# Otonom Taşıt Gruplarında Veri Güdümlü Anomali Belirlenmesi

## Data-Driven Anomaly Detection in Autonomous Platoon

Seyhan Uçar[1], Sinem Çöleri Ergen[2] ve Öznur Özkasap[1]
[1]Bilgisayar Mühendisliği Bölümü, [2]Elektrik, Elektronik Mühendisliği Bölümü
Koç Üniversitesi, İstanbul, Türkiye
{sucar, sergen, oozkasap}@ku.edu.tr

***Özetçe* —Teknoloji, insan girdisi olmaksızın kendi başına seyredebilen otonom taşıtları gerçek kılmıştır. Diğer yandan, otonom taşıt grupları otonom taşıtların kablosuz iletişim aracılığı ile yakın takipte seyahat etmesidir. Otonom taşıt gruplarında, taşıtlar işbirliksel biçimde hız ve mesafelerini lidere, diğer bir deyişle otonom taşıt grubundaki ilk sıradaki taşıta, göre ayarlamak için veri alışverişinde bulunmaktadırlar. Fakat, bu işbirliğine dayalı veri alışverişi güvenliği riske atmaktadır. Yanlış davranımlı otonom taşıt grubu üyesi, veri paketi içeriğini değiştirebilir ve otonom taşıt grubu kararsızlığına neden olabilmektedir. Bu sebeple, içeriği ile oynanmış paket saptanımı önemli bir gereklilik haline gelmiştir. Bu çalışmamızda, otonom taşıt grubu için veri güdümlü anomali belirlenmesini ele almaktayız. İçeriği ile oynanmış paketleri ve yanlış davranımlı taşıt tespiti için istatistiksel öğrenme tabanlı özgün bir teknik önermekteyiz. Otonom taşıt grup liderine olan uzaklık değişiminin anomali belirlenmesi ve yanlış davranımlı taşıt tespiti için yeterli olduğunu göstermekteyiz.**

***Anahtar Kelimeler*—*tasarsız taşıt ağları, otonom taşıtlar, otonom taşıt grupları, veri anomalisi, yanlış davranımlı taşıt.***

***Abstract*—Technology brings autonomous vehicles into a reality where vehicles cruise themselves without human input. Vehicular platoon, on the other hand, is a group of autonomous vehicles that are organized into close proximity through wireless communication. In an autonomous platoon, vehicles cooperatively send data to each other to adjust their speed and distance to the leader, the first vehicle in the platoon. However, this cooperative data exchange can lead to security risks. A misbehaving platoon member could alter the data packets which may cause platoon instability. Therefore, identifying the modified packets has become an important requirement. In this paper, we investigate data-driven anomaly detection mechanisms for the autonomous platoon. We propose a novel statistical learning based technique to detect the modified packets and misbehaving vehicles. We demonstrate that the distance change to the leader would be sufficient to detect anomalies and misbehavior.**

***Keywords*—*vehicular ad-hoc network, autonomous vehicle, platoon, data anomaly, misbehaving vehicle.***

## I. GİRİŞ

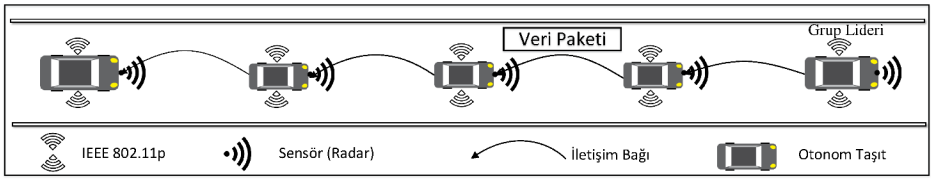
Teknoloji, insan girdisi olmaksızın kendi başına seyredebilen otonom taşıtları gerçek kılmıştır. Otonom taşıtlar ileri yazılım ve gelişmiş sensörleri aracılığı ile daha güvenli seyahati hedeflemektedirler. Yapılan araştırmalar otonom taşıtların tasarsız taşıt ağlarını (VANET) yeniden şekillendirme ve akıllı taşıma sistemleri (ITS) seyahat güvenliğinde köklü değişiklikler yapabilme yetisine sahip olduğunu göstermiştir.

Kendi başına seyredebilen taşıtlar gelişimine devam ederken taşıttan-taşıta (V2V) ve taşıttan-baz istasyonuna (V2I) haberleşim işbirliksel uyarlanabilir seyir kontrolünü (CACC) mümkün kılmıştır. CACC, taşıtların işbirliksel ve periyodik olarak paylaştığı veriler ile taşıtlar arası uzaklığı sabit tutmakta ve otonom sürüş kararları alabilmektedir. Otonom taşıtların grup şeklinde işbirliksel veri paylaşımına dayalı yakın mesafelerde seyahat etmesi otonom taşıt grupları olarak adlandırılmıştır [1]. Otonom taşıtlara giderek artan ilgi otonom taşıt gruplarının gelecekte hayatımızda önemli bir yer tutacağını kanıtlar niteliktedir. Otonom taşıt grupları çeşitli faydaları vardır. Örneğin, otonom taşıtların yakın mesafelerde seyir etmesi trafik homojenliğini ve verimliliğini arttırabilecektir. Sürücülere karşı verilen hızlı kaza anı tepkileri VANET güvenliğine büyük oranda katkı sağlayacaktır. Ayrıca, otonom yapı sürücülerin gereksiz ivmelenme ve yavaşlama alışkanlıklarının önüne geçebilecek ve yakıtsal anlamda tasarruf sağlanabilecektir.

Otonom taşıt grubu lider ve üye taşıtlardan oluşmaktadır. Lider taşıt otonom taşıt grubunda en baştaki taşıt olup grup yöneticisidir. Üye taşıtlar ise liderden periyodik olarak iletilen veri paketlerini kullanarak hız ve uzaklıklarını lidere göre yapılandırmaktadırlar. Lidere göre hız ve uzaklık değişiminin zamana karşı en az olması otonom taşıt grubunun kararlı bir şekilde seyahat ettiğini göstermektedir. Kararlı şekilde seyahat, otonom taşıt grubu yönetim protokolünün gerçekleştirmesi gereken önemli hedeflerden biridir. Literatürde otonom taşıt grubu kararlılığını sağlamak adına bir çok protokol önerilmiştir [2]–[4]. Önerilen protokoller grup kararlılığı sağlamanın yanı sıra taşıt girişi, taşıt çıkışı, otonom grup birleşimi ve otonom grup bölünmesi gibi manevraları gerçeklemektedir. Taşıt girişi gruba otonom bir aracın dahil olması, taşıt çıkışı gruptan bir aracın ayrılması, grup birleşmesi iki farklı otonom grubun taşıt sayısı baz alınarak birleşmesi ve grup bölünmesi otonom grubun iki ayrı gruba ayrılması olarak tanımlanmaktadır.

Otonom taşıt grubu yönetim protokolleri iletişim için radyo frekans bazlı IEEE 802.11p'yi kullanmaktadır. IEEE 802.11p'nin yüksek iletim menzili aynı anda bir çok taşıta erişim sağlamasına rağmen geniş kapsama alanı bu teknolojiyi saldırganlara karşı savunmasız hale getirmektedir. Otonom taşıt grupları literatürde bir çok çalışmada işlenmiş olsa da otonom taşıt grubu güvenliği ciddi önem arz etmektedir. Yanlış davranımlı otonom taşıt grubu üyesi, veri paketi içeriğini

978-1-5386-1501-0/18/$31.00 




Şekil 1: Otonom Taşıt Grubu İletişim Mimarisi

değiştirebilir ve otonom taşıt grubu kararsızlığına neden olabilmektedir [5], [6]. Kriptografi ve sertifika kullanım odaklı çözümler ile dışarıdan gelen saldırılar önlenebilmiş olsa da, saldırganın otonom taşıt grubu içinden geçerli bir sertifikaya sahip olduğu durumlarda bu çözümler yetersiz kalmaktadır [7]. Bu durum için önerilen çözüm teknikleri yanlış davranımlı taşıt tespiti ve veri anomali belirlenmesini gerektirmektedir. Bu sebeple, içeriği ile oynanmış paket saptanımı ve yanlış davranımlı taşıt tespiti önemli bir gereklilik haline gelmiştir.

Güven odaklı yönetim VANET için önerilmiş yanlış davranımlı taşıtların tespiti için kullanılan, taşıtların doğru söylem itibarları kullanılarak güven modeli oluşturulan bir tekniktir [8]. Taşıtlar belirli olaylar karşısında birbirleri için oy kullanmakta ve güven modeli oluşturulmaktadır. Oluşturulan güven modeli ile veri anomali belirlenmesi ve yanlış davranımlı taşıt tespiti amaçlanmakta, dürüst taşıtlardan gelen verilere önem verilmek amaçlanmaktadır. VANET için güven modeli oluşturulması üç kategoride incelenmektedir; varlık yönelimli, veri güdümlü ve melez [9]. Varlık yönelimli güven modeli taşıtın kendisinin güvenilirliğini modellemek üzerine kuruludur. Taşıtların önceden tanımlı olayları kullandığı, veri güdümlü güven modeli ise verilerin güvenilirliği üzerine yoğunlaşmıştır. Diğer yandan, melez güven model oluşturumu hem taşıt hem de olay odaklı güvenilirliği hedeflemektedir.

Daha önce yapılan çalışmalar veri güdümlü güven modeli oluşturumunun VANET için daha uygun olduğunu göstermiştir [10]. Taşıtlar için güven değeri önceden tanımlı olaylar dahilinde taşıtların vermiş olduğu yanıtlar baz alınarak hesaplanmaktadır [11], [12]. Fakat, veri güdümlü bu yaklaşımlar doğrudan otonom taşıt gruplarına uygulanamamaktadır ve üç açıdan dezavantajlıdır. İlk olarak, güven değeri tüm otonom taşıtların standart bir aksesuarı olmayan harita veya yoğunluk bilgi kaynağına dayandırılmaktadır. İkincil olarak, veri güdümlü modeller tanımlı olayın seyrek gerçekleştiği durumda güven değeri hesaplanmasında yanıltıcıdır. Tanımlı olayın seyrek gerçekleşmesi otonom taşıt grubunda saldırgan veya dürüst grup üyesi ayrımını zora sokmaktadır. Üçüncül olarak, veri güdümlü modeller olay seyrekliği ve bilgi kaynağı bağımlılığına bir çözüm yolu olarak yol-kenar birimi (RSU) ile iletişimi gerektirmektedir. Fakat bu çözüm iki yönü ile problem teşkil etmektedir. Birincisi, RSU ile merkezsel iletişim tek bir hata noktası oluşturmaktadır ve bir çok saldırıya açıktır. İkincil olarak, verinin güvenilirliği amaçlı her paket için gereken iletişim ek yükü ve gecikme otonom taşıt gruplarında tolere edilememektedir.

Bu çalışmamızda otonom taşıt grupları için veri güdümlü anomali belirlenmesine odaklanmaktayız. Saldırganın otonom taşıt grubu içinden olduğu ve veri paketi içeriği ile oynandığı senaryoları ele almaktayız. İçeriği ile oynanmış paketlerin belirlenmesi ve yanlış davranımlı taşıt tespiti için istatiksel öğrenme tabanlı özgün bir teknik önermekteyiz. Otonom taşıt grubu liderine olan uzaklık değişiminin anomali belirlenmesi ve yanlış davranımlı taşıt tespiti için yeterli olduğunu göstermekteyiz. Bildiri içeriği şu şekilde düzenlenmiştir: Bölüm II'de kullanılan otonom taşıt grubu modeli ve yanlış davranım taşıt karakteristiği anlatılmaktadır. Bölüm III'de önerdiğimiz veri güdümlü anomali belirlenmesi algoritması sunulmaktadır. Bölüm IV'te saldırı altında otonom taşıt grubu tepkisi ele alınmakta ve önerilen algoritma ile saptanan anomaliler incelenmektedir. Bölüm V'te simülasyon sonuçları üzerinden sonuç değerlendirmesi yapılmaktadır.

## II. SİSTEM MODELİ

### A. *Otonom Taşıt Grubu Modeli*

Şekil 1 IEEE 802.11p tabanlı iletişim mimarisini betimlemektedir. Otonom grup dahilindeki taşıtlar sensörlerini ve kameralarını kullanarak önlerindeki taşıt ve objeleri saptayabilmektedirler. Her üye önündeki ve arkasındaki taşıt ile işbirliksel şekilde haberleşmekte ve veri paylaşımı gerçekleştirmektedir. Periyodik şekilde paylaşılan veri, taşıt kimliği, liderin grup belirteçi, hız, pozisyon ve ivmelenme verilerini içermektedir. Otonom taşıt grubu kararlılığı açısından liderden paylaşılan verinin grup üyelerine bozan etken olmaksızın dağıtılması gerekmektedir. Otonom taşıt grubu içindeki otonom taşıt, liderden periyodik olarak dağıtılan veri paketindeki hız ve ivme bilgilerini kullanarak kendi hızını ve öndeki taşıta olan mesafesini ayarlamaktadır. Bu hız ve mesafe ayarlamasının amacı öndeki taşıt ile emniyet mesafesi sabit tutularak seyahat etmektir.

### B. *Yanlış Davranımlı Taşıt Karakteristiği*

Yanlış davranımlı taşıt periyodik olarak dağıtılan veri paketlerini değiştirerek otonom taşıt grubu kararlılığını bozmayı hedeflemektedir. Yanlış davranan taşıtın otonom grup içinden (grup üyesi veya lider taşıt) olduğu varsayılmaktadır. Normal şartlar altında, bu taşıt diğer takım üyesi taşıtlar tarafından dürüst bir araç olarak kabul edilmektedir. Fakat, periyodik olarak liderden dağıtılan veri paketleri yanlış davranımlı taşıt tarafından değiştirilmekte ve yeniden yayımlanmaktadır. İçeriği ile oynanmış veri paketleri otonom taşıt grubu üyelerini yanlış yönlendirmekte ve otonom taşıt grubu kararsızlığına yol açmaktadır. Örneğin, yanlış davranan taşıtın yavaşlamakta olan otonom taşıt grubu ivmelenmesini hızlan olarak değiştirdiği senaryoyu ele alalım. İvmelenmenin hızlan olarak değiştirilmesi yavaşlama eğilimindeki otonom taşıt grubu için zincirleme kazalara sebep olabilmektedir.

## III. VERİ GÜDÜMLÜ ANOMALİ SAPTANIM ALGORİTMASI

Bu bildirimizde, otonom taşıt grubu veri anomali belirlenmesi için istatiksel öğrenme tabanlı özgün bir teknik önermekteyiz. Önerilen yaklaşımın özgün özellikleri sırası ile; yanlış davranımlı taşıt tespiti için yalnız lider taşıta olan uzaklık dikkate alınmaktadır, uzaklık anomali belirlenmesi için zaman serisi ayrıştırım tekniği kullanılmaktadır.

Algoritma 1 veri anomali belirlenmesi için taşıtların lidere olan uzaklık gözlemleri üzerinde çalıştırılmaktadır. Algoritma, lidere olan uzaklık gözlemleri $X$'i birbiri ile örtüşmeyecek ve en az iki gözlem içerecek $C_X$ yığınlarına bölerek çalışmaya başlamaktadır (Satır 1). Bunu takiben, her $C_X$ yığını için veri anomali belirlenmesi algoritması yürütülmektedir (Satır $2-7$). Veri anomali belirlenmesine Mevsimsel ve Eğilim Ayrıştırımına (STL) [13] dayalı ayrışım ile başlanmaktadır (Satır $3-5$). STL lidere olan uzaklık gözlemini mevsimsel ($S_X$), eğilim ($T_X$) ve kalan ($R_X$) olmak üzere üç bileşene ayrıştırmaktadır. Mevsimsel bileşen uzaklık gözlemlerinin periyodik değişimiyken, eğilim bileşeni periyodik olmayan uzun süreli değişimleri tanımlamaktadır. Diğer yandan, kalan bileşen gözlemlerden mevsimsel ve eğilim bileşenlerinin çıkarılması ile ($R_X = X - S_X - T_X$) elde edilir.

**Algorithm 1:** Veri Anomali Belirlenmesi Algoritması

1 Lidere olan uzaklık gözlemleri $X$'i $C_X$ parçalarına böl;
2 **foreach** $C_X$ **do**
3 Mevsimsel $S_X$'i STL'yi kullanarak ayıkla;
4 Medyan $\widetilde{X}$ hesapla;
5 Kalanı $R_X = X - S_X - \widetilde{X}$ hesapla;
6 $X_A = ESD(R_X, N_V)$;
7 Uzaklık anomali vektörü $D$'ye $X_A$ 'yı ekle;
8 Uzaklık anamoli vektörü $D$'yi döndür;

Genel olarak anomali belirlenmesi teknikleri gözlemler üzerinde ortalama ve standart sapma değerlerini kullanmaktadır. Fakat zamanın sonsuza yaklaşması ile ortalama değerde bozulum artmaktadır [14]. Diğer yandan, çalışmamızda önerilen yaklaşım bu tip bozulmalara karşı dayanıklı olan ortanca değer kullanımı üzerine yoğunlaşmaktadır [15]. Ayrışım ve ortanca değer hesaplanımından sonra, yanlış davranımlı taşıt Genelleştirilmiş Uç Student Sapma (ESD) tekniğinin kalan bileşen ($R_X$) üzerinden çalıştırılması ile tespit edilmektedir (Satır 6). ESD yanlış davranım tespiti için verilen gözlem içinde anormal veriyi saptayan bir tekniktir [16]. ESD parametre olarak $R_X$ ve yanlış davranımlı taşıt üst sınır değerini almaktadır. Yanlış davranımlı taşıt otonom grup içinden bir araç olduğu için ESD üst sınır yanlış davranımlı taşıt değeri otonom taşıt grubu taşıt sayısıdır. ESD tekniğinin $R_X$ üzerinden yürütülmesinden sonra uzaklık anomalisi $X_A$ saptanmakta ve uzaklık anamoli vektörü $D$' ye eklenmektedir (Satır $6-7$). $X_A$, ESD tarafından saptanan anomali, taşıt kimliği, uzaklık değeri ve simülasyon zamanı değerlerinden oluşmaktadır. Tüm $C_X$ yığınlarının değerlendirilmesinden sonra lidere uzaklık anomali vektörü $D$ çıktı olarak döndürülmekte ve yanlış davranımlı taşıtlar saptanmaktadır.

Algoritma 1'de, STL mevsimsel ve eğilim bileşenlerini ham verilerden ayırmaktadır. ESD'nin mevsimsel veya eğilim verileri üzerinde uygulanmasının anomalilere karşı duyarlı ve yapay anomalilere neden olduğu çalışmalar ile gösterilmiştir [17]. Önerilen teknik, lidere uzaklık gözlemlerinin STL tekniği ile ayrıştırıldıktan sonra kalan bileşenin önceden tanımlı yığın boyutlarına bölünmesi ve incelenmesi üzerine yoğunlaşmaktadır. Süregiden çalışmanın bir parçası olarak farklı yığın boyutlarında STL mevsimsel ve eğilim uzaklık bileşenleri göz ününde bulundurularak anomali belirlenmesi değerlendirilmesi planlanmaktadır.

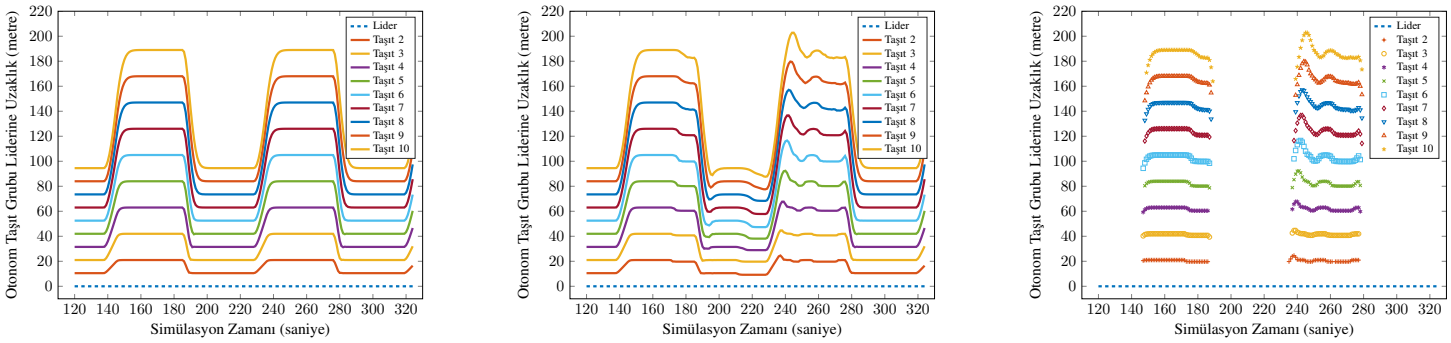
## IV. BAŞARIM ÖLÇÜMÜ

Başarım ölçümlenmesi ile otonom taşıt grubu içindeki yanlış davranımlı taşıt tespiti ve veri anomalileri saptanmak amaçlanmıştır. Taşıtlar arası iletişim IEEE 802.11p protokolü ile sağlanmaktadır. Taşıtların lidere olan uzaklık gözlemleri VEhicular NeTwork Open Simulator (VENTOS) [18] simülasyon platformu ile toplanmış ve R [19] programı ile analiz edilmiştir. VENTOS tümleşik bir simülasyon ortamı olup, taşıt devinimlilik için SUMO [20], paket bazlı simülasyon için OMNET++ [21] simülasyon taşıt kinematiği için Veins [22] platformlarını içermektedir. Diğer yandan, R, istatistiksel analiz, grafik gösterimi ve raporlama için bir programlama dili ve yazılım ortamıdır. Önerilen yöntem dahilinde kullanılan STL ve ESD teknikleri R tarafından sağlanan açık erişim kütüphanelerinden kullanılmaktadır.

VENTOS ile gerçeklenen simülasyon iki şeritli ve 90 km uzunluğundaki yolu içermekte olup sol şerit otonom taşıt grubu için ayrılmıştır. Taşıtlar Poisson işlemine göre sağ şeritten saniyede 0.5 taşıt girdisi ile sisteme giriş yapmaktadırlar. CACC özellikli taşıtlar sol şerite geçerek otonom taşıt grubu parçası olmaktadırlar. Otonom taşıt grubu 10 otonom taşıttan oluşmakta ve ilk taşıt $Lider$ olarak ifade edilmektedir. Lider yol hız limit kuralları dahilinde 5 ve 20 m/s arasında değişen devinimlik modeline sahiptir. Otonom taşıt grubu üyeleri $Lider$'den periyodik olarak dağıtılan veri paketlerini kullanarak lidere göre hız ve uzaklık değişiminin zamana karşı en az fark ile seyahat etmeyi hedeflemektedir. Simülasyonda $Lider$ yanlış davranan taşıt olup simülasyon zamanı $t = 172$ ve $t = 280$ arasında veri paketi ivmelenme değerini normalden sık aralıklarla değiştirmekte ve otonom taşıt grubu kararlılığını bozmayı hedeflemektedir. Her taşıt için 205 adet lidere uzaklık gözlemi toplanmış ve R ile analiz edilmiştir. Bunların dışında, Tablo I diğer parametreleri listelemektedir.

Şekil 2 farklı senaryolar altında otonom taşıt grubu üyelerinin lidere olan uzaklıklarını göstermektedir. Şekil 2 - (a) yanlış davranımlı taşıtın olmadığı durumda otonom taşıt grubu davranışını göstermektedir. Bu kararlı durumda grup üyeleri lidere olan uzaklıklarını hiç bir bozan etken olmaksızın sorunsuz şekilde ayarlayabilmişlerdir. Diğer bir deyişle, şekilde görüldüğü gibi lider ile otonom taşıt grup üyeleri arasındaki uzaklık liderin hız arttırması sonucu artmakta ve daha sonra kararlı duruma dönmektedir. Şekil 2 - (b) $Lider$'in grup kararlılığını bozacak şekilde ani hız değişimleri olduğu durumu göstermektedir. Yanlış davranan $Lider$, veri paketinin ivmelenme değerini normalden sık aralıklar ile değiştirerek otonom grup kararlılığını tehlikeye sokmaktadır. İvmelenme değeri ile oynanmış veri paketleri otonom grup üyelerinin lidere olan uzaklık değerinde yaklaşık [0,20] metre arasında değişime sebep olmuş ve grup kararlılığını bozmuştur. Öte yandan, Şekil 2 - (c), önerilen istatistiksel öğrenme tabanlı teknik aracılığıyla, otonom taşıt grup üyeleri tarafından saptanan anomalileri göstermektedir. Liderden gelen veri paketleri önerilen yöntem dahilinde incelenmiş ve her taşıtın tespit ettiği anomali değeri grafikte işaretlenmiştir. Güvenlik katmanı eksikliği sebebi ile otonom taşıt grubu üyeleri $Lider$'den gelen içeriği ile oynanmış veri paketlerini kabul etmiş ve taşıtlar arası emniyet mesafesi bozulmuştur.

Önerilen istatistiksel öğrenme tekniği kullanarak, $Lider$'in neden olduğu uzaklık anomalilerinin neredeyse tamamı başarıyla saptanmıştır. Fakat, önerilen teknik simülasyon zamanı




(a) (b) (c)

Şekil 2: Otonom Taşıt Grubu Liderine Uzaklık (a) Kararlı Grup (b) Lider Yanlış Davranım (c) Saptanan Anomaliler

Tablo I: Parametreler

| | Parametre | Değer |
|---|---|---|
| Simülasyon | Simülasyon Zamanı | 325 s |
| | Taşıt Uzunluğu | 5 m |
| | Taşıt Sayısı | 10 |
| | IEEE 802.11p Kapsama Alanı | 300 m |
| | Lider Bilgi İletim Sıklığı | 10 Hz |
| | Yığın Boyutu | 10 |
| C(ACC) | Maksimum / Minimum Hız | 30 / 5m/s |
| | Minimum Taşıt Arası Mesafe | 2 m |
| | İstenilen Hız | 20 m/s |
| | Maksimum İvmelenme | 3 $m/s^2$ |
| | Maksimum Yavaşlama | 5 $m/s^2$ |
| | İdeal Otonom Taşıt Grubu Araç Sayısı | 10 |

$t$ =145s $t$ =172s arasındaki uzaklık değişimini yanlış sınıflandırmıştır. Yanlış sınıflandırmanın nedeni taşıtların bağımsız, işbirliği olmaksızın anomali belirlenmesi gerçeklemesidir. İşbirliksel şekilde gerçekleşecek anomali belirlenmesi ve yanlış davranımlı taşıt tespiti yanlış sınıflandırmaların önüne geçebilecek ve yanlış davranımlı taşıt otonom grup üyeliğinden çıkartılabilecektir.

## V. VARGI

Bu çalışmamızda, otonom taşıt grubu içinden yanlış davranımlı taşıt tespitine ve veri anomalisi belirlenmesine odaklandık. Otonom taşıt grubu içinden yanlış davranımlı taşıtların veri paketleri ile oynayabildiği ve içeriği ile oynanmış verilerin otonom taşıt grup kararlılığını tehlikeye soktuğu ortaya konulmuştur. Önerilen istatiksel öğrenme tabanlı teknik ile lidere uzaklık anomalileri saptanmış ve yanlış davranımlı taşıt başarı ile tespit edilmiştir.

Süregiden çalışmamızda güven odaklı yanlış davranımlı taşıtlara karşı dayanıklı otonom taşıt grubu yönetim protokolüne yoğunlaşmaktayız. Böyle bir protokol dinamik olarak taşıtlardan gelen veriyi yorumlamalı, güven ve oylama tekniği ile işbirliksel şekilde yanlış davranımlı taşıtı tespit etmeli ve yanlış davranımlı taşıtın grup üyeliğinden çıkarım işlemlerini gerçeklemelidir. Önerilecek yönetim protokolü değişik senaryolar altında farklı başarım metrikleri ile incelemeyi hedeflemekteyiz.

## KAYNAKLAR


[1] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Vehicular Communications*, 2015.

[2] S. Santini, A. Salvi, A. S. Valente, A. Pescapè, M. Segata, and R. L. Cigno, "A consensus-based approach for platooning with inter-vehicular communications," in *IEEE Conference on Computer Communications (INFOCOM)*, April 2015.

[3] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is Your Commute Driving You Crazy?: A Study of Misbehavior in Vehicular Platoons," in *Proceedings of the 8th Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*. ACM, 2015.

[4] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, and F. Dressler, "Toward Communication Strategies for Platooning: Simulative and Experimental Evaluation," *IEEE Transactions on Vehicular Technology*, Dec 2015.

[5] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security vulnerabilities of IEEE 802.11p and visible light communication based platoon," in *IEEE Vehicular Networking Conference (VNC)*, Dec 2016.

[6] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security vulnerabilities of autonomous platoons," in *Signal Processing and Communications Applications Conference (SIU)*, May 2017.

[7] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Dec 2015.

[8] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET," *IEEE Transactions on Vehicular Technology*, Feb 2017.

[9] J. Zhang, "A Survey on Trust Management for VANETs," in *IEEE International Conference on Advanced Information Networking and Applications*, March 2011.

[10] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *IEEE INFOCOM - The 27th Conference on Computer Communications*, April 2008.

[11] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric Rogue Node Detection in VANETs," in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Sept 2014.

[12] K. Dixit, P. Pathak, and S. Gupta, "A new technique for trust computation and routing in VANET," in *Symposium on Colossal Data Analysis and Networking (CDAN)*, March 2016.

[13] R. B. Cleveland, W. S. Cleveland, J. E. McRae, and I. Terpenning, "STL: A Seasonal-Trend Decomposition Procedure Based on Loess (with Discussion)," *Journal of Official Statistics*, 1990.

[14] F. R. Hampel, E. M. Ronchetti, P. J. Rousseeuw, and W. A. Stahel, *Robust Statistics: The Approach Based on Influence Functions*, ser. Wiley Series in Probability and Statistics, 1986.

[15] F. R. Hampel, *Robust Statistics: The Approach Based on Influence Functions*. University of California, 1986.

[16] B. Rosner, "Percentage Points for a Generalized ESD Many-Outlier Procedure," *Technometrics*, 1983.

[17] M. G. Kendall, A. Stuart, and J. K. Ord, Eds., *Advanced Theory of Statistics*. New York, NY, USA: Oxford University Press, Inc., 1987.

[18] "VENTOS," http://goo.gl/OueFkO.

[19] "R," http://www.R-project.org/.

[20] "SUMO," http://sumo.sourceforge.net/.

[21] "OMNET++ Networ Simulator," https://omnetpp.org/.

[22] "Vehicles in Network Simulation (Veins)," http://veins.car2x.org/.