiedVeremi_Dataset

ölçümlerini kullanmaktadır. Diğer çalışmalarla karşılaştırma yapılmamakta, ancak sonunda MBD ile yapay zekâ işlemleri için basit bir gösterim olabileceği düşünülmüştür.

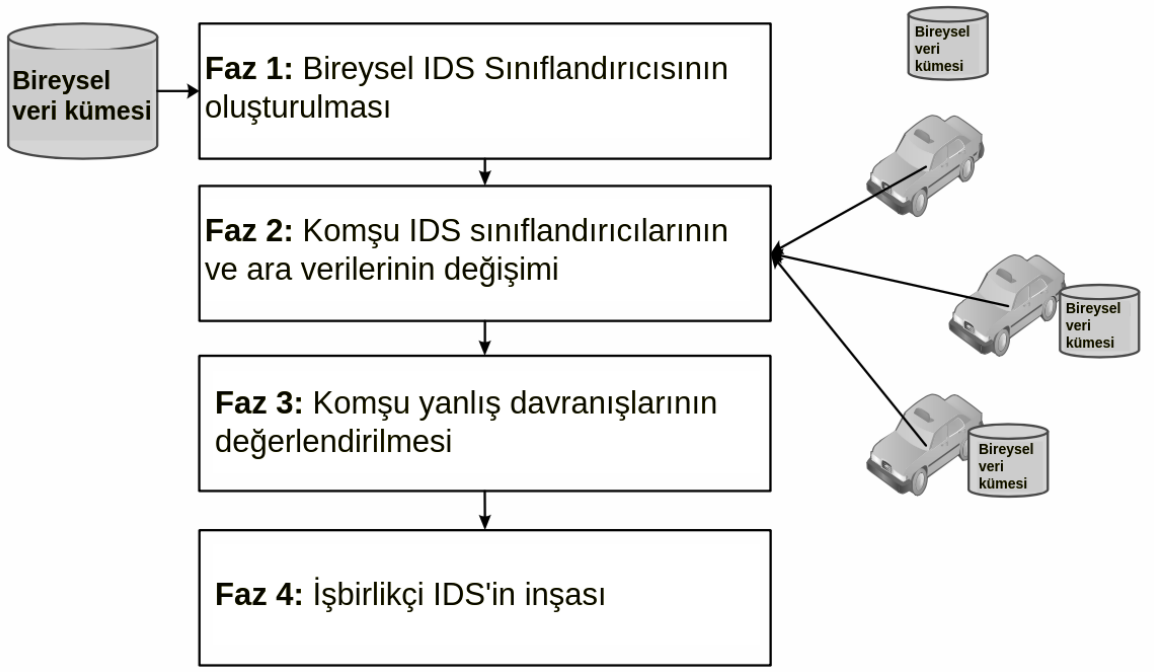
[125], araçların konumuyla ilgili, rastgele lokasyon/pozisyon ve sabit pozisyon saldırıları gibi türlerle kullanılabilecek bir yöntem önermektedir. Yalnızca, yine kendi yayınları olan bir önceki çalışmayla karşılaştırma yapılmaktadır. Bu çalışmanın, [130] araştırmasından daha iyi performans gösterdiği iddia edilmektedir. [128], aynı zamanda pozisyon saldırılarıyla da ilgili olarak, karşı koyma adına bu defa Pearson Korelasyonu kullanmıştır.

[126] araştırması, BC ile FL'yi savunur. BC, makine öğrenimi verilerinin güvenliğini sağlamak için çok uygun bulunmuştur. Dolayısıyla da açıklanabilirliğe yardımcı olduğu düşünülmüştür. Tez bu çalışmaya ulaşamasa da, özetinde savunulan fikir uygulanabilir görünmektedir.

[117, 118] çalışmaları, dinamik olarak V2X veri kümeleri oluşturan öncü bir araştırma öğesi olarak göze çarpmaktadır. Birçok MBD çalışması, bu çalışmayı kendi araştırmaları için kullanmıştır. Ayrıca basit kıyaslamalar ve sensör verileri de sağlanmıştır. Diğer yandan, CP verilerine yer verilmemiştir. Bu nedenle yalnızca CAM/DENM verileri ile çalışılmıştır.

[127] araştırması da, CNN-LSTM yeniden yapılandırma yöntemine (aynı yazarların eski bir çalışması) SVM rutinlerinin eklenmesi ile oluşturulmuştur. Çalışmada ayrıca performans ölçme adına VeReMi veri kümesi kullanılmıştır. CNN, LSTM ve SVM'nin bir arada nasıl kullanılabileceğine dair bir örnek olarak görülebilir.

[129], çalışması yanlış davranışa duyarlı, istem temelli iş birliğine dayalı bir IDS modeli (misbehavior-aware on-demand collaborative IDS, MA-CIDS) tanıtımının ardından, geleneksel IDS'leri ve bunların VANET uyumlu hale gelmeleri için gerekenleri belirtir. Bu model, yerelini eğitmek için, dağıtılmış bir rastgele orman algoritması kullanmaktadır. Daha sonra, her aracın bu modeli yakındaki araçlara dağıtması gerekmektedir. Makale, topluluk (ensemble) öğrenimiyle ilgili, literatürün çoğunun oylamaya dayalı şemalarla nihai kararı verdiğini belirtmektedir (voting-based schemas, majority wins, çoğunluk kazanır). Fakat bu araştırma, ağırlıklı bir oylama şeması önermektedir. Veriler, diğer araçlardan gelmekte ve test verileri de yerel olarak her araç üzerinde bulunmaktadır. Özellik seçimi, Tek Değişkenli İstatistik Testi (Ki Kare) kullanılarak gerçekleştirilmiştir.



Şekil 2.25: [129]'deki IDS & MBD

2.4.5.3. IDS veya MBD Yerleştirme

Standartlar, bir IDS/MBD sunucusunun veya bir uygunsuz davranış otoritesinin (MBA) nerede bulunması gerektiğini dikte etmemektedir. Tek gerekli olan şart, var olmaları ve AV'ler tarafından erişilebilir olmalarıdır. MBD durumunda; MBA, AV'lerden (veya yaya benzeri düğümlerden) gelen MBR'leri işlemelidir. Böylece, çevrim içi olarak mevcut olmalı ve istekleri işlemleyebilmelidir. Çevrimdışı olsa bile, standartlar, yine de toplu operasyon olasılığı olduğunu belirtmektedir. Bunun da, AV'lerin iş birliği yapmasına ve diğer araçlara [33] ("Komşulara MR yayınlayın" bölümü) MBR göndermesine bağlı olduğu belirtilir. Sonuç olarak, MBA bir bulut/uç/sis hizmeti olabilir.

Daha önce belirtildiği gibi, MBD süreci, aşağıdaki fazlardan oluşmaktadır;

- Yerel Algılama
- Rapor İletimi
- Genel Algılama

IDS VE MBD Değerlendirme

Bir FPGA üzerinde uyarlanan OBU özelliğinin, P4 programlama dili ile uygulanması çok uzak bir optimizasyon için çabalamak gibi görünebilir [246]. Ancak bu, onları IDS veya MBD için kullanamayacağımız anlamına gelmemelidir. Birçok yeni araştırma öğesi, IDS/MBD sistemlerinin parçalarını FPGA veya P4'te uygulamaktadırlar.

Küresel tespit yöntemleri söz konusu olduğunda, yeni bir fikir olan ağ içi işleme ortaya çıkmaktadır. Bunda, bir veri, ağ ekipmanı olan V2X altyapısına gelir gelmez; anahtarlar (switch), yerel olarak veriler üzerinde işlem yapabilir [246, 247, 248, 249].

2.4.6. Blok Zinciri

BC, dağıtık ve özerk doğası nedeni ile, VANET'ler ve V2X için gelecek vaat eden bir alandır. AD geleceğinin BC yöntemleri ile gidebileceği yönleri, birçok araştırmacıyı meşgul etmektedir [297, 298, 299]. V2X ve BC ile ilgili çalışmalar üzerinde daha fazla bilgi için [300, 301] makaleleri incelenebilir.

VANET sistemi, dağıtılmış bir bilgi işlem ve iletişim ortamıdır. Bu durumda, güvenliği sağlamak her zaman zor olacaktır. Öte yandan, VANET'in de sahip olduğu sorunlar açısından, bir dağıtılmış bilgi işlem ve iletişim sistemi olan BC, güvenlikle ilgili birçok sorunu çözüyor görünmektedir. Bahse konu problemlerden birisi de sertifika dağıtım sorunudur. Standartlar, bir BC uygulamasıyla kolayca çözülebilen birçok açık uçlu varsayıma sahip bulunmaktadır. Bu tez, bekleyen patentlerimizin kanıtladığı gibi, VANET için optimum olmayan performansıyla BC'nin, IDS ve MBD uygulamalarında bile birçok kullanıma sahip olabileceğini düşünmektedir.

2.4.7. Kıyaslamalar

Yeni bir teknolojinin kabul görmesi için oldukça iyi kriterlere ihtiyaç vardır. Bu kriterler, teknolojinin farklı bölümlerini karşılaştırır. Bir not olarak, belirtilen kıyaslamalar doğrudan V2X ile ilgili de olmayabilir. Ancak genel olarak da ona uygulanabilir olmalıdır. Bu tez, karşılaştırmalı değerlendirme yapan araştırmaların listesini **Tablo 2.44:** içerisinde belirtmiştir.

Tablo 2.44: V2X Kıyaslama Araştırmaları

Araştırma	**Açıklama**	**Veri Kümesi**
[302]	C-V2X ve DSRC	SAE J2945/1'den Gereksinimler (metre cinsinden %90 güvenilirlik vb.)[25]
[303, 304]	LTE, DSRC karşılaştırması	LTE tabanlı karşılaştırma
[305]	V2X ile ilgili	Test yaklaşımı
[198, 234]	Mevcut veri kümelerini kıyaslama	Birkaç mevcut veya sentetik veri kümesi
[216]	Kıyaslama veri kümesi	Tudataset
[212, 200, 216, 163]	Diğer kıyaslama veri kümeleri	Çeşitli

[302]'deki çalışma, **Tablo 2.45:** ve **Tablo 2.46:**'de açıklandığı gibi C-V2X'in tüm testlerde daha iyi olduğunu bulmuştur.

Tablo 2.45: 5GAA Saha Sonuçları Özeti [302]

Test Tipi	**Test Ortamı**	**Test İsmi**	**Test Sonucu**
Tıkanıklık	Laboratuvar	Kablolu Tıkanıklık Kontrolü	İkisi de geçti
Güvenilirlik	Laboratuvar	Kablolu Tx ve Rx Testi	CV2X daha iyi
Güvenilirlik	Saha	Görüş Hattı (LOS) Menzil Testleri	CV2X daha iyi
Güvenilirlik	Saha	Görüş Hattı Dışı (NLOS) Menzil Testleri	CV2X daha iyi
Girişim (Interference)	Laboratuvar	Simüle Edilmiş Ortak Kanal Girişimi ile Kablolu Testi	CV2X daha iyi
Girişim	Laboratuvar	Kablolu Yakın Uzak Testi	İkisi de geçti
Girişim	Saha	UNII-3'te Wi-Fi 80 MHz Bant Genişliği ile kullanım	CV2X daha iyi
Girişim	Saha	V2X'in Bitişik DSRC Taşıyıcıyla (Carrier) birlikte bulunması	İkisi de geçti

2.4.8. Metodolojinin Değerlendirilmesi

Standartlar genellikle projeler olarak başlamıştır. Daha sonra, teknolojinin farklı yönleri için özel ilgi grupları oluşturan SB'lere entegre edilmişlerdir. Akademi ve sektörlerden uzmanlar, standartları oluşturduğu için ise yeterince güven oluşturmuşlardır.

Tek bir standardın birçok versiyonunun olduğu görülebilir. Örneğin, (bu bölümde anlatılan yöntemlerden biri) [34]'in ilk sürümü 2010'da çıkarılmıştır. Son sürümün 2023'nin son aylarında çıkması öngörülmektedir. Tüm bu sürümler, bir değişim ihtiyacından kaynaklanmaktadırlar. Bu ihtiyacın siber güvenlikten mi, yoksa daha fazla kaynak

Tablo 2.46: 5GAA Saha Sonuçları Özeti [302]

Test Yordamı	**DSRC[a]**	**CV2X[a]**
Görüş Hattı (Line-of-sight, LOS) Aralığı	675m	1175 m
Görüş Hattı Dışı (Non-Line-of-Sight, NLOS) Engelleyici (5GAA)	125 m	425m
Görüş Hattı Dışı (Non-Line-of-Sight, NLOS) Engelleyici (CAMP)	400m (200m)[b]	>1350m (625m)
Görüş Hattı Dışı (NLOS) Kavşak	375m	875m
UNII-3'te Wi-Fi 80 MHz Bant Genişliği ile kullanım	300m	625m (75m)
V2X'in DSRC Bitişik Taşıyıcıyla birlikte bulunması	400m (100m)	1050m

- **a**: %90 güvenilirlikle menzil
- **b**: Parantez içindeki sayılar %90 güvenilirliğin altına ilk düşüşü gösterir

Tablo 2.47: TVRA Varlık Etkileri ve Etki Değerleri

Etki	**Açıklama**	**Değer**
Düşük	İlgili taraf çok fazla zarar görmez; olası hasar düşüktür.	1
Orta	Tehdit, sağlayıcıların/abonelerin çıkarlarını ele alır, ihmal edilemez.	2
Yüksek	A iş temeli tehdit altındadır ve bu bağlamda ciddi zararlar meydana gelebilir.	3

beklentisinden mi çıktığı üzerinde çalışılmaktadır. Bu dökümanda yeni bir standart veya teknoloji geliştirmenin yöntemi belirtilmektedir. Örneğin bir VANET ortamında sıfır gün saldırısı bulunur ve bir karşı önlem de önerilirse öncelikli soruların şunlar olduğu belirtilmiştir;

- Bu önlem standartlarda yer almalı mıdır?
- Bu önlem entegre edilirse ise, bunun kurulu VANET sistemlerine etkisi ne olabilir?
- Bu önlem entegre etmeye değer mi?

Bu tezin bulabildiği kadarıyla, SB'lerin izlediği birkaç yöntem vardır;

- TVRA Yöntemi [169, 306, 34]
- Mevcut araştırmaları ve projeleri takip etme [23, 99]

- ETSI Yanlış Davranış Yöntemi [33]

Standartlar, mevcut araştırma makalelerinden ders almak adına, onları takip ediyor görünmektedirler. Standartlarda mevcut araştırmalara birçok atıf yapılmakta ve bunlar da aynı şekilde takip edilmektedir. Önceki veya var olan projelere bakıldığında ise, daha önceki bir proje [23] olarak geliştirilen ve daha sonra IEEE 1609 [12] ile entegre edilen SCMS gibi birçok standart bölüm, bağımsız veya finanse edilen projeler olarak başladı. ETSI'nin TVRA Yöntemi ise, bir standarda veya halihazırda var olan bir teknolojiye yapılan yeni eklemelerin güvenliğe etkisini ölçmenin uygun bir yolu olarak görünmektedir. **Tablo 2.47:**'de tanımlandığı gibi, bir tehdidin, varlığının ve saldırı vektörünün her yönü düzeyler olarak tanımlanmaktadır (burada yalnızca varlık etki değerleri verilmiştir, "motivasyon düzeyleri" gibi kabul edilen "saldırı yoğunluğu seviyeleri" vb. gibi daha birçok ölçüm bulunmaktadır).

ETSI'nin MBD Yöntemi [33], TVRA yöntemlerinden sonra modellenmiştir. Bu sayede, MBD'nin birçok yönü, TVRA veri tabanına konmakta ve sonuç olarak yeni bir puan verilmektedir. Bu teknik bir rapordur, dolayısıyla herkes bunu bir tavsiye olarak kabul edebilir.

2.4.9. V2X'deki Zorluklar

Bu tezdeki açıklamaların ardından, V2X ve V2X için siber güvenlik ile ilgili yürürlükte olan zorlukları şu şekilde sıralamak mümkün olabilir;

- Gerçek zamanlı ve hızlı ağ altyapısı için 5G ve 6G teknolojisinin beklenmesi,
- Kısıtlı araç donanımı,
- Dinamik topoloji,
- Kısa ömürlü bağlantılar,
- Yüksek hareket kabiliyeti,
- Kısa bağlantı süresi,
- Sık kopukluklar,

Tablo 2.48: Tek bir Öğe için TVRA Maliyet & Fayda Proforması (Tahmini) [169]

Önlem	Maliyet		Fayda			Sonuç
	Kategori	Değer	Risk Seviyesi	Orijinal Adet	Revize Adet	
Tekrarlanan mesajların sıklığını azaltma	Standartların dizaynı	Düşük Etki	Küçük	0	0	14
	Gerçekleştirme	Etkisiz	Büyük	0	3	
	Operasyon	Etkisiz	Kritik	3	0	
	Düzenleyici etki			Etkisiz		
	Piyasa Kabulü			Etkisiz		

- Radyo spektrumu,
- Hem LEM hem de GEM'de CP durumu/temsiliyle ilgili fikir birliği,
- CP'de MBD koruması,
- Kuantum sonrası hesaplama,
- DSRC (WAVE) veya C-V2X'e Karar Verme.

Kuantum bilişimin siber güvenlikte çalışma ve ona bakış açımızı değiştireceği genel bir anlayış olarak ortaya çıkmıştır [307]. Bununla beraber VANET sistemleri, SCMS'ler kuantum bilgi işlem açısından güvenli olmadığı düşünülen özel dijital sertifikalarla çalışmaktadır [12]. Öte yandan, V2X'te kuantum güvenliğine geçiş olarak düşünülen şifreleme algoritmaları değiştirilebilir durumda görünmektedir.

VANET, tam potansiyeli için hücresel ve kablosuz teknolojideki yeni nesil gelişmeleri beklemektedir. Hücresel tarafta, 5G ve 6G'nin, tam otonomdaki yerini alması uzun süredir beklenmektedir [308]. Kablosuz tarafta, yeni nesil VANET sistemleri için IEEE 802.11bd'yi geliştirmektedir.

Kısıtlı ekipman ise, otonom sistemlerin geliştirilmesinde karşılaşılan başka bir sorun olarak karşımıza çıkmaktadır. Bazı şirketler, AV'lere dahili olarak kurulu ANN ASIC'lerle bunu atlamayı denemektedir. Karar verme ise, çoğu aracın sahip olamayacağı pahalı bir özellik olarak görünmektedir. Bunu atlayabilmek içinse cep telefonlarını, belki bir bulut bağlantısıyla, kullanmak kadar üstesinden gelinebilir görünmektedir. Ancak gereken "gerçek zamanlı" altyapılar olduğundan, bu biraz zor görünmektedir.

Dinamik topoloji, kısa ömürlü bağlantılar, yüksek hareketlilik ve sık sık bağlantı kesilmeleri en çok belirtilen zorluklar olarak ortaya çıkmakta ve bu tezde ayrıntılı olarak ele alınmamıştır. Daha önce belirtildiği gibi, sabit bant tahsisi de ayrı bir problemdir. Şu anda bu konu ile ilgili bazı kritik araştırmalar bulunmaktadır [5]. Bilişsel radyo ise bir çözüm olarak sunulmaktadır [309, 310]. Bu durumda, ne zaman iletişime ihtiyaç duyulursa, ajan serbest bir spektrum bulmaya çalışabilir ve daha sonra bu serbest spektrumu da radyo iletişiminde kullanabilecektir. Mevcut spektrumu daha iyi kullanmak için de 5G ve 6G de bu tür iletişimin de gerçeklenmesi beklenmektedir. Veri yükleme/boşaltma (offloading) [311], verileri lisanslı

DSRC veya C-V2x spektrumundan, lisanssız Wi-Fi'ye veya tam tersine aktarmaya çalışan başka bir teknolojidir.

CP gösterimi ile ilgili tüm açıklamalardan sonra, nesnelerin durumu, LEM veya GEM ile ilgili birçok sorun bulunmaktadır. Kazara veya yanlış yapılandırılmış, veya hatalı bir sensör tarafından, bir durum AV'ler veya VANET tarafından farklı algılanabileceğinden, GEM üzerinde bazı fikir birliği mekanizmaları gerekmektedir. Bu, şekil olarak BC uzlaşı (konsensüs) mekanizmalarına benzemektedir. Gerçekte ise, performans nedenleriyle, gelecekteki başka bir araştırma adayı olarak öne çıkmaktadır. Bununla birlikte, [42] de belirtildiği gibi, CP, en azından standardizasyonun gözünde, bir MBD mekanizması tarafından korunmamaktadır.

2.4.10. V2X Araştırmalarından Öğrenilen Dersler

MBD veya CP ile ilgili çok sayıda araştırma bulunmaktadır. Ancak, konunun görece yeni bir teknoloji olması, ayrıca fikri mülkiyetlerin korunmak istenmesi nedeni ile, açık kaynak alt yapılar bulmak zordur [117, 118, 122]. Başka bir durum, bu tezin çatallanma (forking) sorunu olarak betimlediği problemdir. Bazı önemli araştırmaların kullandığı açık kaynak kodlar, başka bir araştırma için çok eski bir işlemden (commit) çatallanmış olarak karşımıza çıkmaktadır. Orjinal kaynaktaki geliştirme, önceki çalışmayla, üzerinden çok geliştirme yapıldığından, kolayca birleştirilemez durumdadır. İlk araştırmacılar, asıl geliştirici yazarla çalışıp değişiklikleri ilk depoya (repo) geri göndermediklerinden, bu durum meydana gelmektedir. Aslında, çatallanma problemi, mevcut araştırmaların üzerine devam etmek için, yeni araştırmaların karşı karşıya olduğu ciddi bir sorun olarak karşımıza çıkmaktadır.

Standartların üzerinden bakıldığında ise, pek çok parçanın kapsam dışı olarak tanımlandığı görülecektir. Gelecekteki belgeler ya da gelecekteki araştırmalar için bırakılmış oldukları düşünülmektedir. Bunlardan sayabileceğimiz bazıları sertifika dağıtımı, MBA yapısı veya ilgili V2X ağ düğümlerinin yerleştirmesidir.

Bunların dışında WAVE, M5 veya G5 yerine C-V2X kullanma eğilimi açıkça görülmektedir. V2X'te tanımlanan birçok problemin, C-V2X'de çözümünün olduğu savunulmaktadır [34].

Genel olarak ise, MBD/CP cephesi ile ilgili literatürdeki araştırma eksikliği şu şekilde görünmektedir;

- CPM veri kümesi: Literatürde MBD ile kullanılabilecek açık kaynaklı bir CPM veri kümesi bulunmamaktadır.

- LDM->MBD link: Çizelge tabanlı yapılar literatürde genellikle yerel dinamik harita (LDM)[56] olarak anılır, ancak LDM ve MBD konularını birleştiren bir çalışma yoktur.

- Simülasyon araçlarında CPM desteği: Görüldüğü gibi, Artery'de CPM ile ilgili önceki çalışmalar bulunmaktadır ve devamı da gelmektedir [120]. Ancak, bunun Artery ana dalına (main branch) ne zaman gireceği bilinmemektedir. Diğer simülasyon araçları henüz CPM'yi desteklememektedir [20] [21] .

- Kaynak kodu çatallanma sorunu: Normal şartlarda Veins ve Artery birbirine çok yakın iki açık kaynak yazılımlardır. Veins ABD merkezlidir, Artery ise AB merkezli bir simülasyon aracıdır. Buna karşılık her ikisi de Omnet++ tabanlıdır. F^2MD ayrıca Veins'in eski bir versiyonundan çatallanmıştır. Bu kodları bir araya getirip bir çözüm ortaya çıkarmak mümkün görünmektedir ama şu an için bir yönelim bulunmamakta ve olması da zor görünmektedir.

- Çizelge tabanlı sinir ağları: Literatürde MBD ile ilgili çizelge tabanlı bir çalışma bulunamamıştır. Yine de GNN, modellerdeki (LEM/GEM/LDM/GDM) nesneleri işlemenin doğal bir yolu gibi görünmektedir.

2.4.11. V2X'de Son Durum

Son yıllarda, özellikle son birkaç yılda, Otonom Araçların (AV) ilerlemelerinde büyük bir artış görülmüştür. Yalnızca beş yıl önce, AV'ler hakkında konuşmak bilim kurgu gibi karşılanmaktaydı. Şimdi, bazı alanlarda tam özerkliğe (otonomiye) sahip bulunmaktayız. Bazı yollarda üçüncü düzey özerklik olmakta ve neredeyse her araba şimdi V2X için hazır bir tür ekipmanla gelebilmektedir.

Şirketler, ülkeler ve kıtalar, standartlarıyla geleceği hayal etmek için denemeler yapmaktadırlar. Özellikle Avrupa SB'leri, diğerlerinin de yardımıyla, ileriye giden yolu göstermektedirler. Ayrıca endüstri iş birliği ileri bir düzeydedir. Hücresel ağlar, V2X'i

[20] https://github.com/riebl/artery/pull/251
[21] https://github.com/riebl/artery/pull/252

şimdiden desteklemektedirler ve kendilerini, en son teknoloji, yazılım tanımlı ağ (SDN) ve NFV'yi kullanarak, araçların (IoV) veya genel anlamda nesnelerin internetine (IoT) göre ayarlamaktadırlar.

AI'deki, özellikle DL'deki ilerlemeler, bu V2X teknolojileri için önemli bir kolaylaştırıcı olacaklar gibi görünmektedir. AI için güçlü bir çip üzerinde sistem (SOC) cihazlarına sahip araçlar şimdiden piyasada bulunmaktadırlar. Son dönemde, kendine yer bulmaya çalışan toplu algı (CP), AI'dan en çok yararlanacak altyapı olacak gibi görünmektedir. Blok zinciri çalışmaları bulunmakta, ancak tam entegrasyonu için henüz zaman gerekmektedir.

AV'ler dağıtılmış ve toplu ağ öğeleri olduğundan, ayrıca oldukça hareketli olduklarından, belirli siber güvenlik ve performans özelliklerine sahip VANET adı verilen mobil (ve yerel) ağlara sahiptirler. Siber güvenliğin en çok çalışılan alanlarında birisi de saldırı tespitidir (IDS). Ancak, kısıtlanmış ve daha az güçlü olan VANET ağlarında, IDS'e yer olmayacağı düşünülebilmektedir. Aksine, yol kenarı birimlerinde (RSU) güçlü bir geleceği olduğu düşünülebilir. Ancak bir bütün olarak ağda, yani kısmen ve son zamanlarda, MBD ile de bu aşılmış görünmektedir.

Bu tez, kötü davranış tespiti ve toplu algıyı göz önünde bulundurarak V2X'te siber güvenlik konusunda son beş yıldaki gelişmeleri sunmuştur. Son ağ teknolojilerini, organizasyonları, protokolleri ve ve bunlardan çıkarımları da içermiştir.

2.4.12. V2X'de Gelecek

V2X teknolojisinde gelişme ve ilerleme çok hızlıdır. Ayrıca değişim hacmi de oldukça fazladır. Ancak yine de sistemler gelişmeye ve değişmeye devam etmektedirler. Bu nedenle, V2X için yeni nesil IDS ve MBD'yi düşünmek ve çalışmak için uygun veri kümeleri gerekmektedir. Listelenen veri tabanlarında olduğu gibi, mevcut veri kümelerini mevcut IDS araçlarından imzalar şeklinde kullanmak da mümkündür. Buradaki fikir, onları imza veri kümelerinden dönüştürmek ve V2X için uygun hale getirmektir. Ancak uygulanabilirliği ve performansı tartışmalıdır ve ilerdeki bir araştırma konusu olarak düşünülebilir.

TVRA ve diğer değerlendirme yöntemleri, mevcut kurulumları bozmadan veya en az kesintiye uğratarak nasıl yeni bir yol önerileceği konusunda, gelecekteki araştırmalar yol göstermektedir. Bu tezin öngördüğü gibi, uluslararası toplum tarafından değerlendirme

standartları daha fazla kullanılacak ve araştırılacak gibi görünmektedir.

[42]'nin açıkladığı gibi, CP güvenli değildir. Ancak tersi de söz konusudur; CP ile bir MBD uygulamak mümkün görünmektedir. Bu tez, literatürde konu ve [33] yayın öncesi teknik raporu hakkında daha fazla araştırma gelebileceğini düşünmektedir.

VANET'in yapısı ilerledikçe, toplu veya ilişkisel ANN yöntemleri içinde en uygununun çizelge tabanlı ANN'ler olduğu görülmektedir. Bu yöntemler ve temsili öğrenme ile AV'lerin ürettiği verilerle çalışmak daha kolay olabilecektir. Ayrıca, temsili öğrenme ile ihtiyaç duyulan her veri, çizelge veri yapısı üzerinde bulunmakta ve ANN algoritmalarını çalıştırmak çok daha kolay görünmektedir.

Önceki çığır açan teknolojik yarışlardan dersler alarak, uyumlaştırma çabaları, ITS yapılarını ve konuşlandırma ihtiyaçlarını anlamada esas durumdadır. Zaman ilerledikçe, bu çaba dünya çapında daha hızlı entegrasyonlar ve geliştirme döngüleri ile artacak gibi görünmektedir.

Ayrıca, birçoğu mevcut araştırmalar tarafından geliştirildiğinden, V2X'te kuantum güvenli şifreleme algoritmalarını görmenin zamanı gelmiş görünmektedir.

VANET'te SDN ve ilgili çalışmalar, ağ teknolojileri ilerledikçe daha fazla ilgi görmektedir. [161]'e göre, VANET'ler gibi mobil ağlardan bahsederken, SDN henüz emekleme aşamasında ve MEC gibi teknolojilerle bu cephede nelerin mümkün olduğu görülecektir. Bu nedenle, VANET'te SDN ile ilgili daha fazla çalışmaya ihtiyaç bulunmaktadır.

Sonunda, piyasadaki akıllı olmayan araçlarla giderek daha fazla cep telefonu tabanlı OBU'larla karşılaşacağımız için, insanların (savunmasız yayalar olarak) onları VANET ortamına entegre eden mini OBU'ları olacaktır.

3. MALZEME VE YÖNTEM

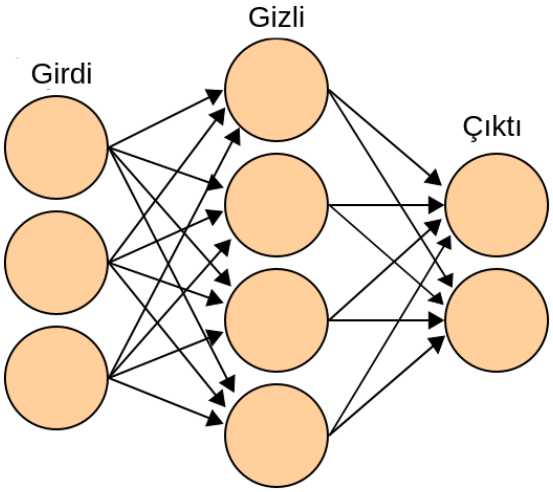
Nesne temsili probleminin en iyi şekilde nasıl çözülebileceği ile ilgili daha önceki bölümlerde açıklamalar yapılmıştı (Bölüm 2.3.2.4.). V2X ağlarının bir çizelge yapısına benzemesi, bu problemin çözümüne çizelge benzeri yapılar ile gidilebileceğini göstermektedir. Bu tezde belirtilen araştırmaların çıktısı olarak da, LEM veya GEM modelinin çizelge benzeri bir yapıda tutulması en iyi yöntem olacağı çıkarsanmıştır. Böylelikle öğeler arasındaki ilişkiler gerçek hayatta olduğu gibi tutulabilecektir [291]. Ardından, iyi bir MBD sistemi için ise, bu bilgileri kaybetmeden işleyebilecek bir altyapının olarak da GNN'ler olduğu görülmüştür. Ancak, V2X ağlarının sürekli değişimde bir sistem olması, bağlantıların ve öğelerin zamanla değişimi nedeni ile de uzay ve zaman (spatio-temporal) ile değişim gösterdiği gerçeği, kullanılacak teknolojinin de bunu desteklemesi zorunluluğunu getirmiştir. Bu bölümde ve daha sonraki bölümlerde, tezin konusu olan MBD yapısı ve bağlı altyapılar anlatılmıştır.

3.1. TEKRARLAYAN NÖRAL AĞLAR

Basit bir ileri doğru giden yapay sinir ağı (FFANN) **Şekil 3.1:**'de belirtilmiştir[22] . Bu çeşit sınırlı sayıda ve ileriye doğru çalışan nöral ağlar, karmaşıklık arttıkça daha büyük boyutlu fonksiyonlara benzetim yapar. Bunlardan perceptron (**Şekil 3.2:**), en basit FFANN yapılarından birisidir ve evrensel fonksiyon benzetimci (approximator) olarak tanımlanır [312].

Ancak bu tür ANN'ler zaman dizisi veya geriye doğru ilişki verilerde iyi sonuçlar verememektedirler. Örneğin "Depremde asansör kullanılmaz" cümlesinde, "asansör" kelimesinden sonra gelecek kelimeyi bilmek için ondan önce gelen "asansör" kelimesi ile ilgili bir durum (state) tutulmalıdır ve bu FFANN'lerde bulunmamaktadır. Bunun aşılabilmesi için 1986 yılında ilk kez İngilizce kelimeleri tahmin edebilmek için [313] Hopfield ANN [314] ve Boltzman makinesi oluşturulmuştur [315].

[22] https://commons.wikimedia.org/wiki/File:Artificial_neural_network.svg



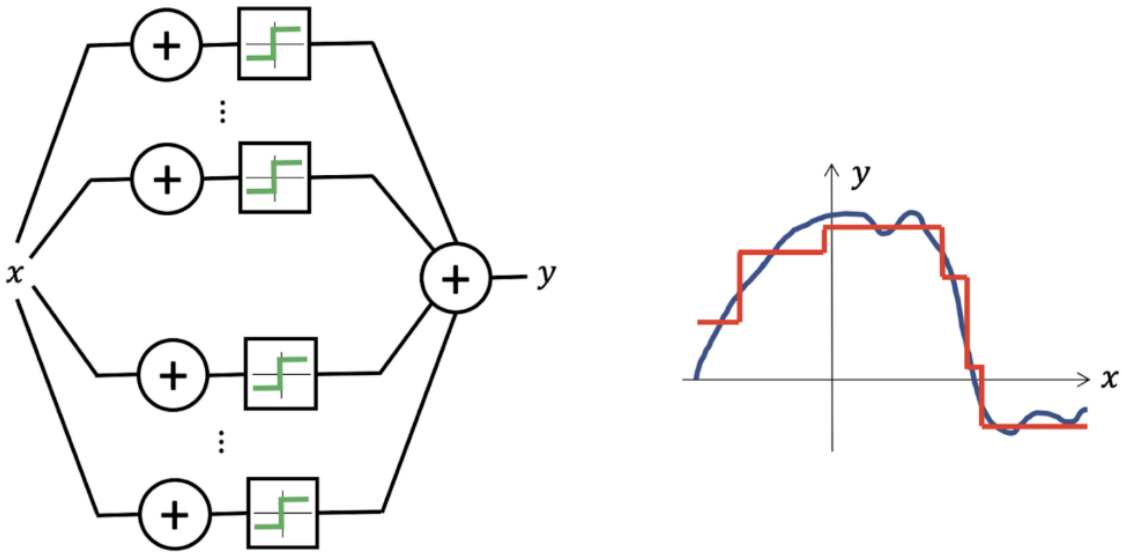
Şekil 3.1: Basit İleri Doğru Giden ANN[22]

Tekrarlayan nöral ağlar (recurrent neural networks, RNN) bir yapay sinir ağı modeline hafıza katıp, sıralı giden verilerde geçmişi hatırlayıp, geleceği buna dayanarak tahmin etme işlemi yapmaktadır. Bu tezde de, RNN alt yapısı kullanıldığından kısaca bahsedilmesi uygun olmaktadır. Ancak, ayrıntılı bilgi için [316] kaynağına bakılabilir.

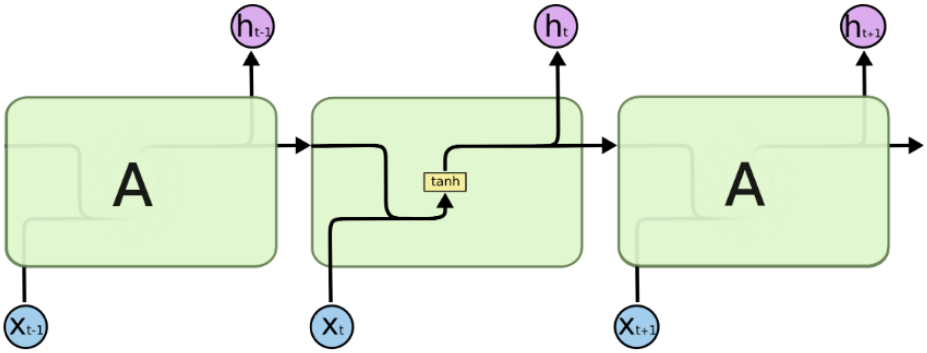
Her ne kadar, daha önce çözülemeyen problemlere çözüm olsa da, RNN'lerde verimliliği etkileyen iki adet durum olmuştur. Bunlar kaybolan ve patlayan gradiyent sorunlarıdır. Kaybolan gradiyent durumunda, eğitim sırasında çok önceden gelen bilgiler kaybolmakta ve gradiyent sıfıra (0) yaklaşmaktadır ve çözüm bulunamamaktadır. Patlayan gradiyent durumunda ise, hata çok büyükse, ağda çok büyük güncellemelere neden olmaktadır. Bun durumlara çözüm olmak adına [317] çalışması ile Uzun kısa-süreli hafıza (Long short-term memory, LSTM) tanıtılmıştır. Basit bir RNN yapısı **Şekil 3.3:** görülmektedir. LSTM'in bu yapıya eklediği ise **Şekil 3.4:**'den anlaşılabilir.

RNN'de bulunan basit "tanh" yapısı, daha iyi bir öğrenim için "kapılar" ("gate") de denen operasyonlarla değiştirilmiştir. Bu kapılardan bazıları "unutmayı" sağlarken ("depremde" kelimesini "asansör"'den sonra unutma gibi), bazıları da hatırlatmayı sağlar. Sıfır (0, unut) ile bir (1, hatırla) arasındaki bir değer ile belirtilen bu durum, arada değerlere de sahip olabilir.

Bu tezde kullanılan bir RNN tipi olan Kapılı Tekrarlama Ünitesi (Gated Recurrent Unit, GRU) ise, LSTM'in biraz değiştirilmesi ile elde edilmiştir [318]. **Şekil 3.5:**'de görüldüğü gibi, unutma kapısından sağındaki kapıya bir birleşim olmuştur. Buna benzer daha başka değişikliklerle LSTM'den daha basit ve gittikçe daha çok kullanılan bir yapı olmuştur.



Şekil 3.2: Perceptron ve Fonksiyon Benzetimi [312]



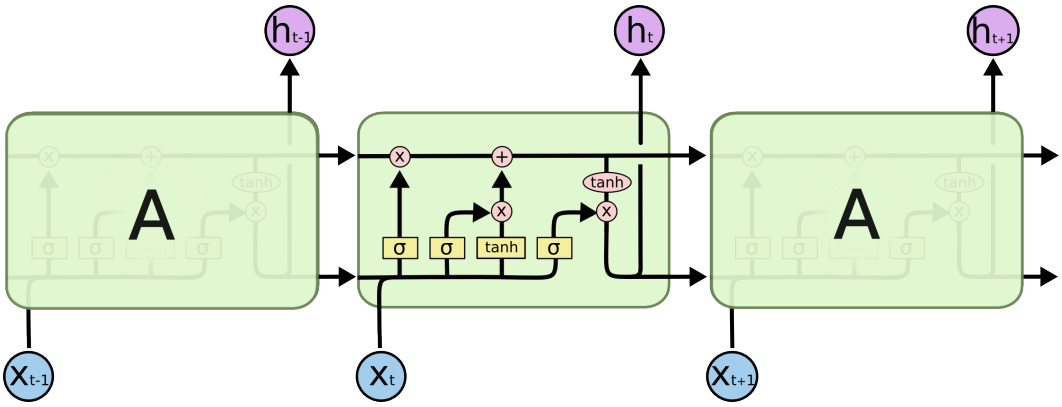
Şekil 3.3: Basit Bir RNN Modeli [316]

3.2. EVRİŞİMLİ NÖRAL AĞLAR

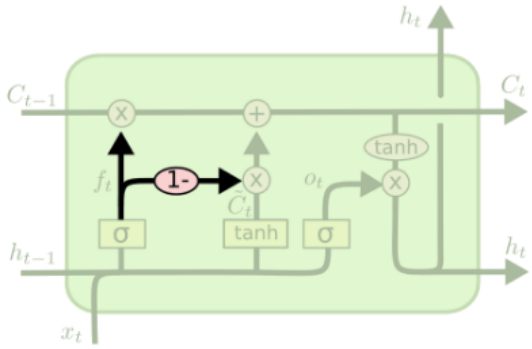
Evrişimli (Convolutional) ANN'ler (CNN), geometrik öğrenme [312] ile bağlantılı olup, insanların kolayca yapabildiği, ancak makinelerin daha önce bunda zorlandığı resim ve konuşma tanıma işlemleri için geliştirilmiş bir gösterimsel öğrenme alt yapısıdır. Konu ile ilgili çok detaylı bilgi [319] kaynağında edinilebilir. Ancak bu tezde de kullanılan GNN altyapılarından birisi (CGNN) olduğundan burada kısa bahsedilecektir.

CNN'ler genellikle altı adet katmandan oluşurlar. Bunlar sırası ile **Şekil 3.7:** içerisinde belirtilmiştir. Bunlar;

1. Giriş katmanı (input)



Şekil 3.4: LSTM Modeli [316]

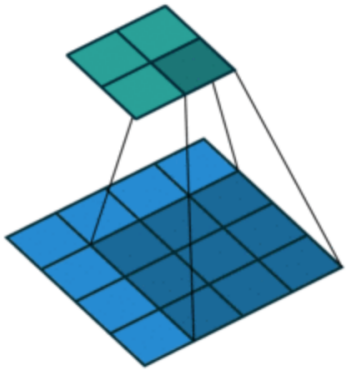


Şekil 3.5: GRU Modeli [316]

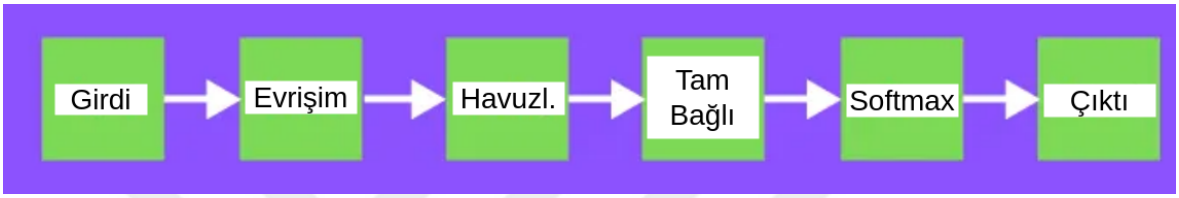
2. Evrişim katmanı (Convolution)(+ReLU),
3. Havuzlama katmanı (Pooling),
4. Tam bağlı katman (Fully connected),
5. Softmax/lojistik katmanı,
6. Çıktı katmanı (output).

Giriş katmanı, basitçe girdi verilerin gönderildiği katmandır. Giriş katmanında gelen veri çok boyutlu olabilir. Ancak bu boyutun yeniden şekillendirilmesi gerekmektedir (reshape). Örneğin 4x4 olan bir girdi, 16x1 şeklinde bir matrise döndürülür. 5 adet eğitim resmi varsa, bu matris 16x5 şeklinde oluşmuş olmalıdır.

Giriş katmanından evrişim katmanına ulaşan veri, daha küçük bir boyuta dönüştürülür. Tabi bu geçiş PCA gibi kayıplı değildir. Bu boyut küçültme filtre denilen işlemlerle yapılır. Filtre sonrası oluşacak boyut bilgisi aşağıdaki formülle hesaplanır;



Şekil 3.6: CNN Evrişimi[23]



Şekil 3.7: CNN Katmanları[23]

Tanımlama 3.2.1 (Resim Boyutu) NxN

Tanımlama 3.2.2 (Filtre Boyutu) FxF

Tanımlama 3.2.3 (Evrişim Katmanı Boyut) $(NxN) * (FxF) = (N-F+1)x(N-F+1)$

Bir örnek olarak, $4X4$ bir resim $3x3$ filtreye uygulanırsa, $2X2$ bir yeni boyut çıkar. **Şekil 3.6:**'da görüldüğü gibi, üst taraf oluşacak yeni boyutlu matrisimizdir. Alt tarafta koyu belirtilen için kısım filtre, tüm alt taraf ise girdi veridir [23] .

Koyu belirtilen filtrenin her bir hareket miktarına kayma (stride) denir. Kayma sayısı arttıkça üstte belirtilen yeni boyutun genişlik veya en değerleri değişebilir. Bazı durumlarda yeni boyut ile eski boyutun aynı olması beklenebilir. Bu durumda da, girdi olan veriyi çevreleyecek şekilde dolgu (padding) eklenir. Örneğin şekilde en altta bulunan girdi verinin etrafına bir birim doldu eklenmiş olsa idi çıktı boyumuz da yine girdi boyutu olan $4X4$ olurdu.

Evrişim katmanının bir özelliği de, bu katmandan çıkış yapmadan önce verinin negatif olmasının önüne geçmek adına doğrultucu aktivasyon fonksiyonu (rectifier activation

[23] https://towardsdatascience.com/covolutional-neural-network-cb0883dd6529

function) (ReLU) uygulanmasıdır. ReLu $f(x) = \max(0,x)$ şeklinde tanımlanmıştır. Böylece negatif değerler sıfır (0) olarak alınmaktadır.

Bir sonraki kısım, havuzlama katmanıdır. Burada evrişimden geçen veri, yine aynı evrişim parametreleri ile (kayma ve filtreleme) boyut olarak daha da küçültülür. Çok fazla kullanılan, en büyük havuzlama (max-pooling, MP), filtreleme yaparken filtre alanındaki en büyük değeri alır. Bu bir bakıma giren resmin küçültülmesi anlamına da gelebilmektedir. MP'nin iki ayrı türü vardır. Filtreleme (F) boyutu genellikle 3, kayma (S) değeri de 2 alınır. Buna örtüşen (overlapping) havuzlama denir. Diğer çok kullanılan bir türü de F ve S'nin ikisinin de 2 olduğu halidir. Bu iki parametrede daha büyük bir değerin genellikle bozucu olduğu belirtilmiştir [24] [25] . Başka havuzlama yöntemleri de bulunmaktadır ancak pratikte çok kullanılmamaktadır. Bu tezde kullanılan havuzlama yöntemi TopKPooling'dir [320]. İstenilen miktarda bir veriyi havuzlama imkânı verir. Havuzlama konusu ile ilgili daha geniş bilgiye [319] kaynağından ulaşılabilir.

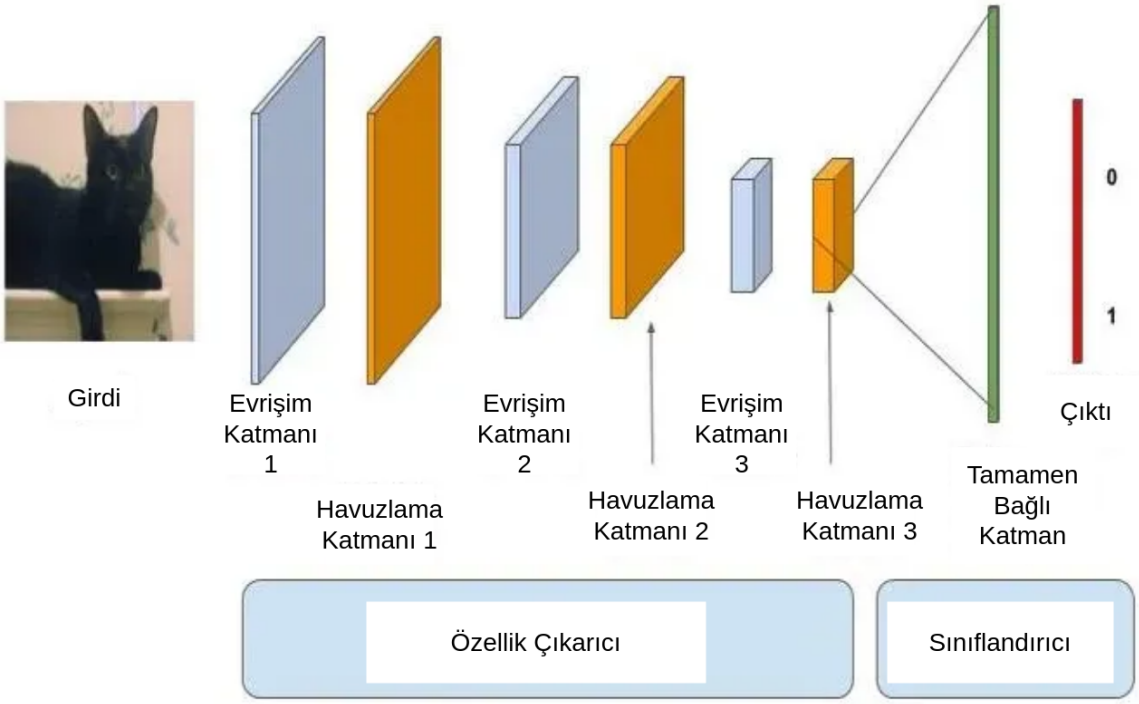
Daha sonraki katman tam iletişimli veya tam bağlı diyebileceğimiz kısımdır. Bu katman bilindik her nodun birbirine bağlı olduğu bir ANN katmanıdır.

Son katman diyebileceğimiz (çıktı katmanını saymazsak) softmax/lojistik katmanı, birli veya çoklu sınıflandırma işlemi yapar. Lojistik ise birli sınıflandırma, softmax ise çoklu sınıflandırma yapılabilir.

Şekil 3.8:'de ilginç bir durum vardır ve hemen fark edilebilir. Burada evrişim ve havuzlama basamakları tekrar edilmiştir. Bu yöntem modelin gösterdiği performansa göre ayarlanır. Deneme, yanılma ve kaynak tüketimi gibi konular devreye girer. Resimde en sonda bir adet softmax sınıflandırıcısı da olmalıdır. Softmax (veya sotargmax, çok sınıflı lojistik regresyon) işleminin yaptığı *k* adet elemanı olan bir vektörü, toplamı bir olan yine *k* elemanlı bir vektöre dönüştürmesidir. Her bir değerin düşük değeri varsa, olasılığı da düşük olur. Ancak tüm değerlerin toplamı sıfır olur.

CNN'lerde başka katmanlar da bulunmaktadır. Örneğin aşırı uyumu (overfitting) engelleme adına yapılan düzenleme (regularization) adı verilen katman bunlardandır. Bu tezde kullanılan dropout yöntemi [321] de aslında bir düzenleme işlemidir. Konu ile ilgili daha

[24] http://cs231n.stanford.edu/
[25] https://cs231n.github.io/convolutional-networks/



Şekil 3.8: Basit Bir CNN Modeli[23]

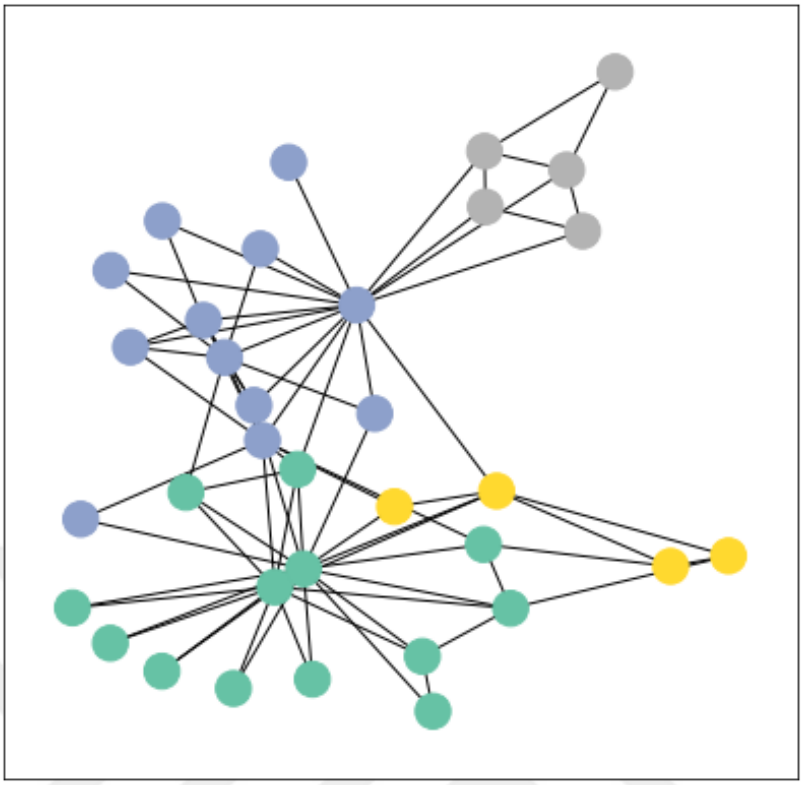
fazla bilgi [322] kaynağında bulunabilir.

3.3. ÇİZELGE NÖRAL SİNİR AĞLARI

GNN, Geometrik Öğrenme (GL veya temsili öğrenme, RL) adlı geniş bir konunun parçasıdır. Terimin de belirttiği gibi, makine öğrenimi operasyonları geometri kaybı olmadan [289] yürütüldüğünde eldeki problemin yapısı (temsili) de dikkate alınır; bunlar şekiller, ilişkiler veya [312] yapısındaki dönüşümler olabilir. Tablo şeklinde gösterimde bu özellikler genellikle kaybolur veya dahil edilmesi zordur.

Geometrik öğrenme, Evrişimli Sinir Ağları (CNN) ve GNN'ler dahil ancak bunlarla sınırlı olmamak üzere iyi bilinen yöntemleri kapsar. İlginç bir şekilde diğer benzer yöntemler GNN'nin özel bir durumu olabilir. Örneğin kümeler, kenarları olmayan GNN'ler olabilir. Ayrıca, GNN'ler var olan en genel makine öğrenimi mimarilerinden biridir [312].

Literatürde GNN'ler çoğunlukla üç tipte karşımıza çıkmaktadır; evrişimli GNN'ler (CGNN), dikkat temelli GNN'ler (AGNN) ve mesaj ileten GNN'ler (MPGNN). Aralarındaki fark mahalle kodlamasıdır. CGNN'de bu kodlama sabit ağırlıklardadır. AGNN'de eğitimli ve



Şekil 3.9: Karate Kulübü Veri Kümesi (KCD) Oluşturma [329]

softmax normalize edilmiş bir öz-dikkat mekanizması mevcuttur. Öte yandan, MPGNN çeşitli vektörlerden (“mesajlar") öğrenir.

GNN’ler son on yılda birinci sınıf bir makine öğrenimi yöntemi olarak şekillenmiştir. Ancak tarihsel olarak GNN başlangıcı Öklid geometrisinden gelmektedir. Ayrıca GNN ifadesinin ilk bahsedilmesi [323, 324] kaynaklarında gözlenmiştir.

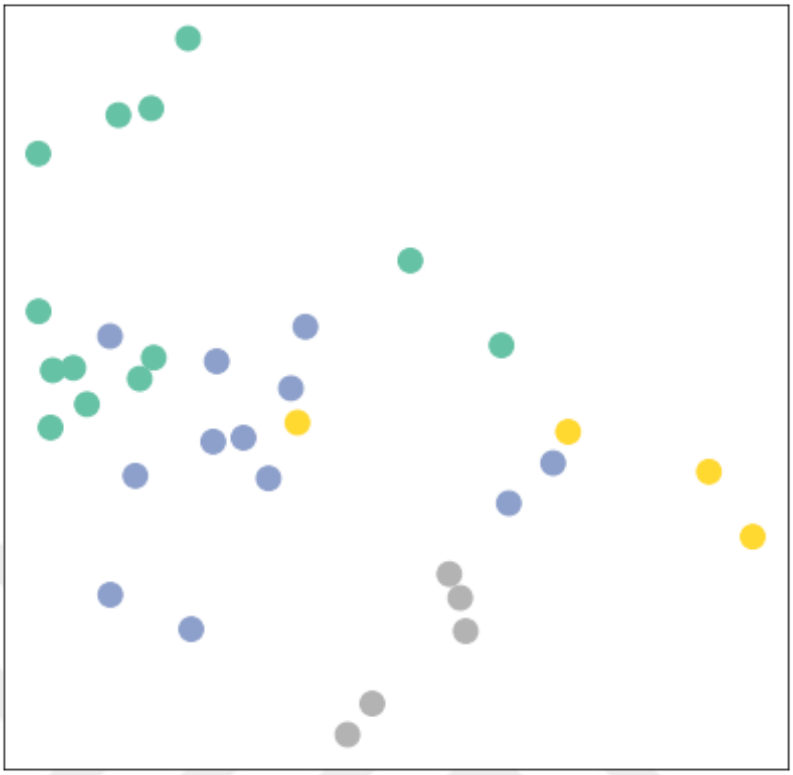
GNN’lere düğüm yerleştirme (embedding) bir diğer önemli konudur. Vektörlerde bir çizelge yapısının temsil edilmesi, kendi kendini denetleyen DeepWalk [325], node2vec [326], LINE [327] ve denetlenen gezegenimsi modellerin [328] geliştirilmesine yol açtı.

Yine, bir veri kümesinin doğrudan ağ olarak çizimi ile yerleştirmelerinin (embedding) çizimini birbirine benzer[26] (**Şekil 3.9:**, **Şekil 3.10:**).

3.3.1. Genel

Çizelge temelli öğrenme metotları genel olarak ikiye ayrılmaktadır [330],

[26] https://colab.research.google.com/drive/1h3-vJGRVloF5zStxL5I0rSy4ZUPNsjy8?#scrollTo=nwHtX5siwe2v



Şekil 3.10: Ağırlık Antrenmanı Olmadan Basit Bir GNN Modeliyle KCD Yerleştirmeleri [329]

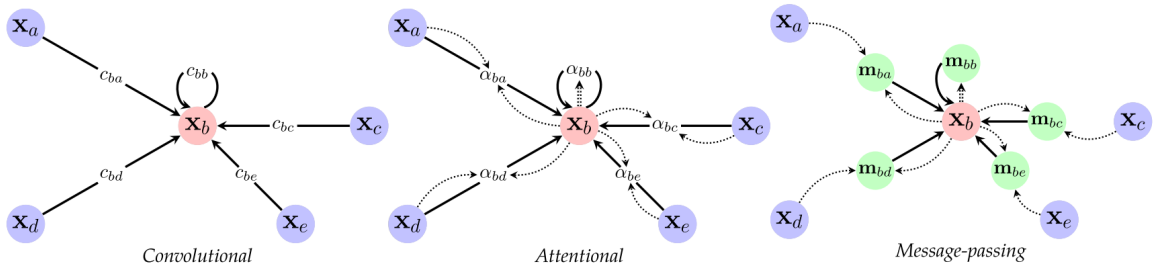
- Laplace düzenlemesine (Laplacian regularization) dayalı yaklaşımlar
- Çizelge düğüm yerleştirmeye (graph embedding) dayalı yaklaşımlar

Laplace düzenlemesine dayalı yaklaşımlar hem çok eski hem de bu tez ile ilgili olmadıklarından üzerinden durulmayacaktır. Ancak bu tezin de kullandığı düğüm yerleştirme metotlarını inceleyeceğiz.

3.3.2. GNN Türleri

Genel olarak GNN yapıları üç ana başlıkta toplanmıştır,

- Evrişimli GNN'ler (CGNN)
- Dikkat temelli GNN'ler (AGNN)
- Mesaj ileten GNN'ler (MPGNN)



Şekil 3.11: GNN Yapıları [312]

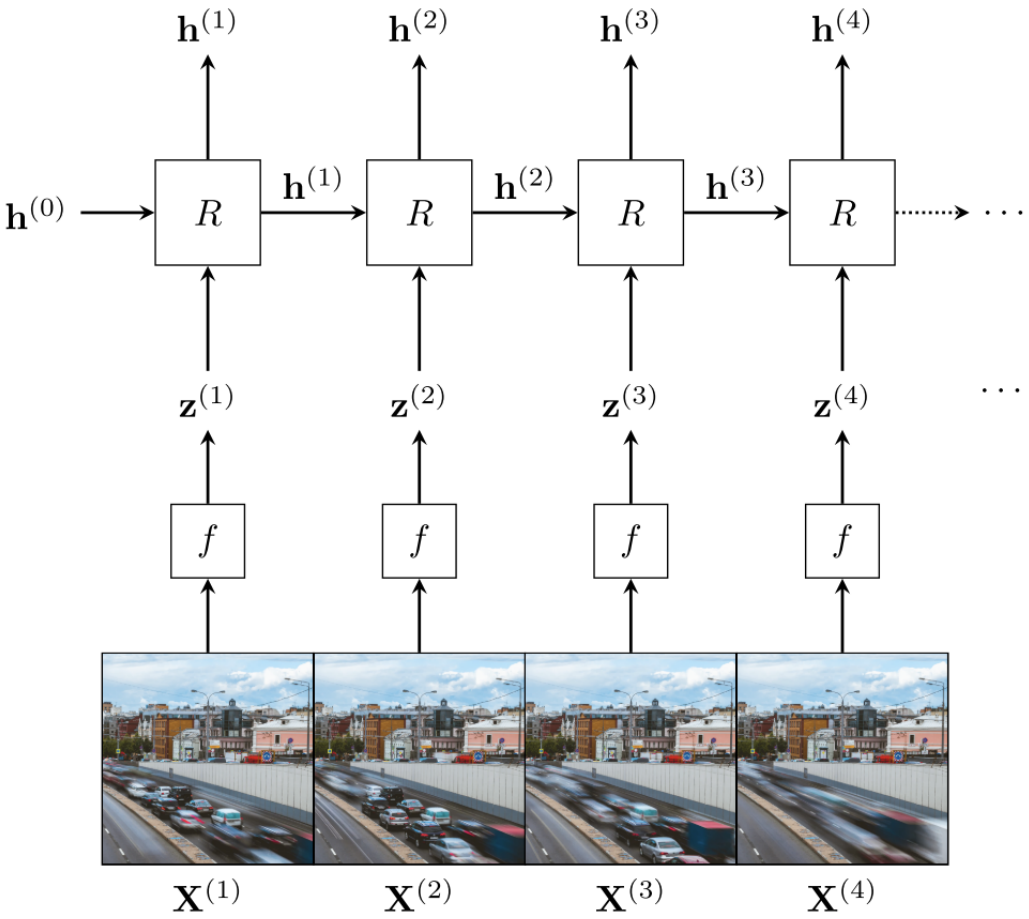
Aralarındaki temel fark Resim **Şekil 3.11:** ile anlaşılabilir. Evrişimli GNN'lerde gönderici nod özellikleri sabit bir değer ile çarpılmaktadır. Dikkat temelli GNN'lerde ise bu değer sabit değildir ancak alıcının gönderici üzerinden hesapladığı bir dikkat mekanizması ile hesaplanır. Mesaj ileten GNN'lerde ise bu değer ise gönderici ve alıcı mesajlarının vektörel olarak hesaplanması ile bulunur. Tüm bu türlerin arasında "evrişimli $\subseteq$ dikkat temelli $\subseteq$ mesaj iletici" şeklinde bir hiyerarşi bulunmaktadır. Ancak bu mesaj iletimli GNN'lerin en iyi tür olduğunu göstermez. Genelde daha çok bellek tüketirler. Yapılan işlemin türüne göre başka çeşit bir GNN daha uygun olabilir [312].

3.3.2.1. Evrişimli GNN'ler (CGNN)

CGNN yapilari evrişimli ANN'lere dayanılarak implemente edilmiştir. Bu nedenle CNN ile ilgili bir kısa giriş için Bölüm 3.2. incelenebilir. ANN yapısı CNN yapıları ile aynı olmakla birlikte, girdi kısımları, örneğin yerleştirmelerle (embedding) CNN'lere uygun hale getirilmiş olabilir. Bu tezin alt yapısı olan EvolveGCN-O da içerisinde bir CNN altyapısı barındırmaktadır.

3.3.2.2. Dikkat Temelli (Attentional) GNN'ler (AGNN)

Dikkat temelli ANN'ler, girid verideki önemli bazı kısımları alıp, kalan önemsiz kısımların unutulması yöntemi ile işleyen ANN yapılarıdır. İşleme alınan gir kısmına dikkat çekildiği için bu ismi almışlar. Bu durum bir bakıma insan gözünün odaklanmasına benzer. Doğal dil işleme (NLP) çalışmalarında bu çok önemli bir özellik olmakta ve yazının bağlamını (context) anladıktan sonra, problemleri çözmede çok kullanılan bir yöntemdir. Bu yöntemi ilk defa çizelge yapılarına uygulayan ise [331] olmuştur.



Şekil 3.12: RNN Çalışma Şekli [312]

3.3.2.3. Mesaj ileten GNN'ler (MPGNN)

İlk olarak [332]'de belirtildiği üzere, CNN'lerde evrişim işlemlerini genelleştirerek, "mesaj gönderme" olarak tanımlayan bir ANN yöntemidir.

3.3.2.4. GNN'leri RNN ile Temporal Hale Getirme

Uzay ve zaman olarak ilerleyen veya daha doğrusu basamaklardan oluşan bir yapı ile karşı karşıya isek, RNN yöntemleri (özellikle LST ve GRU gibi kapılı/gated türleri) temporal bir ANN elde etmemize yardımcı olur. RNN yapılarının basitçe nasıl çalıştığına dair hızlı bir bilgi olarak **Şekil 3.12:** incelenebilir.

Burada görüldüğü gibi, bir $h^{(0)}$ başlangıç vektörü bulunmaktadır ve her bir basamak benzer şekilde bu vektörü güncellemektedir.

3.3.3. Çizelge Yerleştirme Metotları (Embedding)

AI işlemleri vektörel sistemlerde çalıştığından, GNN gibi çok boyutlu verilerin 2 boyutlu vektörel yapıya çevrilmesi gerekebilmektedir. Bu işleme yerleştirme (embedding) denmektedir. Her ne kadar bu tezde ana altyapı olarak kullanılan EvolveGCN modeli GCN ve RNN kullanarak embedding altyapılarını kullanmıyorsa da (GRU çıktısı aslında bir bakıma embedding sayılır), literatürde bulunan birçok modelin yapısında bulunurlar. Daha önce belirtildiği gibi, DeepWalk [325] yönteminden sonra, node2vec [326], LINE [327] ve denetlenen gezegenimsi modelleri [328] geliştirilmiştir. Tez ile ilgili bazıları açıklanacaktır. Ancak UMAP [333] (2018), coreset'ler gibi PCA benzeri boyut küçültme altyapıları da bu işlemler için kullanılabilir. Bu durumda da GNN için bahsedilmekte olan daha çok özellik işlemleyebilme özelliğini devre dışı bırakmış oluruz. Ayrıca [334] kaynağında detaylı bir araştırma bulunmaktadır.

Gram atlama modeli (skip-gram) [335], düğüm yerleştirme yöntemlerinin çoğunun esinlendiği yöntem olmuştur. Skip-gram modeli daha çok doğal dil işleme işlemlerinde kullanılmak üzere geliştirilmiş bir yöntem olmakla birlikte diğer yöntemler için de yol açmıştır denebilir. Asıl amacı günlük olasılığını (log probability) maksimize etmektir.

DeepWalk [325] düğümlerin yerel komşuluğunu tahmini yoluyla yerleştirmeleri (embeddings) öğrenir [330].

LINE [327], DeepWalk'i daha karmaşık rastgele yürüyüşlerle (random walk) ile genişletmiştir.

"structure2vec" ise daha önce sunulan çekirdek yöntemlerinden (kernel methods) iki kat daha hızlı ve 10000 kat daha küçük modeller oluşturma özelliği bulunmaktadır [336]. Yapısal verile için kullanılabildiği için GNN altyapıları ile de kullanılabilmektedir. Çekirdek yöntemleri daha önce çok az sayıda örneklem üzerinde çalışabilirken, structure2vec milyonlarca örneklem üzerinde çalışabilmektedir.

"node2vec" [326], DeepWalk'i genişlik öncelikli arama yöntemleri ile (breadth-first search) ile genişletmiştir.

Yukarıdaki yöntemlerin her bir basamağı ayrı ayrı optimize gerektirir. Rastgele yürüyüş

oluşturma ve yarı denetimli eğitimi içeren çok adımlı bir işlem hattı Denetlenen Gezegenimsi Modeller (Planetoid) modelinde oluşturulmuştur [328].

3.4. UZAY-ZAMANSAL GNN'LER İLE YANLIŞ DAVRANIŞ TESPİTİ

MBD, araç geçici ağı (VANET) işlemleri sırasında bir V2X ağ öğesinin amacını değerlendirme sürecidir. Bir hatalı davranış otoritesi (MBA), bir ağ öğesinin itibarını, uygunsuz davranış raporları (MBR), işbirlikçi farkındalık mesajları (CAM), merkezi olmayan çevresel mesajlar (DENM) veya işbirlikçi algı mesajları (CPM) aracılığıyla gönderilen veriler ve ölçümlerle değerlendirir. Bu mesaj tipleri arasından, tez çalışmaları sırasında anlaşıldığı kadarı ile, en yararlı bilgilere sahip olan MBR'lerdir. MBR, V2X düğümlerinin diğer V2X ağ öğelerinin ve ortamda olabilecek başka tüm nesnelerin algılanması işlemi ardından gönderilir. MBA, böylelikle kendisine gelen tüm raporları toplar ve kötü davranışları değerlendirir. Gerektiği takdirde de, hatalı davranışı sergileyen nesnenin V2X ağına girebilmek için ihtiyacı olan dijital sertifikayı yasaklayacak veya cezalandıracaktır. Böylece düğüm ağa katılamayacak veya en azından aynı kötü amaçlı işlemleri yapamayacaktır. Görüldüğü üzere MBD, IDS'lerle kolay kolay ilişkilendirilemeyen, sertifika bazlı bir siber güvenlik mekanizmasıdır. Klasik IDS'ler çoğunlukla (OSI seviye 3 ve üst katmanlar) veri paketleri üzerinde çalışırken, MBD raporlar veya mesajlar üzerinde çalışır. Bir MBA'nın sahip olduğu tek karşı önlem (mevcut araştırmaların gösterdiği kadarıyla) öğenin itibarını değerlendirmek ve daha sonra bu itibara dayanarak bu V2X öğesini kısıtlamak veya yasaklamaktır.

3.4.1. Giriş

Siber güvenlikle ilgili alanlarda özellikle MBD'de yapay zekâ (AI) yöntemlerinin kullanılması yaygındır. Ancak mevcut tüm veri kümeleri doğrudan GNN'ye veya genel olarak RL'ye uygulanabilir durumda değildirler. Tüm veriler satır bazlıdır; gelen ve giden mesajlar gibi ilişkiler veya bunların ağdaki sayıları belirtilmez. Bu, başlangıç noktası olarak MBD'nin birçok yönünü kaybeder. Yani çok sayıda mesaj gönderen bir öğe pekâlâ kötü niyetli bir öğe olabilir. Bir V2X ağı, ML yöntemlerini daha iyi eğitmek için, kullanılabilecek çok daha fazlasını sağlayabilir. Ayrıca, bazı bilgiler tablo halinde tutulamaması nedeniyle veri kümelerinde filtrelenirler. Bunun dışında V2X operasyonu ister zamanda ister uzayda

olsun geçicidir. İyi bir model bunu dikkate almalıdır. Bu çalışmada, bahsedilen MBD veri kümelerini, herhangi bir GNN algoritmasının kolayca kullanabileceği şekilde yeniden yapılandırmanın bir yolunu öneriyoruz. Bu çizelge veri kümesinin oluşturulması ve bunun MBD'ye geçici (temporal) bir şekilde uygulanması, tezin yapıldığı zaman itibarı ile ve bilinebildiği kadarıyla, yenidir ve literatürde yoktur.

BurST-ADMA [232], Avustralya'nın sürüş alışkanlıklarını temel alan, VeReMi [117]'den ilham alan bir MBD veri kümesidir. Çalışma, benzer veri kümelerini yeniden oluşturmak için kaynak kodunu sunmamıştır, ancak kolayca kullanılabilecek kadar basittir. Bu çalışma ilk önce bir çizelge veri kümesi oluşturmak için BurST-ADMA veri kümesini kullanır. Ardından da, bu yeni oluşturulan veri kümesini, sınıflandırma için bu tez ile geliştirilen özel bir geçici GNN modeline gönderir. Daha sonra görüleceği gibi, ortaya çıkan bazı model metrikleri literatürdeki en iyilerdir.

Bu bölümün yapısı şu şekilde organize edilmiştir;

Bölüm 3.4.2.'de bu çalışmanın neden gerektiği ele alınacaktır. Bölüm 3.4.3.'de ise GNN'ler ve özellikleri hakkında bilgi verilecektir. Bölüm 3.4.4.'de GNN'ler ve MBD ile ilgili çalışmalar ayrıntılı olarak anlatılacaktır. Bölüm 3.4.5., mevcut V2X MBD veri kümelerini ve bunların neden GNN işlemleri için uygun olmadığını açıklayacaktır. Bölüm 3.4.6.'da ise BurST-ADMA veri kümesi, özellikleri, artıları ve eksileri hakkında bilgi verilecektir. Bölüm 3.4.7.'de bu çalışmanın veri kümesi dönüşümünü nasıl yürüttüğüne ilişkin prosedür ele alınacaktır. Bölüm 3.4.8., deneyde kullanılan GNN yöntemini açıklayacaktır. Bölüm 3.4.9., bu çalışmanın kullandığı metrik oluşturma yöntemini ayrıntılı olarak açıklayacaktır.

3.4.2. Motivasyon

Temsili öğrenme, performansı ve kullanım kolaylığı nedeniyle son zamanlarda çok popüler hale gelmiştir. Bu yöntemlerden biri olan GNN de genel bir ML mekanizması olarak oldukça popüler olmuştur. Bu çalışmanın ve diğer araştırmaların önerdiği gibi [289, 312], bunun nedenlerinden bazılarını aşağıdaki gibi belirtmek mümkündür:

1. Tablo formatlarıyla çalışan eski yöntemler, nesneler arasındaki ilişkiyi çok iyi belirtemez. Genellikle yalnızca satır temelli çalışırlar, eldeki temsili kaybederler (ya da kaybetmeye zorlanırlar).

2. Çizelgeler eldeki soruna iyi uyum sağlar ve çok fazla ön işleme gerek kalmadan iyi sonuçlar verebilir. Diğer yöntemlerle veri hazırlamak için çok fazla zaman harcanmasına rağmen GNN'de ham verilerle çok iyi sonuçlar elde edilebilmektedir.
3. GNN tabanlı sistemler gerçek hayata güzel bir şekilde uyum sağlayabilmektedir. İlişkiler ve diğer kavramlarla ilgili önemli verileri yapılarında barındırır ve korurlar.
4. GNN'lerin uzun eğitim dönemlerine ihtiyacı yoktur.
5. Bir V2X yapısı aslında bir çizelgedir ve sonuca etkisi açıktır.
6. Zamansal ve dinamik çizelgeler üzerine yapılan son araştırmalar bu çalışmanın yolunu açmıştır [329, 337, 338, 339, 340]. En önemlisi, bu çalışmada kullanılan [341] zamansal kütüphane, uzay-zamansal GNN yöntemleri için büyük kolaylık sağlamaktadır.
7. Zamansal veri kümesi formatı için standardizasyonda eksiklik vardır. PyTorch'un kendi veri kümesi formatı vardır. Bundan türetilen PyG'nin [342] kendine ait bir yapısı vardır. [341] ise PyG formatını kullanarak yeni bir yapıyı tanıtmıştır. Bunun üzerine bu çalışma daha iyi bir uygulamanın geliştirilmesine yardımcı olacaktır.

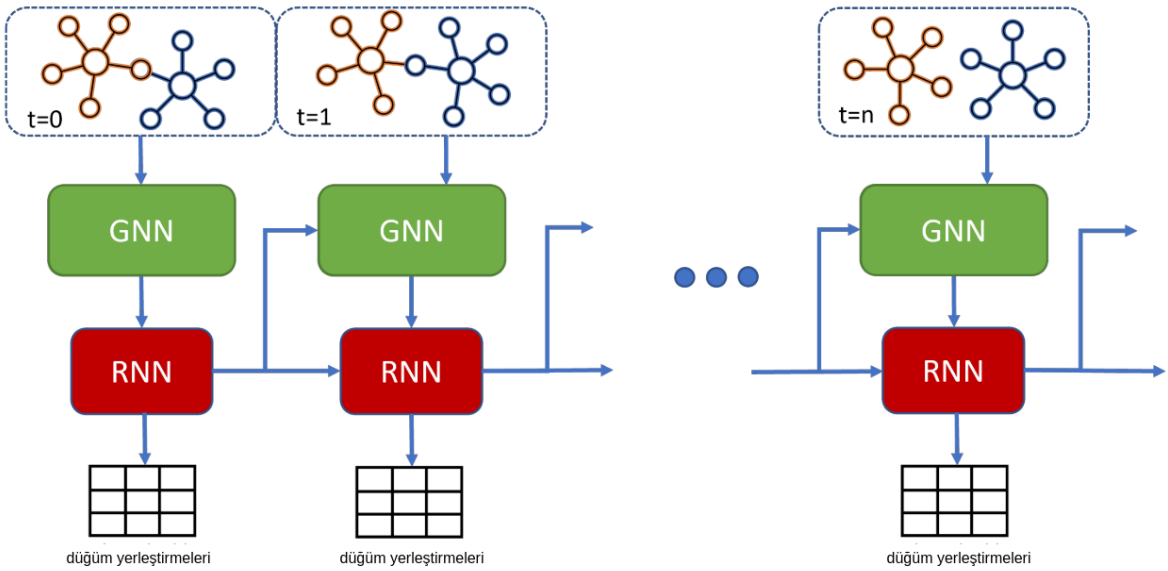
Yukarıda açıklanan öğelerin çoğu, diğer herhangi bir makine öğrenimi araştırması için de iyi bir motivasyon olabilir. Bu çalışmadan da görülebileceği gibi, GNN'ler bizi, içinde daha fazla bilgi bulunan veri kümelerini daha iyi hazırlamaya zorlayacaktır. Bununla birlikte GNN'in iç işleyişi olağan DL işlemlerinden çok da farklı değildir.

3.4.3. Uzay-Zamansal Çizelge Nöral Ağları

GNN ve siber güvenlikle ilgili çalışmalar çoğunlukla IPS/IDS üzerinde yoğunlaşır. Ancak araştırmaların çoğu uzay-zaman özelliklerini hesaba katmaz. Çoğunlukla tablo halindeki bir veri kümesinin satır temelli ML ile işlenmesi üzerinde çalışırlar. Burada çoğunlukla "geçici GNN" ile ilgili araştırmalara ilişkin detaylar verilecektir.

3.4.4. İlgili Çalışmalar

[329]'deki çalışma MBD veya V2X ile ilgili değildir, ancak LANL veri kümesi [343] üzerinde yürütülen geçici bir GNN yöntemiyle ilgilidir. Bu veri kümesi, elli sekiz (58) günlük

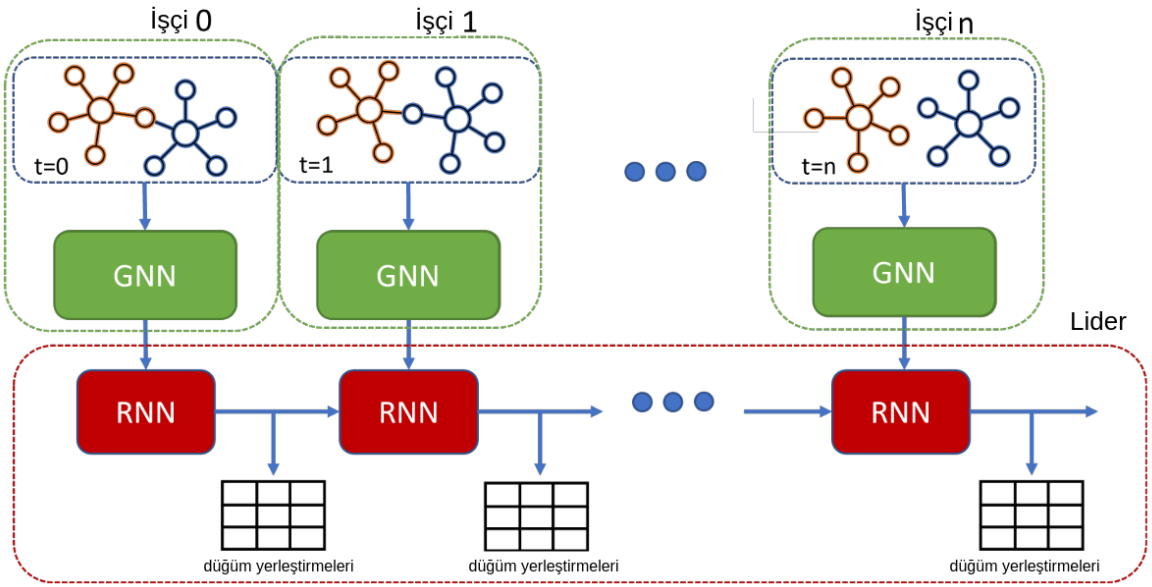


Şekil 3.13: [329]'deki Sıralı Zamansal Bağlantı Tahmincileri

ağ verilerine, Etki Alanı Adı Hizmeti (DNS) aramalarına ve ağ akışlarına ilişkin kimlik doğrulama olaylarını içerir. Çalışma, bir iç bilgisayar ağındaki yanal (birlikte meydana gelen) hareketler üzerine yoğunlaşmıştır. Çalışmanın ilginç bir yönü de PyTorch kütüphanesinin dağıtık hesaplama özelliklerini kullanmasıdır. Bu şekilde büyük veri kümeleri dağıtık hesaplamayla işlenebilir. Çalışma, veri kümesinin zamansal yapısından dolayı (diğer araştırmaların çoğunda olduğu gibi) tekrarlayan sinir ağlarını (RNN) kullanıyor. RNN işlemlerinin performansa ihtiyacı daha azdır ve ana işlem üzerinde çalışır. İşin paralel kısmı GNN operasyonlarıdır.

[344]'deki çalışma GNN tabanlı bir IoT IDS'dir. Çalışma, GNN'yi düğüm yerleştirme (embedding) oluşturucusu olarak kullanıyor (bu, GNN'nin çok kullanılan bir özelliğidir). Daha sonra, bir ağ IDS'sini (NIDS) simüle etmek için kendi özel E-GraphSAGE yöntemini kullanır. E-GraphSAGE, Graph SAmple and aggreGatE (GraphSAGE) yöntemi [345]'ün genişletilmiş versiyonudur ve bu da çizelge öğelerinin örneklenmesine dayanır.

[337]'deki çalışma MBD ile ilgili değildir ancak zamansal özellikleri bir V2X işleminin bunlardan nasıl yararlanabileceğini göstermektedir. Çalışma, daha iyi kaynak kullanımı elde edebilmek için yol kenarı birimleri (RSU) üzerinde trafik akışını tahmin etmeye çalışır. Çalışma, karmaşık trafik akışı özelliklerini yakalamak için kişisel dikkat ağını (self attention network, SAT) temel alan ST-GDN'yi önermektedir. Diğer birçok araştırmada olduğu gibi tam bir GNN çözümü değildir. Daha iyi bir çözüme ulaşmak için birden fazla yöntem



Şekil 3.14: Paralel Çerçeve [329]

birbirine bağlanır. Diğer benzer çalışmalar [338, 339, 340], aynı trafik akışı tahmini için GNN yöntemlerinin zamansal özelliklerini kullanır.

3.4.5. Mevcut V2X MBD Veri Kümeleri

Bu tezde MBD ile ilgili çalışmalarda kullanılabilecek en uygun açık kaynak veri kümelerinin;

- VeReMi [117]
  - VeReMi-Extension [118],
  - F^{2}MD [122],
- BurST-ADMA[232]

olduğu görülmüştür. VeReMi, bir veri kümesini yeniden oluşturmak için gereken hem veri kümesini hem de altyapıyı sağlar. Öte yandan BurST-ADMA, Avustralya için VeReMi'den ilham alan uyarlanmış bir veri kümesidir. Ancak BurST-ADMA, çoğaltılması için açık kaynaklı bir yazılım sağlamamaktadır. **Tablo 3.1:** içerisinde veri kümeleriyle ilgili tezin ulaşabildiği son durum görülebilir.

Tablo 3.1: MBD Veri Kümeleri

Çalışma	Veri Kümesi	Sim.	A.K.	Göst.	CPM	Çizg.	Bölge
[117]	VeReMi (2018)	Veins	✓	✓			ABD
[122]	Dinamik (F^2MD) (2020)	Veins	✓	✓			ABD
[118]	VeReMi-Extension (F^2MD) (2020)	Veins	✓	✓			ABD
[121]	MISO-V (2021)	CARLA			✓		Avrupa
[120]	(+F^2MD) (2022)	ARTERY			✓		Avrupa
[232]	BurST - ADMA (2022)	SUMO	✓				Avrupa
[52]	iLDM (2022)	SUMO			✓	✓	Avrupa
[55]	S-LDB (2022)	ms-van3t	✓		✓	✓	Avrupa

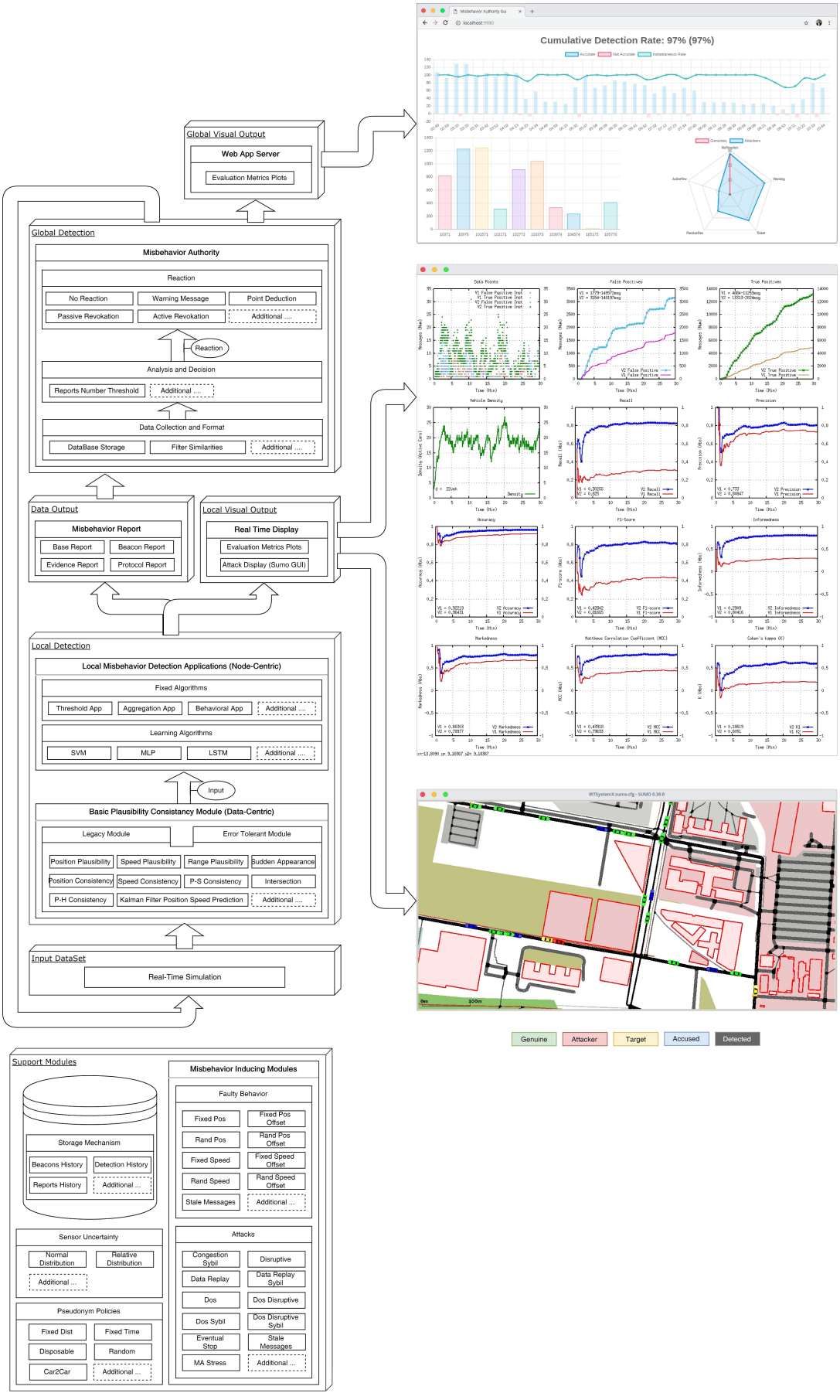
- **Göst.**: Gösterim
- **A.K.**: Açık kaynak
- **Sim.**: Simülatör
- **Çizg.**: Çizelge Temelli

Tabloda bulunan Kolektif Algı Mesajı (CPM), standartlardaki yerini yeni bulmaktadır ve halen geliştirilme aşamasındadır [32, 57]. Bu tezden sonra bir takip araştırması için çok iyi bir adaydır. CPM'ler, CAM/DENM mesajları veya kendi altyapılarıyla (CPM) iletilecek ve paydaşların çevre ve V2X ortamındaki tüm nesneler hakkındaki görüş veya hislerini belirtecektir. Ayrıca belirtilen çizelge temelli yapılara destek ise sadece LDM sistemlerinde bulunabilmiştir.

Ayrıca, BurST-ADMA, VeReMi ve VeReMi-Extension arasındaki farklar için **Tablo 2.35:** incelenebilir.

F^2MD (Yanlış Davranış Tespiti Çerçevesi) [122] ile oluşturulan VeReMi-Extension veri kümesi, araştırmacıların yeni özellikleri ve yöntemleri kullanarak kolayca MBD yazılım çerçeveleri (framework) geliştirmelerine olanak tanır. F^2MD'nin genel yapısı **Şekil 3.15:**'de gösterilmektedir.

Literatürde MBD için GNN tabanlı yöntemlerin eksikliği görülmektedir ve bu çalışma GNN'nin mevcut veri kümelerine nasıl uygulanacağına dair bir yöntem gösterecektir. Bu tez kolaylığı ve birleşik yapısı nedeni ile referans olarak BurST-ADMA'yı seçmiştir. Ardından üzerinde, teze özel geliştirilen bir GNN yöntemini de belirtecektir.



Şekil 3.15: F^{2}MD Sistem Modeli

Tablo 3.2: BurST-ADMA İstatistikleri

Tip	Toplam	Adet	Yüzdelik
Bisiklet	134	44999	21.71
Otobüs	116	25803	12.45
Motosiklet	93	11675	5.63
Yaya	141	68162	32.88
Toplu Taşıma Otobüsü	5	1944	0.94
Toplu Taşıma Tramvay	10	3656	1.76
Kamyon	116	27013	13.03
Binek Araç	115	24063	11.61
Toplam	**730**	**207315**	**100**

Tablo 3.3: BurST-ADMA Etiketleri

Etiket	Tip	Adet	Yüzdelik
0	Normal	179126	86.40
1	Sabit Rastgele Konum	2110	1.02
2	Pozitif Pozisyon Ofseti	4130	1.99
3	Negatif Konum Ofseti	4512	2.18
4	Sabit Rastgele Hız	4106	1.98
5	Pozitif Hız Ofseti	4720	2.28
6	Negatif Hız Ofseti	4755	2.29
7	Ters Yönde Gidiş	3856	1.86
Toplam		**207315**	**100**

3.4.6. BurST-ADMA Veri Kümesi

BurST-ADMA Veri Seti, Avustralya'nın bir banliyö kasabası için yapılan simülasyona dayanmaktadır. Bu veri kümesinde bulunan sekiz tür V2X öğesi ve bu öğelerin veri kümesindeki frekansları **Tablo 3.2:** içeriğinde belirtilmiştir. **Tablo 3.3:**'de tanımlandığı gibi etiket olarak tanımlanan hem normal hem de saldırı tip kayıtlarına sahiptir.

Veri kümesi bir simülasyon sonucudur, dolayısıyla uzay (konum bilgisi alanları) ve zamanda (zaman basamağı alanı) geçici (temporal) bir veri kümesi olarak kullanılabilir. Bin adıma bölünmüştür ve her adımda yeni eleman türleri devreye girebilmekte veya kapsam dışına çıkabilmektedir. Ayrıca her bir adımın satırında, konum ve etiket bilgisi de verilmektedir.

3.4.6.1. BurST-ADMA Eleştirisi

Bu tezde kompakt yapısı ve hafif boyutu nedeniyle BurST-ADMA veri kümesi kullanılmıştır. Ancak geliştirme aşamasında görüş olarak şu değerlendirmeyi belirtmek gerekmektedir;

- Veri kümesindeki tüm alanlar bir sınıflandırma işlemiyle ilişkili değildir. Basit bir Weka[27] öznitelik seçimi (CfsSubsetEval/prensip bileşen analizi, PCA), özelliklerin bir sadece alt kümesinin aslında önemli olduğunu belirtir.
- Çok kolay ve hafif bir veri kümesi olduğundan, üzerinde daha fazla araştırma kolaylıkla yapılabilir.
- Az sayıda alana sahiptir, ancak daha önce de belirtildiği gibi, en azından bir karar ağacı (DT) sınıflandırmasında, sınıflandırma için tüm alanlara ihtiyaç yoktur veya bu alanlar gerekli etkiyi göstermemektedir.
- Zaman sırasında düğümlerin ilişkisi hakkında fazla bilgi yoktur. Böylece ilişkiler ve mesajlar kaybolur veya belirtilemez.
- Görünüşe göre orjinal makale [232]'da kullanılan DT veya rastgele orman (RF) algoritması, ilgili diğer çalışmaların çoğunda olduğu gibi, düğümün "id'si" ile yapılmaktadır. Böylece çok yüksek model performansı elde etmek daha kolay olmaktadır. Bu alan kullanılmadığında ise, Weka'da, sadece bir model oluşturmak için, üç kat fazla zaman gerekmektedir. Buradaki "id" özelliği, görüldüğü gibi aşırı eğitime neden olmaktadır.

Yukarıdaki eleştirilerin tümü, veri kümesinin kullanılacak en iyi veri kümesi olmayabileceğini, ayrıca her satırın sınıfıyla iyi bir ilişkiye sahip olmayabileceğini göstermektedir. Ancak yöntemimiz bunun üstesinden gelip oldukça iyi bir çözüm üretebilmiştir.

3.4.7. Veri Kümesi Dönüşümü

Bu çalışmada, geçici bir GNN veri kümesi elde etmek için BurST-ADMA, öncelikle bin adet zaman adımını belirten bin farklı veri kümesine bölünmüştür. Buna karşılık,

[27] https://git.cms.waikato.ac.nz/weka/weka

her yeni veri kümesi, bir mesafe ölçüsü (DM) kullanılarak bir K-En Yakın Komşu Algoritması (KNN) kullanılarak kendi içinde kümelenmiştir. Bu çalışmada sadece Öklid uzaklığı kullanılmış olup Monte Carlo, Hamming, Manhattan, Minkowski uzaklıkları da kullanılabilirdi. Hamming mesafesi, veri kümesinde mevcut alanların bir alt kümesi kullanılarak oluşturulabilirdi. Manhattan, V2X'teki sinyal özellikleri nedeniyle iyi bir DM olmayabilir. Veri kümesi düğümler arasında bir ilişki ölçüsü içermediğinden çizelge kenarlarının oluşturulması sorunludur. Ancak uzaklık ölçüsünü ve kümeleme kullanarak elimizdeki bilgilere göre kenarlar oluşturabiliriz. Bu çalışma, oluşturulan kenar sayısına bir üst sınır koyar. Herhangi bir zaman adımında bir kümede dört yüze kadar öğe bulunabilir. Her bir elemanın diğer elemanlara bağlanması binlerce kenarla sonuçlanacaktır. Dolayısıyla bu yararlı bir sonuç doğurmayacaktır. Bu nedenle bu tez, her biri, kümedeki kenar sayısında bir sınıra sahip olan birçok veri kümesi oluşturmuştur. Bir kümedeki maksimum kenar sayısının 0,1,2,3,4,5,50,100,150,200 veya 10000 (on bir veri kümesi) olmasına karar verilmiştir. Böylelikle, yeni bir veri kümesinden en iyi sonucu elde etmek için birçok başka veri kümesi sağlanmış olmaktadır.

Algorithm 1 Veri Kümesi Dönüşümü Birinci Aşama: Küme Oluşturma

```
EN_FAZLA_KÜME= 10
for Each zaman_basamağı i do
    KÜME_SAYISI= min((uzunluk(elamanlar(i))/3+1),EN_FAZLA_KÜME)
    KMeans kullanarak en fazla KÜME_SAYISI küme oluştur
    Küme bilgileriyle birlikte tüm adımları belirli bir dosyaya yaz
```

Bu veri oluşturma modelinin ilginç bir yönü, kendi kendine döngü kenarlarıdır (SLE). Özellikleri kenar ağırlıkları olarak almak bilinen bir yöntemdir [346]. Bu yöntemde, çizelge üretimiyle doğrudan ilgili olmayan geri kalan tüm özellikler, SLE'ler olarak veri kümesine entegre edilir, böylece tüm veriler temsil edilir. Her özellik için, kenar ağırlığı değeri özellik değeri olacak şekilde bir SLE eklenir. Ayrıca denemeler sırasında negatif değerli veya bulunmayan (NaN) özellikler GNN eğitimi için sorun olacaktır. Eğitim sırasında bazı negatif değerli veya eksik özellikler varsa, tüm tahmin değerleri NaN olur ve bu da eğitim sürecinin aniden durmasına neden olur. Bu sorunun üstesinden gelmek için eksik özellikler (hızlanma veya ilerleme gibi) 0,0000001 olarak alınır. Negatif değerli özellikler için, özelliğin tüm veri kümesindeki minimumunun mutlak değeri değerlere eklenecektir. Bu kaydırmayla tüm özelliklerde minimum sıfır değeri kullanılmış olur.

Algorithm 2 Veri Kümesi Dönüşümü İkinci Aşama: Geçici GNN Formatı

```
for kenaradedi in [0,1,2,3,4,5,50,100,150,200,10000] do
    for Each zaman_basamağı i do
        Veri Kümesindeki Tüm Özellikler için Kendi Kendine Döngü Kenarları Ekleme
        for kume in zaman_basamağı i do
            for j in kume do
                for k in kume && nod k düğüme eşit değil j && nod k henüz işlenmedi do
                    j ile k arasındaki mesafeyi bul && kenar ağırlığı yap
                    if kümedeki mevcut kenarlar > kenaradedi then
                        küme için dur, sonraki kümeye git
    Bir json dosyasına (dataset_< kenaradedi >.json) kayıt yap
```

3.4.8. GNN Yöntemi

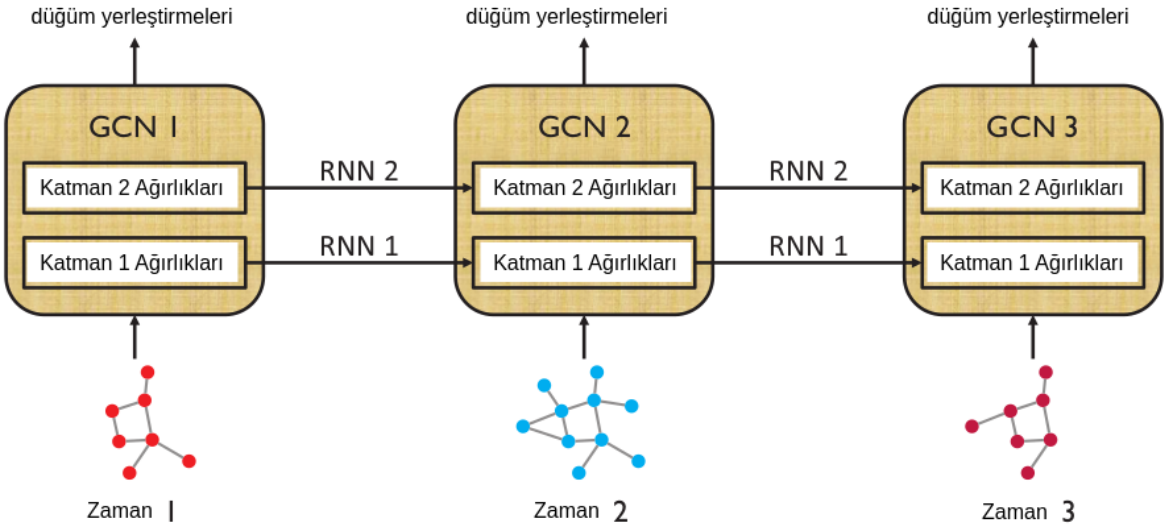
Bir GNN yapısına veri kümesi yükleyebilmek için [341]'daki su çiçeği veri kümesi yükleyicisinden esinlenerek BurST-ADMA veri kümesi benzer yöntemlerle entegre edilmiştir. Su çiçeği veri kümesindeki gecikmeler, yükleyicideki zaman gecikmeleri haline gelmiştir.

Eğitim için, bu tez [347] (DCRNN) ve [348] (EvolveGCN)'den ilham alan ve [341]'da uygulanan bir özel GNN yöntemi kullandı. EvolveGCN iki benzer yöntem sunar; 'EvolveGCN-O' ve 'EvolveGCN-H' (**Şekil 3.16:**). Bu tezde, yinelenen bir katman olarak EvolveGCN-O kullanıldı ve üç evrişim katmanı daha eklendi. Doğrusal olmayışı (nonlinearity) artırabilmek için her evrişim katmanı arasında girdilere hiperbolik tanjant (tanh) uygulanmıştır. Ayrıca, [321]'de açıklandığı gibi nöronların ortak adaptasyonunu daha iyi düzenlemek ve önlemek için %50 olasılıkla bir kesinti (dropout) vardır.

EvolveGCN-O, **Şekil 3.17:**'da belirtildiği gibi ek bir havuzlama katmanı (TopKPooling [320]) kullanır.

Çizelgede, yöntem çift yönlü rastgele yürüyüşler kullanarak uzaysal bağımlılığı yakalıyor. Ayrıca kodlayıcı-kod çözücü (encoder-decoder) mimarisi örnekleme ile zamansal bağımlılığı yakalar. Bundan başka [330] (GCNConv_Fixed_W)'da tanımlandığı gibi evrişimli bir işleme katmanına sahiptir. GNN modelinin tamamı **Şekil 3.18:**'de verilmiştir.

Şekil 3.16:'de de bir özet verilmiştir. Bu tezin ana katkısı, **Şekil 3.18:**'den görülebileceği

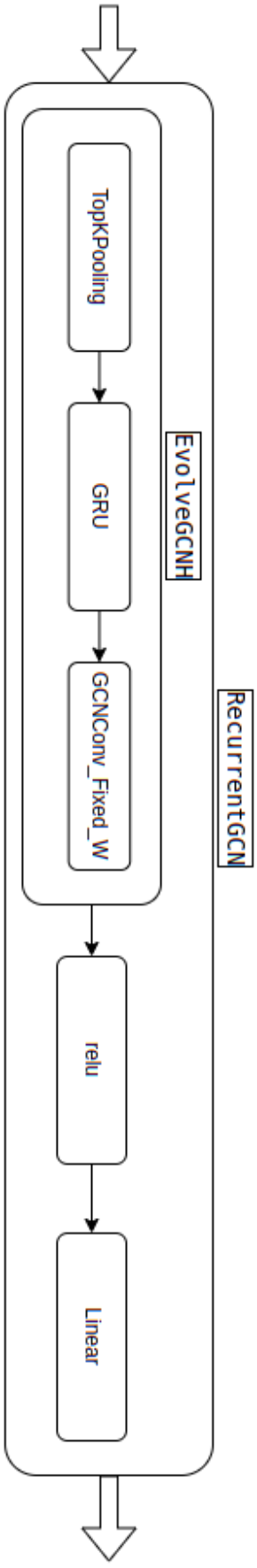


Şekil 3.16: EvolveGCN Modeli

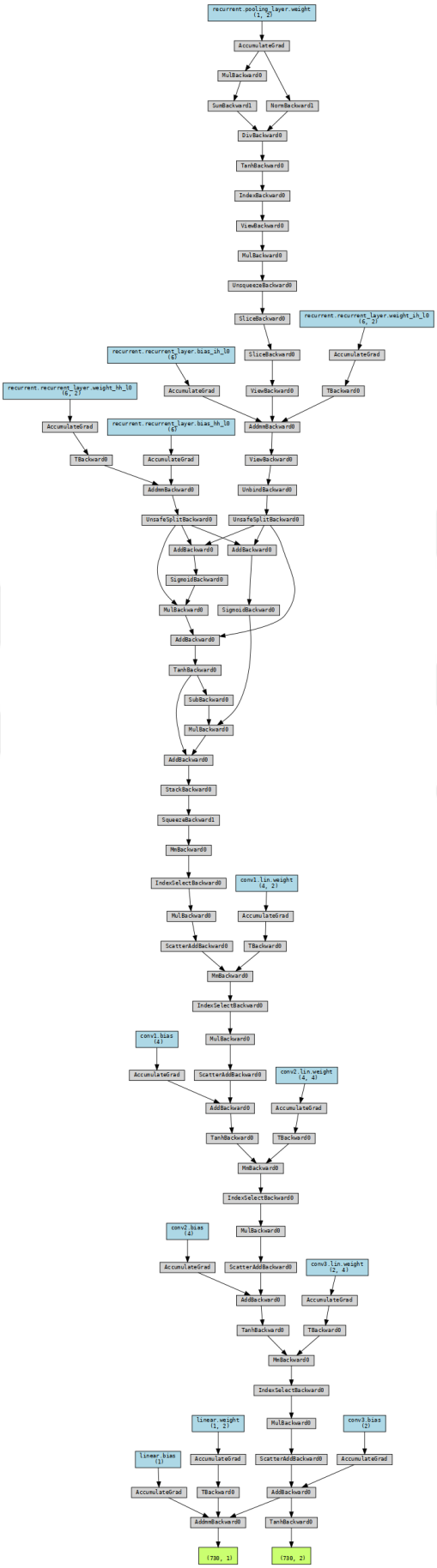
gibi, yöntemin hem RNN kısmında hem de çizelge evrişimi (GCN) kısmındadır. Son olarak kullanılan GCNConv katmanı [330]'dan alınmıştır.

3.4.9. Performans Metrik Oluşturma

Veri kümelerinin geçici (temporal) yapısından dolayı, işlemler sırasında oluşturulan metrikler, doğrudan, diğer makine öğrenimi işlemleriyle ilişkili değildir. Diğer yöntemler genellikle tek bir veri alıp bu veri üzerinde çalışır ve metriklerini kolayca hesaplayabilir. Bu, ünlü PyTorch kütüphanesi de dahil olmak üzere birçok kütüphanede 'verilen', zaten var olan bir durumdur. Temporal durumda, her zaman adımının kendi ölçümleri hesaplanır ve sonunda tüm ölçümlerin bir şekilde toplanması ve ortalanması gerekmektedir. Şu ana kadar, bu çalışmanın kullandığı kütüphane olan [341]'da sağlanan temporal metrik hesaplamaları yalnızca ortalama kare hatasını (MSE) içermektedir. MSE iyi bir metriktir ancak yeterli değildir. Bu çalışmada, [341]'da kullanılan MSE'ye benzer bir yöntem kullanılarak, bu çalışma doğruluk (accuracy), F1-Score, hatırlama (recall), kesinlik (precision) ve Matthews Korelasyon Katsayısını (MCC) hesaplamak için yeni bir yöntem sunulmaktadır. Bunlardan başka herhangi bir ölçüm türü de entegre edilebilir, ancak bu çalışma bağlamında, bunlar, yalnızca diğer GNN dışı yöntemlerle karşılaştırma amacı ile yeterli görünmektedir. Tanımlama 3.4.9.1'de basitçe bu işlemin nasıl yapıldığı belirtilmiştir. Bu tez kapsamında diğer metriklerin hesaplanmasında MSE'ye benzer bir yaklaşım benimsendiği belirtilmişti. Yani her adımda, o adıma ait tüm metrikler hesaplanır ve ardından elde edilen metrik olarak ortalama bir değer olarak alınır.



Şekil 3.17: EvolveGCN Ardışık Modeli



Şekil 3.18: Önerilen GNN Modeli

Tanımlama 3.4.9.1 $(\sum_{n=1}^{\#Zaman\_adimlari} metrik)/\#Zaman\_adimlari$

Metrik oluşturmanın asıl amacı, kullanılan kütüphane içerisinde benzer bir yöntemin olmaması nedeni iledir. Ancak bu yapılırken de, tekerleği yeniden icat etme gibi yönteme girilmemiştir. Literatürde bulunan metrik hesaplama yöntemleri temporal verilere uygulanmıştır. Asıl amaç ise bunu tez sonrası açık kaynak olarak yine aynı kütüphaneye entegre etmektir.

Bölüm 3.4.7.'de tanımlandığı gibi, her zaman adımındaki temporal veri kümesi, tahmin edilecek tüm düğümleri içermektedir. Her ne kadar tüm düğümler o zaman adımında mevcut olmasa bile, matris hesaplamaları açısından bu gerekli bir durumdur. Örneğin bir zaman adımında beş (5) düğüm varsa (simülasyon o adımda olduğunda), henüz mevcut olmayan yedi yüz yirmi beş (725) düğümün tamamı simülasyona eksik olduklarını belirten bir mekanizma ile eklenir. Dolayısıyla GNN, diğer mevcut olmayan düğümlerle birlikte bir sınıf tahmininde bulunsa bile doğruluk o düğümde $4/730 = 0,5\%$ (binde 5) olmalıdır. Bu, alışılagelmiş temporal olmayan yöntemlerden daha iyi bir performans elde etmenin önünde bir engeldir. Bir fikir vermek gerekirse, BurST-ADMA veri kümesi için, eğer GNN her adımda yalnızca mevcut olmayan düğüm sınıflarını da tahmin ediyorsa (çünkü onların yeri matriste mevcuttur), o zaman sondaki ortalama doğruluk %70 'e yakın bir değer olacaktır. Ancak % 99'luk bir doğruluk değeri, (geçici) GNN'lerin daha iyi performans elde etmek için çok daha fazla alana sahip olduğu anlamına gelmektedir. Ancak GNN'nin bu kötüleştiren engeli aştığı görülmektedir.

4. BULGULAR

Bu bölümde, tezin uyguladığı modelin GNN'lerle yapılan denemelerin ayrıntıları incelenecektir. Tezde iki tür deney yürütülmüştür. 3.4.7. bölümünde bahsedilen ve yeni oluşturulan veri kümeleri, ilk deneyde, **Şekil 3.17:**'da tanımlandığı gibi EvolveGCN-O ile işleme tabi tutuldu. İlk işlemde EvolveGCN-O'da hiçbir şey değiştirilmedi ve (mevcut) bir GNN yöntemi ile performans araştırması adına bir çalışma yapıldı. Böylece tez, yöntemin geliştirilme amacı ile iyi bir yol olup olmadığına karar verecekti. İlk denemeler GNN altyapısının oldukça iyi bir performans sergilediğini gösterdi. Ardından da, **Şekil 3.18:**'de tanımlandığı gibi modelin geliştirilmesine geçildi. Yeni geliştirilmiş model kullanılarak da ikinci bir benzer deney daha gerçekleştirildi. Her sonuç ve algoritma aşağıda kendi alt bölümünde tanımlanmıştır.

4.1. MEVCUT EVOLVEGCN MODELİ İLE İLK DENEY

3.4.7.'de belirtildiği gibi, veri kümesi dönüştürme işlemi yapılırken, çeşitli parametreler kullanılarak, tek bir veri kümesinden birçok farklı GNN veri kümesi oluşturulmuştu. Ancak yeni veri kümelerinden hangisinin en iyi performansı vereceğini bilmek gerekmekte idi.

En iyi veri kümesi oluşturma yöntemini bulmak için çalışmalar sırasında, Algoritma 2'de oluşturulan her veri kümesini farklı parametrelerle eğitme işlemi yapıldı. Aslında bir bakıma bu bir hiper parametre uzayı bulma araştırması olmuştur. Her veri kümesi, seçilen uzaklık ölçüsüne (bu çalışmada Öklidyen) göre farklı bir 'kenar sayısı' ile oluşturulmuştur.

Algorithm 3 En İyi Veri Kümesini (En İyi Kenar Sayısı), Yapım Parametrelerini (En İyi Gecikme Sayısı) ve En İyi Eğitme Oranını Bulma

1: **for** Each *kenaradedi* in *[0,1,2,3,4,5,50,100,150,200,10000]* **do**
2: - Verikümesi_<*kenaradedi*>.json için veri kümesi yükleyicisini başlat
3: **for** Each *gecikmeadedi* in *range(1,21)* **do**
4: -Veri kümesini *gecikmeadedi* gecikmelerle yükle.
5: **for** Each *eitim_oranß* in *aralık(0.1,1)* **do**
6: -Eğitimi **Şekil 3.17:**'de belirtilen yöntemle çalıştır
7: - Bu aşama için performans ölçümlerini topla
8: En iyi parametre alanını bul

Tablo 4.1: İlk Deneyden Elde Edilen En İyi Hiper Parametre Uzayı

Metrik	**Değerler**
Bir kümedeki maksimum kenar sayısı	1,2,3,4,5
Yükleme sırasındaki gecikme sayısı	0,2,15,16,17,18
Eğitim Oranı	10%, 20%, 30%, 40%

Tablo 4.2: Makro Performans Hesaplama Sonuçları ile Mevcut Bir Modelle İlk Deney

Metrik	**[232]**	**B.T.**
Hassasiyet	0.9988	0.9875
Hatırlama	0.9775	**0.9873**
F1-Skoru	0.9875	0.9810
Doğruluk	0.9963	0.9589

- **B.T.**: Bu Tezdeki İlk Deney Sonucu

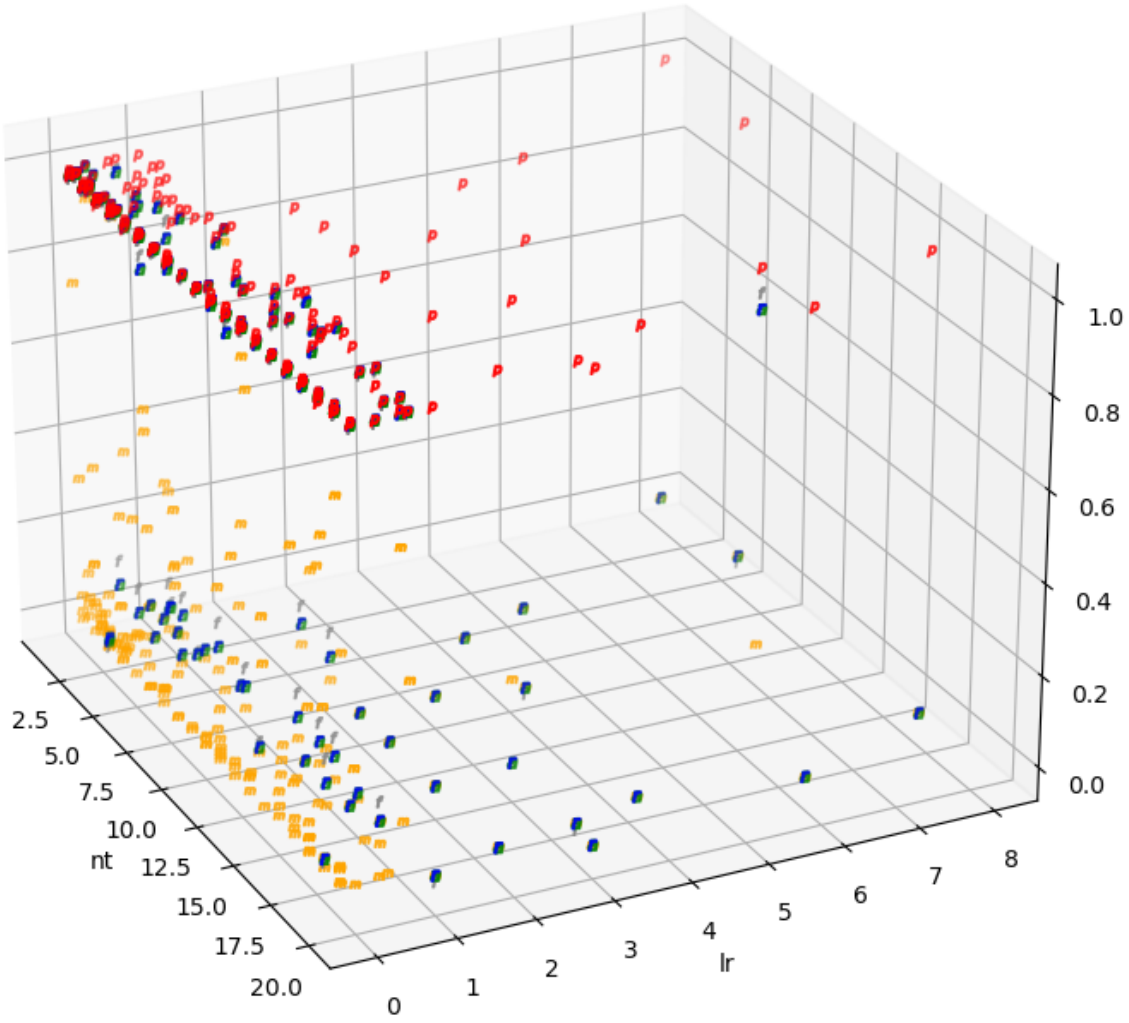
Toplamda değerlendirme sayısı 2079 sayısına ulaşmıştır. En iyi sonuçlar (en iyi parametre alanı) ise **Tablo 4.1:**'de açıklanan metrikler etrafında toplanmıştır.

Deneyden sonra sonuçlar çoğu ölçümde tatmin ediciydi ve hatırlama ölçümünde var olan sonuçlarda daha iyi bir sonuç bulunmuştu. Bu, teze, **Şekil 3.18:**'de tanımlandığı gibi aynı işlemi yeni bir modelle tekrarlamak için büyük bir teşvik anlamına gelmiştir. Burada iki önemli konu, iki adet hiper parametredir: eğitim oranı ve gecikme sayısı. Deney sırasında küçük eğitim oranlarıyla çok iyi sonuçlar elde edilmiş, ancak literatürle karşılaştırma yapmak gerektiği için bu çalışmada kullanılan eğitim oranı son deneyde %70 olmuştur. Öte yandan, eğitim aşamasında tahmin yapmak için gecikmeler kullanılmaktadır. Her ne kadar bir tasnif veya sınıflandırma işlemi için gerekli olmasa da bu çalışmada değerli görülmüştür. Sonuçta, bu hiper parametre mümkün olduğu kadar küçük bir değer olarak, (bir), alınmıştır.

Ölçümler, ilgili çalışmada [232] genel performans veya destek değerleri sağlanmadığından, her veri kümesinde, etiket performansı olarak ortalama (makro) alınmıştır.

4.2. ÖNERİLEN MODEL İLE İKİNCİ DENEY

Yeni modelle yapılan ikinci deney beklentileri aşmıştır ve performans ölçümlerinin yarısında en iyi sonuçları vermiştir. Ayrıca MCC, modelin veriler üzerinde ne kadar iyi performans gösterdiğini tanımlamak için kullanılmıştır.



Şekil 4.1: Hiper Parametre İnce Ayarı

- **nt**: Eğitim sayısı (dönemler)
- **lr**: Öğrenme oranı
- **a,r,p,f**: Doğruluk, geri çağırma, kesinlik, F1 puanı
- **m**: MM

Tablo 4.3: Hiper Parametreler

Hiper Parametre	**Değerler**
Veri Kümesi	BurST-ADMA
Yöntem	Geliştirilmiş GNN EvolveGCN-O
Tekrar Sayısı	1-20
Gecikme Sayısı	1-21
Kenar Sayısı	0-10000
Eğitim Oranı	70%
Öğrenme Oranı	0,0001-9
Gözlem Sayısı	207315
Optimize Edici	Adam
Doğrulama	%30 Test Kümesi
Özellik Seçimi	Tüm özellikler
Eğitim Süresi Sınırı	Yok
Kayıp Fonksiyonu	MSE

Şekil 4.1:, hiper parametre ayarlamasını nasıl yaptığımızın küçük bir bölümünü göstermektedir. Sonuçların sol üst köşesi en iyi ölçümlerin oluşturulduğu bölge olarak göze çarpmaktadır. Dolayısıyla en iyi sonuçları bulma süreci bu değerlerle başlamalıdır. **Şekil 4.1:**'den çıkarılabilecek sonuçlar aşağıdaki gibidir;

1. Neredeyse her eğitim sayısında (1'den 20'ye kadar) iyi sonuçlar alınmıştır. Bu kısmen gradyan iniş (gradient descent) algoritması ve yerel minimum (local minimum) döngülerle ilgilidir. Ayrıca, önceki açıklamalara ek olarak, küçük eğitim sayılarının hala iyi sonuçlar verebileceğini belirtmek gerekmektedir.

2. Bu veri kümesi için öğrenme oranı 0,007 kadar küçük olmalıdır

Tablo 4.4:'den görülebileceği gibi, V2X ağlarındaki bir öğenin kötü niyetli olup olmadığına karar vermede daha iyi bir performans sergilemiştir. Bu, insan hayatının ne pahasına olursa olsun güvende tutulması gereken V2X gibi gerçek zamanlı ağlarda daha da önemli olmaktadır.

Tablo 4.5:, **Tablo 4.6:** ve **Tablo 4.7:**, "torch.autograd.profiler.profile(use_cuda=False)" kullanılarak oluşturulmuştur. Oluşturulan değer 100 adet deneme ardından çıkan değerlerin ortalaması olarak alınmıştır. Bu denemelerin istatiksel sonuçları **Tablo 4.8:** içerisinde belirtilmiştir.

Tablo 4.4: İkinci Deney Sonuçları

Metrik	**[232]**	**[349]**	**[350]**	**[351]**	**B.T.**
Doğruluk	0.9963	0.9960	0.9890	0.9989	**0.9992**
F1-Skoru	0.9875	-		0.9998	0.9988
Hatırlama	0.9775	-	-	0.999147	**0.999196**
Hassasiyet	0.9988	-	-	1 (**C**)	0.9993
İşlem Karmaşıklığı (Tahminde)	-	-	-	1270 ms	**518.91 ms**
MCC	-	-	-	-	0.9735

- **B.T.**: Bu Tez
- **C**: 3.4.6.1. ve 4.2.'de tanımlandığı gibi, bu yüksek oranlar, bu çalışmanın başvurmadığı eğitimde yer alan düğüm ID'si alanıyla ilgilidir.

Tablo 4.4:'deki oranlar, ağırlıklı ortalama (mikro) olarak ilgili araştırmalardan alınmıştır. [232] gibi bazı araştırmalarda destek sağlanmadığı için değerlerin makro ortalamaları kullanılmıştır. [349]'de yalnızca genel doğruluk sağlandığından, dolayısıyla mikro ortalama olarak kabul edilmiştir.

3.4.6.1.'de tanımlandığı gibi, RF benzeri algoritmalar düğüm ID'si alanını çok iyi kullanmaktadır. Bu alan genellikle bir düğümün iyi davranışlı olup olmadığını belirtmektedir ve %100 oranlarla doğruluk bulmak kolaydır. Düğüm ID'si bu algoritmalara beslenmezse bu kadar yüksek oranlara ulaşılamadığı çalışmalar sırasında görülmüştür. Dolayısıyla, bu algoritmalarda %100 kadar yüksek doğruluk oranlarına ihtiyatla yaklaşılmalıdır.

Tablo 4.11:, her zaman adımı kümesinde beş kenarlı veri kümesi ve %70 eğitim ile en iyi performans gösteren modeli gösterir. En iyi performans gösteren model, **Tablo 4.11:**'da belirtildiği gibi 87 parametreye sahiptir.

Tablo 4.5: İşlem Karmaşıklığı (Devamı **Tablo 4.6:**'da)

Ad	Kendi CPU'su (%)	Kendi CPU'su	CPU toplam (%)	CPU toplam	CPU süresi ort.	# Çağrı
aten::lift_fresh	0.00%	2.000us	0.00%	2.000us	2.000us	1
aten::to	0.00%	6.000us	0.01%	52.000us	52.000us	1
aten::_to_copy	0.00%	18.000us	0.01%	46.000us	46.000us	1
aten::empty_strided	0.00%	7.000us	0.00%	7.000us	7.000us	1
aten::copy_	0.00%	21.000us	0.00%	21.000us	21.000us	1
aten::lift_fresh	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::to	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::lift_fresh	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::to	0.00%	8.000us	0.00%	8.000us	8.000us	1
aten::_to_copy	0.00%	3.000us	0.00%	8.000us	8.000us	1
aten::empty_strided	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::copy_	0.00%	4.000us	0.00%	4.000us	4.000us	1
aten::lift_fresh	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::to	0.00%	10.000us	0.00%	10.000us	10.000us	1
aten::_to_copy	0.00%	5.000us	0.00%	10.000us	10.000us	1
aten::empty_strided	0.00%	2.000us	0.00%	2.000us	2.000us	1
aten::copy_	0.00%	3.000us	0.00%	3.000us	3.000us	1
aten::new_zeros	0.00%	17.000us	0.00%	25.000us	25.000us	1
aten::new_empty	0.00%	4.000us	0.00%	7.000us	7.000us	1
aten::empty	0.00%	3.000us	0.00%	3.000us	3.000us	1
aten::zero_	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::mul	0.00%	28.000us	0.00%	28.000us	28.000us	1
aten::sum	0.00%	29.000us	0.00%	32.000us	32.000us	1
aten::as_strided	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::fill_	0.00%	2.000us	0.00%	2.000us	2.000us	1
aten::norm	0.00%	17.000us	0.00%	17.000us	17.000us	1
aten::as_strided	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::div	0.00%	10.000us	0.00%	10.000us	10.000us	1
aten::tanh	0.03%	232.000us	0.03%	232.000us	232.000us	1
aten::new_ones	0.00%	5.000us	0.00%	11.000us	11.000us	1
aten::new_empty	0.00%	1.000us	0.00%	2.000us	2.000us	1
aten::empty	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::fill_	0.00%	4.000us	0.00%	4.000us	4.000us	1
aten::expand	0.00%	6.000us	0.00%	7.000us	7.000us	1
aten::as_strided	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::max	0.00%	9.000us	0.00%	10.000us	10.000us	1
aten::empty	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::fill_	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::item	0.00%	4.000us	0.00%	5.000us	5.000us	1
aten::_local_scalar_dense	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::zeros	0.00%	2.000us	0.00%	3.000us	3.000us	1
aten::empty	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::zero_	0.00%	0.000us	0.00%	0.000us	0.000us	1

Tablo 4.6: İşlem Karmaşıklığı (Devam)

Ad	Kendi CPU'su (%)	Kendi CPU'su	CPU toplam (%)	CPU toplam	CPU süresi ort.	# Çağrı
aten::scatter_add_	0.00%	22.000us	0.00%	22.000us	22.000us	1
aten::max	0.00%	2.000us	0.00%	4.000us	4.000us	1
aten::empty	0.00%	2.000us	0.00%	2.000us	2.000us	1
aten::fill_	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::item	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::_local_scalar_dense	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::new_zeros	0.00%	2.000us	0.00%	3.000us	3.000us	1
aten::new_empty	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::empty	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::zero_	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::cumsum	0.00%	14.000us	0.00%	14.000us	14.000us	1
aten::to	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::slice	0.00%	5.000us	0.00%	6.000us	6.000us	1
aten::as_strided	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::cat	0.00%	15.000us	0.00%	17.000us	17.000us	1
aten::narrow	0.00%	1.000us	0.00%	2.000us	2.000us	1
aten::slice	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::as_strided	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::arange	0.00%	23.000us	0.00%	23.000us	23.000us	1
aten::empty	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::arange	0.00%	13.000us	0.00%	16.000us	16.000us	1
aten::resize_	0.00%	3.000us	0.00%	3.000us	3.000us	1
aten::index	0.00%	25.000us	0.00%	33.000us	33.000us	1
aten::as_strided	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::reshape	0.00%	8.000us	0.00%	8.000us	8.000us	1
aten::_reshape_alias	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::sub	0.00%	7.000us	0.00%	7.000us	7.000us	1
aten::mul	0.00%	4.000us	0.00%	4.000us	4.000us	1
aten::add	0.00%	9.000us	0.00%	9.000us	9.000us	1
aten::new_full	0.00%	2.000us	0.00%	5.000us	5.000us	1
aten::new_empty	0.00%	1.000us	0.00%	2.000us	2.000us	1
aten::empty	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::fill_	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::index_put_	0.00%	10.000us	0.00%	25.000us	25.000us	1
aten::_index_put_impl_	0.00%	11.000us	0.00%	15.000us	15.000us	1
aten::as_strided	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::reshape	0.00%	4.000us	0.00%	4.000us	4.000us	1
aten::_reshape_alias	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::view	0.00%	5.000us	0.00%	5.000us	5.000us	1
aten::sort	0.00%	41.000us	0.01%	54.000us	54.000us	1
aten::copy_	0.00%	3.000us	0.00%	3.000us	3.000us	1
aten::arange	0.00%	5.000us	0.00%	9.000us	9.000us	1

Tablo 4.7: İşlem Karmaşıklığı (Devam)

Ad	Kendi CPU'su (%)	Kendi CPU'su	CPU toplam (%)	CPU toplam	CPU süresi ort.	# Çağrı
aten::empty	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::arange	0.00%	3.000us	0.00%	4.000us	4.000us	1
aten::resize_	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::as_strided	0.00%	0.000us	0.00%	0.000us	0.000us	1
aten::copy_	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::view	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::add	0.00%	6.000us	0.00%	6.000us	6.000us	1
aten::view	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::to	0.00%	1.000us	0.00%	9.000us	9.000us	1
aten::_to_copy	0.00%	5.000us	0.00%	8.000us	8.000us	1
aten::empty_strided	0.00%	2.000us	0.00%	2.000us	2.000us	1
aten::copy_	0.00%	1.000us	0.00%	1.000us	1.000us	1
aten::mul	0.00%	6.000us	0.00%	11.000us	11.000us	1
aten::to	0.00%	2.000us	0.00%	5.000us	5.000us	1
aten::_to_copy	0.00%	1.000us	0.00%	3.000us	3.000us	1

Tablo 4.8: Çalışma Zamanı Hesaplama

İsim	Değer
Koşma sayısı	100
Kendi CPU süresi toplamı ortalaması	518.91198ms
Standart sapma	44.02
Varyans (standart sapmanın karesi)	1937.7756
Kareler toplamı	193777.56

5. TARTIŞMA VE SONUÇ

RF ve DT'ler gerçek zamanlı hekatonlarda tercih edilen mekanizmalardır. Kazananların genellikle DT veya RF kullanma eğiliminde oldukları görülmüştür. Yapay sinir ağlarına sahip yarışmacılar bile, yarışmanın daha sonraki bölümlerinde, daha iyi performans için DT veya RF'ye başvurmaktadır. Bu tezden elde edilen genel bir sonuç olarak GNN, daha önce belirtildiği gibi, kötüleştiren birçok neden olmasına rağmen, DT ve RF ile aynı performansı göstermektedir. Ancak, en iyi hiper parametre alanını bulmak, kural tabanlı veya karar ağacı tabanlı yöntemlere göre hala daha uğraştırıcı olabilmektedir. Bu, gelecekteki araştırmalarla

Tablo 4.9: Önerilen Model İçin Önerilen Hiper Parametreler

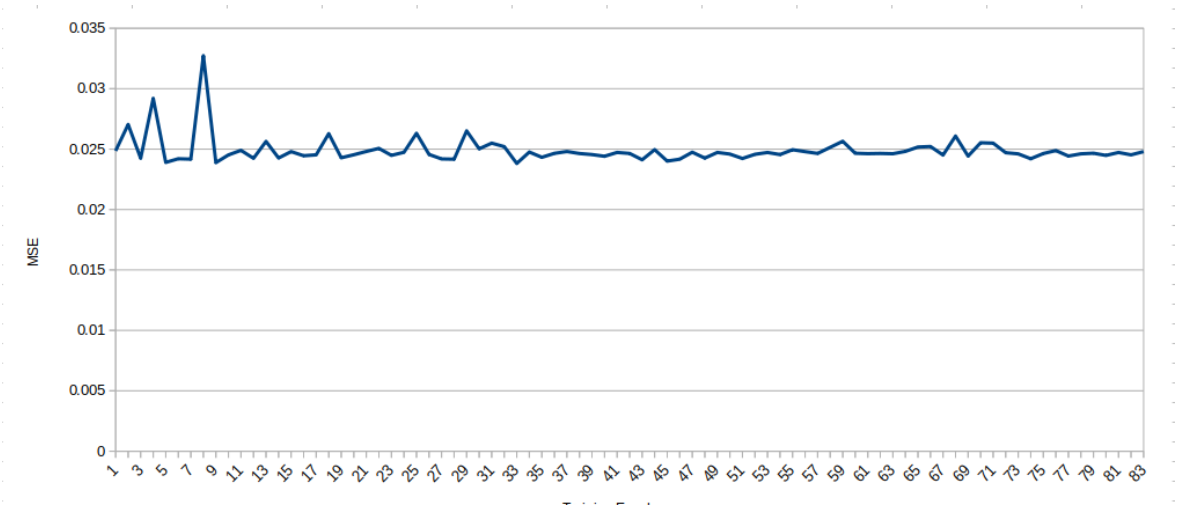
Hiper Parametre	**Değerler**
Tekrar Sayısı	4
Gecikme Sayısı	1
Kenar Sayısı	5
Tren Oranı	70%
Öğrenme Oranı	0,007
Optimize Edici	Adam
Doğrulama	Test Kümesi (%30)
Özellik Seçimi	Düğüm ID'si hariç tüm özellikler
Eğitim Süresi Sınırı	Yok
Kayıp Fonksiyonu	MSE

Tablo 4.10: Model Parametre Boyutları

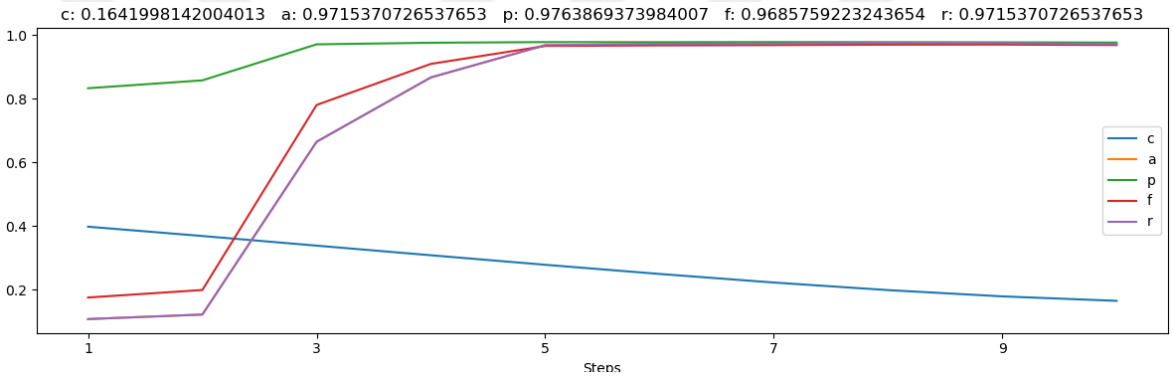
Katman	**Değer**
Toplam Parametre Sayısı	87
recurrent.initial_weight	torch.Size([2, 2])
recurrent.pooling_layer.weight	torch.Size([1, 2])
recurrent.recurrent_layer.weight_ih_l0	torch.Size([6, 2])
recurrent.recurrent_layer.weight_hh_l0	torch.Size([6, 2])
recurrent.recurrent_layer.bias_ih_l0	torch.Size([6])
recurrent.recurrent_layer.bias_hh_l0	torch.Size([6])
conv1.bias	torch.Size([4])
conv1.lin.weight	torch.Size([4, 2])
conv2.bias	torch.Size([4])
conv2.lin.weight	torch.Size([4, 4])
conv3.bias	torch.Size([2])
conv3.lin.weight	torch.Size([2, 4])
linear.weight	torch.Size([1, 2])
linear.bias	torch.Size([1])

Tablo 4.11: En İyi Performans Gösteren Model Parametreleri

Katman	**Değer**
recurrent.initial_weight	tensor([[-1.0349, 0.0754], [-0.6090, -0.1277]])
recurrent.pooling_layer.weight	tensor([[0.1856, 0.3595]])
recurrent.recurrent_layer.weight_ih_l0	tensor([[-0.4761, -0.6280], [-0.3019, -0.4507], [0.5056, -0.4898], [-0.6068, -0.1743], [-0.3531, -0.1133], [0.6701, -0.2959]])
recurrent.recurrent_layer.weight_hh_l0	tensor([[0.6559, 0.5987], [0.2628, -0.1165], [0.3318, -0.5921], [-0.3826, -0.6094], [-0.6758, -0.1678], [-0.4119, 0.3833]])
recurrent.recurrent_layer.bias_ih_l0	tensor([0.6435, -0.4851, -0.5692, 0.2601, -0.4728, -0.0274])
recurrent.recurrent_layer.bias_hh_l0	tensor([-0.6676, 0.1287, 0.1577, -0.1924, -0.6243, 0.6132])
conv1.bias	tensor([-0.0189, 0.0200, 0.0199, -0.0199])
conv1.lin.weight	tensor([[0.7865, -0.3251], [0.5017, -0.5404], [-0.8783, -0.2476], [0.4634, -0.4860]])
conv2.bias	tensor([-0.0199, 0.0200, 0.0200, -0.0199])
conv2.lin.weight	tensor([[0.5763, -0.4444, 0.0462, 0.3567], [0.5111, 0.2518, 0.0152, -0.7694], [-0.2101, -0.3438, 0.0797, 0.3367], [0.6744, -0.5637, -0.7265, 0.3215]])
conv3.bias	tensor([0.0200, 0.0200])
conv3.lin.weight	tensor([[-0.5373, 0.0107, 0.6952, 0.5738], [-0.2362, 0.9847, -0.0046, -0.5596]])
linear.weight	tensor([[0.1325, 0.6047]])
linear.bias	tensor([-0.4182])



Şekil 5.1: Eğitim Sayısı ve MSE



Şekil 5.2: Eğitim

geliştirilecek bir öğe olarak karşımıza çıkmaktadır. Ayrıca, daha önce de belirtildiği gibi, diğer bazı yöntemler, işleme sırasında bir düğümün “kimliğini" kullanma eğilimindedir, ancak bu da aşırı eğitime sebep olmaktadır. Öte yandan topluluk (ensemble) yöntemleri de karmaşıktır, ancak bu topluluk (ensemble) parçaları GNN’lerle de kullanılabilir.

Bir diğer husus ise eğitim sayısının ortaya çıkan performans üzerindeki olmayan etkisidir. Bu tez, tek bir eğitim ile bile iyi sonuçlar buldu. Bu tezin deney sırasında, eğitim oranı, eğitim sayısı, kenar sayısı vb. gibi farklı parametrelerle topladığı verilerin sonucu olan **Şekil 5.1:** (dönemler ve MSE)’de görülebilir. Epoch’un çok fazla olması genellikle genel olarak daha iyi bir puanlama performansı sağlamadı (**Şekil 5.2:**). Eğitim sırasında metriklerin çok fazla değişmediği, ortasından sonuna kadar her zaman bir plato olduğu görülmüştür. Bu, kısmen Adam optimize edicideki gradyan iniş algoritması ve öğrenme oranıyla ilgilidir.

PyG (PyTorch Geometric), GNN konusunda bilinen en iyi altyapıdır ve standardizasyon

yönünde iyi bir gelişmedir. Bilinen PyTorch ile uyumludur ve sonuçları PyTorch yardımcı programlarıyla da analiz edilebilir. Buna ek olarak, bu çalışma bu yönde daha iyi yardımcı olmak için, var olan tek geçici GNN kütüphanesini (bu tezin toplayabildiği kadarıyla) kullandı. Ancak bu kütüphanenin de mevcut ekosistemle kolayca entegre olabilmesi için iyileştirmelere ihtiyacı vardır. Her ne kadar skorlama aşamasında alışılagelmiş süreçten farklı bir durumun olmadığı görünse de, sürecin geçici (temporal) doğası nedeniyle eğitim, her adım için birden fazla eğitim oturumuyla farklı şekilde ele alınmaktadır.

Orjinal EvolveGCN-O modelinin aksine, bu tez hem mimari hem de algoritma performansındaki karmaşıklığı artırdı. Ancak bu çalışma, orjinal EvolveGCN-O modelinden beklenenden daha erken ve daha sık ve daha iyi sonuçların alındığını gözlemledi.

5.1. SONUÇ

Bu tez ardından GNN'nin MBD için oldukça iyi bir yöntem olduğu görülebilir. Fazla bir ön işlem yapmadan, ancak iyi bir yapıya sahip olan, herhangi bir veri kümesi GNN ile yüklenip eğitilebilir ve ardından sonuçlar tatmin edici olacaktır. Bu durum da daha çok GL/RL ilkeleriyle ilgilidir. GL/RL'de gerekli hiçbir bilgi kaybolmaz ve gerekli her veri algoritmaya beslenir. Bunu yaptığınızda iyi sonuçlar, modelin olabildiğince çok bilgiye sahip olduğundan, kaçınılmaz görünmektedir.

Bu tezde kümeleme kullanılarak ilişkiler ve özellikler oluşturulmaktadır. Birbirine yakın araçların aynı kümede olduğu ve birbirlerine sinyal verme olasılıklarının daha yüksek olduğu düşünülmüştür. Ancak, bu tez ilişki ağırlıkları olarak kullanılacak sinyal frekansına sahip değildi. Her adımda yalnızca her araç arasındaki mesafeye sahipti. Gerçek dünyada bu bilgi V2X sinyalleşmesinden kolaylıkla çıkarılabilir.

Sonuçta mevcut veri kümelerinden GNN veri kümesi oluşturmak, nihai hedefte hala bir düzeltme veya yamadır. GNN veri kümeleri, GNN düşünülerek sıfırdan oluşturulmalıdır. Tablo biçiminde düşünmeye gerek olmadan ve gerekli olan her bilgi SLE'ler, ağırlıklar veya düğüm özellikleri olarak eklenebilir.

Deneysel sonuçlar, sunulan GNN yaklaşımının DT ve RF yöntemlerinden daha iyi performans gösterdiğini göstermektedir. Ancak en iyi hiper parametre alanını bulmak, kurala dayalı veya karar ağacına dayalı yöntemlere göre hâlâ zorlayıcı olabilir. Ayrıca, diğer bazı

yöntemler işleme sırasında bir düğümün "ID"sini kullanma eğilimindedir ve bu da onlara açık bir avantaj sağlamaktadır. Ancak bu, aşırı uyum sorunuyla sonuçlanacaktır ve yeni örneklemlere uygulanamazlar.

Bir başka konu ise, eğitim sayısının genel performansı nasıl etkilediğidir. Bu çalışma, tek bir eğitim döneminde bile iyi sonuçlar bulmuştur. Eğitim sayısını arttırmak genellikle daha iyi bir performans sağlamamıştır. **Şekil 5.1:** (bireysel eğitim çalıştırmaları) ve **Şekil 5.2:** (tek çalıştırma)'da görülebileceği gibi, her zaman ortadan uca doğru metriklerin eğitim sırasında fazla değişmediği bir plato vardır. Bu kısmen Adam optimize edicinin gradyan iniş algoritması ve öğrenme oranıyla ilgilidir.

PyG, standardizasyon yönünde iyi bir gelişmedir. Düz PyTorch ile uyumludur ve sonuçları PyTorch yardımcı programları ile analiz edilebilmektedir. Ek olarak, bu çalışma var olan tek açık kaynaklı geçici GNN kütüphanesini kullanmıştır (bu çalışmanın topladığı kadarıyla). Ancak bu çalışmanın, Weights & Biases[28] ve GraphGym[29] gibi mevcut GNN hiperparametre arama yardımcı programlarıyla daha iyi entegre olabilmesi için iyileştirmelere ihtiyacı vardır. Ayrıca bu çalışmada PyG'deki yapay zekâ açıklanabilirlik yöntemlerinin ST GNN'lerle çalışmasının zor olduğu ortaya çıkmıştır.

Her ne kadar skorlama aşamasında bilinen süreçlerden farklı bir durum yok gibi görünse de, sürecin zamansal doğası nedeniyle eğitim, her adım için birden fazla eğitim oturumuyla farklı şekilde ele alınmaktadır.

Sade EvolveGCN-O modelinin aksine bu çalışma, karmaşıklığı artırarak, daha iyi sonuçların, bir EvolveGCN-O modelinden beklenenden daha erken ve daha sık geldiğini gözlemlemiştir.

5.2. GELECEK ÇALIŞMALAR

Bir sonraki araştırma yönü olarak, özellikle VeReMi ve VeReMi-Extension gibi diğer veri kümelerini iyileştirmeye çalışmak iyi bir seçenek gibi görünmektedir.

Diğer bir araştırma alanı ise simülatörlerinde halen devam eden bir çalışma olan CP mesajlarıyla yeni veri kümeleri oluşturmak olacaktır.

---

[28] https://wandb.ai/site

[29] https://github.com/snap-stanford/GraphGym

Veri kümesi dönüşümü olarak bu çalışma, yalnızca tek bir mesafe ölçüsü kullanarak aynı kümedeki düğümler arasında kenar oluşturmayı kullanmıştır. Ancak diğer mesafe ölçümleri de kullanılabilir. Yine de, bir başka iyi kenar oluşturma yöntemi, çizelge geçiş (graph traversal) algoritmaları olacaktır.

Metrik toplama ve oluşturma hala başka bir araştırma alanıdır. Burada standartlara uygun toplanan ek metrikler daha sonra açık kaynak olarak da bağışlanacaktır.

Ek olarak, eğitim performansının neden kenar sayısıyla bu kadar ilgili olmadığının araştırılması gerekmektedir. Ayrıca ilginç düşük eğitim sayısı da gözden geçirilmesi gereken başka bir husustur.

Daha önce belirtildiği gibi, bu tezin kullandığı kütüphanede, Weights & Biases [28] ve GraphGym [29] gibi hiper parametre arama yardımcı programlarına daha iyi bir entegrasyon ihtiyacı bulunmaktadır. Ayrıca, PyG'deki yapay zekâ açıklanabilirlik yöntemlerinin uzay-zamansal GNN'lerle çalışması zor olduğu da deneyimlenmiştir. Ayrıca her bir zaman basamağında ayrı bir karmaşıklık matrisi bulunması, bu kütüphanede genel bir karmaşıklık matrisi çıkarma özelliğinin eksik olduğu ve eklemek için de oldukça fazla bir çalışma gerektiği görülmüştür. Ancak yine de zaman ve uzay GNN'ler açısından iyi bir kütüphane olduğu görülmüştür.

Geliştirilen uygulama Python dilinde ve merkezi işlemci kullanılarak geliştirilmiştir. Bu nedenle çalışma zamanı hızlandırma açısından grafik işlemci üzerinde gidilmesi işlemleri daha da hızlandıracaktır. Bununla birlikte Julia programlama dili de bu konuda yardımcı olabilir. Ancak henüz görece yeni bir dil olması ve kullanılan altyapıların varlığı bir araştırma alanı olarak kalmaktadır.

Sonuçta, özellikle RL ve GNN, ML yöntemlerinin en genel yollarından biridir ve eldeki diğer birçok sorun için ilgi çekici bir araştırma yönü gibi görünmektedir.

KAYNAKLAR

[1]. L. Chen, P. Wu, K. Chitta, B. Jaeger, A. Geiger, and H. Li, 2023. End-to-end autonomous driving: Challenges and frontiers. *arXiv e-prints*, pages arXiv–2306.

[2]. J. A. Donenfeld, 2017. Wireguard: next generation kernel network tunnel. In *NDSS*, pages 1–12.

[3]. S. Giordano, 2002. Mobile ad hoc networks. *Handbook of wireless networks and mobile computing*, 1:325–346.

[4]. R. Miucic, 2018. *Connected vehicles: Intelligent transportation systems*. Springer. ISBN 3319947850.

[5]. M. Calabrese and A. Nasr, 2020. The 5.9 ghz band removing the roadblock to gigabit wi-fi. *New America Open Technology Institute Wireless Future Project*.

[6]. FCC, 1999. Fcc allocates spectrum in 5.9 ghz range for intelligent transportation systems uses.

[7]. Commission, 2008. Commission decision of 5 august 2008: on the harmonised use of radio spectrum in the 5 875-5 905 mhz frequency band for safety-related applications of intelligent transport systems (its). *Official Journal of the European Union*.

[8]. T. E. Commission, 2020. Commission implementing decision (eu) 2020/1426 of 7 october 2020 : on the harmonised use of radio spectrum in the 5 875-5 935 mhz frequency band for safety-related applications of intelligent transport systems (its) and repealing decision 2008/671/ec. *Official Journal of the European Union*.

[9]. F. Register, 2021. Use of the 5.850-5.925 ghz band. *Federal Register*, 86(83):23323–23340.

[10]. G. Gallo, M. L. Bernardi, M. Cimitile, and P. Ducange, 2021. An explainable approach for car driver identification. In *2021 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1–7. IEEE.

[11]. IEEE-SA, 2016. Ieee standard for wireless access in vehicular environments–security services for applications and management messages. *IEEE Std IEEE 1609.2*, pages 1–240. doi:10.1109/IEEESTD.2016.7426684.

[12]. IEEE-SA, 2020. Ieee standard for wireless access in vehicular environments (wave)–certificate management interfaces for end entities. *IEEE Std 1609.2.1-2020*. ISSN 978-1-5044-6974-6. doi:10.1109/ieeestd.2020.9311462.

[13]. I. C. S. L. S. Committee, 2020. Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2020*.

[14]. C. . C. C. Consortium, 2011. Memorandum of understanding for oems within the car 2 car communication consortium on deployment strategy for cooperative its in europe. *C2C-CC Final Version*, 4(02):1–5.

[15]. ETSI, 2012. Intelligent transport systems (its); security; access control. *ETSI TS 102 942 V1.1.1 (2012-06)*.

[16]. ETSI, 2011. Intelligent transport systems (its); classification and management of its application objects. *ETSI TS 102 860 V1.1.1 (2011-05)*.

[17]. 3GPP, 2021. 3rd generation partnership project; technical specification group core network and terminals; vehicle-to-everything (v2x) services in 5g system (5gs); stage 3 (release 17). *3GPP TS 24.587 V17.4.0 (2021-12)*.

[18]. M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, and M. Isard, 2016. TensorFlow: A system for Large-Scale machine learning. In *12th USENIX symposium on operating systems design and implementation (OSDI 16)*, pages 265–283. ISBN 1931971331.

[19]. A. Agrawal and C. Kim, 2020. Intel tofino2-a 12.9 tbps p4-programmable ethernet switch. In *Hot Chips Symposium*, pages 1–32.

[20]. C. I. C. A. I. I. Alliance, 2020. Cooperative intelligent transportation system - vehicular communication application layer specification and data exchange standard (phase ii). *T/CSAE 157-2020*.

[21]. N. Alliance, 2018. V2x white paper. *White Paper*, 1.

[22]. S. Aust, 2018. Paving the way for connected cars with adaptive autosar and agl. In *2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops)*, pages 53–58. IEEE. ISBN 1538650975.

[23]. B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, 2018. A security credential management system for v2x communications. *Ieee Transactions on Intelligent Transportation Systems*, 19(12):3850–3871. ISSN 1524-9050. doi:10.1109/Tits.2018.2797529.

[24]. A. A. T. Committee, 2022. V2x sensor-sharing for cooperative and automated driving. *J3224*.

[25]. D. T. Committee, 2020. On-board system requirements for v2v safety communications. *J2945/1_202004*. doi:10.4271/j2945/1$_$202004.

[26]. T. Motors, 2017. Open source routing engine for openstreetmap.

[27]. H. B. Zhou, W. C. Xu, J. C. Chen, and W. Wang, 2020. Evolutionary v2x technologies toward the internet of vehicles: Challenges and opportunities. *Proceedings of the Ieee*, 108(2):308–323. ISSN 0018-9219. doi:10.1109/Jproc.2019.2961937.

[28]. Y. Li, L. Yang, S. Han, X. Wang, and F.-Y. Wang, 2018. When lpwan meets its: Evaluation of low power wide area networks for v2x communications. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 473–478. IEEE. ISBN 1728103231.

[29]. M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, 2018. Intrusion detection systems for iot-based smart environments: a survey. *Journal of Cloud Computing-Advances Systems and Applications*, 7(1):1–20. ISSN 2192-113X. doi:ARTN2110.1186/s13677-018-0123-6.

[30]. F. Hauser, M. Haberle, M. Schmidt, and M. Menth, 2020. P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. *Ieee Access*, 8:139567–139586. ISSN 2169-3536. doi:10.1109/Access.2020.3012738.

[31]. B. Lewis, M. Broadbent, and N. Race, 2019. P4id: P4 enhanced intrusion detection. In *2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–4. IEEE. ISBN 1728145457.

[32]. ETSI, 2023. Intelligent transport systems (its); vehicular communications; basic set of applications; collective perception service; release 2. *ETSI TS 103 324 V2.1.1 (2023-06)*.

[33]. ETSI, 2020. Intelligent transport systems (its); security; pre-standardization study on misbehaviour detection; release 2. *ETSI TR 103 460 V2.1.1 (2020-10)*.

[34]. ETSI, 2017. Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra). *ETSI TR 102 893 V1.2.1 (2017-03)*.

[35]. Y. Wen, Y. Wang, Z. Zhang, J. Wu, L. Zhong, M. Papageorgiou, and P. Zheng, 2023. Effects of connected autonomous vehicles on the energy performance of signal-controlled junctions. *Sustainability*, 15(7):5672.

[36]. A. Swaminathan, A. Nirmal, L. K. Krishna, R. K. Soundappan, R. Lekshmi, and K. V. Chandrakala, 2023. Development of low-cost electronic control unit for hybrid electric vehicle. In *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*, pages 1–6. IEEE.

[37]. S. V. Balkus, H. Wang, B. D. Cornet, C. Mahabal, H. Ngo, and H. Fang, 2022. A survey of collaborative machine learning using 5g vehicular communications. *IEEE Communications Surveys & Tutorials*. ISSN 1553-877X.

[38]. M. T. Abbas, A. Muhammad, and W. C. Song, 2020. Sd-iov: Sdn enabled routing for internet of vehicles in road-aware approach. *Journal of Ambient Intelligence and Humanized Computing*, 11(3):1265–1280. ISSN 1868-5137. doi:10.1007/s12652-019-01319-w.

[39]. NHTS, 2015. Traffic safety facts, crash stats. Technical report, National Center for Statistics and Analysis.

[40]. O.-R. A. D. O. committee, 2021. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *J3016_202104*. doi:10.4271/j3016$_$202104.

[41]. W. Gay, 2024. Can bus. In *Beginning STM32: Developing with FreeRTOS, libopencm3, and GCC*, pages 395–413. Springer.

[42]. M. R. Ansari, J. P. Monteuuis, J. Petit, and C. Chen, 2021. V2x misbehavior and collective perception service: Considerations for standardization. *2021 Ieee Conference on Standards for Communications and Networking (Ieee Cscn)*. doi:10.1109/Cscn53733.2021.9686156.

[43]. A. Kedar, 2023. Phased array antenna for radar application. In *Handbook of Metrology and Applications*, pages 1443–1469. Springer.

[44]. M. Khodarahmi and V. Maihami, 2023. A review on kalman filter models. *Archives of Computational Methods in Engineering*, 30(1):727–747.

[45]. V. Lekic and Z. Babic, 2019. Automotive radar and camera fusion using generative adversarial networks. *Computer Vision and Image Understanding*, 184:1–8. ISSN 1077-3142. doi:10.1016/j.cviu.2019.04.002.

[46]. F. Estrada-Belli, L. Gilabert-Sansalvador, M. A. Canuto, I. Šprajc, and J. C. Fernandez-Diaz, 2023. Architecture, wealth and status in classic maya urbanism revealed by airborne lidar mapping. *Journal of Archaeological Science*, 157:105835.

[47]. S. Lunz, Y. Li, A. Fitzgibbon, and N. Kushman, 2020. Inverse graphics gan: Learning to generate 3d shapes from unstructured 2d data. *arXiv preprint arXiv:2002.12674*.

[48]. J. Fayyad, M. A. Jaradat, D. Gruyer, and H. Najjaran, 2020. Deep learning sensor fusion for autonomous vehicle perception and localization: A review. *Sensors (Basel)*, 20(15):4220. ISSN 1424-8220 (Electronic) 1424-8220 (Linking). doi:10.3390/s20154220.

[49]. H. Qin, J. Li, J. Wang, and Q. Wu, 2020. Local map construction based on 3d-lidar and camera. In *2020 39th Chinese Control Conference (CCC)*, pages 3887–3891. IEEE. ISBN 9881563909.

[50]. V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, 2019. Physical signal-driven fusion for v2x misbehavior detection. In *2019 IEEE Vehicular Networking Conference (VNC)*, pages 1–4. IEEE. ISBN 1728145716.

[51]. Z. Zhang, S. Wang, Y. Hong, L. Zhou, and Q. Hao, 2021. Distributed dynamic map fusion via federated learning for intelligent networked vehicles. In *2021 IEEE International Conference on Robotics and Automation (ICRA)*, pages 953–959. IEEE. ISBN 1728190770.

[52]. M. García, I. Urbieta, M. Nieto, J. González de Mendibil, and O. Otaegui, 2022. ildm: An interoperable graph-based local dynamic map. *Vehicles*, 4(1):42–59.

[53]. A. Kumar and H. Wagatsuma, 2021. An implementation of linear temporal logic for driving safety suitable for the concept of local dynamic map. In *2021 IEEE/SICE International Symposium on System Integration (SII)*, pages 708–709. IEEE. ISBN 1728176581.

[54]. J. W. Lee, W. Lee, and K. D. Kim, 2021. An algorithm for local dynamic map generation for safe uav navigation. *Drones*, 5(3):88. ISSN 2504-446X. doi:ARTN8810.3390/drones5030088.

[55]. F. Raviglione, C. M. R. Carletti, C. Casetti, F. Stoffella, G. M. Yilma, and F. Visintainer, 2022. S-ldm: Server local dynamic map for vehicular enhanced collective perception. In *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*, pages 1–5. IEEE.

[56]. E. ETSI, 2014. Intelligent transport systems (its); vehicular communications; basic set of applications; local dynamic map (ldm). *ETSI EN 302 895 V1.1.1 (2014-09)*.

[57]. ETSI, 2019. Intelligent transport systems (its); vehicular communications; basic set of applications; analysis of the collective perception service (cps); release 2. *ETSI TR 103 562 V2.1.1 (2019-12)*.

[58]. A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, 2017. CARLA: An open urban driving simulator. In *Proceedings of the 1st Annual Conference on Robot Learning*, pages 1–16.

[59]. X. Zhao, Y. Fang, H. Min, X. Wu, W. Wang, and R. Teixeira, 2023. Potential sources of sensor data anomalies for autonomous vehicles: An overview from road vehicle safety perspective. *Expert Systems with Applications*, page 121358.

[60]. Y. Kortli, S. Gabsi, L. F. C. L. Y. Voon, M. Jridi, M. Merzougui, and M. Atri, 2022. Deep embedded hybrid cnn-lstm network for lane detection on nvidia jetson xavier nx. *Knowledge-Based Systems*, 240:107941. ISSN 0950-7051. doi:ARTN10794110. 1016/j.knosys.2021.107941.

[61]. A. P. Neto and F. Tonidandel, 2022. Analysis of wifi localization techniques for kidnapped robot problem. In *2022 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, pages 53–58. IEEE.

[62]. D. Lee, M. Jung, W. Yang, and A. Kim, 2024. Lidar odometry survey: recent advancements and remaining challenges. *Intelligent Service Robotics*, pages 1–24.

[63]. M. Bojarski, D. Del Testa, D. Dworakowski, B. Firner, B. Flepp, P. Goyal, L. D. Jackel, M. Monfort, U. Muller, J. Zhang, et al., 2016. End to end learning for self-driving cars. *arXiv preprint arXiv:1604.07316*.

[64]. M. Bojarski, P. Yeres, A. Choromanska, K. Choromanski, B. Firner, L. Jackel, and U. Muller, 2017. Explaining how a deep neural network trained with end-to-end learning steers a car. *arXiv preprint arXiv:1704.07911*.

[65]. F. A. Schiegg, I. Llatser, D. Bischoff, and G. Volk, 2020. Collective perception: A safety perspective. *Sensors (Basel)*, 21(1):159. ISSN 1424-8220 (Electronic) 1424-8220 (Linking). doi:10.3390/s21010159.

[66]. A. Sahu, 2023. An analytical study on the legal liability caused by autonomous vehicles with reference to the motor vehicles act of 1988. *Issue 2 Indian JL & Legal Rsch.*, 5:1.

[67]. R. Mills, J. Sobin, R. Patterson, S. Brodet, S. Pilkington, and A. Olsen, 2023. Addressing the need to grow auv operator workforce: Advanced autonomy and goal based mission planning. In *OCEANS 2023-MTS/IEEE US Gulf Coast*, pages 1–6. IEEE.

[68]. R. Graham, 2023. Industrial nature: The unrealised king lear of norman bel geddes. *Shakespeare*, pages 1–32.

[69]. R. Duggal, M. Khosravy, and O. Witkowski, 2024. Application of genetic algorithms to electrical vehicle industries. In *Frontiers in Genetics Algorithm Theory and Applications*, pages 179–194. Springer.

[70]. T. Caldeira, J. Santos-Victor, and P. U. Lima, 2023. Visual-based localization for autonomous vehicles in simulated environments. In *2023 21st International Conference on Advanced Robotics (ICAR)*, pages 238–243. IEEE.

[71]. DARPA, 2016. Darpa celebrates cyber grand challenge winners.

[72]. T. B. S. Institution, 2020. Connected and automated vehicles – vocabulary v2.0 2020.05. *Center for Connected & Autonomous Vehicles*.

[73]. D. Mitra, 2019. What is the difference between dsrc, 802.11p, ieee 1609, and wave?

[74]. IEEE-SA. Ieee draft standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment: Enhancements for next generation v2x.

[75]. IEEE-SA. Ieee p802.11-task group bd (ngv) meeting update.

[76]. IEEE-SA. Ieee announces formation of two new ieee 802.11™ study groups.

[77]. auto talks, 2021. Functional-safety for enabling present and future v2x use-cases.

[78]. S. Kim and R. Shrestha, 2020. *Intelligent autonomous vehicle*, pages 15–33. Springer.

[79]. S. Kim and R. Shrestha, 2020. *V2X Current Security Issues, Standards, Challenges, Use Cases, and Future Trends*, pages 183–212. Springer.

[80]. S. Kim and R. Shrestha, 2020. *Automotive Cyber Security*. Springer.

[81]. R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, 2021. The importance of selecting clustering parameters in vanets: A survey. *Computer Science Review*, 40:100392. ISSN 1574-0137. doi:ARTN10039210.1016/j.cosrev.2021.100392.

[82]. W. Bayaa, 2021. Vepmad: A vehicular platoon management anomaly detection system: A case study of car-following mode, middle join and exit maneuvers.

[83]. Y. Yin, J. Shi, Y. Li, and P. Zhang, 2006. Cluster head selection using analytical hierarchy process for wireless sensor networks. In *2006 IEEE 17th international symposium on personal, indoor and mobile radio communications*, pages 1–5. IEEE. ISBN 1424403294.

[84]. H. Hu and M. J. Lee, 2022. Graph neural network-based clustering enhancement in vanet for cooperative driving. In *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 162–167. IEEE. ISBN 1665458186.

[85]. S. Sharma and A. Kaul, 2018. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized ids for vanet. *Vehicular Communications*, 12:23–38. ISSN 2214-2096. doi:10.1016/j.vehcom.2017.12.003.

[86]. K. Hamouid and K. Adi, 2019. Secure and reliable certification management scheme for large-scale manets based on a distributed anonymous authority. *Peer-to-Peer Networking and Applications*, 12(5):1137–1155. ISSN 1936-6442. doi:10.1007/s12083-019-00787-3.

[87]. A. Srivastava and J. Prakash, 2021. Future fanet with application and enabling techniques: Anatomization and sustainability issues. *Computer Science Review*, 39:100359. ISSN 1574-0137. doi:ARTN10035910.1016/j.cosrev.2020.100359.

[88]. S. Fitzgerald, 2020. Vehicle to bicycle (v2b) safety interactions using 4g mobile devices.

[89]. S. S. Vladimirov, D. A. Karavaev, A. B. Stepanov, M. A. Yurchenko, and A. G. Vladyko, 2019. An application of lora technology for sd-iov network. In *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–4. IEEE. ISBN 1728157641. doi:10.1109/ICUMT48472.2019.8970938.

[90]. D. Kafetzis, S. Vassilaras, G. Vardoulias, and I. Koutsopoulos, 2022. Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions. *IEEE Access*. ISSN 2169-3536.

[91]. H. Rosier, 2019. V2x – ready to turn autonomous into cooperative driving. Report, rohde-schwarz.

[92]. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, 2019. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*, pages 1–8. IEEE. ISBN 1728115760.

[93]. F. Paolucci, L. De Marinis, P. Castoldi, and F. Cugini, 2021. Demonstration of p4 neural network switch. In *Optical Fiber Communication Conference*, page M2B. 10. Optical Society of America.

[94]. T. L. Mai, S. Garg, H. P. Yao, J. T. Nie, G. Kaddoum, and Z. H. Xiong, 2021. In-network intelligence control: Toward a self-driving networking architecture. *Ieee Network*, 35(2):53–59. ISSN 0890-8044. doi:10.1109/Mnet.011.2000412.

[95]. I. V. T. Society, 2019. Ieee guide for wireless access in vehicular environments (wave) architecture. *IEEE Std 1609.0™-2019 (Revision of IEEE Std 1609.0-2013)*.

[96]. ETSI, 2012. Intelligent transport systems (its); security; confidentiality services. *ETSI TS 102 943 V1.1.1 (2012-06)*.

[97]. ETSI, 2021. Intelligent transport systems (its); security; its communications security architecture and security management; release 2. *ETSI TS 102 940 V2.1.1 (2021-07)*.

[98]. ETSI, 2021. Intelligent transport systems (its); security; trust and privacy management; release 2. *ETSI TS 102 941 V2.1.1 (2021-10)*.

[99]. B. Brecht and T. Hehn, 2019. *A security credential management system for V2X communications*, pages 83–115. Springer.

[100]. J. Hortelano, J. C. Ruiz, and P. Manzoni, 2010. Evaluating the usefulness of watchdogs for intrusion detection in vanets. In *2010 IEEE international conference on communications workshops*, pages 1–5. IEEE.

[101]. E. Aliwa, O. Rana, C. Perera, and P. Burnap, 2021. Cyberattacks and countermeasures for in-vehicle networks. *Acm Computing Surveys*, 54(1):1–37. ISSN 0360-0300. doi:Artn2110.1145/3431233.

[102]. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, 2019. A survey of network-based intrusion detection data sets. *Computers & Security*, 86:147–167. ISSN 0167-4048. doi:10.1016/j.cose.2019.06.005.

[103]. J. Hortelano, J. C. Ruiz, and P. Manzoni, 2010. Evaluating the usefulness of watchdogs for intrusion detection in vanets. In *2010 IEEE international conference on communications workshops*, pages 1–5. IEEE.

[104]. J. W. Liang, J. Y. Chen, Y. Y. Zhu, and R. Yu, 2019. A novel intrusion detection system for vehicular ad hoc networks (vanets) based on differences of traffic flow and position. *Applied Soft Computing*, 75:712–727. ISSN 1568-4946. doi:10.1016/j.asoc.2018.12.001.

[105]. T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, 2020. Performance analysis of machine learning algorithms in intrusion detection system: a review. *Procedia Computer Science*, 171:1251–1260.

[106]. H. D. Dixit, S. Pendharkar, M. Beadon, C. Mason, T. Chakravarthy, B. Muthiah, and S. Sankar, 2021. Silent data corruptions at scale. *arXiv preprint arXiv:2102.11245*.

[107]. C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, 2021. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110:102436. ISSN 0167-4048.

[108]. H. M. Song, J. Woo, and H. K. Kim, 2020. In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, 21:100198. ISSN 2214-2096. doi:ARTN10019810.1016/j.vehcom.2019.100198.

[109]. E. Seo, H. M. Song, and H. K. Kim, 2018. Gids: Gan based intrusion detection system for in-vehicle network. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–6. IEEE. ISBN 1538674939.

[110]. M. De Vincenzi, G. Costantino, I. Matteucci, F. Fenzl, C. Plappert, R. Rieke, and D. Zelle, 2024. A systematic review on security attacks and countermeasures in automotive ethernet. *ACM Computing Surveys*, 56(6):1–38.

[111]. M. Prabhakar, J. Singh, and G. Mahadevan, 2013. Defensive mechanism for vanet security in game theoretic approach using heuristic based ant colony optimization. In *2013 International Conference on Computer Communication and Informatics*, pages 1–7. IEEE. ISBN 146732907X.

[112]. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419. ISSN 2214-2126. doi:ARTN10241910.1016/j.jisa.2019.102419.

[113]. H. Bangui, M. Ge, B. Buhnova, and L. H. Trang, 2021. Towards faster big data analytics for anti-jamming applications in vehicular ad-hoc network. *Transactions on Emerging Telecommunications Technologies*, 32(10):e4280. ISSN 2161-3915. doi:ARTNe428010.1002/ett.4280.

[114]. B. Sousa, N. Magaia, and S. Silva, 2023. An intelligent intrusion detection system for 5g-enabled internet of vehicles. *Electronics*, 12(8):1757.

[115]. A. Burkov, 2019. *The hundred-page machine learning book*, volume 1. Andriy Burkov Canada. ISBN 978-1999579517. doi:https://doi.org/10.1080/15228053.2020.1766224.

[116]. Y. Y. Wang and N. Masoud, 2021. Adversarial online learning with variable plays in the pursuit-evasion game: Theoretical foundations and application in connected and automated vehicle cybersecurity. *Ieee Access*, 9:142475–142488. ISSN 2169-3536. doi:10.1109/Access.2021.3120700.

[117]. R. W. van der Heijden, T. Lukaseder, and F. Kargl, 2018. Veremi: A dataset for comparable evaluation of misbehavior detection in vanets. *arXiv preprint arXiv:1804.06701*.

[118]. J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, 2020. Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE. ISBN 1728150892.

[119]. F. A. Ghaleb, A. Zainal, M. A. Rassam, and F. Mohammed, 2017. An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In *2017 IEEE conference on application, information and network security (AINS)*, pages 13–18. IEEE. ISBN 1538607255.

[120]. M. Tsukada, S. Arii, H. Ochiai, and H. Esaki, 2022. Misbehavior detection using collective perception under privacy considerations. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 808–814. IEEE. ISBN 166543161X.

[121]. X. Liu, L. Yang, I. Alvarez, K. Sivanesan, A. Merwaday, F. Oboril, C. Buerkle, M. Sastry, and L. G. Baltar, 2021. Miso-v: Misbehavior detection for collective perception services in vehicular communications. In *2021 IEEE Intelligent Vehicles Symposium (IV)*, pages 369–376. IEEE. ISBN 1728153948.

[122]. J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. Ben Jemaa, and P. Urien, 2020. Simulation framework for misbehavior detection in vehicular networks. *Ieee Transactions on Vehicular Technology*, 69(6):6631–6643. ISSN 0018-9545. doi:10.1109/Tvt.2020.2984878.

[123]. A. Boualouache and T. Engel, 2022. A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks. *arXiv preprint arXiv:2201.10500*.

[124]. R. Sedar, C. Kalalas, F. Vázquez-Gallego, and J. Alonso-Zarate, 2021. Reinforcement learning-based misbehaviour detection in v2x scenarios. In *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pages 109–111. IEEE. ISBN 166544505X.

[125]. S. So, J. Petit, and D. Starobinski, 2019. Physical layer plausibility checks for misbehavior detection in v2x networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 84–93.

[126]. P. Lv, L. Xie, J. Xu, and T. Li, 2021. Misbehavior detection in vanet based on federated learning and blockchain. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 52–64. Springer.

[127]. H.-Y. Hsu, N.-H. Cheng, and C.-W. Tsai, 2021. A deep learning-based integrated algorithm for misbehavior detection system in vanets. In *Proceedings of the 2021 ACM International Conference on Intelligent Computing and its Emerging Applications*, pages 53–58.

[128]. P. Sharma, J. Petit, and H. Liu, 2018. Pearson correlation analysis to detect misbehavior in vanet. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pages 1–5. IEEE. ISBN 1538663589.

[129]. F. A Ghaleb, F. Saeed, M. Al-Sarem, B. Ali Saleh Al-rimy, W. Boulila, A. Eljialy, K. Aloufi, and M. Alazab, 2020. Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for vanet. *Electronics*, 9(9):1411.

[130]. S. So, P. Sharma, and J. Petit, 2018. Integrating plausibility checks and machine learning for misbehavior detection in vanet. In *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 564–571. IEEE. ISBN 153866805X.

[131]. M. Hadded, P. Merdrignac, S. Duhamel, and O. Shagdar, 2020. Security attacks impact for collective perception based roadside assistance: A study of a highway on-ramp merging case. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1284–1289. IEEE. ISBN 1728131294.

[132]. M. Shan, K. Narula, Y. F. Wong, S. Worrall, M. Khan, P. Alexander, and E. Nebot, 2020. Demonstrations of cooperative perception: Safety and robustness in connected and automated vehicle operations. *Sensors (Basel)*, 21(1):200. ISSN 1424-8220 (Electronic) 1424-8220 (Linking). doi:10.3390/s21010200.

[133]. A. Treichel, 2022. Model archive for bmw models· the all-new bmw x1 and the first-ever bmw ix1· wednesday, 1st june 2022· bmwarchive. org. *bmwarchive.org*.

[134]. J. S. Guzmán, A. F. Agudelo, I. Toledo, D. Bambague, H. Luna-García, and C. A. Collazos, 2022. Evaluation and redesign proposal of an infotainment system: A case study with a parked vehicle. In *Iberoamerican Workshop on Human-Computer Interaction*, pages 101–113. Springer.

[135]. M. Martinez, 2024. Bronco sport freshens up with a new screen, tires. *Automotive News*, 98(7124):0006–0006.

[136]. J. S. Weber, M. Neves, and T. Ferreto, 2021. Vanet simulators: an updated review. *Journal of the Brazilian Computer Society*, 27(1):1–31. ISSN 1678-4804.

[137]. G. Nardini, G. Stea, and A. Virdis. Lte user plane simulation model for inet & omnet++.

[138]. C. Sommer, 2021. The open source vehicular network simulation framework.

[139]. Artery, 2020. Omnet++ v2x simulation framework for etsi its-g5.

[140]. R. Riebl, H.-J. Günther, C. Facchi, and L. Wolf, 2015. Artery: Extending veins for vanet applications. In *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, pages 450–456. IEEE. ISBN 9633131421.

[141]. K. Garlichs, M. Wegner, and L. C. Wolf, 2018. Realizing collective perception in the artery simulation framework. In *2018 IEEE Vehicular Networking Conference (VNC)*, pages 1–4. IEEE. ISBN 153869428X.

[142]. H.-J. Günther, J. Timpner, M. Wegner, R. Riebl, and L. Wolf, 2017. Extending a holistic microscopic ivc simulation environment with local perception sensors and lte capabilities. *Vehicular Communications*, 9:211–221. ISSN 2214-2096.

[143]. A. Hegde, 2021. Artery-c: An omnet++ based discrete event simulation framework for cellular v2x.

[144]. CTTC, 2019. 5g-lena simulator.

[145]. V. Todisco, S. Bartoletti, C. Campolo, A. Molinaro, A. O. Berthet, and A. Bazzi, 2021. Performance analysis of sidelink 5g-v2x mode 2 through an open-source simulator. *IEEE Access*, 9:145648–145661.

[146]. A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, 2017. Carla: An open urban driving simulator. In *Conference on robot learning*, pages 1–16. PMLR. ISBN 2640-3498.

[147]. S. Shah, D. Dey, C. Lovett, and A. Kapoor, 2018. Airsim: High-fidelity visual and physical simulation for autonomous vehicles. In *Field and service robotics*, pages 621–635. Springer.

[148]. G. Rong, B. H. Shin, H. Tabatabaee, Q. Lu, S. Lemke, M. Možeiko, E. Boise, G. Uhm, M. Gerow, S. Mehta, et al., 2020. Lgsvl simulator: A high fidelity simulator for autonomous driving. *arXiv preprint arXiv:2005.03778*.

[149]. SolarWinds, 2022. The software that empowers network professionals.

[150]. E.-N. Ltd, 2021. Eve - the emulated virtual environment for network, security and devops professionals.

[151]. Reddit, 2017. Comparing gns3 and eve-ng, what are their pros and cons?

[152]. T.-K. Lee, T.-W. Wang, W.-X. Wu, Y.-C. Kuo, S.-H. Huang, G.-S. Wang, C.-Y. Lin, J.-J. Chen, and Y.-C. Tseng, 2019. Building a v2x simulation framework for future autonomous driving. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 1–6. IEEE. ISBN 4885523206.

[153]. F. Klingler, 2020. Open source experimental and prototyping platform supporting etsi its-g5.

[154]. B. McCarthy, A. Burbano-Abril, V. R. Licea, and A. O'Driscoll, 2021. Opencv2x: modelling of the v2x cellular sidelink and performance evaluation for aperiodic traffic. *arXiv preprint arXiv:2103.13212*.

[155]. M. Boehme, M. Stang, F. Muetsch, and E. Sax, 2020. Talkycars: A distributed software platform for cooperative perception. In *2020 IEEE Intelligent Vehicles Symposium (IV)*, pages 701–707. IEEE. ISBN 172816673X.

[156]. Valhalla, 2022. Open source routing engine for openstreetmap.

[157]. F. A. Schiegg, S. Li, and N. Mikhaylov, 2020. Teplits: A comprehensive test platform for intelligent transportation systems. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pages 1–5. IEEE. ISBN 1728152070.

[158]. R. Riebl, 2022. Open-source implementation of the etsi c-its protocol stack.

[159]. I. A. GmbH, 2022. Carmaker.

[160]. T. Wang, 2020. Cvb release 4 architecture doc.

[161]. D. Sabella, A. Reznik, and R. Frazao, 2019. *Multi-access edge computing in action*. CRC Press. ISBN 0429056494.

[162]. AECC, 2021. Distributed computing in an aecc system. *AECC White Paper Version 1.0.0*.

[163]. Y. Wang, W. Sun, C. Liu, Z. Cui, M. Zhu, and Z. Pu, 2021. Cooperative perception of roadside unit and onboard equipment with edge artificial intelligence for driving assistance. *Connected Cities for Smart Mobility toward Accessible and Resilient Transportation Center*.

[164]. W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, 2013. A security credential management system for v2v communications. In *2013 IEEE Vehicular Networking Conference*, pages 1–8. IEEE. ISBN 1479926876.

[165]. ETSI, 2018. Multi-access edge computing (mec); study on mec support for v2x use cases. *ETSI GR MEC 022 V2.1.1 (2018-09)*.

[166]. ETSI, 2022. Multi-access edge computing (mec); v2x information service api. *ETSI GS MEC 030 V2.2.1 (2022-05)*.

[167]. ETSI, 2019. Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *ETSI EN 302 637-2 V1.4.1 (2019-04)*.

[168]. ETSI, 2019. Intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service. *ETSI EN 302 637-3 V1.3.1 (2019-04)*.

[169]. ETSI, 2022. Cyber; methods and protocols; part 1: Method and pro forma for threat, vulnerability, risk analysis (tvra). *ETSI TS 102 165-1 V5.2.5 (2022-01)*.

[170]. V. C. T. Committee, 2020. V2x communications message set dictionary. *J2735_202007*. doi:10.4271/j2735$_$202007.

[171]. M. J. Chang, Z. Abichar, and C.-Y. Hsu, 2010. Wimax or lte: Who will lead the broadband mobile internet? *IT professional*, 12(3):26–32. ISSN 1520-9202.

[172]. T. Foss and K. Evensen, 2019. Its standardisering: oversikt og statusrapport 2019. *Norwegian Public Roads Administration*.

[173]. A. Bryden and V. Timofeev, 2005. Itu-iso agreement.

[174]. D. Sabella, 2021. *Multi-access Edge Computing: Software Development at the Network Edge*. Springer. ISBN 3030796175.

[175]. CHV, 2022. Car hacking village.

[176]. ocslab, 2019. Information security r&d data challenge.

[177]. zerodayinitiative, 2020. Pwn2own returns to vancouver for 2020.

[178]. H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, 2021. Car hacking and defense competition on in-vehicle network. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, volume 2021, page 25. ISBN 1-891562-68-1. doi:10.14722/autosec.2021.23035.

[179]. QUT, 2020. Homeabout.

[180]. Bugcrowd, 2022. Tesla bug bounty program.

[181]. J. Lian and L. Zhang, 2018. One-month beijing taxi gps trajectory dataset with taxi ids and vehicle status. In *Proceedings of the First Workshop on Data Acquisition To Analysis*, pages 3–4.

[182]. UCI, 1999. Kdd cup 1999 data.

[183]. f1tenth, 2020. one tenth the size. ten times the fun.

[184]. A. Wischnewski, M. Geisslinger, J. Betz, T. Betz, F. Fent, A. Heilmeier, L. Hermansdorfer, T. Herrmann, S. Huch, P. Karle, et al., 2022. Indy autonomous challenge-autonomous race cars at the handling limits. In *12th International Munich Chassis Symposium 2021*, pages 163–182. Springer.

[185]. J. Hauenstein, J. Gromer, J. C. Mertens, F. Diermeyer, and S. Kraus, 2021. Collective perception: Impact on fuel consumption for heavy trucks. In *VEHITS*, pages 350–361.

[186]. G. Thandavarayan, M. Sepulcre, and J. Gozalvez, 2020. Cooperative perception for connected and automated vehicles: Evaluation and impact of congestion control. *Ieee Access*, 8:197665–197683. ISSN 2169-3536. doi:10.1109/Access.2020.3035119.

[187]. J. Schindler, R. Markowski, D. Heß, D. Wesemeyer, C. Böker, B. Coll Perales, G. Thandavarayan, M. Sepulcre, J. Gozalvez, and M. Rondinone, 2021. Transaid deliverable 7.2: System prototype demonstration (iteration 2). *German Institute of Transportation Systems, Cooperative Systems*.

[188]. J. Schindler, R. Markowski, F. Andert, A. Correa, B. Coll Perales, M. Rondinone, and R. Blokpoel, 2020. Transaid deliverable 7.1: System architecture for real world vehicles and road side. *TransAID*.

[189]. M. Obst, A. Marjovi, M. Vasic, I. Navarro, A. Martinoli, A. Amditis, P. Pantazopoulos, I. Llatser, A. d. L. Fortelle, and X. Qian, 2017. Challenges for automated cooperative driving: The autonet2030 approach. In *Automated Driving*, pages 561–570. Springer.

[190]. V. M. Raju, V. Gupta, and S. Lomate, 2019. Performance of open autonomous vehicle platforms: Autoware and apollo. In *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, pages 1–5. IEEE.

[191]. maven its, 2016. Maven ts.

[192]. C. Pilz, A. Ulbel, and G. Steinbauer-Wagner, 2021. The components of cooperative perception-a proposal for future works. In *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pages 7–14. IEEE. ISBN 1728191424.

[193]. M. Karner, J. Hillebrand, M. Klocker, and R. Sámano-Robles, 2021. Going to the edge-bringing internet of things and artificial intelligence together. In *2021 24th Euromicro Conference on Digital System Design (DSD)*, pages 295–302. IEEE.

[194]. G. Rigazzi, J.-P. Kainulainen, C. Turyagyenda, A. Mourad, and J. Ahn, 2019. An edge and fog computing platform for effective deployment of 360 video applications. In *2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW)*, pages 1–6. IEEE.

[195]. G. K. Tran, H. Nishiuchi, V. Frascolla, K. Takinami, A. De Domenico, E. C. Strinati, T. Haustein, K. Sakaguchi, S. Barbarossa, S. Barberis, et al., 2018. Architecture of mmwave edge cloud in 5g-miedge. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE.

[196]. M. L. Han, B. I. Kwak, and H. K. Kim, 2018. Anomaly intrusion detection method for vehicular networks based on survival analysis. *Vehicular Communications*, 14:52–63. ISSN 2214-2096. doi:10.1016/j.vehcom.2018.09.004.

[197]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Icissp: Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 1:108–116. doi:10.5220/0006639801080116.

[198]. M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, 2017. Flow-based benchmark data sets for intrusion detection. In *Proceedings of the 16th European Conference on Cyber Warfare and Security. ACPI*, pages 361–369.

[199]. M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, 2017. Creation of flow-based data sets for intrusion detection. *Journal of Information Warfare*, 16(4):41–54. ISSN 1445-3312.

[200]. A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, 2012. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security*, 31(3):357–374. ISSN 0167-4048. doi:10.1016/j.cose.2011.12.012.

[201]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, 2009. A detailed analysis of the kdd cup 99 data set. In *2009 IEEE symposium on computational intelligence for security and defense applications*, pages 1–6. Ieee. ISBN 1424437636.

[202]. S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, 2000. Cost-based modeling for fraud and intrusion detection: Results from the jam project. In *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, volume 2, pages 130–144. IEEE. ISBN 0769504906.

[203]. N. Moustafa and J. Slay, 2015. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 military communications and information systems conference (MilCIS)*, pages 1–6. IEEE. ISBN 1467370088.

[204]. M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, 2020. *Netflow datasets for machine learning-based network intrusion detection systems*, pages 117–135. Springer.

[205]. N. Moustafa, G. Creech, and J. Slay, 2017. *Big data analytics for intrusion detection system: Statistical decision-making using finite dirichlet mixture models*, pages 127–156. Springer.

[206]. R. Lippmann, 1999. Proposed 1999 darpa off-line intrusion detection evaluation plans. Report, MIT Lincoln Laboratory.

[207]. M. Zissman, 2000. Darpa intrusion detection scenario specific data sets.

[208]. N. Lee, 2015. *DARPA's Cyber Grand Challenge (2014–2016)*, pages 429–456. Springer.

[209]. G. Creech and J. Hu, 2013. Generation of a new ids test dataset: Time to retire the kdd collection. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 4487–4492. IEEE. ISBN 1467359394.

[210]. P. A. A. Resende and A. C. Drummond, 2018. Http and contact-based features for botnet detection. *Security and Privacy*, 1(5):e41. ISSN 2475-6725. doi:ARTNe4110.1002/spy2.41.

[211]. M. S. Elsayed, N. A. Le-Khac, and A. D. Jurcut, 2020. Insdn: A novel sdn intrusion dataset. *Ieee Access*, 8:165263–165284. ISSN 2169-3536. doi:10.1109/Access.2020.3022633.

[212]. M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. Othman, 2021. A detailed analysis of benchmark datasets for network intrusion detection system. *Asian Journal of Research in Computer Science*, 7(4):14–33.

[213]. C. Chen, 2002. *Freeway performance measurement system (PeMS)*. University of California, Berkeley. ISBN 0496299891.

[214]. C. Chen, J. Kwon, J. Rice, A. Skabardonis, and P. Varaiya, 2003. Detecting errors and imputing missing data for single-loop surveillance systems. *Transportation Data Research*, 1855(1855):160–167. ISSN 0361-1981. doi:Doi10.3141/1855-20.

[215]. D. Biedermann, M. Ochs, and R. Mester, 2016. Evaluating visual adas components on the congrats dataset. In *2016 IEEE Intelligent Vehicles Symposium (IV)*, pages 986–991. IEEE. ISBN 1509018212.

[216]. C. Morris, N. M. Kriege, F. Bause, K. Kersting, P. Mutzel, and M. Neumann, 2020. Tudataset: A collection of benchmark datasets for learning with graphs. *arXiv preprint arXiv:2007.08663*.

[217]. W. Hu, M. Fey, H. Ren, M. Nakata, Y. Dong, and J. Leskovec, 2021. Ogb-lsc: A large-scale challenge for machine learning on graphs. *arXiv preprint arXiv:2103.09430*.

[218]. A. Gharib, I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, 2016. An evaluation framework for intrusion detection dataset. In *2016 International Conference on Information Science and Security (ICISS)*, pages 1–6. IEEE. ISBN 1509054936.

[219]. B. Sangster, T. O'Connor, T. Cook, R. Fanelli, E. Dean, C. Morrell, and G. J. Conti, 2009. Toward instrumenting network warfare competitions to generate labeled datasets. In *CSET*.

[220]. I. Perona, O. Arbelaitz, I. Gurrutxaga, J. Martín, J. Muguerza, and J. M. Perez, 2016. Generation of the database gurekddcup.

[221]. G. Maciá-Fernández, J. Camacho, R. Magán-Carrión, P. García-Teodoro, and R. Therón, 2018. Ugr '16: A new dataset for the evaluation of cyclostationarity-based network idss. *Computers & Security*, 73:411–424. ISSN 0167-4048.

[222]. E. K. Viegas, A. O. Santin, and L. S. Oliveira, 2017. Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*, 127:200–216. ISSN 1389-1286. doi:10.1016/j.comnet.2017.08.013.

[223]. M. J. Turcotte, A. D. Kent, and C. Hash, 2019. *Unified host and network data set*, pages 1–22. World Scientific. ISBN 2059-1063.

[224]. Y. Li, Z. An, Z. Wang, Y. Zhong, S. Chen, and C. Feng, 2022. V2x-sim: A virtual collaborative perception dataset for autonomous driving. *arXiv preprint arXiv:2202.08449*.

[225]. R. Krajewski, J. Bock, L. Kloeker, and L. Eckstein, 2018. The highd dataset: A drone dataset of naturalistic vehicle trajectories on german highways for validation of highly automated driving systems. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 2118–2125. IEEE. ISBN 1728103231.

[226]. L. L. Cárdenas, A. M. Mezher, P. A. B. Bautista, J. P. A. León, and M. A. Igartua, 2021. A multimetric predictive ann-based routing protocol for vehicular ad hoc networks. *IEEE access*, 9:86037–86053. ISSN 2169-3536.

[227]. L. L. Cárdenas, J. P. A. León, and A. M. Mezher, 2022. Gratree: A gradient boosting decision tree based multimetric routing protocol for vehicular ad hoc networks. *Ad Hoc Networks*, 137:102995.

[228]. W. D. o. Transportation, 2021. Wyoming cv pilot basic safety message one day sample. doi:http://doi.org/10.21949/1504479.

[229]. D. Bezzina and J. Sayer, 2015. Safety pilot model deployment: Test conductor team report usdot report no. dot hs 812 171.

[230]. K. Tavares and T. C. Ferreto, 2021. P4-onids: A p4-based nids optimized for constrained programmable data planes in sdn. *Anais do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2021, Brasil.*

[231]. L. Zheng, Z. Bie, Y. Sun, J. Wang, C. Su, S. Wang, and Q. Tian, 2016. Mars: A video benchmark for large-scale person re-identification. In *European conference on computer vision*, pages 868–884. Springer.

[232]. M. A. Amanullah, M. B. Chhetri, S. W. Loke, and R. Doss, 2022. Burst-adma: Towards an australian dataset for misbehaviour detection in the internet of vehicles. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 624–629. IEEE.

[233]. A. Thakkar and R. Lohiya, 2020. A review of the advancement in intrusion detection datasets. *International Conference on Computational Intelligence and Data Science*, 167:636–645. ISSN 1877-0509. doi:10.1016/j.procs.2020.03.330.

[234]. M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. Othman, 2021. A detailed analysis of benchmark datasets for network intrusion detection system. *Asian Journal of Research in Computer Science*, 7(4):14–33.

[235]. B. Vijayalakshmi, K. Ramar, N. Jhanjhi, S. Verma, M. Kaliappan, K. Vijayalakshmi, S. Vimal, and U. Ghosh, 2021. An attention-based deep learning model for traffic flow prediction using spatiotemporal features towards sustainable smart city. *International Journal of Communication Systems*, 34(3):e4609. ISSN 1074-5351.

[236]. R. Doenges, M. T. Arashloo, S. Bautista, A. Chang, N. Ni, S. Parkinson, R. Peterson, A. Solko-Breslin, A. Xu, and N. Foster, 2021. Petr4: formal foundations for p4 data planes. *Proceedings of the ACM on Programming Languages*, 5(POPL).

[237]. V. Belenko, V. Krundyshev, and M. Kalinin, 2010. Synthetic datasets generation for intrusion detection in vanet. In *Proceedings of the 11th international conference on security of information and networks*, pages 1–6.

[238]. F. Gonçalves, B. Ribeiro, O. Gama, J. Santos, A. Costa, B. Dias, M. J. Nicolau, J. Macedo, and A. Santos, 2020. Synthesizing datasets with security threats for vehicular ad-hoc networks. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pages 1–6. IEEE. ISBN 1728182980.

[239]. D. Swessi and H. Idoudi, 2021. A comparative review of security threats datasets for vehicular networks. In *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pages 746–751. IEEE. ISBN 1665440325.

[240]. M. Andreessen, 2011. Why software is eating the world. *Wall Street Journal*, 20(2011):C2.

[241]. M. Hergaarden, 2011. Graphics shaders. *Graphics Shaders*, page 1.

[242]. B. O'Connor, Y. Tseng, M. Pudelko, C. Cascone, A. Endurthi, Y. Wang, A. Ghaffarkhah, D. Gopalpur, T. Everman, and T. Madejski, 2019. Using p4 on fixed-pipeline and programmable stratum switches. In *2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, pages 1–2. IEEE. ISBN 172814387X.

[243]. PLVision, 2021. The best open source network operating system: Sonic, stratum or dent os? *plvision.eu*.

[244]. K. Y. Guo, S. L. Zeng, J. C. Yu, Y. Wang, and H. Z. Yang, 2019. [dl] a survey of fpga-based neural network inference accelerators. *Acm Transactions on Reconfigurable Technology and Systems*, 12(1):1–26. ISSN 1936-7406. doi:Artn210.1145/3289185.

[245]. L. Danys, R. Martinek, R. Jaros, J. Baros, P. Simonik, and V. Snasel, 2021. Enhancements of sdr-based fpga system for v2x-vlc communications. *Cmc-Computers Materials & Continua*, 68(3):3629–3652. ISSN 1546-2218. doi:10.32604/cmc.2021.017333.

[246]. K. Kiela, M. Jurgo, and R. Navickas, 2020. Structure of v2x-iot framework for its applications. In *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, pages 229–234. IEEE. ISBN 1728163765.

[247]. P. Kumar, 2021. Toward predictable networks. *acm theses*.

[248]. R. Glebke, J. Krude, I. Kunze, J. Rüth, F. Senger, and K. Wehrle, 2019. Towards executing computer vision functionality on programmable network devices. In *Proceedings of the 1st ACM CoNEXT Workshop on Emerging in-Network Computing Paradigms*, pages 15–20.

[249]. C. Busse-Grawitz, R. Meier, A. Dietmüller, T. Bühler, and L. Vanbever, 2019. pforest: In-network inference with random forests. *arXiv preprint arXiv:1909.05680*.

[250]. S. A. Gutiérrez, J. W. Branch, L. P. Gaspary, and J. F. Botero, 2021. Watching smartly from the bottom: Intrusion detection revamped through programmable networks and artificial intelligence. *arXiv preprint arXiv:2106.00239*.

[251]. E. Talpes, A. Gorti, G. S. Sachdev, D. D. Sarma, G. Venkataramanan, P. Bannon, B. McGee, B. Floering, A. Jalote, C. Hsiong, and S. Arora, 2020. Compute solution for tesla's full self-driving computer. *Ieee Micro*, 40(2):25–35. ISSN 0272-1732. doi:10.1109/Mm.2020.2975764.

[252]. P. K. D. Jagannadha, M. Yilmaz, M. Sonawane, S. Chadalavada, S. Sarangi, B. Bhaskaran, S. Bajpai, V. A. Reddy, J. Pandey, and S. Jiang, 2019. Special session: in-system-test (ist) architecture for nvidia drive-agx platforms. In *2019 IEEE 37th VLSI Test Symposium (VTS)*, pages 1–8. IEEE. ISBN 1728111706.

[253]. V. T. Tran, M. R. Islam, K. M. Muttaqi, and D. Sutanto, 2019. An on-board v2x electric vehicle charger based on amorphous alloy high-frequency magnetic-link and sic power devices. In *2019 IEEE Industry Applications Society Annual Meeting*, pages 1–6. IEEE. ISBN 1538645394.

[254]. Z. Chen, S. Zhang, S. Cao, S. Xu, and Y. Shi, 2020. A novel terminal aided synchronization scheme for intelligent transportation systems with vehicle-to-anything (v2x) communications. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE. ISBN 1728133203.

[255]. C. Zhang, H. Hu, S. Cao, and Z. Jiang, 2021. A novel blind detection method and fpga implementation for energy-efficient sidelink communications. In *2021 IEEE Workshop on Signal Processing Systems (SiPS)*, pages 7–11. IEEE. ISBN 1665401443.

[256]. K.-t. Lim, S.-k. Jin, and J.-m. Kwak, 2018. Design of hybrid v2x communication module for cooperative automated driving. *Journal of Advanced Navigation Technology*, 22(3):213–219. ISSN 1226-9026.

[257]. A. Guillot, A. Jallouli, A. Ly, A. Sayarath, L. Rezakhanlou, Q. Cabanes, and B. Senouci, 2017. Multi-fpga platform for smart automobiles embedded electronics design and prototyping. In *Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS)*, pages 49–53. The Steering Committee of The World Congress in Computer Science, Computer ....

[258]. H. S. Ogawa, T. E. Luther, J. E. Ricardini, H. Cunha, M. Simplicio Jr, D. F. Aranha, R. Derwig, and H. Kupwade-Patil, 2019. Accelerated v2x provisioning with extensible processor platform. *Cryptology ePrint Archive*.

[259]. Y. Park, J. Ha, S. Kuk, H. Kim, C. J. M. Liang, and J. Ko, 2014. A feasibility study and development framework design for realizing smartphone-based vehicular networking systems. *Ieee Transactions on Mobile Computing*, 13(11):2431–2444. ISSN 1536-1233. doi:10.1109/Tmc.2014.2309959.

[260]. S. Panichpapiboon and P. Leakkaw, 2017. Traffic density estimation: A mobile sensing approach. *Ieee Communications Magazine*, 55(12):126–131. ISSN 0163-6804. doi:10.1109/Mcom.2017.1700693.

[261]. Z. Xiao, F. C. Li, R. H. Wu, H. B. Jiang, Y. P. Hu, J. Ren, C. L. Cai, and A. Iyengar, 2020. Trajdata: On vehicle trajectory collection with commodity plug-and-play obu

devices. *Ieee Internet of Things Journal*, 7(9):9066–9079. ISSN 2327-4662. doi:10.1109/Jiot.2020.3001566.

[262]. T.-N. Dao, V.-P. Hoang, and C. H. Ta, 2021. Development of lightweight and accurate intrusion detection on programmable data plane. In *2021 International Conference on Advanced Technologies for Communications (ATC)*, pages 99–103. IEEE. ISBN 1665433795.

[263]. G. K. Ndonda and R. Sadre, 2018. A two-level intrusion detection system for industrial control system networks using p4. In *5th International Symposium for ICS & SCADA Cyber Security Research 2018 5*, pages 31–40.

[264]. S. Mahrach, O. Mjihil, and A. Haqiq, 2017. Scalable and dynamic network intrusion detection and prevention system. In *International Conference on Innovations in Bio-Inspired Computing and Applications*, pages 318–328. Springer.

[265]. Q. Qin, K. Poularakis, K. K. Leung, and L. Tassiulas, 2020. Line-speed and scalable intrusion detection at the network edge via federated learning. In *2020 IFIP Networking Conference (Networking)*, pages 352–360. IEEE. ISBN 3903176281.

[266]. N. Gray, K. Dietz, M. Seufert, and T. Hossfeld, 2021. High performance network metadata extraction using p4 for ml-based intrusion detection systems. In *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, pages 1–7. IEEE. ISBN 1665440058.

[267]. E. M. de Oca, 2021. Sdmn security. *The Wiley 5G REF: Security*, page 25. ISSN 1119820316.

[268]. H. Siddique, M. Neves, C. Kuzniar, and I. Haque, 2021. Towards network-accelerated ml-based distributed computer vision systems. *IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS)*.

[269]. A. Bazzi, C. Campolo, B. M. Masini, and A. Molinaro, 2020. How to deal with data hungry v2x applications? In *Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, pages 333–338.

[270]. R. Simões, K. Dias, and R. Martins, 2021. Dynamic allocation of sdn controllers in nfv-based mec for the internet of vehicles. *Future Internet*, 13(11):270.

[271]. M. Arif, G. J. Wang, O. Geman, V. E. Balas, P. Tao, A. Brezulianu, and J. E. Chen, 2020. Sdn-based vanets, security attacks, applications, and challenges. *Applied Sciences-Basel*, 10(9):3217. doi:ARTN321710.3390/app10093217.

[272]. A. L. R. Madureira, F. R. C. Araujo, and L. N. Sampaio, 2020. On supporting iot data aggregation through programmable data planes. *Computer Networks*, 177:107330. ISSN 1389-1286. doi:ARTN10733010.1016/j.comnet.2020.107330.

[273]. A. O. Mufutau, F. P. Guiomar, A. Oliveira, and P. P. Monteiro, 2021. Sdr enabled c-ran implementation using openairinterface. *OpenAirInterface*.

[274]. B. Dowling and K. G. Paterson, 2018. A cryptographic analysis of the wireguard protocol. In *Applied Cryptography and Network Security: 16th International Conference, ACNS 2018, Leuven, Belgium, July 2-4, 2018, Proceedings 16*, pages 3–21. Springer.

[275]. J. A. Donenfeld and K. Milner, 2017. Formal verification of the wireguard protocol. *Technical Report, Tech. Rep.*

[276]. B. Lipp, B. Blanchet, and K. Bhargavan, 2019. A mechanised cryptographic proof of the wireguard virtual private network protocol. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 231–246. IEEE.

[277]. T. Perrin, 2018. The noise protocol framework.

[278]. A. Abdulazeez, B. Salim, D. Zeebaree, and D. Doghramachi, 2020. Comparison of vpn protocols at network layer focusing on wire guard protocol. *International Journal of Interactive Mobile Technologies (iJIM)*, 14(18).

[279]. S. Mackey, I. Mihov, A. Nosenko, F. Vega, and Y. Cheng, 2020. A performance comparison of wireguard and openvpn. In *Proceedings of the Tenth ACM Conference on data and application security and privacy*, pages 162–164.

[280]. M. Pudelko, P. Emmerich, S. Gallenmüller, and G. Carle, 2020. Performance analysis of vpn gateways. In *2020 IFIP Networking Conference (Networking)*, pages 325–333. IEEE.

[281]. S. Haga, A. Esmaeily, K. Kralevska, and D. Gligoroski, 2020. 5g network slice isolation with wireguard and open source mano: A vpnaas proof-of-concept. In *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 181–187. IEEE.

[282]. G. Thandavarayan, M. Sepulcre, and J. Gozalvez, 2019. Analysis of message generation rules for collective perception in connected and automated driving. In *2019 IEEE Intelligent Vehicles Symposium (IV)*, pages 134–139. IEEE. ISBN 1728105609.

[283]. M. Shan, S. Worrall, and E. Nebot, 2021. Development and demonstrations of cooperative perception for connected and automated vehicles. *imoveaustralia*.

[284]. G. Thandavarayan, M. Sepulcre, and J. Gozalvez, 2020. Generation of cooperative perception messages for connected and automated vehicles. *Ieee Transactions on Vehicular Technology*, 69(12):16336–16341. ISSN 0018-9545. doi:10.1109/Tvt.2020.3036165.

[285]. H. Huang, W. Fang, and H. Li, 2019. Performance modelling of v2v based collective perceptions in connected and autonomous vehicles. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 356–363. IEEE. ISBN 1728110289.

[286]. M. Tsukada, T. Oi, A. Ito, M. Hirata, and H. Esaki, 2020. Autoc2x: Open-source software to realize v2x cooperative perception among autonomous vehicles. In *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pages 1–6. IEEE. ISBN 1728194849.

[287]. M. Zhou, L. S. Han, H. W. Lu, and C. Fu, 2020. Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant. *Computer Networks*, 172:107174. ISSN 1389-1286. doi:ARTN10717410.1016/j.comnet.2020.107174.

[288]. A. Samadianzakaria, 2021. *Relational Machine Learning Algorithms*. Thesis, Department of Computer Science.

[289]. W. L. Hamilton, 2020. Graph representation learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, 14(3):77–103.

[290]. M. Nickel, K. Murphy, V. Tresp, and E. Gabrilovich, 2015. A review of relational machine learning for knowledge graphs. *Proceedings of the IEEE*, 104(1):11–33. ISSN 0018-9219.

[291]. P. Goyal and E. Ferrara, 2018. Graph embedding techniques, applications, and performance: A survey. *Knowledge-Based Systems*, 151:78–94. ISSN 0950-7051. doi:10.1016/j.knosys.2018.03.022.

[292]. F. Poggenhans, J.-H. Pauls, J. Janosovits, S. Orf, M. Naumann, F. Kuhnt, and M. Mayr, 2018. Lanelet2: A high-definition map framework for the future of automated driving. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 1672–1679. IEEE. ISBN 1728103231.

[293]. F. Gonçalves, B. Ribeiro, O. Gama, A. Santos, A. Costa, B. Dias, J. Macedo, and M. J. Nicolau, 2019. A systematic review on intelligent intrusion detection systems for vanets. In *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–10. IEEE. ISBN 1728157641.

[294]. G. Raja, S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S. V. Suryanarayan, and X.-W. Wu, 2020. Sp-cids: Secure and private collaborative ids for vanets. *IEEE Transactions on Intelligent Transportation Systems*. ISSN 1524-9050.

[295]. G. Raja, S. Anbalagan, G. Vijayaraghavan, P. Dhanasekaran, Y. D. Al-Otaibi, and A. K. Bashir, 2020. Energy-efficient end-to-end security for software-defined vehicular networks. *IEEE Transactions on Industrial Informatics*, 17(8):5730–5737. ISSN 1551-3203.

[296]. H. Bangui, M. Ge, and B. Buhnova, 2022. A hybrid machine learning model for intrusion detection in vanet. *Computing*, 104(3):503–531.

[297]. J. Meijers, E. Au, Y. Cai, H.-A. Jacobsen, S. Motepalli, R. Sun, A. Veneris, G. Zhang, and S. Zhang, 2021. Blockchain for v2x: A taxonomy of design use cases and system requirements. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 113–120. IEEE. ISBN 1665439246. doi:10.1109/BRAINS52497.2021.9569796.

[298]. H. R. Liang, J. Wu, S. Mumtaz, J. H. Li, X. Lin, and M. W. Wen, 2019. Mbid: Micro-blockchain-based geographical dynamic intrusion detection for v2x. *Ieee Communications Magazine*, 57(10):77–83. ISSN 0163-6804. doi:10.1109/Mcom.001.1900143.

[299]. H. Farran, D. Khoury, E. Kfoury, and L. Bokor, 2021. A blockchain-based v2x communication system. In *2021 44th International Conference on Telecommunications and Signal Processing (TSP)*, pages 208–213. IEEE. ISBN 166542933X.

[300]. M. Dibaei, X. Zheng, Y. H. Xia, X. W. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. J. Yu, and A. V. Vasilakos, 2021. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. *Ieee Transactions on Intelligent Transportation Systems*. ISSN 1524-9050. doi:10.1109/Tits.2020.3019101.

[301]. T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, 2022. A comprehensive survey on the applications of blockchain for securing vehicular networks. *arXiv preprint arXiv:2201.04803*.

[302]. 5GAA, 2018. V2x technology benchmark testing. Report, 5GAA.

[303]. T. Bey and G. Tewolde, 2019. Evaluation of dsrc and lte for v2x. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1032–1035. IEEE. ISBN 1728105544.

[304]. R. Molina-Masegosa, J. Gozalvez, and M. Sepulcre, 2020. Comparison of ieee 802.11 p and lte-v2x: An evaluation with periodic and aperiodic messages of constant and variable size. *IEEE Access*, 8:121526–121548. ISSN 2169-3536.

[305]. J. Wang, Y. Shao, Y. Ge, and R. Yu, 2019. A survey of vehicle to everything (v2x) testing. *Sensors (Basel)*, 19(2):334. ISSN 1424-8220 (Electronic) 1424-8220 (Linking). doi:10.3390/s19020334.

[306]. ETSI, 2017. Telecommunications and internet converged services and protocols for advanced networking (tispan); methods and protocols; part 2: Protocol framework definition; security counter measures. *ETSI TS 102 165-2 V4.2.1 (2007-02)*.

[307]. Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, 2022. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*. ISSN 1553-877X.

[308]. M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, 2022. Cellular, wide-area, and non-terrestrial iot: A survey on 5g advances and the road towards 6g. *IEEE Communications Surveys & Tutorials*. ISSN 1553-877X.

[309]. F. Salahdine and N. Kaabouch, 2020. Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. *Physical Communication*, 39:101001. ISSN 1874-4907. doi:ARTN10100110.1016/j.phycom.2020.101001.

[310]. A. Ali, L. Feng, A. K. Bashir, S. El-Sappagh, S. H. Ahmed, M. Iqbal, and G. Raja, 2018. Quality of service provisioning for heterogeneous services in cognitive radio-enabled internet of things. *IEEE Transactions on Network Science and Engineering*, 7(1):328–342. ISSN 2327-4697.

[311]. G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M. Baskaran, K. Raja, and A. K. Bashir, 2020. Intelligent reward-based data offloading in next-generation vehicular networks. *Ieee Internet of Things Journal*, 7(5):3747–3758. ISSN 2327-4662. doi:10.1109/Jiot.2020.2974631.

[312]. M. M. Bronstein, J. Bruna, T. Cohen, and P. Veličković, 2021. Geometric deep learning: Grids, groups, graphs, geodesics, and gauges. *arXiv preprint arXiv:2104.13478*.

[313]. L. R. Medsker and L. Jain, 2001. Recurrent neural networks. *Design and Applications*, 5(64-67):2.

[314]. J. J. Hopfield, 1982. Neural networks and physical systems with emergent collective computational abilities. *Proceedings of the national academy of sciences*, 79(8):2554–2558.

[315]. G. E. Hinton, T. J. Sejnowski, et al., 1986. Learning and relearning in boltzmann machines. *Parallel distributed processing: Explorations in the microstructure of cognition*, 1(282-317):2.

[316]. C. Olah, 2015. Understanding lstm networks. *https://colah.github.io/posts/2015-08-Understanding-LSTMs/*.

[317]. S. Hochreiter and J. Schmidhuber, 1997. Long short-term memory. *Neural computation*, 9(8):1735–1780.

[318]. K. Cho, B. Van Merriënboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, and Y. Bengio, 2014. Learning phrase representations using rnn encoder-decoder for statistical machine translation. *arXiv preprint arXiv:1406.1078*.

[319]. A. Zafar, M. Aamir, N. Mohd Nawi, A. Arshad, S. Riaz, A. Alruban, A. K. Dutta, and S. Almotairi, 2022. A comparison of pooling methods for convolutional neural networks. *Applied Sciences*, 12(17):8643.

[320]. H. Gao and S. Ji, 2019. Graph u-nets. In *international conference on machine learning*, pages 2083–2092. PMLR.

[321]. G. E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever, and R. R. Salakhutdinov, 2012. Improving neural networks by preventing co-adaptation of feature detectors. *arXiv preprint arXiv:1207.0580*.

[322]. C. F. G. D. Santos and J. P. Papa, 2022. Avoiding overfitting: A survey on regularization methods for convolutional neural networks. *ACM Computing Surveys (CSUR)*, 54(10s):1–25.

[323]. M. Gori, G. Monfardini, and F. Scarselli, 2005. A new model for learning in graph domains. In *Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.*, volume 2, pages 729–734. IEEE.

[324]. F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, 2008. The graph neural network model. *IEEE transactions on neural networks*, 20(1):61–80.

[325]. B. Perozzi, R. Al-Rfou, and S. Skiena, 2014. Deepwalk: Online learning of social representations. In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 701–710.

[326]. A. Grover and J. Leskovec, 2016. node2vec: Scalable feature learning for networks. In *Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 855–864.

[327]. J. Tang, M. Qu, M. Wang, M. Zhang, J. Yan, and Q. Mei, 2015. Line: Large-scale information network embedding. In *Proceedings of the 24th international conference on world wide web*, pages 1067–1077.

[328]. Z. Yang, W. Cohen, and R. Salakhudinov, 2016. Revisiting semi-supervised learning with graph embeddings. In *International conference on machine learning*, pages 40–48. PMLR.

[329]. I. J. King and H. H. Huang, 2022. Euler: Detecting network lateral movement via scalable temporal link prediction. In *Network and Distributed System Security Symposium*, pages 1–36.

[330]. T. N. Kipf and M. Welling, 2016. Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907*.

[331]. P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, 2017. Graph attention networks. *arXiv preprint arXiv:1710.10903*.

[332]. J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, and G. E. Dahl, 2017. Neural message passing for quantum chemistry. In *International conference on machine learning*, pages 1263–1272. PMLR.

[333]. L. McInnes, J. Healy, and J. Melville, 2018. Umap: Uniform manifold approximation and projection for dimension reduction. *arXiv preprint arXiv:1802.03426*.

[334]. M. K. Rahman and A. Azad, 2021. A comprehensive analytical survey on unsupervised and semi-supervised graph representation learning methods. *arXiv preprint arXiv:2112.10372*.

[335]. T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, 2013. Distributed representations of words and phrases and their compositionality. *Advances in neural information processing systems*, 26.

[336]. H. Dai, B. Dai, and L. Song, 2016. Discriminative embeddings of latent variable models for structured data. In *International conference on machine learning*, pages 2702–2711. PMLR.

[337]. X. Zhang, C. Huang, Y. Xu, L. Xia, P. Dai, L. Bo, J. Zhang, and Y. Zheng, 2021. Traffic flow forecasting with spatial-temporal graph diffusion network. In *Proceedings of the AAAI conference on artificial intelligence*, volume 35(17), pages 15008–15015.

[338]. X. Wang, Y. Ma, Y. Wang, W. Jin, X. Wang, J. Tang, C. Jia, and J. Yu, 2020. Traffic flow prediction via spatial temporal graph neural network. In *Proceedings of the web conference 2020*, pages 1082–1092.

[339]. H. Peng, H. Wang, B. Du, M. Z. A. Bhuiyan, H. Ma, J. Liu, L. Wang, Z. Yang, L. Du, S. Wang, et al., 2020. Spatial temporal incidence dynamic graph neural networks for traffic flow forecasting. *Information Sciences*, 521:277–290.

[340]. L. Zhao, Y. Song, C. Zhang, Y. Liu, P. Wang, T. Lin, M. Deng, and H. Li, 2019. T-gcn: A temporal graph convolutional network for traffic prediction. *IEEE transactions on intelligent transportation systems*, 21(9):3848–3858.

[341]. B. Rozemberczki, P. Scherer, Y. He, G. Panagopoulos, A. Riedel, M. Astefanoaei, O. Kiss, F. Beres, G. López, N. Collignon, et al., 2021. Pytorch geometric temporal: Spatiotemporal signal processing with neural machine learning models. In *Proceedings of the 30th ACM International Conference on Information & Knowledge Management*, pages 4564–4573.

[342]. M. Fey and J. E. Lenssen, 2019. Fast graph representation learning with pytorch geometric. *arXiv preprint arXiv:1903.02428*.

[343]. A. D. Kent, 2015. Comprehensive, multi-source cyber-security events data set. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States).

[344]. W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, 2022. E-graphsage: A graph neural network based intrusion detection system for iot. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pages 1–9. IEEE.

[345]. W. Hamilton, Z. Ying, and J. Leskovec, 2017. Inductive representation learning on large graphs. *Advances in neural information processing systems*, 30.

[346]. A. Sehanobish, N. G. Ravindra, and D. van Dijk, 2020. Self-supervised edge features for improved graph neural network training. *arXiv preprint arXiv:2007.04777*.

[347]. Y. Li, R. Yu, C. Shahabi, and Y. Liu, 2017. Diffusion convolutional recurrent neural network: Data-driven traffic forecasting. *arXiv preprint arXiv:1707.01926*.

[348]. A. Pareja, G. Domeniconi, J. Chen, T. Ma, T. Suzumura, H. Kanezashi, T. Kaler, T. Schardl, and C. Leiserson, 2020. Evolvegcn: Evolving graph convolutional networks for dynamic graphs. In *Proceedings of the AAAI conference on artificial intelligence*, volume 34(04), pages 5363–5370.

[349]. G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, 2023. Novel hyper-tuned ensemble random forest algorithm for the detection of false basic safety messages in internet of vehicles. *ICT Express*, 9(1):122–129.

[350]. G. O. Anyanwu, C. I. Nwakanma, J.-H. Kim, J.-M. Lee, and D.-S. Kim, 2022. Misbehavior detection in connected vehicles using burst-adma dataset. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 874–878. IEEE.

[351]. G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, 2023. Falsification detection system for iov using randomized search optimization ensemble algorithm. *IEEE Transactions on Intelligent Transportation Systems*.

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Mehmet Fatih YÜCE
Uyruğu	[X] T.C. [ ] Diğer:
Web Adresi	

Eğitim Bilgileri	
Lisans	
Üniversite	Dokuz Eylül Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölümü	Bilgisayar Mühendisliği (İngilizce)
Mezuniyet Yılı	2011

Yüksek Lisans	
Üniversite	İstanbul Aydın Üniversitesi
Enstitü Adı	Fen Bilimleri
Anabilim Dalı	Bigisayar Mühendisliği
Programı	Bilgisayar Mühendisliği
Mezuniyet Tarihi	2017

Doktora	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri
Anabilim Dalı	Akıllı Ulaşım Sistemleri Anabilim Dalı
Programı	Akıllı Ulaşım Sistemleri Programı
Mezuniyet Tarihi	2024

Makale ve Bildiriler

Makaleler

Yuce, M. F., Erturk, M. A., & Aydin, M. A. (2024). Misbehavior detection with spatio-temporal graph neural networks. Computers and Electrical Engineering, 116, 109198.

Yuce, M. F. (2024), "BurST-ADMA Dataset For Spatio-Temporal GNNs", Mendeley Data, V1, doi: 10.17632/m92r72fv23.1

"EvolveGCNO_improved", https://github.com/mfyuce/EvolveGCNO_improved", last accessed: 2024-03-25

Yuce, M. F., Erturk, M. A., & Aydin, M. A. (Under Review). Misbehavior Detection with Collective Perception in V2X Networks: A Survey. Transactions on Emerging

Telecommunications Technologies

Yuce, M. F., Kesin, O., Yerlikaya, E., Kirca, A., Erturk, M. A., Gurkas-Aydin, Z., Turna, O.C., Durukan-Odabasi, S., & Aydin, M. A. (Under Review). WireGuard with Hardware Encryption. Turkish Journal of Electrical Engineering & Computer Sciences

Patent (Beklemede) 2021/017991 Özel Blok Zinciri Tabanlı Güvenli Eternet ve Local Ağlar

Patent (Beklemede) 2021/021908 Bir Sertifika Oluşturma ve Dağıtma Sistemi

Bildiriler

Final Review of IMMINENCE project (2024-03-21), in Nokia premises (María Tubau, 9 – Madrid),Celtic-Next project IMMINENCE