DeepL

Subscribe to DeepL Pro to translate larger documents.
Visit www.DeepL.com/pro for more information.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Alındı 13 Mart 2023, kabul edildi 29 Mart 2023, yayın tarihi 6 Nisan 2023, güncel versiyon tarihi 13 Nisan 2023.

Dijital Nesne Tanımlayıcı 10.1109/ACCESS.2023.3265018

RESEARCH ARTICLE

Araç İçi Ağ için Çoklu Gözlem HMM Tabanlı CAN Veri Yolu İzinsiz Giriş Tespit Sistemi

CHEN DONG , HAO WU , (Üye, IEEE), VE QINGYUAN LI
Demiryolu Trafik Kontrolü ve Güvenliği Devlet Anahtar Laboratuvarı, Pekin Jiaotong Üniversitesi, Pekin 100044, Çin

Sorumlu yazar: Hao Wu (hwu@bjtu.edu.cn)

Bu çalışma kısmen Hibe 2022JBQY004 kapsamında Merkezi Üniversiteler için Temel Araştırma Fonları tarafından ve kısmen Hibe 62221001 kapsamında Çin Ulusal Doğa Bilimleri Vakfı tarafından ve kısmen de Frontiers Science Center for Smart tarafından desteklenmiştir.
Yüksek Hızlı Demiryolu Sistemi.

ÖZET Modern araçlar daha akıllı ve bağlantılı hale geldikçe, ECU'ların ve harici ağlarla (3G/4G ve Bluetooth gibi) iletişim arayüzlerinin sayısı önemli ölçüde artmış ve bu da potansiyel ağ güvenliği risklerini artırmıştır. Etkili güvenlik önlemlerinin yokluğu nedeniyle, araçları, özellikle de araç içi CAN veri yolu ağını hedef alan siber güvenlik olayları sık sık meydana gelmektedir. ana veri yolu CAN veri yolu, güvenlik mekanizmalarının eksikliği nedeniyle güvenliğinde önemli zorluklarla karşı karşıyadır. Bu nedenle, aracın güvenliğini artırmak için araç içi ağlar için çoklu gözlem HMM'ye dayalı bir CAN veri yolu saldırı tespit sistemi öneriyoruz. Özellikle, önerilen algoritma normal CAN veri yolu trafiğinin kimlik ve veri alanlarına dayalı bir çoklu gözlem HMM'si oluşturur. Oluşturulan HMM'lere göre, tanımlanan zaman penceresi altındaki çerçevenin var olma olasılığını algılama eşiği olarak hesaplıyoruz. Tespit edilecek çerçevenin var olma olasılığı normal eşik aralığını aştığında, anormal olarak kabul edilir. Ayrıca, toplanan gerçek araç verilerine dayanarak dört yaygın saldırı modeli oluşturuyor ve önerilen algoritmanın bu saldırı senaryolarındaki performansını değerlendiriyoruz. Deneysel sonuçlar, önerilen yöntemin dört saldırı senaryosunda diğer kare kare anormallik tespit yöntemlerinden daha iyi tespit performansına sahip olduğunu göstermektedir.

DİZİN TERİMLERİ CAN veri yolu saldırı tespiti, HMM, çoklu gözlem dizisi, araç içi ağlar.

I. GİRİŞ

Son yıllarda Akıllı Ulaşım Sistemlerinin (ITS) sürekli gelişimi ile akıllı ve bağlantılı araçlar (ICV'ler), araç içi ağların (IVN'ler) artan karmaşıklığına yol açan modern araçların umut verici bir paradigması haline gelmiştir [1]. IVN'lerde fren kontrolü, şanzıman kontrolü, karoseri kontrolü gibi çeşitli işlevleri destekleyen 100'den fazla elektronik kontrol ünitesi (ECU) kullanılmakta ve araç içi veri yolu üzerinden bilgi alışverişi gerçekleştirilmektedir [2]. Ayrıca, karar vermeye yardımcı olmak için çevreyle daha fazla bilgi paylaşmayı amaçlayan [3], [4], ICV'ler Bluetooth, WiFi ve hücresel ağ gibi bir dizi harici kablosuz etkileşim yüzeyi eklemiş, ancak aynı zamanda uzaktan saldırı yüzeylerini de artırmıştır. Sonuç olarak, bilgisayar korsanları araçla doğrudan temas etmeden IVN'lere erişebilir, aracın özel bilgilerini elde edebilir ve hatta araç güvenliği için büyük tehdit oluşturacak ölümcül kazalara neden olabilir.

En yaygın kullanılan araç içi iletişim veriyolu olan kontrolör alan ağı (CAN), giderek artan benzeri görülmemiş güvenlik tehditleriyle karşı karşıyadır. Ancak CAN veri yolu, bir zamanlar aracın kapalı bir mekanik sistem olduğu düşünüldüğünden, günümüzün siber saldırılarıyla başa çıkmak için yeterli güvenlik mekanizmalarıyla tasarlanmamıştır. Örneğin, ECU'lar CAN veri üzerinden veri yayınladığından, veri yoluna bağlı tüm ECU'lar bu verileri gerçek zamanlı olarak izler, bu da bir saldırganın kolayca dinlemek için yalnızca bir ECU'yu kontrol etmesi gerektiği anlamına gelir. Son yıllarda CAN b us'a yönelik saldırılar sıklıkla ortaya çıkmıştır. 2015 yılında Miller ve Valasek [5] Jeep Cherokee'yi aracın eğlence sistemindeki bir güvenlik açığı aracılığıyla ele geçirmiş ve ardından adresinden CAN veri yoluna uzaktan mesaj göndererek frenlerin havasını alabilmiştir. 2019 yılında, Cai ve diğerleri [6]

Bu makalenin incelenmesini koordine eden ve yayınlanması için onay veren yardımcı editör Shaohua Wan'dır.

Bu çalışma Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 Lisansı altında lisanslanmıştır.
Daha fazla bilgi için bkz. https://creativecommons.org/licenses/by-nc-nd/4.0/

bir saldırganın sürücü koltuğunu hareket ettirmek ve ECU'ları sıfırlamak için CAN veri yoluna uzaktan mesajlar göndererek BMW araçlarındaki güvenlik açıklarından yararlanabileceğini göstermiştir. 2022 küresel otomotiv siber güvenlik raporunda [7] , Upstream Securityotomotiv hack saldırılarının sayısının 2021'de 2018'e kıyasla 2,25 kattan fazla arttığını belirtmiştir.

Hızla büyüyen araç siber güvenliği sorunları nedeniyle, özellikle CAN veri yolundaki risk ve tehditleri ele almak için kapsamlı araştırmalar yapılmıştır. Genel olarak, CAN veri yolu için güvenlik çözümleri üç yöne ayrılır: mesaj kimlik doğrulama ve şifreleme [8], saldırı tespit sistemi [9] ve genel güvenlik çerçeveleri. Şifreleme ve kimlik doğrulamanın ana koruma yöntemleri çerçeve mesajlarının kimlik doğrulaması veya anahtar şifrelemesidir. Bununla birlikte, CAN veri yolunun sınırlı iletişim kapasitesi nedeniyle, şifreleme ve kimlik doğrulama algoritmaları CAN veri yolu üzerindeki yükü artıracak ve hatta veri yolu gerçek zamanlı iletişimini etkileyecektir. Öte yandan, genel güvenlik koruma şeması, aracın mevcut donanım ve yazılımını değiştirmeyi gerektirdiğinden kısa sürede uygulanamaz. Mevcut deneysel koşullar altında, saldırı tespiti araç ağ güvenliği araştırmalarında giderek önemli bir konu haline gelmektedir. Bununla birlikte, CAN veri yolu için mevcut son teknoloji saldırı tespit yöntemleri önemli zorluklarla karşılaşmaktadır. Birçok yöntem tek bir çerçeveyi saldırı çerçevesi olarak tanımlamak yerine belirli bir süre boyunca saldırıları tespit etmeyi amaçlamaktadır. Ayrıca, birçok saldırı tespit şeması, gerçek dünya senaryolarında toplanması genellikle zor olan önemli miktarda saldırı verisi gerektirir. Bu amaçla, çoklu gözlem HMM tabanlı, kare kare CAN saldırı tespit sistemi öneriyoruz.

Spesifik olarak, ana katkılarımız aşağıdaki gibi özetlenebilir.

(1) Araç içi ağ çalışmaları için çoklu gözlem HMM tabanlı bir CAN veri yolu İzinsiz Giriş Tespit Sistemi (MOHIDS) öneriyoruz. Şema, çerçevelerin kimlik özelliklerini ve veri alanı özelliklerini kapsamlı bir şekilde dikkate alır ve yalnızca normal araç çalışması sırasında veri yolu verilerine bağlıdır.

(2) Mevcut araç yapısını değiştirmeden algılama ayrıntı düzeyini iyileştiren ve saldırı yanıt süresini kısaltan bir kare kare algılama algoritması önerdik. Buna ek olarak, önerdiğimiz algoritma saldırı blokları yerine belirli saldırı çerçevelerini doğru bir şekilde bulabilmektedir.

(3) Dört yaygın saldırı senaryosu oluşturduk ve önerilen algoritmayı gerçek araç verileri ve CAN veri yolu için saldırı platformu ile değerlendirdik. Değerlendirme sonuçları, önerilen yöntemin dört saldırı senaryosunu etkili bir şekilde tespit edebildiğini ve diğer tek kare tespit algoritmalarından daha üstün olduğunu göstermektedir. Bu makalenin geri kalanı aşağıdaki şekilde düzenlenmiştir. Bölüm IIde, CAN veri yolu için güvenlik durumları ve saldırı tespit sistemleri üzerine yapılan ilgili çalışmalar tartışılmaktadır. Bölüm III'te CAN veri yolunun temel özellikleri, güvenlik açıkları ve saldırı senaryoları tanıtılmaktadır. Bölüm IV'te MOHIDS'in tasarımı açıklanmaktadır. Bölüm V'te, değerlendirme için deneysel kurulumu açıklıyor ve deneyleri sunuyoruz ve sonuçlar. Bölüm VI'da MOHIDS'in sınırlamaları ve gelecekteki çalışmalar için olası yönler tartışılmaktadır.

II. İLGİLİ ÇALIŞMALAR

A. CAN GÜVENLIK ANALIZI

2010 yılında Koscher ve arkadaşları [10] modern araçların CAN güvenliği üzerine çok kapsamlı bir analiz gerçekleştirerek modern araçların güvenlik riskleri için ilk deneysel rehberlik araştırmasını sağlamışlardır. CAN veri yolunun güvenlik zafiyetini kapsamlı bir şekilde değerlendirmişler ve aracın önemli ECU'suna karşı koklama, bulanık test ve tersine mühendislik gibi saldırıları ele almışlardır. Deneyde yazar, CAN veri yolunun motor, radyo ekipmanı, gösterge sistemi, kilit ve silecek gibi temel bileşenlerini başarıyla kontrol etmiş ve ardından çeşitli bileşenlerin güvenlik özelliklerini ayrıntılı olarak analiz etmiştir. 2012 yılında Lin ve arkadaşları [11] saldırı düğümlerini saldırı yeteneklerindeki farklılığa göre güçlü saldırganlar ve zayıf saldırganlar olarak ikiye ayırmış ve yeniden oynatma saldırısı ve sahtecilik dahil olmak üzere dört saldırı senaryosunu tanımlamak için bir saldırı modeli oluşturmuştur. Son olarak, düşük veri yolu yüküne ve düşük zaman maliyetine sahip bir güvenlik mekanizması sunulmuştur. 2015 yılında Woo ve arkadaşları [12], bir saldırganın akıllı telefon uygulamasına kötü amaçlı yazılım yerleştirerek araç CAN veri yoluna uzaktan kablosuz saldırı gerçekleştirmesinin mümkün olduğunu deneyler yoluyla kanıtlamıştır. Kurban akıllı telefonu hedef araca bağlamak için Blue tooth veya WiFi kullandığında, yazar dört tür saldırı deneyimini tamamlamıştır: gösterge panelinin tahrip edilmesi, motor durdurma, tutamak kontrolü ve yerleştirilen kötü amaçlı program aracılığıyla hızlanma . 2022 yılında Jo ve arkadaşları [13] araç içi CAN saldırıları üzerine mevcut araştırmaları sistematik olarak analiz etmiş ve ardından ortak saldırı yüzeylerini, farklı saldırgan türlerini araç CAN'ının ilgili çoklu saldırı senaryolarını özetlemiştir.

B. SALDIRI TESPİT SİSTEMİ (IDS)

CAN veri yolunun mevcut saldırı tespit teknolojileri üç kategoriye ayrılabilir: (1) frekans tabanlı saldırı tespit teknikleri, (2) veri alanı tabanlı saldırı tespit teknikleri ve (3) hibrit tabanlı saldırı tespit teknikleri.

(1) frekans tabanlı saldırı tespit teknikleri: Çerçeveler genellikle CAN veri yolu üzerinde periyodik olarak iletilir, bu da iletim aralığının veya frekansının tespit için bir temel oluşturmasına yardımcı olur. 2016 yılında Song ve arkadaşları [14] CAN veri yolu çerçevelerinin periyodik özelliklerine dayalı olarak CAN veri yolu saldırı tespiti için hafif bir tespit algoritması önermiştir, ancak saldırı verileri analiz edilirken karmaşık saldırı senaryoları dikkate alınmamıştır, bu nedenle tespit hassasiyeti düşüktür ve periyodik olmayan çerçevelere yönelik saldırılar tespit edilememiştir. 2020 yılında, Ezeobi ve diğerleri [15] CAN veri yolu için gerçek zamanlı programlama yeteneği yanıt süresine odaklanan spesifikasyon tabanlı bir algılama önermiştir. Algılama modelini oluşturmak için normal çalışma zamanı veriyolunun gerçek zamanlı zamanlamasının analizini kullandılar ve uyumlu olmayan yanıt sürelerine sahip mesajların anormal olarak kabul edildiğini tanımladılar.

2021 yılında Han ve arkadaşları [16] CAN ID'nin periyodik olay tetikleme aralığına dayalı bir tespit algoritması önermiştir. Bu yaklaşım, her CAN ID için olay tetikleme aralığının istatistiksel değerlerini karar ağaçları, rastgele ormanlar ve XGB dahil olmak üzere makine öğrenimi modellerine uygulamış ve birden fazla saldırı türüne ve iki tür araca karşı performansı değerlendirmiştir, ancak saldırının belirli ayrıntılarını vermemiştir.

(2) veri alanı tabanlı saldırı tespit teknikleri: Frekans tabanlı tespit yöntemlerine ek olarak, veri alanlarındaki değişiklikler ve mesajlardaki anlamsal değişiklikler gibi diğer özellikleri dikkate alan bazı karmaşık algoritmalar da vardır. Taylor ve arkadaşları [17]2016 yılında CAN ağlarındaki mesaj dizilerini tespit etmek için Uzun Kısa Süreli Bellek (LSTM) ağlarını kullanmıştır. Algoritma, anormal davranışları düşük bir yanlış pozitif oranla tespit edebilmektedir, ancak uygulanabilir saldırı senaryolarını açıkça sağlamamıştır. Ayrıca, algoritma her bir ID'nin veri dizisini bağımsız olarak ele aldığından, ID'ler arasındaki korelasyonu dikkate almamıştır. 2016 yılında Kang ve arkadaşları [18], özellikleri veri alanının 8 baytından alınan CAN veri yolu verileri için derin sinir ağına (DNN) dayalı bir saldırı tespit sistemi önermiştir. Önerilen algoritma, yaklaşık %98'lik ortalama tespit oranıyla saldırılara gerçek zamanlı bir yanıt sağlayabilmektedir. Bununla birlikte, ele alınabilecek saldırı türleri ayrıntılı değildir.

(3) hibrit tabanlı saldırı tespit teknikleri: 2017 yılında Markovitz ve Wool [19] CAN veri yolu için yeni bir alan farkındalı saldırı tespit sistemi önermiştir. Bilinmeyen mesajları farklı alanlara ayırmak için açgözlü bir algoritma kullandılar ve semantik analiz yoluyla bir saldırı tespit sistemi geliştirdiler. Algoritma, gerçek CAN mesajlarına dayalı olarak değerlendirildi ve düşük yanlış pozitifler elde etti. 2021 yılında Xie ve arkadaşları [20] karmaşık CAN mesaj bloklarına dayalı gelişmiş bir derin öğrenme GAN modeli önermiştir. GAN tabanlı diğer izinsiz giriş tespit modelleriyle karşılaştırıldığında, önerilen algoritma kurcalama saldırılarını etkili bir şekilde tespit edebilir, ancak kare kare tespit yapamaz ve bu da daha uzun bir yanıt süresine neden . Son yıllarda araştırmacılar, gerçek zamanlı algılama için düşük yanıt gecikmesi elde etmek için çeşitli kare kare algılama şemaları önermişlerdir. Khan ve arkadaşları [21] 2021 yılında çiçek filtresi ve çift yönlü LSTM'ye dayalı iki aşamalı bir saldırı tespit şeması önermiştir. İlk aşamada, giriş verileri Bloom filtrelerine dayalı bir sınıflandırıcıya gönderilir. Hesaplanan durum normal aralık içindeyse, daha sonra LSTM tabanlı bir dedektöre iletilir. Önerilen algoritma doğruluk ve yanlış alarm oranı açısından iyi bir performans elde etti, ancak iki aşamalı algılama süreci algılama süresini artırdı ve bu da araç donanımının hesaplama performansına belirli gereksinimler getirdi. 2021 yılında Sun ve arkadaşları [22] araç içi CAN için CNN-LSTM with Attention Model (CLAM) adında bir saldırı tespit modeli önermiştir. CLAM modeli, giriş sinyalinden özellikleri çıkarmak için tek boyutlu konvolüsyon (Conv1D) ve ardından zamansal bağımlılıkları yakalamak için çift yönlü LSTM kullanmıştır. Son olarak, tespit doğruluğunu artırmak için yumuşak bir dikkat mekanizması kullanılmıştır. Model olağanüstü anomali tespit performansı elde etmiştir.

ŞEKİL 1. CAN veri yolu mesajının çerçeve yapısı.

beş tipik saldırı senaryosundaki performansı. Bununla birlikte, eğitim süreci, pratik uygulamalarda zorluklara yol açabilecek saldırı örneklerinin miktarı ve kapsamlılığı için yüksek bir talep getirmektedir.

III. CAN BUS VE SALDIRI MODELI

Bu bölümde, araç içi CAN veri yolunun özelliklerini detaylandırıyor, güvenlik açıklarını analiz ediyor ve dört yaygın saldırı senaryosu öneriyoruz.

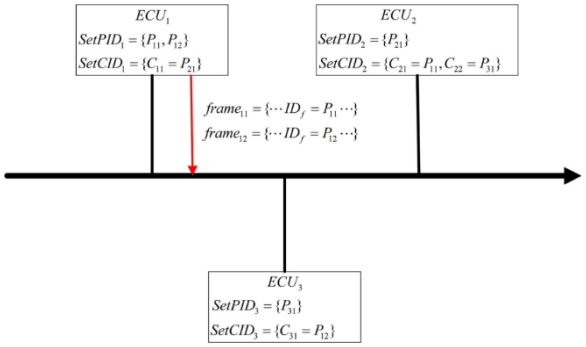
A. CAN BUS

Mesaj veya çerçeve olarak adlandırılan CAN ağ protokolü iletim birimleri şu dört türe ayrılır: veri , uzak , hata çerçeveleri ve aşırı yük çerçeveleri [22]. Bu dört çerçeve türü sırasıyla veri iletimi, komut istekleri, hata uyarıları ve aşırı yük bildirimleri görevlerini taşır. CAN veri yolu üzerindeki düğümler çerçeveleri bit bit gönderir, burada veri çerçeveleri iletimde kullanılan baskın çerçevelerdir. Tanımlayıcının (ID) uzunluğuna bağlı olarak, CAN veri yolu veri çerçeveleri 11 bitlik tanımlayıcılara sahip temel çerçevelere (CAN 2.0A) ve 29 bitlik tanımlayıcılara sahip genişletilmiş çerçevelere (CAN 2.0B) ayrılır. Bir veri çerçevesinin yapısı
[23] Şekil 1'de gösterilmiştirVeri çerçevesi çerçeve başlangıcı (SOF) ile başlar ve sonu (EOF) ile biter. Tahkim alanındaki kimlik, alıcı düğümleri ve iletim önceliğini belirleyen çerçevenin gösterir. Uzunluğu 8 bayta kadar olan veri alanı araç hızı, su sıcaklığı ve motor devri gibi özel bilgiler içerir. Kontrol alanındaki Veri Uzunluk Kodu (DLC) veri alanının boyutunu bayt cinsinden gösterir.

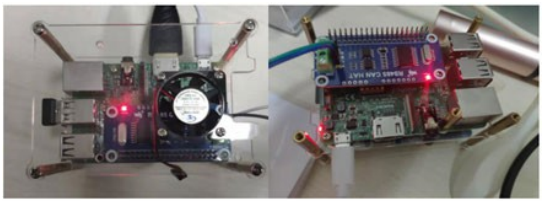
Otomatik mobil cihazlardaki çok sayıda güvenliğe duyarlı uygulama nedeniyle CAN veri yolu, mesajların yayınlandığı bir Multi-Master iletişim sistemi kullanır. CAN veri yolu kaynakları, Çarpışma Tespiti ile Taşıyıcı Algılama Çoklu Erişim (CSMA/CD) bit-bit tahkim mekanizması kullanılarak tahsis edilir. Düğüm, veriyolunu gerçek zamanlı olarak dinler ve yalnızca veriyolu boş olduğunda mesaj gönderir. Birden fazla düğüm aynı anda çerçeve gönderirse, tüm çerçevelerin kimlikleri bit bit karşılaştırılır ve daha yüksek kimliğe sahip çerçeveler düşürülür. Başka bir deyişle, daha düşük ID'li çerçeveler daha yüksek önceliğe sahiptir. Bir veri yoluna bağlı düğümler veri yolunun tüm mesajlarını dinleyebilir ve mesajları çerçeve tanımlayıcısına göre filtreleyebilir. Buna ek olarak, çerçeve gönderen ve alan düğümlerin adreslerini içermez. Düğüm, veriyolunu dinlerken kimliklere göre istenen çerçeveleri filtreler. Aslında, her ECU sınırlı sayıda çerçeve tanımlayıcısından oluşan iki set içerir.

Şekil 2'de üç ECU'lu bir CAN veri yolu iletişim sistemi gösterilmektedir. ECU_i düğümü için üretici tanımlayıcıları kümesini $SetPID_{(i)}= \{P_{(i)}{}_1, - - - , P_{in}\}$ olarak tanımlarız.
toplayıcı tanımlayıcıları $SetCID_i= \{C_{(i)(1)}, - - - , C_{in}\}$ olarak tanımlar. ECU_i olduğunda

$_{ID(f)}$ $= P_{i1}$ *ile* bir çerçeve gönderdiğinde, $ECU_{(j)}(i \neq j)$



ŞEKİL 2. CAN iletişim modeli.



ŞEKİL 3. RS465 CAN HAT ve raspberry pie mikrobilgisayar ile oluşturulmuş CAN veri yolu alıcı-vericisi.

$ID_f \in SetCID_j$ ise çerçeve. Şekil'de 3 ECU'lu bir CAN veri yolu iletişim sistemi gösterilmektedir. ECU_1 veri yoluna $ID_{(f)} = P_{11}$ ile $çerçeve_{11}$ ve $ID_f = P_{(12)}$ ile $çerçeve_{12}$ gönderir.

$P_{11} = C_{21} \in SetCID_2$ ve $P_{(11)} \notin SetCID_2$ için, $frame_{(11)}$ ECU_3 yerine $ECU_{(2)}$ tarafından alınır. Benzer şekilde, $çerçeve_{12}$ ECU_2 yerine $ECU_{(3)}$ tarafından alınır.

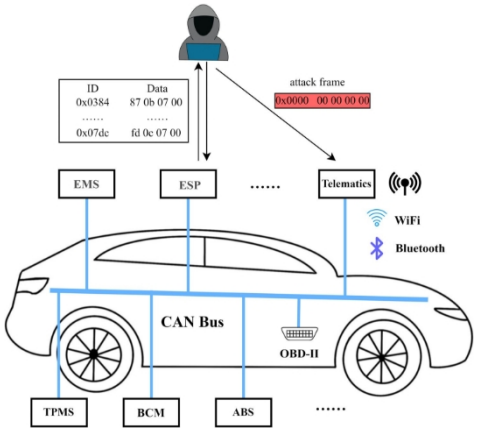
B. PRATIK DENEYLER VE GÜVENLIK AÇIĞI ANALIZI YAPABILIR

Gerçek araç CAN veri yolunun çalışma durumunu ve saldırının gerçek etkisini tam olarak incelemek için, OBD-II aracılığıyla veri yolu verilerini almak ve göndermek için Şekil 3'te gösterildiği gibi iki CAN veri yolu alıcı-verici cihazı inşa ettik. Alıcı-verici RS465 CAN HAT ve Raspberry Pie ile oluşturulmuştur. İlk olarak, RS465 CAN HAT tarafından ayrılan kontrol arayüzü Raspberry Pie'ın GPIO arayüzüne bağlanır. İkinci olarak, RS465 CAN HAT'ın H ve L arayüzleri, CAN veriyolunun OBD-II arayüzünün H ve L hatlarına bağlanır. İlk olarak, RS465 CAN HAT tarafından ayrılan kontrol arayüzü Raspberry Pie'ın GPIO arayüzüne bağlanır. İkinci olarak, RS465 CAN HAT'ın H ve L arayüzleri OBD-II arayüzünün H ve L hatlarına bağlanır. Ayrıca, veri yolu verilerini gerçek zamanlı olarak gönderebileceğimiz ve alabileceğimiz Python tabanlı bir program yazıyoruz.

Çalışan bir araca saldırı sinyalleri göndermenin yaratabileceği potansiyel tehdidi göz önünde bulundurarak, Şekil 4'te gösterildiği gibi bir CAN veri yolu saldırı platformu oluşturduk. Saldırı platformu temel olarak gerçek bir araç enstrümantasyon sistemi ve bir ağ geçidinden oluşmaktadır. Ayrıca, CAN veri yolunun güvenlik açığını doğrulamak ve veri yolu üzerindeki farklı saldırıların spesifik etkisini analiz etmek için inşa edilen alıcı-verici ile platforma saldırı uyguluyoruz.

CAN protokolünün derinlemesine analizi ve saldırı platformlarına dayalı saldırı testleri sayesinde, bazı doğal güvenlik

ŞEKİL 4. CAN veri yolu için saldırı platformu.



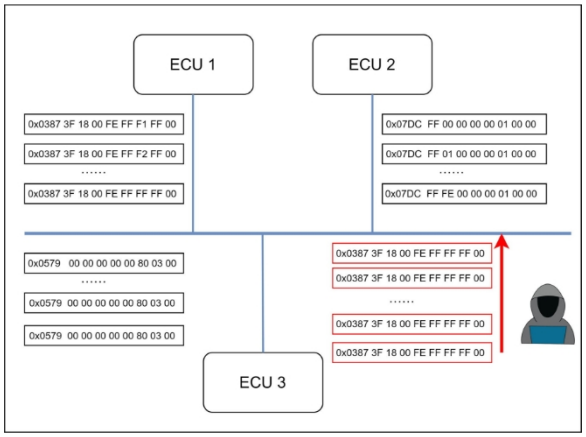
ŞEKİL 5. Araç içi CAN yapılan bir saldırının genel akışı.

CAN veri yolunun tasarımındaki güvenlik açıkları. Her şeyden önce, çoklu ana yayın iletişimi, bir düğüm bir saldırgan tarafından ele geçirilir geçirilmez, veri yolunun tüm veri sızıntısının mümkün hale gelmesine neden olur. Ayrıca, ağ trafiğini tamamen engelleyebilen dağıtılmış hizmet reddi (DDoS) saldırısına karşı savunmasızdır. Etkili bir şifreleme mekanizmasının olmaması, saldırganların özel bilgileri elde etmesini veya saldırıları enjekte etmesini kolaylaştırır. Daha da kötüsü, CAN veri yolu çerçeveleri gönderici ve alıcı bilgisi ya da zaman damgası içermez. Sonuç olarak, alıcının göndericinin meşruiyetini ve çerçevenin gerçekliğini doğrulaması zordur. Bu da saldırganın meşru kabul edilen bir çerçeve oluşturmasını büyük ölçüde zorlaştırır.

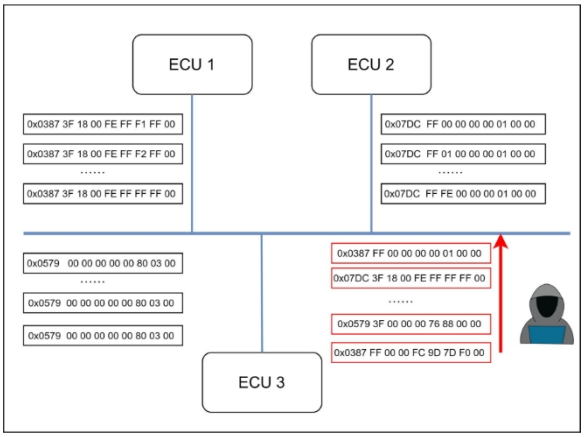
Araç içi CAN veri yoluna yönelik bir saldırının genel akışı Şekil 5'te gösterilmektedir. İlk adımda, bilgisayar korsanı hedef aracın potansiyel saldırı yüzeyini arar ve ardından veri yoluna erişmek için kablolu veya kablosuz saldırı yüzeylerini kullanır. İkinci adımda, bilgisayar korsanı çok sayıda meşru çerçeve elde etmek için veriyolunu bir dinleyici aracılığıyla izler. Üçüncü adımda, bilgisayar korsanı kötü niyetli çerçeveler oluşturur ve belirli bir saldırıyı gerçekleştirmek için bunları hedef aracın CAN veri yoluna enjekte eder.

C. SALDIRI MODELİ

Bu bölümde, saldırganın OBD-II gibi araca doğrudan bağlanarak veya WiFi ve Bluetooth gibi araca uzaktan bağlanarak araca başarılı bir şekilde girdiğini varsayıyoruz. Buna göre



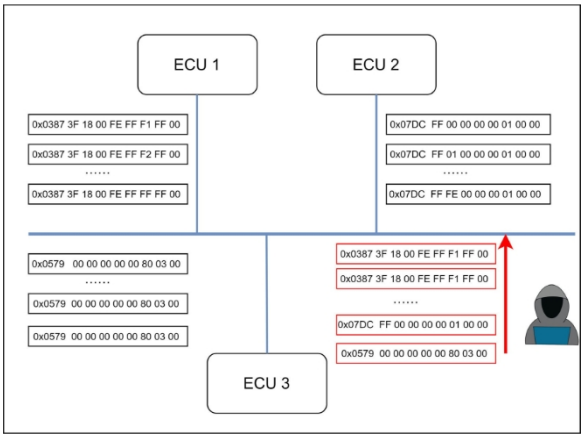
ŞEKİL 6. DDoS saldırı senaryosu.



ŞEKİL 7. Bulanık saldırı senaryosu.

Saldırganın saldırıya uğrayan veri yolu hakkındaki bilgisi, saldırı niyeti ve saldırı tekniği göz önünde bulundurularak saldırı senaryoları DDoS saldırısı, Bulanık saldırı, Tekrarlama saldırısı ve Maskeli saldırı olarak sınıflandırılmıştır. Bu saldırıların her birini, otobüs üzerindeki özel etkilerini analiz etmek için oluşturulan saldırı platformunda uyguladık.

DDoS Saldırısı: Daha önce açıklandığı gibi, CAN veri yolunun çoklu ana yayın iletim mekanizmasında, çerçeve gönderme önceliği çerçeve kimliğinin değerine bağlıdır. Şekil 6, CAN veri yoluna karşı DDoS saldırı senaryosunu göstermektedir. Veri yoluna aynı anda birden fazla çerçeve gönderildiğinde, en küçük ID değerine sahip olan çerçeve gönderme izni alacaktır. DDoS saldırıları, kısa bir süre içinde veriyoluna düşük ID'li ve yüksek öncelikli çok sayıda mesaj göndererek veriyolunu bloke eder, böylece meşru ECU tarafından gönderilen geçerli mesajlar gönderme ayrıcalıkları elde edemez ve sonuçta araç felç olur. Araçta mesaj kimliği meşruiyetinin tanımlama mekanizmasının olmaması nedeniyle, kimlik değeri yeterince küçük olduğu sürece, örneğin
0× 00, bu mesaj, bu kimlik herhangi bir çerçeve tarafından kullanılmamış olsa bile, tüm meşru çerçevelerden daha yüksek gönderme ayrıcalıklarına sahip olabilir.
meşru çerçeveyi hiç kullanamaz. Bu nedenle, saldırganın çok az ön bilgiyle böylesine ciddi bir saldırı başlatması için aracın CAN veri yolu işleyişi hakkında derin bir bilgiye sahip olması gerekmez.
Bulanık Saldırı: Bulanık saldırının prensibi, güvenlik açıklarını bulmak amacıyla veri yolunun tepkisini test etmek için veri yoluna rastgele oluşturulmuş bir mesajın gönderildiği bulanık teste benzer. Şekil 7 CAN veri karşı bulanık saldırı senaryosunu göstermektedir. Bu saldırı türünde, saldırgan veri yoluna rastgele oluşturulmuş mesajlar gönderir ve veri yolunun farklı mesajlara nasıl tepki verdiğine bağlı , saldırgan kimlik tarafından temsil edilen belirli işlev ve veri alanının değerindeki değişikliğin belirli anlamı dahil olmak üzere daha derinlemesine bilgi elde edebilir. DDoS saldırılarının aksine, bir bulanık saldırıda mesajın kimliği meşru kimlikler arasından rastgele seçilir ve veri alanının her bir bitinin değeri 0 ile 255 arasında rastgele oluşturulur. bulanık saldırıların kısa bir içinde çok sayıda mesaj göndermesi gerekmez ve saldırgan, kimliğin belirli işlevini bulmaya çalışmak için küçük bir oranda sabit kimliklere sahip rastgele çerçeveler gönderebilir.



ŞEKİL 8. Tekrar saldırı senaryosu.

1) SALDIRILARI TEKRARLAYIN

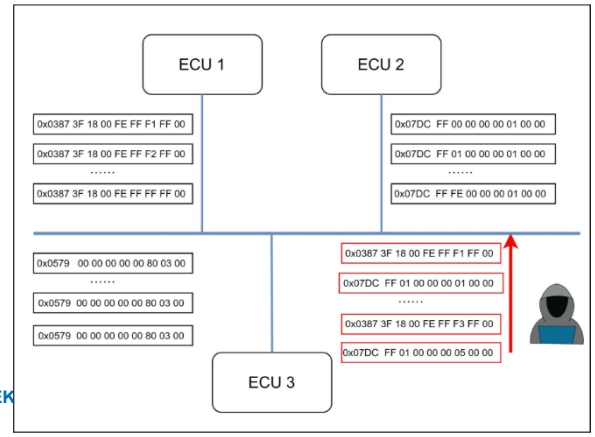
Şekil 8 CAN veriyoluna karşı Tekrarlama saldırısı senaryosunu göstermektedir. Saldırgan, daha önce belirli bir zamanda veriyolundan yakalanan meşru bilgileri veriyoluna gönderir. Tekrarlama saldırısının tipik bir örneği, bilgisayar korsanlarının araç sahibinin uzaktan kumanda anahtarı tarafından araca gönderilen sinyalleri dinlemesi ve bu mesajları tekrar oynatarak aracın kilidini açması veya hatta motoru çalıştırmasıdır. Bu saldırı çerçeveleri aslında saldırgan tarafından ele geçirilmiş meşru çerçevelerdir, bu nedenle çerçeve formatı ve içeriği ile tespit edilmesi zordur.

2) MASKELİ SALDIRILAR

Maskeli saldırılar, saldırganın araç CAN veri yolu operasyonu hakkında derinlemesine bilgi sahibi olmasını gerektirir. Şekil 9 CAN veriyoluna karşı maskeli saldırı senaryosunu göstermektedir. Saldırgan belirli normal çerçeve veri alanlarını hedef kontrol bilgileriyle değiştirerek belirli ECU'ların silecekleri, frenleri veya direksiyonu açmak gibi önceden belirlenmiş eylemleri gerçekleştirmesini sağlar. Ayrıca, bu tür saldırı çerçevelerinin kimlikleri ve veri alanları yasal aralıktadır ve bu nedenle tespit edilmesi zordur.

IV. IZINSIZ GIRIŞ TESPITI IÇIN ÖNERILEN YÖNTEM

ISO 11898 gibi araç CAN veri yolunun ilgili protokollerine ve gerçek araçlardan toplanan verilerimize göre,



ŞEK

Araç CAN veri yolunun mesajlarının çoğu periyodiktir, yani çerçeveler belirli zaman aralıklarında periyodik olarak veri yoluna gönderilir.

Periyodik mesajların özel ID'leri aracın marka ve modeline bağlı olarak farklı değerlere ve işlevlere sahiptir ve veri alanlarının formatı ve özel anlamı değişir. Bununla birlikte, her bir araç türü için kullanılan yasal ID sayısının, her bir araç türü için kullanılan ID sayısından çok daha az olduğu kesindir.

protokolde sağlanan kimlik sayısı (0x0000-0xFFFF),

ve farklı kimlik türleri için veri alanları aşağıdakilerle ilgilidir onları. Periyodik gönderimin özellikleri göz önüne alındığında mesajların ve belirli ortamların periyodiklik üzerindeki etkisinin yanı sıra kimliklerle ilişkili veri alanlarına dayanan bir anormallik tespit şeması öneriyoruz.

Çok Gözlemli Saklı Markov Modeli.

Anomali tespit problemini çoklu anomali tespit problemi olarak tanımlıyoruz.

Çerçevenin zamanlamasına, kimliğine ve özelliklerine bağlı olarak belirli bir anda çerçevenin oluşma olasılığını hesaplayarak bir çerçevenin anormal durumunu belirleyen gözlem HMM modeli

veri alanı. T zamanındaki otobüs trafiğini şu şekilde tanımlıyoruz:

$$F= \{f_1, f_2, \ldots, f_T\}. \quad (1)$$

Daha sonra, bunu kimlik dizisi S ve veri dizisi O'ya böleriz. S, T zamanındaki HMM durum dizisini temsil eder, öyle ki

$$S= \{ID_1, ID_2, \ldots, ID_T\}. \quad (2)$$

O, T zamanındaki çoklu HMM gözlem dizilerinin kümesini temsil eder, öyle ki

$$O = \{O_1, O_2, \ldots, O_L\}, \quad (3)$$

Burada L veri alanındaki bayt sayısıdır ve $O_{(l}$= $\{Veri_{(l)(1)}, Veri_{l2}, \ldots, Data_{lT}\}$, T zamanındaki veri alanının ith baytının dizisidir. Ve tüm olası veri alanlarının kümesini elde edebiliriz.

devletler:

$$Q= \{q_1, q_2, \ldots, q_N\}, \quad (4)$$

Burada N tüm olası durumların sayısıdır. V, tüm olası gözlem kümelerinin kümesidir:

$$V= \{V_1, V_2, \ldots, V_L\}, \quad (5)$$

burada $V_{(l)}= v_{(l)(1)}, v_{(l)(2)}, \ldots, v_{lM}$, $O_{(l)}$gözlem dizisinin tüm olası gözlemlerinin kümesi ve $M_{(l)}$ise
$V_{(l)}$nin tüm olası gözlemlerinin sayısı. Durum geçiş olasılığı matrisi şu şekilde tanımlanır:

$$A= [a_{ij}]_{N\times N}, \quad (6)$$

burada $a_{ij}= P(ID_{t+1}= q_i | ID_{(t)}= q_j)$. O_l gözlem dizisinin gözlem olasılığı matrisi şu şekilde tanımlanır:

$$B_l= [b_j(k)]_{N\times Ml}, \quad (7)$$

burada $b_j(k)= P(Data_{(lt)}= v_{ik} | ID_t= q_j)$. Başlangıç olasılık dağılım vektörü $\pi= (\pi_i)$ olarak tanımlanır, burada $\pi_i= P(ID_1= q_{(i)})$.

Dolayısıyla, bir çoklu gözlem HMM kümesi şu şekilde tanımlanabilir:

$$\lambda= \{\lambda_1, \lambda_2, \ldots, \lambda_L\}, \quad (8)$$

burada $\lambda_l= \{\pi, A, B_l\}$.

λ_i için, t anındaki ileri olasılığı tanımlarız:

$$\alpha_{lt}(j)= P(Veri_{(l)(1)}, Veri_{l2}, \ldots, Data_{lt}, ID_t= q_j | \lambda_{(l)}). \quad (9)$$

Benzer şekilde, şu anda geriye dönük olasılığı tanımlarız t:

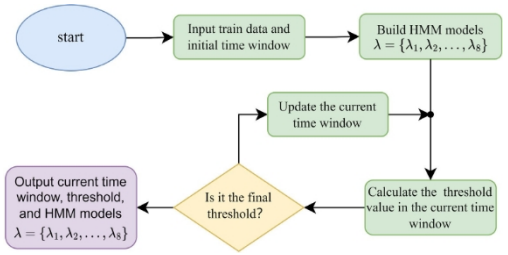
$$\beta_{lt}(j)= P(Veri_{l(t+1)}, Veri_{l(t+2)}, \ldots, Veri_{lT} | ID_t= q_j, \lambda_l). \quad (10)$$

λ_l modeli ve O_l gözlemi göz önüne alındığında, t anında q_j durumunda olma olasılığı aşağıda gösterilmiştir:

$$\gamma_{lt}(j)= P(ID_t= q_j | \lambda_{(l)}, O_l= \frac{\alpha_{lt}(j)\beta_{(lt)}(j)}{\sum_{k=1}^{N} \alpha_{lt}(k)\beta_{(lt)}(k)}. \quad (11)$$

Spesifik olarak, genel çözümümüz üç bölümden oluşmaktadır: veri hazırlama, eğitim modülü ve tespit modülü. Veri hazırlama sürecinde, ilk olarak araçtan uzun vadeli bir veri çerçevesi akışı elde ediyoruz ve her bir bilgi çerçevesinin kimliğini, veri alanını ve zaman damgasını saklıyoruz. Daha sonra, bilgiler ondalık forma dönüştürülür. Şekil 10'da gösterildiği gibi eğitim modülü, önceden işlenmiş verilere ve yakalanan aracın normal akışına dayanan bir başlangıç zaman penceresine bağlı olarak HMM'ler ve ölçüm eşikleri oluşturmayı amaçlamaktadır. Eğitim modülünde, önceden işlenmiş normal akış F, çoklu gözlemi hesaplamak için sisteme beslenir
HMM'ler. Daha sonra, $\gamma_i= \{\gamma_{1i}, \gamma_{(2)(i)}, \ldots$ hesaplanır. $, \gamma_{Li}\}$
elde edilen kullanarak F'deki her bir f_i çerçevesi için $=$
$\{eşik_1, eşik_2, \ldots, threshold_L\}$, tespit modülü için temel olarak kullanılır. Algoritma 1 şunları gösterir
HMM'lerin ve eşiklerin tam olarak elde edilmesi süreci.

Tespit aşamasında, tespit edilen *çerçevenin* $\gamma_{(W)}$değerini hesaplarız, burada$_{(W)}= \{\gamma_{1(W)}, \gamma_{(2)(W)}, \ldots, \gamma_{LW}\}$. Algoritma 2, eşik değerini karşılaştırarak anomali tespit sürecini detaylandırır
ve γ_W . Herhangi bir γ_{lW} ilgili $eşik_l$ aralığında değilse, *çerçeve* anormal bir *çerçeve* olarak sınıflandırılır. Eğitim ve tespit aşamaları, en uygun W zaman penceresi belirlenene kadar çoklu W zaman pencerelerinde tekrarlanır.



ŞEKİL 10. Eğitim süreci.

Algoritma 1 HMM'lerin ve Başlangıç Eşiklerinin Oluşturulması

Giriş: *Çerçeve* (CAN çerçevesi listesi), *W* (İlk zaman penceresi)

Başlatma:*eşik*
$N \leftarrow$ CAN ID tipleri
$L \leftarrow$ CAN veri alanındaki maksimum bayt sayısı
$M = \{M_1, M_2, \ldots, M_L\} \leftarrow$ Bayt başına veri alanı türleri kümesi
for $1 \leq i \leq N$ **do**
    $\pi_i \leftarrow ID_{(i)'nin}$ Frekansı
için sonlandır
for $1 \leq i \leq N$ **do**
    1 için $\leq j \leq N$ **do**
        $A_{ij} \leftarrow ID_{(i)}$den aktarılan frekans sayısı $ID_{(j)}$'ye
        $a_{(ij)} = \overline{P}_{l=}^{N^j} A_{ij}$
    için son
end for
for $1 \leq l \leq L$ **do**
    1 için $\leq j \leq N$ **do**
        1 için $\leq k \leq M_l$ **do**
            $B_{ijk} \leftarrow ID_{(j)}$'ye o_l frekanslarının sayısı $= k$
            $b_{ijk} = \overline{P}_{l=}^{M_l k} B_{ijk}$
        için son
    için son
    $\lambda_l = \{\pi, A, B_l\}$
end for
for $1 \leq i \leq lenthofFrame$ **do**
    1 için $\leq l \leq L$ **do**
        $eşik\ [i]\ [l] \leftarrow \gamma_{lW}(j_{çerçeve_i})$
    için son
end for

Çıktı: HMM'ler $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_L\}$, *eşik*

V. DENEY VE SONUÇLAR

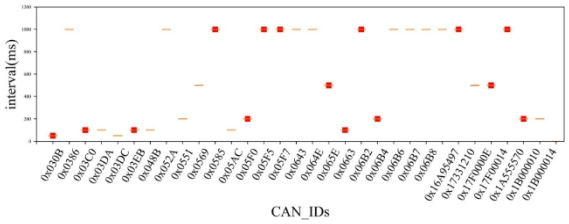
A. DENEYSEL AYARLAR VE PERFORMANS ÖLÇÜTLERİ

Deneydeki normal veriler, kentsel bir alanda yoğun olmayan saatlerde yarım saat boyunca normal bir şekilde seyreden bir arabadan toplanmıştır. Deneydeki saldırı senaryoları, oluşturulan saldırı platformuna dayalı olarak üretilmiştir. Test verilerinin zenginliği ve eksiksizliği göz önünde bulundurularak
Hızlanma ve yavaşlama, direksiyon, kaldırma ve indirme dahil olmak üzere sürüş sırasında araç üzerinde çeşitli manevralar

Algoritma 2 Anomali Tespit Modülü

Girdi: *Çerçeve* (tespit edilecek CAN çerçevesinin listesi), *W* (Başlangıç zaman penceresi), HMM'ler $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_L\}$, *eşik*

for $1 \leq i \leq$ *Çerçeve* uzunluğu **do**
    $çerçeve_{(i)'nin}$ $\gamma_{W\ değerini}$ hesaplayın
    1 için $\leq l \leq L$ **do**
        Eğer $eşik\ [:]\ [l]\ MIN \leq \gamma_{lW} \leq threshold\ [:]\ [l]\ MAX$ **then**
            $frame_i$ noraml'$_{dir}$
        başka
            $çerçeve_{(i)}$ anormal
        end if
    için son
end for



ŞEKİL 11. Zaman aralığı 31 CAN ID'sinin veri yolunda belirdi.

pencereler, vb. Şekil 11, deneysel araçtan toplanan 31 CAN ID'sinin otobüste göründüğü zaman aralığını göstermektedir; buradan önemli bir periyodiklik çıkarılabilir
gözlemlenmiştir. Grafikten de görülebileceği gibi, 0x0386 gibi bazı ID'ler 1 ms'den bile daha az aralıklarla dalgalanmaktadır; 0x030B gibi bazı ID'ler daha büyük aralıklara sahip gibi görünse de 10 ms'yi geçmemektedir. CAN veri yolu anomali tespiti göz önüne alındığında
tipik bir ikili sınıflandırma problemidir, aşağıdaki deneysel değerlendirmede tespit edilen verileri doğru pozitif (TP), yanlış pozitif FP), doğru negatif (TN) ve yanlış negatif (TN) olarak sınıflandırıyoruz.
negatif (FN).

Yukarıdaki metriklere dayanarak, önerilen algoritmanın performansını Doğruluk, , Geri Çağırma ve F1-Skoru kullanarak değerlendiriyoruz.

Doğru Pozitif Oran olarak da adlandırılan Geri Çağırma, doğru tespit edilen saldırı çerçevelerinin gerçek saldırı çerçevelerine oranını ifade eder ve şu şekilde gösterilir

$$Geri\ Çağırma = \frac{TP}{TP + FN}. \quad (12)$$

Doğruluk, doğru tespitin tüm tespitlere oranını ifade eder ve şu şekilde gösterilir

$$Doğruluk = \frac{TP + TN}{TP + TN + FP + FN}. \quad (13)$$

Hassasiyet, doğru tespit edilen saldırı çerçevelerinin tespit edilen toplam saldırı çerçevelerine oranını ifade eder ve şu şekilde gösterilir

$$Hassasiyet = \frac{TP}{TP + FP}. \quad (14)$$

F1 puanı, Hassasiyet ve Geri Çağırma değerlerinin ağırlıklı ortalamasıdır ve şu şekilde gösterilir

$$F1 = \frac{2 \times Recall \times Precision}{Geri\ Çağırma + Hassasiyet} \quad (15)$$

Önerilen senaryonun uygulanabilirliğini ve genelliğini göstermek amacıyla testlerimizde dört saldırı senaryosu tanımlanmıştır. Saldırı senaryolarının oluşturulmasında iki varsayım göz önünde bulundurulmuştur. Bir yandan, saldırganın kablolu ya da kablosuz olarak veri yolu erişimine sahip olduğu bu sayede veri çerçevelerini serbestçe alıp gönderebildiği varsayılmaktadır. Öte yandan, saldırganın meşru kimlik kümesini ele geçirdiğini ve böylece saldırı çerçevesinin meşru kimliklerden ve değiştirilmiş veri alanlarından oluştuğunu varsayıyoruz.

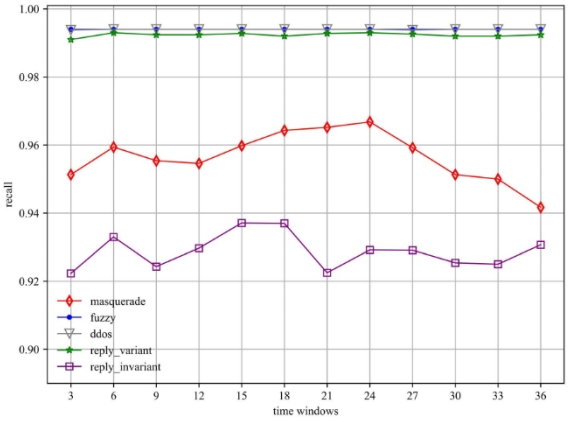
B. SONUÇLAR

Önerilen algoritmanın performansını tam olarak tahmin etmek için, Bölüm III'te sunulan dört saldırı senaryosunun her biri için geri çağırma, doğruluk, ön karar ve f1 temelinde değerlendirdik. Deneyler sırasında, bazı ID'lerin veri alanının sabit kaldığını ancak diğerlerinin değiştiğini gördük. Bu nedenle, yeniden oynatma saldırısı bu iki çerçeve türüne göre reply_invariant ve reply_variant olarak ikiye ayrılmıştır.

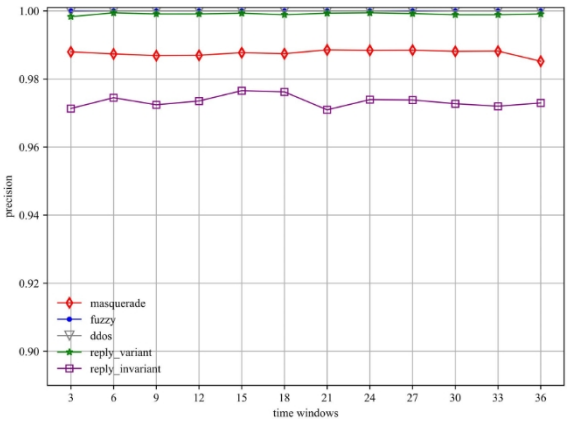
Bu deneyde zaman penceresi, $\gamma_{(W)'nin}$ hesaplanması için bir dizi CAN mesajının boyutu olarak kabul edilmiştir. Zaman penceresinin boyutunun tespit performansını etkileyip etkilemediğini araştırmak için, önerilen algoritmanın performans metriklerini farklı zaman pencerelerine sahip beş saldırı senaryosu altında değerlendirdik. Zaman pencereleri 3-36 olarak tanımlanmış ve 3 üzerinde artmıştır.

Şekil 12, farklı zaman pencerelerine sahip beş saldırı senaryosu için önerilen algoritmanın geri çağırma oranını göstermektedir. Özetle, önerilen algoritma en iyi geri çağırmayı zaman penceresi 18 olduğunda elde etmektedir. DDoS saldırıları, fuzzy saldırıları ve reply_variant saldırıları için geri çağırma oranı tüm zaman pencerelerinde 0,99'u aşabilmektedir. Bu üç tür saldırı çerçevesi, kimlik alanı veya veri alanındaki normal çerçevelerden büyük sapmalara sahiptir, bu nedenle tespit edilmeleri kolaydır. Maskeli saldırılar ve reply_invariant için, geri çağırma oranı önce artar, sonra zaman penceresinin artmasıyla azalır ve zaman penceresi 18 olduğunda en iyi performansa ulaşır. Bunun nedeni, bu iki saldırı türü ile normal arasındaki yüksek benzerliktir. Pencere boyutu çok küçük olduğunda, birçok anormal çerçeve normal çerçeve olarak algılanır. Pencere boyutu çok büyük olduğunda, bazı normal çerçeveler yanlışlıkla anormal çerçeveler olarak algılanır. Genel olarak, önerilen algoritma mevcut saldırı çerçevelerini etkili bir şekilde tespit edebilir ve %92'den fazla bir hatırlama oranı elde edebilir.

Şekil 13, farklı zaman pencerelerine sahip beş saldırı senaryosu için önerilen algoritmanın hassasiyetini göstermektedir. Farklı saldırı senaryolarında hassasiyetin zaman penceresine göre değişim eğiliminin geri çağırma değerine benzer olduğu görülebilir. Farklı saldırı senaryolarında zaman penceresi boyunca hassasiyetin değişim eğiliminin geri çağırma değerine benzer olduğu görülebilir. DDoS saldırıları, fuzzy saldırıları ve reply_variant saldırıları için



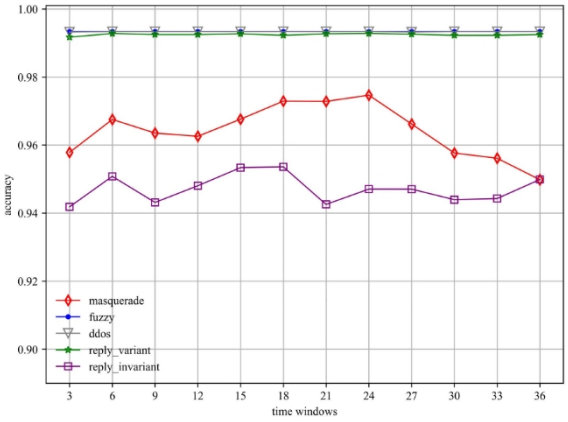
ŞEKİL 12. Önerilen algoritmanın farklı pencere boyutları ile geri çağrılması.



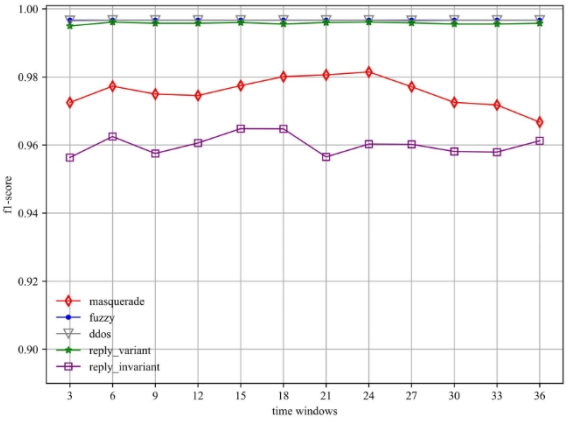
ŞEKİL 13. Önerilen algoritmanın farklı pencere boyutları ile hassasiyeti.

hassasiyet tüm zaman pencerelerinde 0,99'u aşabilir. Maskeli saldırılar ve reply_invariant saldırıları için kesinlik, geri çağırmadan %97 daha yüksektir, bu da algoritmamızın çok az yanlış pozitif olduğu anlamına gelir. Şekil 14, farklı zaman pencerelerine sahip beş saldırı senaryosu için önerilen algoritmanın doğruluğunu göstermektedir. Şekil 15, farklı zaman pencerelerine sahip beş saldırı senaryosu için önerilen algoritmanın f1 değerini göstermektedir. Benzer şekilde, farklı saldırı senaryolarında zaman pencereleri üzerindeki f1 ve doğruluk eğilimi geri çağırma değerine benzerdir. Bu da önerilen algoritma için gereken tespit süresinin çok yüksek olmadığı anlamına gelmektedir. DDoS saldırıları, bulanık saldırılar ve reply_variant saldırıları için hem F1 hem de doğruluk %100'e yaklaşabilir, bu da bu tür saldırıların neredeyse tamamen doğru bir şekilde tespit edilebileceği anlamına gelir. Maskeli saldırılar ve reply_invariant saldırılar açısından, tespit çok zor olmasına rağmen, önerilen algoritma yine de çok iyi performans göstermektedir. Zaman penceresi boyutu 18 olduğunda, her iki performans ölçütü de %95'i aşmaktadır.

Önerilen algoritmanın DDoS, fuzzy ve reply_variant senaryoları için 1'e yakın hatırlama, doğruluk, hassasiyet ve f1 elde ettiği açıktır. Ayrıca reply_variant ve masquer- ade senaryolarında da performans ölçütleri 93'ü aşmaktadır. Önerilen algoritmanın hem basit hem de karmaşık saldırı senaryolarında mükemmel tespit gösterdiği söylenebilir. Ayrıca,



ŞEKİL 14. Önerilen algoritmanın farklı pencere boyutları ile doğruluğu.



ŞEKİL 15. Önerilen algoritmanın farklı pencere boyutlarındaki f1 değeri.

TABLO 1. Bulanık saldırı.

Method	Recall	Precision	Accuracy	F1-score
KNN	0.88416667	0.99717444	0.992111	0.936926
DT	0.8758888	0.99961374	0.9595	0.933473
SVM(rbf)	0.998	0.9827033	0.994222	0.991234
CLAM	0.996964721	0.993947	0.99620584	0.995403
Our Proposed	0.99337014	0.999	0.994	0.996674

dengede, en uygun zaman penceresi boyutu 18 ila 24 arasındadır.

Bu alt bölümde, önerilen yaklaşımın performansını k-en yakın komşu (KNN), karar ağacı (DT), destek vektör makinesi (SVM) ve CLAM [22] . gibi mevcut saldırı tespit yöntemleriyle karşılaştırıyoruzİkna edici karşılaştırma sonuçları elde etmek için aynı eğitim ve test setlerini kullandık. Tablo 1, yukarıdaki algoritmaların bulanık saldırı senaryosundaki test sonuçlarını göstermektedir. SVM, CLAM ve önerilen algoritmanın bulanık saldırılar altında benzer performans gösterdiği, ancak KNN ve DT'nin daha düşük geri çağırmaya sahip olduğu görülebilir. Sık sık yapılan bulanık saldırıların normal çerçevelerin süresi boyunca normal değerlerden sapmalara yol açtığını ve bunun da KNN ve DT için yüksek FN ile sonuçlandığını tahmin ediyoruz.

Tablo 2, DDoS saldırı senaryosu altında yukarıdaki algoritmaların test sonuçlarını göstermektedir. Aslında, DDoS saldırı çerçevelerinin tespit edilmesi daha az zordur çünkü genellikle

TABLO 2. DDoS saldırısı.

Method	Recall	Precision	Accuracy	F1-score
KNN	0.99337	0.999	0.994	0.99667404
DT	0.9993	0.998004	0.999333333	0.999000999
SVM(rbf)	0.998	0.982703	0.99422222	0.99123358
CLAM	1	0.99976	0.999531	0.99959881
Our Proposed	1	0.9981	0.999333333	0.999000999

TABLO 3. Reply_variant saldırısı.

Method	Recall	Precision	Accuracy	F1-score
KNN	0.975359	0.931373	0.968666667	0.952858576
DT	0.875889	0.999614	0.9595	0.93347309
SVM(rbf)	0.985626	0.930233	0.971333333	0.957128614
CLAM	0.975155	0.9677419	0.99236641	0.979899497
Our Proposed	0.99337	0.999	0.994	0.99667404

TABLO 4. Masquerade ve reply_invariant saldırısı.

Method	Recall	Precision	Accuracy	F1-score
KNN	0.778455	0.813163	0.868666667	0.795430945
DT	0.672065	0.715517	0.804	0.693110647
SVM(rbf)	0.927984	0.742998	0.872666667	0.825251601
CLAM	0.90929183	0.96028014	0.94335937	0.9340407
Our Proposed	0.957837	0.987985	0.9513	0.97250461

en yüksek önceliğe sahip ID tarafından. Açıkçası, yukarıdaki yöntemlerin tümü DDoS saldırıları için mükemmel tespit sonuçlarına sahiptir.

Tablo 3, yukarıdaki algoritmaların reply_variant saldırı senaryosundaki test sonuçlarını göstermektedir. Önerilen algoritma dört metrik için de hala iyi performans göstermektedir, ancak diğer algoritmalar geri çağırma ve hassasiyet arasında iyi bir denge sağlayamamaktadır.

Tablo 4 yukarıdaki algoritmaların reply_invariant saldırı senaryosu ve masquer- ade saldırısı altındaki test sonuçlarını göstermektedir. Bu iki saldırı senaryosu farklı hedeflere ancak benzer saldırı biçimlerine sahiptir. Önerilen algoritmamızın bu iki saldırı altındaki tespit performansı, reply_invariant ve masquerade saldırı çerçevelerinin normal çerçevelere çok benzemesi nedeniyle düşmektedir. Daha sonra, bozulmaya rağmen, algoritmamız tüm metriklerde %95'in üzerine çıkmayı başararak diğer algoritmaları önemli ölçüde geride bırakmaktadır. Bu durum, önerilen algoritmanın sadece ID'ler arasındaki bağımlılıkları değil, aynı zamanda ID'ler ve veri alanları arasındaki korelasyonu da dikkate almasına bağlanmaktadır.

VI. SONUÇ

Bu makalede, araç zekası ve ağından kaynaklanan güvenlik olaylarıyla başa çıkmak için araç türüne ve özel saldırı bilgilerine bağlı olmayan çoklu gözlem HMM tabanlı, kare kare CAN veri yolu saldırı tespit algoritması önerdik. İlk olarak, normal CAN veri yolu trafiğinin kimlik alanı ve veri alanına dayalı çoklu HMM'l oluşturuyoruz ve normal çerçevenin var olma olasılığını algılama eşiği olarak kapsamlı bir şekilde hesaplıyoruz. Tespit edilecek çerçevelerin var olma olasılığı normal eşik değerine girmediğinde, bunların anormal olduğu belirlenir. Ardından, önerilen algoritmayı kapsamlı bir şekilde değerlendirmek için, toplanan gerçek araç verilerine dayanarak dört saldırı modeli oluşturuyoruz.

Deneysel simülasyonda, her bir saldırı senaryosunda önerilen algoritmanın hesaplamak için dört gösterge kullandık: doğruluk, kesinlik, geri çağırma ve f1. Deneysel sonuçlar önerilen algoritmanın diğer klasik kare kare tespit algoritmalarından daha üstün olduğunu göstermektedir. Gelecekteki çalışmalarda, CAN veri yolunun gerçek güvenlik korumasına yakın hale getirmek için deneyimli bilgisayar korsanları tarafından daha yüksek dereceli saldırılara karşı izinsiz giriş tespit modelinin performansını artırmaya çalışacağız.

REFERANSLAR

[1] C. Chen, G. Yao, C. Wang, S. Goudos ve S. Wan, "Enhancing the robustness of object detection via 6G vehicular edge computing," *Digit. Commun. Netw.*, vol. 8, no. 6, pp. 923-931, 2022.
[2] W. Choi, K. Joo, H. J. Jo, M. C. Park, ve D. H. Lee, "VoltageIDS: Otomotiv saldırı tespit sistemi için düşük seviyeli iletişim özellikleri," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114-2129, Aug. 2018.
[3] S. Liu, J. Yu, X. Deng ve S. Wan, "FedCPF: 6G iletişim ağlarında araçsal uç için verimli iletişimli bir federe öğrenme yaklaşımı," *IEEE Trans. Intell. Transp. Syst*., cilt 23, no. 2, pp. 1616-1629, Şubat 2022.
[4] C. Chen, L. Liu, S. Wan, X. Hui Q. Pei, "Kısa vadeli trafik tahminine dayalı Araçların İnternetinde endüstri 4.0 uygulamaları için veri dağıtımı," *ACM Trans. Internet Technol.*, vol. 22, no. 1, pp. 1-18, Feb. 2022.
[5] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. 91, pp. 1-91, 2015.
[6] Z. Cai, A. Wang, W. Zhang, M. Gruffke ve H. Schweppe, "0 gün ve hafifletmeler: Bağlı BMW otomobillerini istismar etmek ve güvenliğini sağlamak için yollar," *Black Hat USA*, cilt. 2019, s. 39, Ağustos 2019.
[7] Akıntıya karşı. (10 Mayıs 1991). *Upstream's 2022 Global Automotive Cybersecurity Report*. [Çevrimiçi]. Mevcut: https://upstream.auto/2022report/
[8] B. Palaniswamy, S. Camtepe, E. Foo, and J. Pieprzyk, "An efficient authentication scheme for intra-vehicular controller area network," *IEEE Trans. Inf. Forensics Security*, cilt 15, s. 3107-3122, 2020.
[9] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola ve A. Benslimane, "NovelADS: Araç içi ağlar için yeni bir anomali tespit sistemi," *IEEE Trans. Intell. Transp. Syst.*, cilt 23, no. 11, pp. 22596-22606, Kasım 2022.
[10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, ve S. Savage, "Modern bir otomobilin deneysel güvenlik analizi," in *Proc. IEEE Symp. Secur. Privacy*, Mayıs 2010, s. 447-462.
[11] C.-W. Lin ve A. Sangiovanni-Vincentelli, "Cyber-security for the con- troller area network (CAN) communication protocol," in *Proc. Int. Konf. Cyber Secur.*, Aralık 2012, s. 1-7.
[12] S. Woo, H. J. Jo ve D. H. Lee, "Bağlı araca pratik bir kablosuz saldırı ve araç içi CAN için güvenlik protokolü," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993-1006, Eylül 2015.
[13] H. J. Jo ve W. Choi, "Denetleyici alan ağlarına yönelik saldırılar ve ilgili karşı önlemler üzerine bir araştırma," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6123-6141, Jul. 2022.
[14] H. M. Song, H. R. Kim ve H. K. Kim, "Araç içi ağ için CAN mesajlarının zaman aralıklarının analizine dayalı izinsiz giriş tespit sistemi," in *Proc. Int. Konf. Inf. Netw. (ICOIN)*, Ocak 2016, s. 63-68.
[15] U. Ezeobi, H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "Reverse engineering controller area network messages using unsupervised machine learning," *IEEE Consum. Electron. Mag.*, vol. 11, no. 1, pp. 50-56, Jan. 2022.
[16] M. L. Han, B. I. Kwak, ve H. K. Kim, "Araç içi ağ için olay tetiklemeli aralık tabanlı anomali tespiti ve saldırı tanımlama yöntemleri," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2941-2956, 2021.
[17] A. Taylor, S. Leblanc ve N. Japkowicz, "Uzun kısa süreli bellek ağları ile otomo- bil kontrol ağı verilerinde anormallik tespiti," *Proc. IEEE Int. Konf. Data Sci. Adv. Anal. (DSAA)*, Ekim 2016, s. 130-139.
[18] M.-J. Kang ve J.-W. Kang, "Araç içi ağ güvenliği için derin sinir ağı kullanan saldırı tespit sistemi," *PLoS ONE*, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.
[19] M. Markovitz ve A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Veh. Commun.*, cilt 9, pp. 43-52, Temmuz 2017.
[20] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li ve M. Alazab, "Otomotiv kanal ağları için tehdit analizi: GAN modeli tabanlı bir saldırı tespit tekniği," *IEEE Trans. Intell. Transp. Syst.*, cilt 22, no. 7, pp. 4467-4477, Temmuz 2021.
[21] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting mali- cious activities from autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25469-25478, Dec. 2022.
[22] H. Sun, M. Chen, J. Weng, Z. Liu ve G. Geng, "Dikkat mekanizması ile CNN-LSTM kullanarak araç içi ağ için anomali tespiti," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10880-10893, Ekim 2021.
[23] H. Sun, M. Sun, J. Weng, and Z. Liu, "Analysis of ID sequences simi- larity using DTW in intrusion detection for CAN bus," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10426-10441, Oct. 2022.

CHEN DONG 1995 yılında Çin'in Hebei kentinde doğdu. Lisans derecesini 2017 yılında Pekin, Çin'de bulunan Beijing Informa- tion Science and Technology University'den elektronik ve enformasyon mühendisliği alanında, yüksek lisans derecesini ise 2019 yılında Beijing Jiaotong University Elektronik ve Enformasyon Mühendisliği Okulu'ndan almıştır ve şu anda State Key Laboratory of Rail Traffic Control and Safety'de doktora eğitimine devam etmektedir.
Şu anki araştırma alanları arasında araç içi ağlar, Araçların İnterneti, Nesnelerin İnterneti (IoT), gizlilik ve güvenlik yer almaktadır.

HAO WU (Üye, IEEE) 2000 yılında Harbin Teknoloji Enstitüsü'nden bilgi ve iletişim alanında doktora derecesini almıştır. Halen Çin'deki Pekin Jiaotong Üniversitesi (BJTU) Demiryolu Trafik Kontrolü ve Güvenliği Devlet Anahtar Laboratuvarı'nda tam profesör olarak görev yapmaktadır. Uluslararası dergi ve konferanslarda 100'den fazla makale yayınlamıştır. Araştırma alanları arasında akıllı ulaşım sistemleri (ITS'ler), telekomünikasyonda güvenlik ve QoS konuları yer almaktadır.
daha az ağlar (VANET'ler, MANET'ler ve WSN'ler) ve Nesnelerin İnterneti (IoT). IEEE'nin kablosuz ağlar ve güvenlik alanındaki önemli konferans ve dergilerinde hakemlik yapmaktadır.

QINGYUAN LI 1989 yılında Çin'in Hebei kentinde doğdu. Lisans derecesini 2012 yılında Şangay Bilim ve Teknoloji Üniversitesi Optoelektronik Bilgi ve Bilgisayar Mühendisliği Fakültesi'nden, yüksek lisans derecesini 2015 yılında Pekin Jiaotong Üniversitesi Elektronik ve Bilgi Mühendisliği Fakültesi' almıştır ve halen Devlet Demiryolu Trafik Kontrolü ve Güvenliği Anahtar Laboratuvarı' doktora eğitimine devam . Şu anki araştırma alanları ı, Nesnelerin İnterneti (IoT), gizlilik ve güvenlik yer almaktadır.