

ARAÇSAL TASARSIZ AĞLAR İÇİN İSTATİSTİKSEL TABANLI BİR SALDIRI TESPİT YÖNTEMİ

A STATISTICAL-BASED INTRUSION DETECTION METHOD FOR VEHICULAR AD HOC NETWORKS

FEHİME AYDIN

Doç. Dr. SEVİL ŞEN AKAGÜNDÜZ
Tez Danışmanı

Hacettepe Üniversitesi
Lisansüstü Eğitim-Öğretim ve Sınav Yönetmenliğinin
Bilgisayar Mühendisliği Anabilim Dalı için Öngördüğü
YÜKSEK LİSANS tezi olarak hazırlanmıştır.

2018

Fehime AYDIN'ın hazırladığı "**Araçsal Tasarsız Ağlar için İstatistiksel Tabanlı Bir Saldırı Tespit Yöntemi**" adlı bu çalışma aşağıdaki jüri tarafından **BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

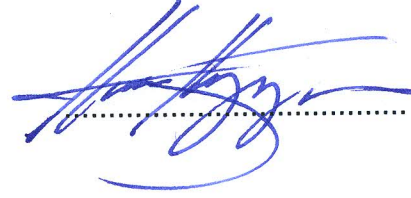
Prof. Dr. O. Ayhan ERDEM
Başkan



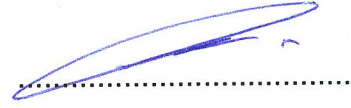
Doç. Dr. Sevil ŞEN AKAGÜNDÜZ
Danışman



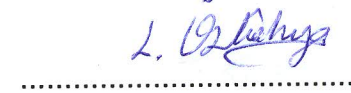
Doç. Dr. Oumout CHOUSEINOGLU
Üye



Doç. Dr. Ahmet Burak CAN
Üye



Doç. Dr. Lale ÖZKAHYA
Üye



Bu tez Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tarafından **YÜKSEK LİSANS TEZİ** olarak onaylanmıştır.

Prof. Dr. Menemşe GÜMÜŞDERELİOĞLU
Fen Bilimleri Enstitüsü Müdürü

ETİK

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmada,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

29/11/2018



FEVRIYE AYDIN

YAYINLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

- ☒ **Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.**

(Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etseniz ve kütüphane bu talebinizi yerine getirirse bile, tezinin arama motorlarının önbelleklerinde kalmaya devam edebilecektir.)

- ☐ **Tezimin/Raporumun tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.**

(Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisi alınabilir)

- ☐ **Tezimin/Raporumun tarihine kadar erişime açılmasını istemiyorum, ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.**

- ☐ **Serbest Seçenek/Yazarın Seçimi**

29/ 11 / 2018

Fehime AYDIN

ÖZET

ARAÇSAL TASARSIZ AĞLAR İÇİN İSTATİSTİKSEL TABANLI BİR SALDIRI TESPİT YÖNTEMİ

Fehime AYDIN

Yüksek Lisans, Bilgisayar Mühendisliği Bölümü

Tez Danışmanı: Doç. Dr. Sevil ŞEN AKAGÜNDÜZ

Kasım 2018, 83 sayfa

İnternete bağlı hızlı hareket edebilen cihazların sayısı gün geçtikçe artış göstermektedir. Buna bağlı olarak, bu tür hareketli cihazların birbirleriyle iletişim kurmaları için önerilen hareketli tasarsız ağlar da yaygınlaşmaktadır. Hareketli tasarsız ağların özel bir türü olan araçsal tasarsız ağların, yakın zamanda varolan en büyük ağlardan birisi olacağı tahmin edilmektedir.

Araçsal tasarsız ağlar, araçlar arasında haberleşmeyi sağlamaktır. Araçsal tasarsız ağlarda bulunan araçlar birbirleriyle trafik ve yol durumu gibi önem taşıyan mesajları paylaşarak, trafikte can ve mal güvenliğini sağlamaktadırlar. Bu açıdan, bu iletişime karşı saldırıları engellemek, engelleyemediğimiz saldırıları ise tespit etmek önem arz etmektedir. Bu ağların dinamik topolojiye sahip olmaları, onları saldırılara daha açık bir hale getirmekte beraber, etkili güvenlik mekanizmalarının geliştirilmesini de zorlaştırmaktadır.

Literatürde, araçsal tasarsız ağlar için önerilen birçok saldırı tespit sistemi bulunmaktadır. Ancak, istatistiksel tabanlı çalışmaların az olduğu ve son yıllarda bu alana bir yönelim olduğu gözlemlenmiştir. Bu tez

alışmasında, sahte bilgi saldırısı adı altında kaza uzaklığını deęiřtirme ve saldırgan konumunu deęiřtirme saldırıları için istatistiksel anomali tabanlı bir saldırı tespit sistemi önerilmiştir. Önerilen saldırı tespiti, saldırısız ortamdaki komřu araç sayısı ile komřu araçların kazaya uzaklıkları arasındaki ilişkinin yönü ve derecesini Pearson korelasyon katsayısı ile belirlemekte, bu ilişkiden farklı yöndeki durumları saldırı olarak tespit etmektedir. Kümülatif ve çoęunluk tabanlı olmak üzere iki farklı saldırı tespit mimarisi önerilmektedir.

Önerilen sistemin başarımı, Unterstrass - Zürih haritası üzerinde, 370 araçlı bir aę trafięinde, farklı oranlarda saldırganlar ile aę benzetimleri yapılarak deęerlendirilmiştir. Önerilen sistem, %1 saldırgan oranı için yüksek tespit oranı sağlarken, beklenildięi gibi saldırgan oranı arttıkça sistemin başarımı düşmektedir. Bu tez alışması ile sahte bilgi saldırısı için ilk defa istatistiksel tabanlı tespit yöntemlerinin uygulanabilirlięi araştırılmıştır. Bu alışmanın, ileride yapılacak alışmalar için bir temel olacaęı düşünölmektedir.

Anahtar Kelimeler: Arasal tasarsız aęlar, istatistiksel saldırı tespiti, sahte bilgi saldırısı, Pearson korelasyon katsayısı

ABSTRACT

A STATISTICAL-BASED INTRUSION DETECTION METHOD FOR VEHICULAR AD HOC NETWORKS

Fehime AYDIN

Master, Department of Computer Engineering

Supervisor: Doc. Dr. Sevil ŞEN AKAGÜNDÜZ

November 2018, 83 pages

The number of fast-moving devices connected to the internet is increasing day by day. Accordingly, the proposed mobile ad hoc networks are becoming widespread for these mobile devices to communicate with each other. As special types of mobile ad hoc networks, vehicular ad hoc networks are estimated to be one of the largest existing networks in near future.

Vehicular ad hoc networks provide communication between vehicles. Cars in vehicular ad hoc networks can share messages regarding traffic and road conditions, which guarantees the traffic safety. In this respect, prevention of the attacks against this communication and detection of those we cannot prevent, is of great importance. Having a dynamic topology not only causes vehicular ad hoc networks to be vulnerable for certain attacks but also complicates the development of effective safety mechanisms.

In the literature, there are several intrusion detection systems for vehicular ad hoc networks recommended. However, it has been observed that there are only a few statistical-based studies and there has been a

trend towards this area in recent years. In this thesis, a statistical anomaly based intrusion detection system has been proposed for under the name of bogus information attack, changing the distance of the accident and changing the attacker position.

The intrusion detection suggested here identifies the direction and degree of the relation between the number of neighboring vehicles and their distance from the accident in an attack-free environment, through Pearson correlation coefficient. It also identifies situations in directions different from this relation as an attack. Two different intrusion detection architectures are proposed: cumulative and majority-based.

The performance of the proposed system has been evaluated on the map of Unterstrass - Zurich with a network traffic of 370 vehicles with different rates of attackers. While the proposed system provides a high detection rate for the 1% attacker rate; it has been observed that its performance declines in parallel with the increasing attacker rate, as expected. This study is considered significant in terms of analysing the applicability of the statistical-based intrusion detection methods against bogus information attacks, for the first time. It is thought that this study will constitute a basis for future studies.

Keywords: Vehicular ad hoc networks, statistical intrusion detection, bogus information attack, Pearson correlation coefficient

TEŞEKKÜR

Tez çalışmam boyunca kıymetli desteklerini esirgemeyen, katkıları ile yol gösteren ve tez hazırlığının bütün aşamalarına değerli bilgi ve deneyimleriyle ışık tutan danışmanım Doç. Dr. Sevil ŞEN AKAGÜNDÜZ'e sonsuz teşekkürlerimi sunuyorum.

Değerli yorum ve önerileriyle katkıda bulunan jüri üyelerim Sayın Prof. Dr. O. Ayhan ERDEM, Sayın Doç. Dr. Oumout CHOUSEINOGLU, Sayın Doç. Dr. Ahmet Burak CAN ve Sayın Doç. Dr. Lale ÖZKAHYA'ya teşekkür ederim.

Son olarak çalışmamın her aşamasında manevi olarak yanımda olan aileme ve beni her koşulda destekleyen ve cesaretlendiren değerli eşim Hakan AYDIN'a içtenlikle teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET	i
ABSTRACT	iii
TEŞEKKÜR.....	v
İÇİNDEKİLER	vi
ŞEKİLLER.....	viii
TABLolar	x
SİMGELER VE KISALTMALAR.....	xi
1. GİRİŞ.....	1
2. İLİŞKİLİ ÇALIŞMALAR	5
2.1. Saldırı Tespit Sistemleri	5
2.1.1. Saldırı Tespit Mimarisi	5
2.1.1.1. Tekil Mimari.....	6
2.1.1.2. Dağıtık ve İşbirlikçi Mimari	6
2.1.1.3. Hiyerarşik Mimari	7
2.1.2. Saldırı Tespit Yöntemleri.....	7
2.1.2.1. İmza Tabanlı Saldırı Tespiti	8
2.1.2.2. Anormali Tabanlı Saldırı Tespiti	8
2.1.2.3. Spesifikasyon Tabanlı Saldırı Tespiti	9
2.2. Araçsal Tasarsız Ağlar	9
2.2.1. Araçsal Tasarsız Ağlarda Güvenlik	12
2.2.1.1. Araçsal Tasarsız Ağlardaki Saldırıları.....	13
2.2.1.2. Sahte Bilgi Saldırısı	13
2.2.1.3. Kimlik Değiştirme Saldırısı	14
2.2.1.4. Kara Delik Saldırısı	16
2.2.1.5. Hizmet Engelleme Saldırısı	17
2.2.1.6. Paket Düşürme Saldırısı	18
2.2.1.7. Gri Delik Saldırısı	19
2.2.1.8. Hız - Telaş Saldırısı	19
2.2.1.9. Tekrar Saldırısı	20

2.3.	Araçsal Tasarsız Ağlarda Saldırı Tespiti.....	20
2.3.1.	İstatistiksel Tabanlı Saldırı Tespit Yöntemleri.....	25
3.	İSTATİSTİKSEL TABANLI SALDIRI TESPİTİ.....	27
3.1.	Yöntem	27
3.1.1.	Pearson Korelasyon Katsayısı	28
3.1.2.	Pearson Korelasyon Katsayısının Saldırı Tespitine Uygulanması.....	30
3.1.2.1.	Kümülatif Tabanlı Pearson Analizi	32
3.1.2.2.	Çoğunluk Tabanlı Pearson Analizi.....	33
3.2.	Benzetim Ortamı.....	34
3.1.	Uygulanan Saldırıların Analizi	36
3.1.1.	Sahte Bilgi Saldırısı – Kaza Uzaklığı Değiştirme.....	36
3.1.2.	Sahte Bilgi Saldırısı – Saldırgan Konumu Değiştirme	39
3.2.	Değerlendirme Metrikleri	40
3.2.1.	Tespit Oranı (TO)	40
3.2.2.	Yanlış Pozitif Oranı (YPO)	41
4.	ÖNERİLEN SALDIRI TESPİT SİSTEMİNİN DEĞERLENDİRİLMESİ.....	42
4.1.	Sahte Bilgi – Kaza Uzaklığı Değiştirme Saldırısının Tespiti.....	42
4.2.	Sahte Bilgi – Saldırgan Konumu Değiştirme Saldırısının Tespiti	47
4.3.	Sonuçların Genel Değerlendirilmesi	51
5.	SONUÇ	54
6.	KAYNAKÇA	58
	ÖZGEÇMİŞ.....	65

ŞEKİLLER

	<u>Sayfa</u>
Şekil 2-1. Saldırı Tespit Mimarisi.....	6
Şekil 2-2. Saldırı Tespit Yöntemleri	8
Şekil 2-3. Araçsal Tasarsız Ağ Örneği	11
Şekil 2-4. Araçsal Tasarsız Ağlar için Yönlendirme Protokolleri.....	12
Şekil 2-5. Sahte Bilgi Saldırısı	14
Şekil 2-6. Kimlik Değiştirme Saldırısı	15
Şekil 2-7. Kara Delik Saldırısı	16
Şekil 2-8. Sel Saldırısı	18
Şekil 3-1. Komşu Araç Sayılarının Normal Dağılım Grafiği.....	31
Şekil 3-2. Unterstrass/Zurih/İsviçre	36
Şekil 3-3. Sahte Bilgi Saldırısı – Kaza Uzaklığı Değiştirme	38
Şekil 3-4. Sahte Bilgi Saldırısı - Saldırgan Konumunu Değiştirme	39
Şekil 4-1. Ağda %1 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-2. Ağda %1 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-3. Ağda %5 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-4. Ağda %5 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-5. Ağda %10 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-6. Ağda %10 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	44
Şekil 4-7. Kaza Uzaklığı Değiştirme Saldırı için Ortalama Tespit Oranları.....	45
Şekil 4-8. Sahte Bilgi - Kaza Uzaklığı Değiştirme Saldırısı için Yanlış Pozitif Oranları	46
Şekil 4-9. Ağda %1 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48

Şekil 4-10. Ağda %1 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48
Şekil 4-11. Ağda %5 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48
Şekil 4-12. Ağda %5 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48
Şekil 4-13. Ağda %10 Oranında Saldırgan Olduğunda, Kümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48
Şekil 4-14. Ağda %10 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı.....	48
Şekil 4-15. Saldırgan Konumu Değıştirme Saldırı için Tespit Oranları	50
Şekil 4-16. Sahte Bilgi Saldırısı - Saldırgan Konumu Değıştirme Saldırısı için Yanlış Pozitif Oranları.....	50

TABLolar

	<u>Sayfa</u>
Tablo 2-1. Araçsal Tasarsız Ağlar ile ilgili Yapılan Çalışmalarda Kullanılan Protokoller ve Saldırı Türleri.....	24
Tablo 3-1. Pearson Korelasyon Katsayısı Değerleri	30
Tablo 3-2. Kümülatif Tabanlı Saldırı Tespit Algoritmasının Temel Adımları.....	33
Tablo 3-3. Çoğunluk Tabanlı Saldırı Tespit Algoritmasının Temel Adımları.....	34
Tablo 3-4. Benzetim Parametreleri	35



SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

r	Pearson Korelasyon Katsayısı
Σ	Toplam Sembolü

Kısaltmalar

AİÜ	Araç İçi Ünitesi
AODV	Ad-Hoc on Demand Distance Vector Routing Protocol
AU	Application Unit
DSR	Dynamic Source Routing
FIFO	First Input First Output
FP	False Positive
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
MOVE	Mobility Vehicles
NS	Network Simulator
OBS	On Board Unit
OLSR	Optimized Link State Routing
RREQ	Route Request Packet
RSU	Road Side Unit
SPSS	Statistical Package for the Social Sciences
STS	Saldırı Tespit Sistemi

SUMO	Simulation of Urban Mobility
VANET	Vehicular Ad Hoc Networks
V2V	Vehicle to Vehicle Communication
V2I	Vehicle to Infrastructure Communication
V2R	Vehicle to Roadside Communication
TLS	Transport Layer Security
TPR	True Positive Rate
TO	Tespit Oranı
UÜ	Uygulama Ünitesi
YKB	Yol Kenarı Birimleri
YPO	Yanlış Pozitif Oranı
WAVE	Wireless Access in Vehicular Environments

1. GİRİŞ

İnternetin hayatımızın önemli bir parçası haline gelmesiyle, internete bağlı cihaz sayısı da hızlı bir artış göstermektedir. Business Insider'ın araştırmasına göre, internete bağlı cihaz sayısı 2020 yılında 24 milyarı bulacaktır [1]. Gelişen internet teknolojisi ile farklı cihaz türleri, internete erişim sağlayarak bilgiye ulaşabilmektedirler. Ayrıca internete bağlı hareketli cihazlar, kablosuz iletişim ile kendi ağlarını oluşturmakta ve veri paylaşımı yapabilmektedirler.

Hareketli cihazların kendi aralarında, bir altyapıdan bağımsız olarak haberleşmelerini sağlayan ağlara en güzel örneklerden birisi hareketli tasarsız ağlardır. Bu ağlardaki cihazlar, kablosuz ağlar aracılığı ile birbirleri ile iletişim halindedirler. Dolayısıyla, birbirlerinin kapsama alanındaki cihazlar doğrudan iletişim halindeyken, birbirlerinden uzakta olan cihazların haberleşmesi için ara düğümlere güvenilmektedir. Bu nedenle, bu ağlardaki cihazlar, hem veri alıp gönderen bir sistem, hem de yönlendirici olarak davranabilmektedirler [2]. Bu tür ağların kullanımına örnek olarak, sabit yapının kurulamayacağı askeri uygulamalar veya deprem gibi afetlerin kurtarma operasyonlarındaki veri paylaşım uygulamaları gösterilebilir. Sabit bir yapıya sahip olmadıkları ve kablosuz ağ kullandıkları için bu tür ağlar, kablolu ağlar ile kıyaslandığında saldırılara karşı daha dayanıksızdırlar [3].

Araçsal tasarsız ağlar, ulaşım alanında araçların birbirleriyle kablosuz olarak iletişim kurmalarını sağlayan, hareketli tasarsız ağların özel bir türüdür [4]. Araçsal tasarsız ağlarda, cihazların hareketliliği hareketli tasarsız ağlardaki cihazlara göre çok daha fazladır. Araçsal tasarsız ağların, hayati öneme sahip uygulamaları bulunmaktadır. Örneğin, trafikte can ve mal kayıplarına neden olan kazaların önlenmesi için araçlar

arası iletişim önem kazanmaktadır. Araçsal tasarsız ağlar ile trafikteki araçlar arasında gerçek zamanlı ve anlık iletişimin sağlanması ile ağdaki olası kazalar önlenabilmektedir [5]. Ağda bulunan bir kazanın bilgisi, anında komşu araçlara bildirildiği takdirde, bu kazadan kaynaklı oluşabilecek trafik sıkışıklıkları da engellenebilecektir. Trafiğe çıkan araç sayısındaki artış göz önüne alındığında, araçsal tasarsız ağların, yakın gelecekte varolan en büyük ağlardan birisi olacağı düşünülmektedir.

Araçsal tasarsız ağlardaki araçların yüksek hareketliliği nedeniyle, ağ topolojisi sürekli değişim göstermektedir. Bu tür ağlardaki hızlı topoloji değişikliği, ağda kopmalara ve paket iletim oranının düşmesine sebep olmaktadır. Ayrıca bu dinamik topoloji, ağ trafiğinin kontrolünün yapılmasını zorlaştırmakta, dolayısıyla ağ tehditlere ve saldırılara açık hale getirmektedir. Bu saldırıların, ağ kullanılamaz hale getirme gibi önemli sonuçları bulunmaktadır [6]. Bu tür saldırılara karşı güvenlik önlemlerinin alınması gerekmektedir. Fakat, alınan güvenlik önlemlerine rağmen, ağa karşı hala saldırılar gerçekleştirilebilmektedir. Bu tür saldırıların zamanında tespit edilmesi, bu saldırıların etkisinin hızlıca azaltılması ve durdurulması için önemlidir. Bu amaçla önerilen saldırı tespit sistemleri, güvenlik yaşam döngüsünün vazgeçilmez bileşenlerinden birisidir.

Araçsal tasarsız ağlar için önerilen birçok saldırı tespit sistemi bulunmasına rağmen, istatistiksel tabanlı çalışmaların az olduğu ve son yıllarda istatistiksel tabanlı yöntemlerde bir artış olduğu gözlemlenmektedir. Literatürde karşılaşılan istatistiksel tabanlı tespit yöntemlerinin çoğu, kimlik değiştirme saldırısını tespit etmek amaçlıdır. Araçlar tasarsız ağlarda, araçlar hız ve konum bilgilerini birbirlerine göndermektedirler. Bu bilgilerin yardımı ile araçların konum bilgisinin yakın gelecekteki değeri tahmin edilebilmektedir. Dolayısıyla, normal dağılımdan faydalanılarak tahmin edilen konum bilgisi, kimlik değiştirme saldırısının istatistiksel yöntemler ile tespitini mümkün kılmaktadır.

Sahte bilgi saldırısı için benzer bir tahmin verisinin elde edilememesinden dolayı, benzer tespit yöntemlerinin bu saldırı türüne uygulamasına rastlanmamıştır. Sahte bilgi saldırısında saldırgan, ağda bulunan kazanın konumu veya kendi konumu hakkında yanlış bilgi verir. Bu çalışmada, bu tür sahte bilgi saldırılarının tespiti için istatistiksel tabanlı yöntemler araştırılmıştır. Önerilen yöntem, iki değişken arasındaki ilişkiyi ifade etmek için kullanılan Pearson korelasyon katsayısı yöntemi tabanlıdır. Kümülatif ve çoğunluk tabanlı Pearson analizi isimli iki yöntem önerilmiştir.

Pearson analizi, komşu sayısı ile komşuların kazaya olan uzaklıkları arasındaki ilişkiyi analiz eder ve bu iki değişken arasındaki ilişkinin yönü ve şiddeti hakkında fikir verir. Saldırı olmadığı ortamda bu iki değişkenin ilişkisi incelenmiş, normaldeki durumdan sapmalar saldırı olarak değerlendirilmiştir. Bu iki yöntem, ağda saldırı olması durumunda, komşu sayısı ve komşuların kazaya olan uzaklıkları arasındaki ilişkinin yön değiştireceği varsayımına dayanmaktadır. Kümülatif tabanlı pearson analizi yönteminde saldırıyı tespit eden araç, komşu araçlardan kazaya olan uzaklıklarını almaktadır. Alınan uzaklık bilgilerinin ortalaması ile komşu sayısı arasındaki ilişkiyi inceleyerek, normalden sapmaları saldırı olarak işaretlemektedir. Çoğunluk tabanlı pearson analizi yönteminde ise komşu araçlardan, kendi hesapladıkları korelasyon değeri ve yönünü toplamakta, komşu araçların çoğunluğunun gönderdiği Pearson korelasyon katsayısı yönü, saldırı olmayan ortamdaki değerden farklı ise bu durum saldırı olarak işaretlenmektedir.

Önerilen yöntemler, Unterstrass - Zürih haritası üzerinde, 370 araçlı bir ağ trafiğinin benzetimi yapılarak değerlendirilmiştir. Ağda farklı oranlarda (%1, %5 ve %10) saldırgan olması durumları incelenmiş ve ilgili yöntemlerin tespit ve yanlış tespit oranları değerlendirilmiştir.

Deney sonuçları, saldırganız ortamdaki komşu sayısı ve kazaya olan uzaklık arasında bulunan negatif yönlü ilişkinin, saldırı olması durumunda değıştiğı varsayımını desteklemektedir. Ağdaki saldırgan sayısı, tüm araçların %1'i oranında olduğunda, önerilen yöntemler yüksek başarı sergilemektedir. Fakat, saldırgan oranı arttıkça tespit oranı da düşmekte, ağdaki saldırgan oranı %10'u geçtiğinde yeterli başarı elde edilememektedir.



2. İLİŞKİLİ ÇALIŞMALAR

Bu bölümde, öncelikle saldırı tespit sistemlerinin mimarisi ve yöntemleri hakkında genel bilgiler verilecektir. Sonrasında, bu bilgiler doğrultusunda, literatürde bulunan araçsal tasarsız ağlar için önerilen saldırı tespit yöntemleri, ele alınan saldırılar ile beraber incelenecektir.

2.1. Saldırı Tespit Sistemleri

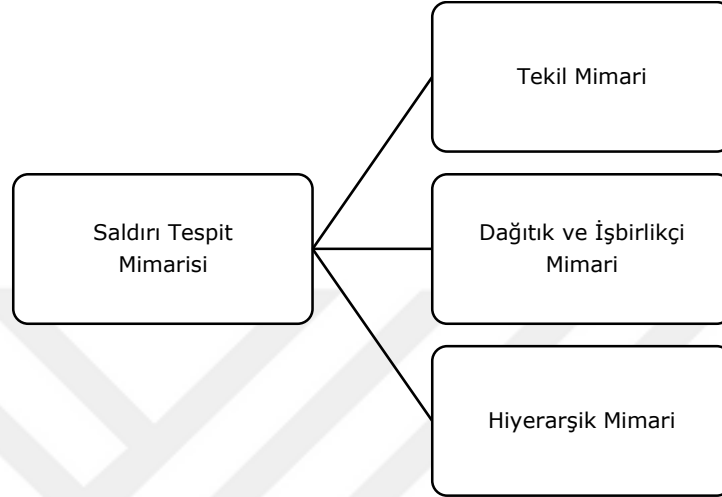
Günümüzde ağ sistemlerine karşı yapılan saldırıları tespit etmek ve önlemek için yeni teknikler veya uygulamalar gerekmektedir. Saldırı tespit sistemleri de, ağ trafiğini ve/veya bilgisayar sistemlerini izleyip, analiz ederek, olası saldırıları tespit etmeye çalışan sistemlerdir [7]. Bir saldırı tespit sisteminin temel görevi, gözlenen ağ hakkında bilgi toplamak ve bu bilgilere göre ağa karşı yapılan saldırıları tespit edip raporlamaktır. Saldırı tespit sistemleri imza, anomali ve spesifikasyon tabanlı olarak sınıflandırılmaktadır. Aynı sınıflandırma, araçsal tasarsız ağlar için de geçerlidir. Ayrıca, literatürde araçsal tasarsız ağlarda önerilen saldırı tespit sistemleri, veri toplama yöntemi, tespit yöntemi, ağın mimarisi vb. göre sınıflandırmalar yapılmıştır [8]. Bu bölümde, ilgili saldırı tespit mimarileri ve yöntemleri incelenmektedir.

2.1.1. Saldırı Tespit Mimarisi

Kablosuz ağlar için önerilen saldırı tespit mimarileri, ağ alt yapısına göre değişiklik göstermektedir. Ağ altyapısı, düz ve çok katmanlı olmak üzere iki kategoride değerlendirilmektedir. Düz ağ altyapısında, her araç eşit olarak kabul edilmekte ve saldırı tespitini kendisi gerçekleştirmektedir. Çok katmanlı ağ altyapısında ise, ağdaki düğümler bazı gruplara (kümeleme, vb. gibi) bölünmektedirler. Bu gruplarda, bazı düğümler

(küme başı, vb. gibi), diğerlerinden daha fazla sorumluluğuna sahiptir [9][10].

Hareketli tasarsız ağlarda saldırı tespiti için bulunan üç tür mimari Şekil 2-1’de gösterilmektedir. Bu mimariler tekil, dağıtık ve işbirlikçi ve hiyerarşik olarak adlandırılmaktadır [11].



Şekil 2-1. Saldırı Tespit Mimarisi

2.1.1.1. Tekil Mimari

Bu mimariye göre her araç sadece kendi başına saldırı tespiti yapmakta, bunun için kendisinde bulunan yerel verileri kullanmaktadır. Bu mimari içerisindeki araçlar, saldırı tespiti ve sonrası için diğer araçlar ile herhangi bir bilgi paylaşımı yapmazlar. Her düğüm ya da araç, sadece mevcut bilgilerine göre karar verdiğinden, saldırıları tespit etme yetenekleri sınırlıdır [12].

2.1.1.2. Dağıtık ve İşbirlikçi Mimari

Dağıtık ve işbirlikçi mimaride, tekil mimaride olduğu gibi her araç bağımsız olarak kendi saldırı tespiti sistemini içermektedir. Ancak sonunda ortak bir karar ile saldırıyı belirlemek için işbirliği

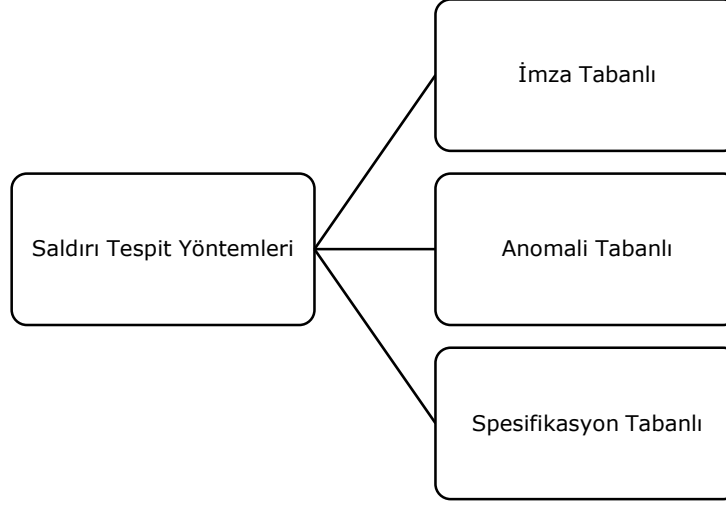
yapmaktadırlar. Bu mimari, ortak bir karar mekanizması ile daha çok veri üzerinde işlem yapabildiğinden, kablosuz sensör ağları için daha uygun olduğu görülmüştür [13].

2.1.1.3. Hiyerarşik Mimari

Hiyerarşik mimariye sahip saldırı tespit sistemleri de bir tür dağıtık ve işbirlikçi mimaridir, fakat bu mimaride, ağdaki bazı araçlar diğer araçlara kıyasla daha fazla sorumluluğa sahiptir [14]. Bu mimari, çok katmanlı kablosuz ağlar için önerilmektedir [9]. Ağ kümelerine ayrılmış bir yapıya sahiptir. Her kümede yol kenarı birimi gibi çalışan bir küme lideri bulunmaktadır. Küme liderleri, kendi kümelerinde bulunan araçlardan bilgileri toplamakta ve bu bilgilere göre kümede saldırı olup olmadığına karar vermektedirler. Küme liderleri, kümelerinde bir saldırı tespit ettiklerinde, saldırı paketini yeniden yönlendirme, değiştirme, ağdan düşürme, vb. gibi yanıtlar verebilirler. Araçsal tasarsız ağlarda, her küme lideri, merkezi yetki birimi ile işbirliği yaparak, bu hiyerarşiyi daha da katmanlı bir hale getirebilir.

2.1.2. Saldırı Tespit Yöntemleri

Araçsal tasarsız ağlarda saldırı tespit sistemleri imza, anomali ve spesifikasyon tabanlı olarak sınıflandırılmaktadır (Şekil 2-2).



Şekil 2-2. Saldırı Tespit Yöntemleri

2.1.2.1. İmza Tabanlı Saldırı Tespiti

İmza tabanlı saldırı tespit sistemlerinde, saldırıların imzalarına dayanarak saldırılar tespit edilmektedir. Saldırıları tespit edebilmek için saldırıların imza bilgilerinin daha önceden biliniyor olması gerekmektedir. Bu yöntem ile, bilinen ve imza bilgisi bulunan bir saldırının tespiti yapılabilmekte, ancak yeni saldırıların tespiti sağlanamamaktadır. Ayrıca, tanımlanmış olay, imza veya modeller ile eşleştirme yaparak saldırı olup olmadığına karar veren bir yapısı olduğundan çok fazla yanlış pozitif sonuçlar üretmemektedir [15][16].

2.1.2.2. Anomali Tabanlı Saldırı Tespiti

Anomali tabanlı saldırı tespit yöntemlerinde, ağdaki normal trafik ya da davranışların bilindiği varsayılarak, bu normal davranışlardan sapma, saldırı olarak tespit edilir [17]. Araçsal tasarsız ağlarda, normal davranışlar, ağdaki bulunan araçlar incelenerek belirlenmektedir. Bu aşama çok önemlidir, çünkü yetersiz veya eksik modelleme ile ağdaki normal bir davranış, saldırı olarak algılanabilir. Bu yöntemin en önemli

avantajı, yeni saldırıların tespitini de sağlamasıdır [18]. Genellikle, makine öğrenmesi kullanılarak geliştirilen anormali tabanlı saldırı tespit yöntemlerinin, yeni saldırıların tespit edilmesinde daha etkili olduğu gösterilmiştir [19].

2.1.2.3. Spesifikasyon Tabanlı Saldırı Tespiti

Spesifikasyon tabanlı saldırı tespit sistemi, imza ve anormali tabanlı saldırı tespit sistemlerinin avantajlarını içermektedir. Genelde belirli protokoller için uygulanır, tüm protokoller için uygulanması zor olduğu için kablolu ağlar için yaygın bir kullanımı yoktur. Bu yöntem ile, bir programın veya protokolün spesifikasyonları tanımlanmakta, bu spesifikasyonlara uymayan durumlar saldırı olarak işaretlenmektedir [20]. Spesifikasyon tabanlı saldırı tespitinde saldırgan araçların tespitinden çok, saldırıların etkisi ve belirlenen spesifikasyonların ihlal edilme durumları incelenmektedir [21][22].

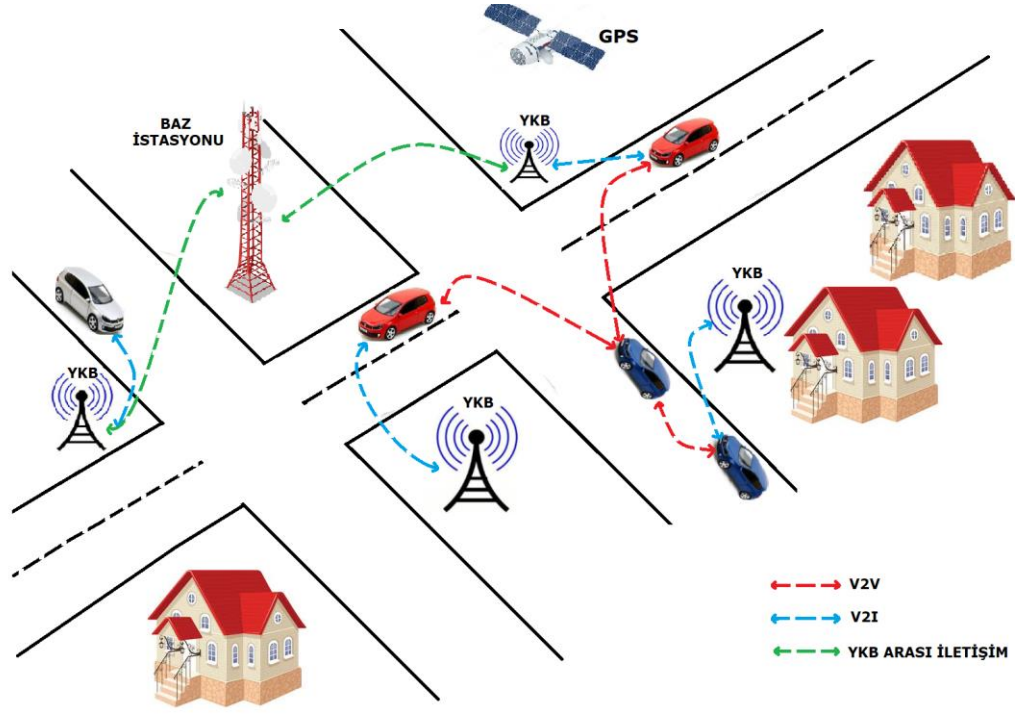
2.2. Araçsal Tasarsız Ağlar

Mobil cihazların kullanımının artmasıyla bu cihazların sabit ağ altyapısı olmadan iletişim kurmaları gereksinimi ortaya çıkmıştır. Hareketli tasarsız ağların özel bir türü olan araçsal tasarsız ağlar ise, araçlar arasında haberleşmeyi sağlamaktır. Trafikte bulunan araç sayısı dikkate alındığında, araçsal tasarsız ağların ileriki yıllarda, en büyük ağlardan birisi olacağı düşünülmektedir [23].

Araçsal tasarsız ağlardaki düğümlerin hızı, hareketli tasarsız ağları oluşturan düğümlerin hızlarından daha yüksek olması sebebiyle, bu ağlar daha dinamik bir topolojiye sahiptirler. Hareketli tasarsız ağlarda hareketlilik, cihazların enerji sorunu bulunmasından dolayı daha azdır.

Araçsal tasarsız ağlar ise, araçlardan oluştuğu için kullanılan ağ protokolleri ve algoritmaları için enerji sorunu bulunmamaktadır [4]. Araçsal tasarsız ağlar, hareketli araçlar arası haberleşmeyi sağlamakla beraber, bazı sorunları da beraberinde getirmiştir. Araçların yüksek hareketli olması ve bu ağların hızlı değişen topolojiye sahip olması sebebiyle araçlar arasında bağlantılar kısa süreli olmaktadır. Bu da, bu ağlar üzerinde gerçekleştirilecek güvenlik mekanizmaları için bir zorluk oluşturmaktadır [24].

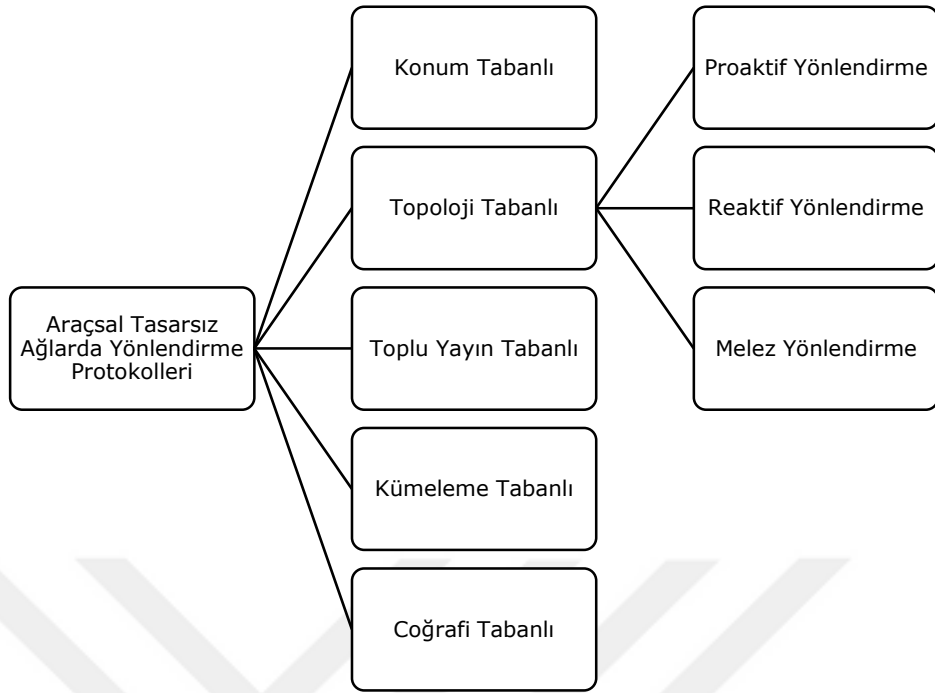
Araçsal tasarsız ağ mimarisinin temel bileşenleri Uygulama Ünitesi (UÜ), Araç İçi Ünitesi (AİÜ) ve Yol Kenarı Birimleri (YKB)'dir. Araç içi ünitesi, uygulama ünitesi için iletişim arayüzüdür [6]. AİÜ, diğer araç ve birimler ile haberleşmeyi sağlar ve araç kimlik bilgilerini barındıran birimdir. Yol kenarı birimleri ise ağa belirli aralıklarla yerleştirilen, belirli kapsama alanları olan sabit ünitelerdir. Bilgi sağlayıcı olarak hareket eden yol kenarı birimlerinin temel işlevi bilginin dağıtımını sağlayarak iletişim alanını genişletmek ve araçlar arası iletişimi sağlamaktır [7]. Yol kenarı birimleri, az yoğunluklu ağlarda performansı arttırmak için kullanılmaktadır. Böylece araçlar, yol kenarı birimleri sayesinde komşusu olmayan araçlara da bilgi iletimi sağlayabilirler [8]. Fakat, bu yol kenarı birimlerinin yerleştirilmesi maliyetli bir yöntemdir ve henüz tüm yollara uygulanmamıştır.



Şekil 2-3. Araçsal Tasarsız Ağ Örneği

Araçsal tasarsız ağlarda iletişim araçtan araca (V2V) ve araçtan yapıya (V2I) olmak üzere ikiye ayrılmaktadır. Araçtan araca iletişim, iki veya daha fazla aracın aralarında gerçekleşmektedir ve bu iletişimde trafik ile ilgili mesajlar paylaşılmaktadır. Araçtan yapıya iletişimde ise araçlar YKB'lar ile haberleşmektedir. V2V ve V2I iletişim ile araçlar bulundukları alan, yol, trafik, kaza, vb. gibi bilgilere erişim sağlamaktadırlar [25]. Şekil 2-3'de araçsal tasarsız ağlarda iletişim ile ilgili bir örnek gösterilmiştir.

Araçsal tasarsız ağlarda, iletişim kurmak isteyen iki aracın, nasıl bir yol izleyeceğini yönlendirme protokolü belirlemektedir [26]. Yönlendirme protokolü, iletişim için kullanılacak olan yolun bulunmasını ve ilgili iletişim paketlerinin bu yoldan gönderilmesini sağlamaktadır. Araçsal tasarsız ağlardaki yönlendirme protokollerinin sınıflandırması Şekil 2-4'te gösterilmiştir [27].



Şekil 2-4. Araçsal Tasarsız Ağlar için Yönlendirme Protokolleri

2.2.1. Araçsal Tasarsız Ağlarda Güvenlik

Araçsal tasarsız ağlarda araçlar arası iletişimde ağdaki trafik hakkında bilgi alış verişi yapılmaktadır. Bu sebeple, araçsal tasarsız ağlarda güvenilir haberleşmenin sağlanması büyük önem taşımaktadır.

Araçsal tasarsız ağlarda, kötü niyetli araçların aynı anda hem kullanıcı hem de yönlendirici olabilmesi ve bu araçlarda temel ağ güvenlik bileşenlerinin olmaması sebebiyle güvenlik zafiyetleri ortaya çıkmaktadır. Ayrıca araçsal tasarsız ağlarda iletişim, kablosuz ağ üzerinden sağlanmamakta, bu da ağı saldırılara açık hale getirmektedir.

Araçsal tasarsız ağlarda ağ topolojisi, hareketli tasarsız ağlara göre daha sıklıkla değişmesine rağmen, hareketli tasarsız ağlar ile benzer güvenlik sorunları bulundurmaktadır [28][29]. Araçsal tasarsız ağlarda yüksek hareketliliğin bulunması ve dinamik bir topolojiye sahip olması bu

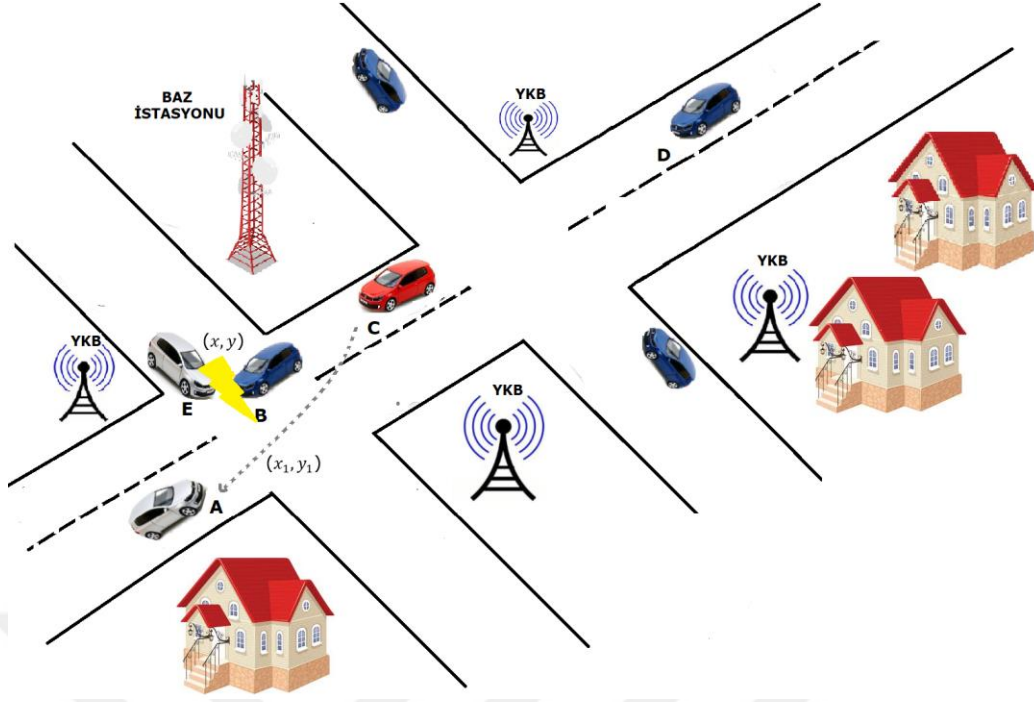
güvenlik sorunlarını daha da arttırmaktadır. Dolayısıyla, araçsal tasarsız ağlar, hem hareketli tasarsız ağlar ile ortak saldırılara karşı zayıf olmakla beraber, literatürde bu ağlara özgü yeni saldırılar da tanımlanmıştır.

2.2.1.1. Araçsal Tasarsız Ağlardaki Saldırılar

Bu bölüm, araçsal tasarsız ağlara karşı yapılabilecek en bilinen saldırıları içermektedir. Bu saldırılar sahte bilgi, kimlik değiştirme, kara delik, hizmet engelleme, paket düşürme, gri delik, hız – telaş ve tekrar saldırılarıdır.

2.2.1.2. Sahte Bilgi Saldırısı

Saldırı olmayan araçsal tasarsız ağlarda, araçlar ürettikleri mesajları komşu araçlara iletebildikleri gibi sadece kendileri için de kullanabilmektedirler. Ağda bir saldırgan olması durumunda, alınan mesajlar gerçek bilgi içermeyebilir. Ayrıca, saldırgandan gelen mesajı alan iyi niyetli bir araç, bu mesajı ağdaki diğer araçlar ile paylaşabilir [30]. Değiştirilmiş veya doğru olmayan bir mesaj, rota değişimi, yanlış rota hesaplama vb. gibi çeşitli sonuçlara neden olmaktadır. Ağda bu mesajı doğrulayacak araç olmaması durumunda saldırının doğuracağı olumsuz sonuçlar artacaktır. Araçsal tasarsız ağlarda bilgi dağıtımı araçlar tarafından yapıldığı için güvenilir komşu araçlar olmadığında ya da gelen mesajın doğrulaması yapılamadığında ciddi kazalar ortaya çıkabilmektedir [31].



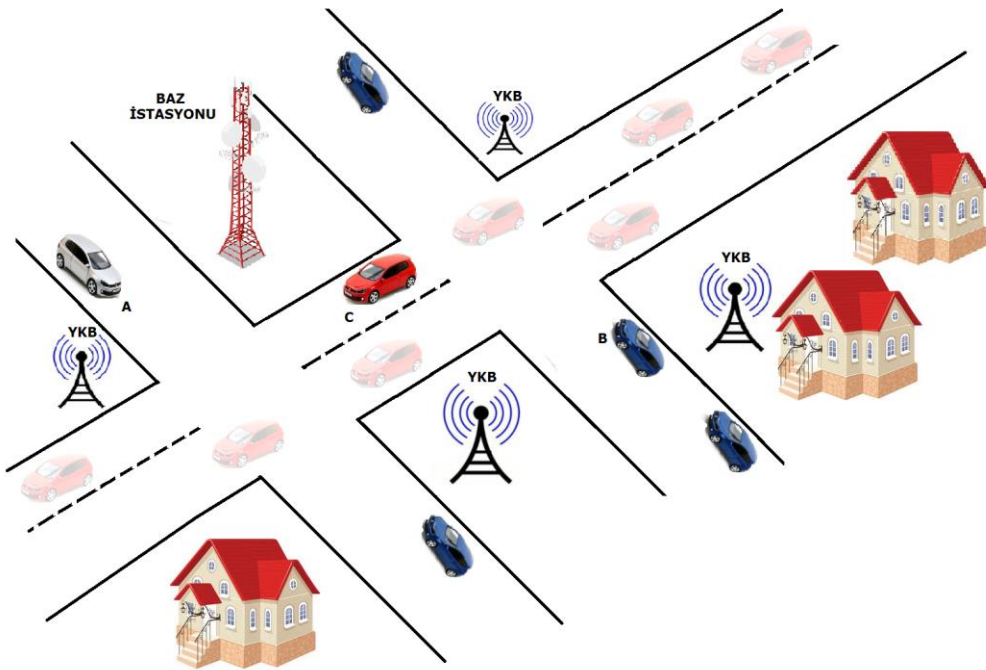
Şekil 2-5. Sahte Bilgi Saldırısı

Şekil 2-5’de bulunan B ve E araçları arasında bir kaza meydana gelmiştir ve trafiğe engel olmaktadır. Saldırgan C aracı, A aracına kaza konumunu hatalı gönderdiği veya yolun açık olduğu bilgisini gönderdiği için A aracı kazaya doğru ilerlemeye devam etmekte, bu durum da nihayetinde trafikte sıkışıklığa neden olacaktır. Eğer C aracı kaza bilgisini doğru olarak bildirseydi, A aracı yeni rota oluşturabilir ve kazadan uzaklaşabilirdi. Saldırgan C aracı, D aracına da aynı hatalı mesajı gönderdiğinde, aynı şekilde, D aracı da bu bilgiyi başka araçlar aracılığı ile doğrulayamazsa, olası olumsuz sonuçlar artacaktır.

2.2.1.3. Kimlik Değiştirme Saldırısı

Saldırgan bir aracın, kendini birden fazla kimlik ile ağda tanıtması durumunda karşılaşılan saldırı türüdür [32]. Bu saldırıda saldırgan araç, ağdaki diğer araçların kimlik bilgilerini toplamaktadır. Bu bilgileri kullanarak, farklı kimlik ya da kimlikler ile ağda bulunan diğer araç ve birimlere mesaj göndermektedir [33]. Saldırgan aracın gerçek kimliğinin

belirlenememesinden dolayı, özellikle diğer saldırılar ile beraber kullanıldığında, kimlik değiştirme saldırıları araçsal tasarsız ağlar için ciddi sorunlar yaratabilmektedirler. Örneğin, kimliğini değiştiren saldırgan, hem kendi konumunu farklı yerlerde gibi diğer araçlara iletebilir hem de ağda var olan bir kazanın konumunu farklı bir yerde gerçekleşmiş gibi gösterebilir [34]. Bu yüzden kimlik değiştirme saldırısı, araçsal tasarsız ağlar için büyük bir tehdit oluşturmaktadır.

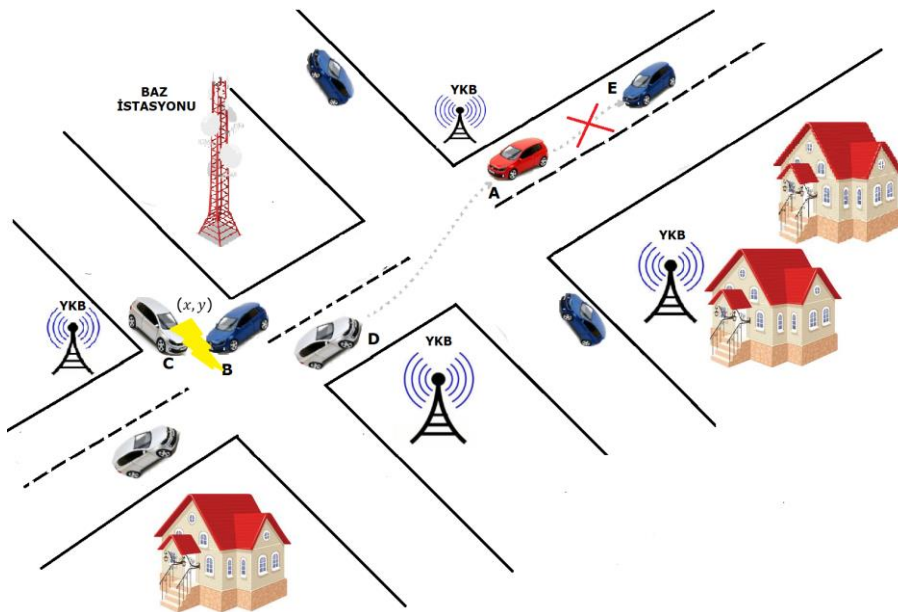


Şekil 2-6. Kimlik Değiştirme Saldırısı

Şekil 2-6'de, C aracı birden fazla kimlik oluşturmakta ve ağdaki diğer araçlara trafiğin yoğun olduğu bilgisini göndermektedir. Farklı kimliklerden aynı mesajı alan A ve B araçları, yoğun trafiğe sahip bir ağda ilerlerken, C aracı ise gönderdiği sahte mesajlar sayesinde yoğunluğunu azalttığı yolda rahat bir şekilde yolculuğuna devam etmektedir [35].

2.2.1.4. Kara Delik Saldırısı

Kara delik saldırısı, ağ iletişiminin engellenmesi veya ağ kaynaklarının kullanımının kısıtlanması amacıyla gerçekleştirilmektedir [36]. Bu saldırı, araçsal tasarsız ağlardaki araçlar arası iletişimin en kısa yoldan yapılması veya enerjisi yoğun olan araç üzerinden yapılması gibi özellikleri kullanarak ağı yönetebilir ve ölümcül sonuçlar doğurabilir. Bu saldırı türünde saldırgan trafiği farklı bir rotadan çekmeye çalışmaktadır. Kötü amaçlı araç, hedefe giden bir rotası olmamasına rağmen, gelen isteklere ilk yanıt veren araç olarak hızlı bir geri bildirim yapmakta ve hedef araca olan rotayı ele geçirmektedir. Sonrasında, saldırgan araç, bu hedef araca gelen paketleri düşürerek, ilgili araç ile tüm iletişimi kesebilir [37]. Kötü amaçlı araç, tüm bilgi paketlerini düşürdüğünde ağda dolaşan önemli bilgi paketlerini de düşürmüş olacaktır. Saldırı sonucu düşen bu paketler, gitmesi gereken araçlara ulaşmadığında ağda kaza, trafik yoğunluğu vb. gibi önemli sonuçlara da neden olabilir. Bu saldırı, değişik ağ katmanları seviyelerinde uygulanabilmektedir. Özellikle, yönlendirme katmanında uygulanması ile yönlendirme protokolünün başarımını da olumsuz etkilemektedir. Literatürde en yoğun olarak benzetimi yapılan kara delik saldırılarından birisi, AODV yönlendirme protokolüne karşıdır [38][39].



Şekil 2-7. Kara Delik Saldırısı

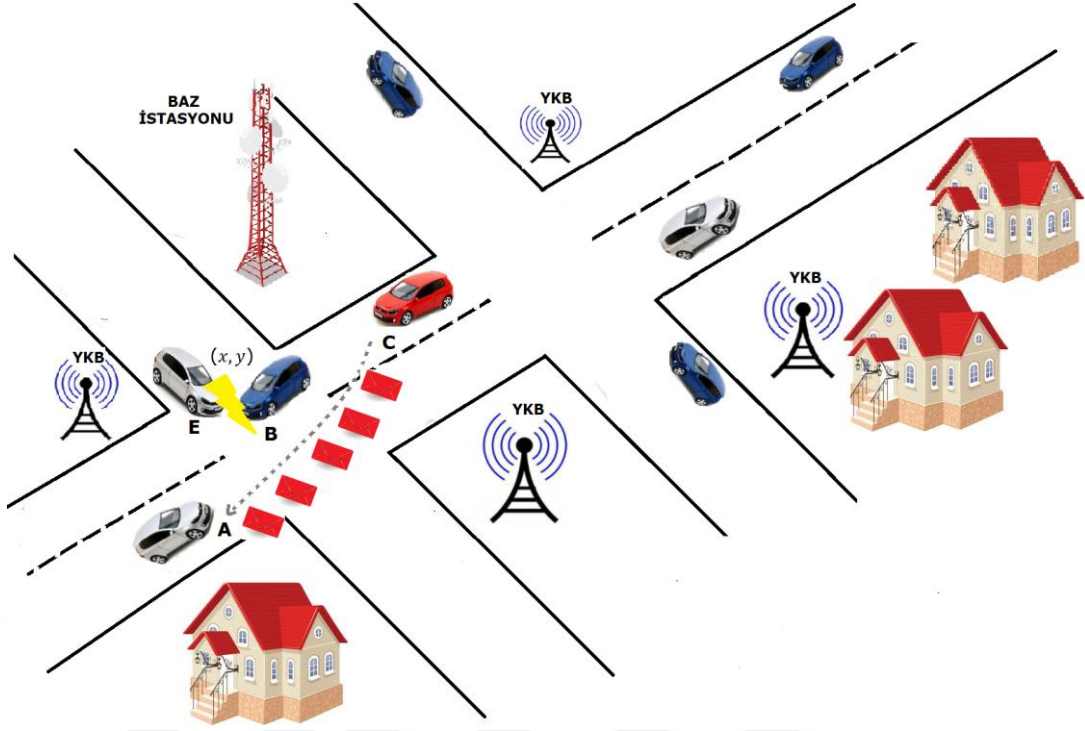
Şekil 2-7’te kara delik saldırısı için bir örnek gösterilmiştir. Saldırgan A aracı, E aracına gitmesi gereken paketi kendi üzerine çektikten sonra düşürerek, E aracının kaza mesajını almasını engellemektedir.

2.2.1.5. Hizmet Engelleme Saldırısı

Hizmet engelleme saldırıları, bir sistemin en önemli güvenlik gereksinimlerinden birisi olan sistemin kullanılabilirliğini hedef almaktadırlar. Hizmet engelleme saldırısı araçların kaynak, işlemci gücü, bellek ve bant genişliği gibi iletişim kaynaklarını tüketerek araçlara zarar vermektedir. Bu tür saldırılar altında olan araçsal tasarsız ağlar, hizmet sağlama becerisinin bir kısmını veya tamamını kaybedebilir [40]. Araçsal tasarsız ağlarda en etkili saldırılardan birisidir.

Bu saldırı, gereksiz ve aşırı talepler veya mesajlar ile ağ kaynaklarının kullanımını aksatmayı hedefleyen bir siber saldırıdır [41]. Saldırgan aracın düzenli ve sürekli gönderdiği işlevsiz mesajlarla ağda oluşan mesaj trafiği, diğer araçların gönderdikleri mesajların iletilmemesine sebep olmaktadır. Saldırgan araçların birden fazla olması durumunda ağ taleplere cevap veremez hale gelebilir ve daha ileri boyutta hizmet sağlayamaz hale gelmesi gibi ciddi sorunlara yol açabilir. Bu saldırı, hizmet engelleme saldırısının bir türü olan dağıtık hizmet engelleme saldırı olarak adlandırılır. AODV yönlendirme protokolünde, rota keşfi için ağdaki tüm paketlere gönderilen RREQ paketleri ile yapılan sel saldırı, hareketli tasarsız ağlara uygulanan en bilinen saldırılardandır [26].

Şekil 2-8’de sel saldırısı ile ilgili bir örnek gösterilmiştir.



Şekil 2-8. Sel Saldırısı

2.2.1.6. Paket Düşürme Saldırısı

Saldırgan aracın, ağa diğer araçlar gibi katılıp kendisine gelen paketleri diğer araçlara aktarmaması ile oluşan bir saldıdır. Ağdaki hizmeti engellemeye yönelik bir saldırı olduğu için hizmet engelleme saldırısının bir türü olarak değerlendirilmektedir.

Genellikle paket düşürme saldırısı, rota oluşumu sırasında kötü niyetli bir aracın kendini ilgili rotaya sokması ile başlamaktadır. Genellikle, ağdaki araçlar arasındaki güvenilirlik varsayımına dayanan yönlendirme protokollerine karşı yapılmaktadırlar [42]. Saldırganın, üzerinden geçen tüm paketleri düşürmesi ile kolayca tespit edilebilir ve yeni bir rota keşfi başlatılır.

2.2.1.7. Gri Delik Saldırısı

Gri delik saldırısı, saldırgan aracın sadece belli paketleri veya belli bir hedefe giden paketleri düşürmesi sebebiyle tespit edilmesi ve önlenmesi en zor saldırı türlerinden birisidir. Saldırgan, seçilen belli formattaki paketlerin düşürülmesi ve diğer paketlerin iletilmesi ile ağ trafiğinin güvenilir olduğu izlenimini bırakarak, tespit edilmeden saldırısını gerçekleştirmeye devam edebilir [43].

Gri delik olarak adlandırılan saldırgan çeşitli teknikler ile kötü niyetli davranış sergileyebilir. Bunlardan biri, ağda paketleri belirli bir süre boyunca düşürüp daha sonra normal bir araç gibi davranmaya başlamasıdır [44]. Bu tekniklerin diğeri ise, ağdaki belirli araç veya araçlardan gelen veya giden paketleri düşürmesidir. Ayrıca, sadece belirli türdeki paketler seçilebilir. Ayrıca saldırgan, bu iki tekniğin birleşimi bir davranış da sergileyebilir, böylece saldırının tespit edilmesini daha da zorlaştırmaktadır. [45].

2.2.1.8. Hız - Telaş Saldırısı

Hız – Telaş saldırısı, paketin ağ trafiğinde en hızlı iletileceği rotada gönderilmesi sırasında gerçekleştirilir. Sadece ilk gelen yönlendirme isteğine cevap verilen ve sonrasında gelen yönlendirme isteklerini dikkate almayan yönlendirme protokollerine karşı oldukça etkili bir saldırı türüdür [46]. Ağda rotaya ihtiyaç duyan bir araca gönderilecek ilk rota içerikli paket geçerli kabul edilecektir. Bu paketin ağda bir saldırgan araç tarafından gelmesi durumunda, saldırgan araç kaynak ve hedef araç arasındaki iletişime erişim sağlayacaktır [47].

2.2.1.9. Tekrar Saldırısı

Araçsal tasarsız ağlara karşı gerçekleştirilen bir diğer saldırı türü de tekrar saldırısıdır. Bu saldırılarda saldırgan araç, ağ içerisinde yeni mesajlar üretmez. Bunun yerine, aldıkları mesajları saklamakta, bunları ağa farklı zamanlarda tekrar göndererek ağda trafiğin artmasına sebep olmaktadır [48]. Saldırgan araç, kendisine gelen mesajları saklayabildiği gibi kendisinin üretilip gönderdiği mesajları da saklayabilmektedir. Bu saldırıyı kendi ürettiği mesajları tekrar tekrar göndererek de gerçekleştirebilmektedir [28].

2.3. Araçsal Tasarsız Ağlarda Saldırı Tespiti

Araçsal tasarsız ağlarda çeşitli saldırılar için uygulanan saldırı tespit yöntemleri bulunmaktadır. Bu bölümde, araçsal tasarsız ağlarda uygulanmış olan saldırılar ve bu saldırılara karşı gerçekleştirilen saldırı tespit yöntemleri incelenmektedir.

Literatürde araçsal tasarsız ağlarda kimlik değiştirme saldırısı için normal dağılım testi kullanan bir uygulama incelenmiştir. Yu ve ekibi [49], kimlik değiştirme saldırısı için normal dağılım testi uygulamışlardır. GrooveNet ve NS2 araçları kullanılarak Detroit haritası üzerinde 100 araç üzerinde uygulama yapılmıştır. Önerilen işbirlikçi mimarideki saldırı tespit yöntemi, sinyal gücü analizi ile araçların kimlik doğrulamasını yapmaktadır. Araçların GPS konum ve sinyal bilgileri toplamaktadır. Bu çalışma, araçların gerçek konumları ve olması gereken konumları arasında fark yoktur hipotezi ile ağı incelenmektedir. Analizler sonucunda, düşük yoğunlukta başarılı bir saldırı tespit sistemi önerilmiştir.

Zaidi ve Nallanathan [50], yanlış bilgi ve kimlik değiştirme saldırılarına karşı bir saldırı tespit sistemi önermişlerdir. Bu çalışmada, SUMO, OMNET++ ve VACaMobil benzetim araçları kullanarak 400 saniye süren ağlar tanımlamışlardır. Bu ağlar üzerinde yaptıkları analizler sonucunda, saldırgan araç sayısının, ağdaki araç sayısının %40'ın altında olduğu durumlarda saldırı tespitinin başarıyla yapıldığı belirtilmiştir. Bu benzetimlerde, ağdaki araçlar hızlarını, hesaplanan ortalama akışı, ortalama yoğunluğu ve konum bilgilerini diğer araçlara göndermektedirler. Bu bilgiler, tüm komşu araçlardan toplanmaktadır. Hesaplanan ve toplanan değerler arasında önemli bir fark olup olmadığı t-testi analizi ile yapılmıştır. Hesaplanan t değeri ile istatistiksel analizlerde kullanılan t tablosundaki ilgili değerler kıyaslanır ve hesaplanan t değeri, t testi kabul bölgesi içinde bir sonuç verirse, veriler kabul edilir ve hipotez reddedilir. Veriler reddedilirse, araç saldırgan olarak belirlenmektedir. Bir saldırı tespit edildiğinde, ağdaki diğer araçlara, saldırgan aracı ve o araç tarafından başlatılan saldırı türünü bildiren bir mesaj gönderilmektedir.

Wahab ve ekibi [51], kümeler arası iletişim ile saldırgan araçların tespitinde kullanılan adımların azaltılması amacıyla makine öğrenmesi tabanlı yeni bir saldırı tespit yöntemi önermişlerdir. QoS-OLSR protokolünde paket düşürme, yönlendirme gider deliği ve hizmet engelleme saldırılarına karşı uygulamalarını gerçekleştirmişlerdir. Saldırı tespiti, dört aşamada gerçekleştirilmiştir. Veri toplama aşamasında, küme lideri de dahil olmak üzere tüm küme üyeleri, kendilerine hizmet eden küme lideri tarafından seçilen ve kümeleri birbirine bağlayan araçlarının davranışını sürekli olarak izlemek ve analiz etmektedirler. Veri değiştirme aşamada, aynı kümede bulunan elemanlar izleme sonucu toplanan bilgileri paylaşmaktadır. Veri analizi aşamada, toplanan veriler analiz edilir ve küme lideri tarafından seçilen ve kümeleri birbirine bağlayan araçlar sınıflandırılır. Veri çoğaltma aşamasında; bu süreç küme

lideri tarafından seçilen ve kümeleri birbirine bağlayan araç ve küme lideri arasındadır. Küme liderleri, her araç grubu ile sonuçları paylaşmaktadır. Tespit edilen kötü amaçlı araçlar için, saldırı tespit yönteminin adımlarını tekrar etmekten doğan yükü azaltmak için birbirleri arasında sınıflandırma sonuçlarını değiştirmelerine izin vermektedir.

Sedjelmaci ve ekibi çalışmalarında [52], hiyerarşik mimariye sahip bir araçsal ağ için üç modülden oluşan bir saldırı tespit yöntemi önermektedir. Yerel saldırı tespit sistemi olarak adlandırılan birinci modül, tüm küme elemanlarının davranışlarını izlemeyi sağlamaktadır. Küresel saldırı tespit sistemi olan ikinci modül, küme liderlerinin davranışlarını izlemektedir. Küresel karar sistemi olan üçüncü modül ise yol kenarı birimleri seviyesinde çalıştığı için araçlardan gelen bilgilerin güvenilirliği üzerine çalışmaktadır. Ayrıca, bu sistem yol kenarı birimlerine bağlı bulunan araçların güven seviyelerini hesaplayarak, bu güven seviyelerini liste şeklinde tüm araçlara bildirir.

Alheeti ve ekibi [53], gri delik ve hız-telaş saldırılarını tespit edebilmek için anomali tabanlı bir saldırı tespit sistemi önermektedirler. Aynı yazarlar, başka bir çalışmalarında da [54], AODV protokolünde [55] kara delik saldırısını tespit etmeyi hedefleyen bir yaklaşım önermişlerdir. Önerilen yaklaşım, yapay sinir ağları ve bulanık veri mantığı yöntemlerini kullanmaktadır. İmza ve anomali tabanlı iki tespit sistemi bir arada kullanılmaktadır.

Yao ve ekibi çalışmalarında [56], araçsal tasarsız ağlar için GPSR yönlendirme protokolüne [57] karşı gerçekleştirilen kara delik ve seçici iletim saldırılarına karşı bir saldırı tespit sistemi geliştirmiştir. Ağda her aracın güven düzeyi bulunmaktadır. Yüksek düzeyde araçlardan gelen mesajlar daha güvenilir olarak ağdaki diğer araçlara rapor edilmektedir. Mesajların güven düzeyleri, mesajı gönderen aracın güven seviyeleriyle

orantılı olarak ağırlıklandırılmıştır. Veri merkezli bir güven modeli oluşturarak, verilerin güvenilirliği değerlendirilmiş ve bu değerlendirme sonucuna göre saldırı tespiti gerçekleştirilmiştir.

Leckie ve ekibi çalışmasında ise [58], dağıtık mimaride uygulanan anomali tabanlı bir saldırı tespit yöntemi geliştirmiştir. Hizmet engelleme ve gider deliği saldırılarına karşı üretilen bu saldırı tespit sistemi dinamik bir varlık merkezli güven modeli tabanlı olarak geliştirilmiştir. Bu saldırı tespit sistemi, eğitim ve test olmak üzere iki aşamadan oluşmaktadır. Eğitim aşamasında, ağdaki tüm verilerin toplanması sağlanmaktadır. Bu veriler arasında, saldırgan araçlardan gelen verilerin de olduğu varsayılmaktadır. Bu verilere göre ağ modeli oluşturulmaktadır. Test aşamasında ise, toplanan bu verilere dayanarak ağ trafiğini analiz etmektedir. Analiz sonucunda, eğitim aşamasında elde edilen ağ modeli ile eşleşme gerçekleştirmektedir. Eşleşmenin sağlanmadığı durumu, anormal veri olarak etiketleyip, saldırı olarak değerlendirmektedir.

Yapılan araştırmalar sonucu araçsal ağlarda yönlendirme için kullanılan birçok protokol, uygulanan saldırılar, bu saldırıları tespit etmek için kullanılan yöntemler ve kullanılan benzetim araçlarının özeti Tablo 2-1’de gösterilmiştir.

Tablo 2-1. Araçsal Tasarsız Ağlar ile ilgili Yapılan Çalışmalarda Kullanılan Protokoller ve Saldırı Türleri

STS Adı	Yönlendirme Protokolü	Saldırı Türü	Benzetim Ortamı	Saldırı Tespit Yöntemi
CEAP [51]	QoS-OLSR	Paket düşürme, Yönlendirme gider deliği, Hizmet engelleme	VanetMobi Sim	Anomali Tabanlı
AECFV [52]	-	Seçici iletim, Kara delik, Solucan deliği, Kimlik değiştirme	NS-3, SUMO	Anomali Tabanlı
Sahip Tabanlı STS[50]	WAVE	Yanlış bilgi, Kimlik değiştirme	OMNET++	İstatistiksel Tabanlı
Alheeti ve ekibi [53]	AODV	Gri delik, Hız – telaş	NS-2	Anomali Tabanlı
Yao ve ekibi [56]	GPSR	Kara delik, Seçici iletim		İmza Tabanlı
Alheeti ve ekibi [54]	AODV	Kara delik	NS-2, SUMO, MOVE	Karma Tabanlı
Leckie ve ekibi [58]	-	Hizmet engelleme, Aktif ve Pasif gider deliği		Anomali Tabanlı
Yu ve ekibi [49]	-	Kimlik değiştirme	NS2	Anomali Tabanlı

Tablodan da görüldüğü üzere, araçsal tasarsız ağlar için genellikle anomali tabanlı saldırı tespit sistemleri önerilmesine rağmen, bu çalışmalar arasında istatistiksel tabanlı çalışmaların sayısı oldukça azdır.

2.3.1. İstatistiksel Tabanlı Saldırı Tespit Yöntemleri

Bu tez çalışmasında yapılan literatür araştırmasında, kimlik değiştirme saldırısını tespit etmek için önerilen iki tane istatistiksel tabanlı saldırı tespiti sistemine rastlanmıştır. Yu ve ekibi çalışmalarında [49], kimlik değiştirme saldırısını tespit etmek için istatistiksel analizlerde sıklıkla kullanılan normal dağılım yöntemini kullanmışlardır. Ağda saldırı yokken araçlardan gelen konum bilgileri ve araçların birbirlerine olan uzaklık bilgileri toplanmıştır. Bu bilgiler, ağda bulunan bir saldırı veya kaza durumunda toplanan bilgiler ile kıyaslanmıştır. Araçların konum bilgileri ve komşu araçlara olan uzaklıkları bilindiği için, her araç için olmasını beklediğimiz konum bilgisi de elde edilebilmektedir. Ağda saldırgan olması durumunda, araçların olması beklenen konumları ve bulundukları konumları arasındaki fark alınarak ki-kare testi ile analiz gerçekleştirilmiştir. Normal dağılım için belirlenen kritik değer ile ki-kare değeri kıyaslanmış ve hipotezin reddedildiği yerde saldırı olduğu bilgisi verilmiştir. Ağda bir saldırı tespit edildiğinde, araçlar saldırının olduğu yolda ise rotalarını değiştirerek hareketlerine devam etmektedirler.

Zaidi ve ekibi [50] daha önceki çalışmalarında kullandıkları bir trafik modeli üzerinde [59] istatistiksel yöntemler kullanarak, yol kenarı birimi veya baz istasyonları gibi maliyetli altyapılara bağlı olmayan bir saldırı tespit sistemi önermişlerdir. Bu çalışmada ağ modellemesi olarak, akış ve yoğunluk standart parametrelerinin belirlenmesine imkan tanıyan Greenshield modeli kullanılmıştır. Önerdikleri trafik modellerinde, her araç çevresindeki trafiği, komşu araçlardan gelen mesajlara göre modellemektedir. Yine bu çalışmada da, araçların konumları ile ilgili bilgiler kullanılarak, saldırgan araçlardan gelen yanlış değerleri tespit etmek için t-testi kullanılmıştır. İlgili saldırı tespit sisteminin her araçta bulunduğu, ayrıca ilgili sistemin saldırıların oluşturduğu hasarı giderecek mekanizmaları içerdiği varsayılmıştır. Ağdaki araçlar, hızlarını,

hesaplanan ortalama akışı, ortalama yoğunluğu ve konum bilgilerini diğer araçlara göndermektedirler. Bu bilgiler, tüm komşu araçlardan toplanarak hesaplanmakta ve toplanan değerler arasında önemli bir fark olup olmadığı t testi ile kontrol edilmektedir. Bu değerler kullanılarak hesaplanan t değeri, kabul bölgesi içinde bir sonuç verirse, veriler kabul edilir ve hipotez reddedilir. Veriler reddedilirse, araç saldırgan olarak belirlenir ve gerçekleştirdiği saldırı, sahte bilgi saldırısı olarak sınıflandırılır. O andan itibaren, saldırgan araçtan gelen her değer reddedilir. Diğer araçlara, saldırgan aracı ve o araç tarafından başlatılan saldırı türünü bildiren bir mesaj gönderilir. Saldırı mesajlarını alan araçlar ağda rotalarını değiştirerek ilerlemeye devam ederler.

Literatürde radyo kaynak testi ve rastgele anahtar dağıtımı yöntemleri kullanılarak da kimlik değiştirme saldırısı tespit edilmektedir [60]. Konum ve kod doğrulaması yaparak kullanılan tespit yöntemleri de bulunmaktadır [32]. Ayrıca araçlar arasında haberleşme olduğu anda doğrulama ve gizlilik kullanılarak kimlik değiştirme saldırısına karşı tespit yöntemleri bulunmaktadır [61]. Grover ve ekibi de [62] iki aracın belli bir süre içinde aynı komşulara sahip olamayacağı varsayımıyla kimlik değiştirme saldırısı için saldırı tespit yaklaşımı önermişlerdir.

Yukarıda görüldüğü gibi, araçsal tasarsız ağlarda genellikle kimlik değiştirme saldırısı için istatistiksel tabanlı saldırı tespit sistemleri geliştirilmiştir. Ancak, diğer saldırı türleri için bu alanda saldırı tespiti çalışmalarına rastlanmamıştır. Bu çalışma kapsamında, literatürden farklı olarak, araçsal tasarsız ağlar için istatistiksel anomali tabanlı bir saldırı tespit yöntemi önerilmiş, bu saldırı tespit yöntemi iki farklı sahte bilgi saldırısı için uygulanmış ve benzetim ortamında farklı saldırgan oranları dikkate alınarak değerlendirmeler yapılmıştır.

3. İSTATİSTİKSEL TABANLI SALDIRI TESPİTİ

İstatistiksel tabanlı saldırı tespiti yöntemleri, anomali tabanlı saldırı tespit sistemleri altında değerlendirilmektedir [63]. Ağdaki normal trafiğin ve akışın bilgisine sahip olunan durumlarda uygulanır.

Literatürde, istatistiksel tabanlı saldırı tespiti üzerine birçok çalışma mevcuttur. Bu çalışmalarda, genellikle saldırı tespiti sonucunda elde edilen değerler temel istatistiksel yöntemleri kullanılarak yorumlanmış, fakat istatistiksel analizler doğrultusunda ağda saldırı olup olmadığı incelenmemiştir. Literatürde kablolu ağlar için önerilmiş birçok istatistiksel tabanlı saldırı tespit sistemi olmasına rağmen, bu tür yöntemlerin araçsal tasarsız ağlara uygulamaları yenidir. Bildiğimiz kadarıyla, bu tezde önerilen Pearson korelasyon katsayısı yöntemi de, araçsal tasarsız ağlarda saldırı tespiti için ilk defa kullanılmıştır. Bu bölümde, bu yöntemin detayları anlatılacaktır.

3.1. Yöntem

Araçsal tasarsız ağlarda hareketliliğin fazla olması nedeniyle ağ topolojisinin hızlı değişmesi, ağı saldırılara karşı savunmasız hale getirmekte ve ağdaki saldırgan araçların belirlenmesini zorlaştırmaktadır. Sabit bir yapıya sahip olmayan bu ağlara karşı yapılan saldırılar, can ve mal kaybına neden olabileceği için, bu saldırıların zamanında tespit edilmesi büyük önem arz etmektedir. Bu çalışmada, aşağıda ayrıntıları verilen Pearson korelasyon katsayısı kullanılarak araçsal tasarsız ağlarda istatistiksel tabanlı bir saldırı tespit yöntemi önerilmektedir.

Literatürde, Pearson korelasyon katsayısının araçsal tasarsız ağlarda uygulamaları vardır [64][65]. Gordon P.H. ve ekibi çalışmalarında [64], Pearson korelasyon katsayısı kullanarak, araçsal tasarsız ağlarda paket iletim oranı ve paket gecikmesi arasındaki ilişkileri incelemişlerdir. Ağ benzetimi için Ns-3 aracını kullanmışlardır. Bu çalışmada, Pearson korelasyon katsayısı sadece ağdaki paket iletimini iyileştirmek için kullanılmış, bir saldırı tespiti söz konusu değildir. Renda ve ekibi çalışmasında [65], 906 ve 176 km uzunluğundaki iki yol üzerinde, araçların paket iletim oranları ile araçlar arasındaki mesafeler arasındaki ilişkiyi incelemişlerdir. Pearson korelasyon katsayısı yöntemi ile, araçlar arası iletim mesafesi genelde kısa olduğu için, paket teslim oranı ile mesafe arasındaki ilişkiyi zayıf olarak bulmuştur. Görüldüğü üzere bu çalışmalar, Pearson korelasyon katsayısı yöntemini, ağdaki bazı ilişkileri tanımlamak için kullanmışlardır. Bildiğimiz kadarıyla, literatürde bu yöntemin araçsal tasarsız ağlarda saldırı tespiti için kullanılması için bir öneri yoktur. Bu tez çalışmasında, Pearson korelasyon katsayısı ile aşağıda ayrıntıları verilen iki değişken arasında ilişkinin saldırılı ortamda değişip değişmediğine bakarak, bir anomali tabanlı bir tespit sistemi önerilmiştir.

3.1.1. Pearson Korelasyon Katsayısı

Korelasyon, istatistikte rastgele iki değişken arasındaki ilişkinin doğrusal derecesini ve gücünü belirlemek için kullanılmaktadır. Korelasyon katsayısını hesaplamak için birden fazla yöntem bulunmaktadır. Bu yöntemlerin en bilinenlerinden birisi Pearson korelasyon katsayısıdır (r).

$$r = \frac{\sum x_i y_i - \frac{\sum x_i \sum y_i}{n}}{\sqrt{(\sum x_i^2 - \frac{(\sum x_i)^2}{n})} \sqrt{(\sum y_i^2 - \frac{(\sum y_i)^2}{n})}}$$

Yukarıdaki formülde, X ve Y, ilgili değişkenlerin değerlerini, n ise gözlem sayısını ifade etmektedir. Pearson korelasyon katsayısı (r), iki değişkenin kovaryansının, yine bu değişkenlerin standart sapmalarının çarpımına bölünmesiyle elde edilir.

Pearson korelasyon katsayısı, normal dağılım gösteren iki sayısal değişken arasında doğrusal bir ilişki olup olmadığını, bu ilişkinin yönünü belirlemek ve derecesi ölçmek için kullanılan bir istatistiksel yöntemdir. İki değişken arasındaki ilişkinin anlam düzeyini ve güvenilirliğini göstermektedir. Bu ilişki pozitif veya negatif yönde eğilim gösterebilmektedir [66]. Pozitif korelasyon, bir değişkenin değerinin artması/azalması ile diğer değişkenin de değerinin arttığını/azaldığını göstermektedir. Negatif korelasyon, bir değişkenin değerinin artması/azalması ile diğer değişkenin tam tersi yönde değişim gösterdiğini belirtmektedir.

Pearson korelasyon katsayısı, $-1 \leq r \leq 1$ aralığında değer almaktadır. r değeri -1'e doğru gittikçe değişkenler arasındaki ilişki azalmakta, +1'e doğru gittikçe artış göstermektedir. Pearson korelasyon katsayısı değer aralıkları, derece ve yönleri ile Tablo 3-1'de listelenmiştir.

Tablo 3-1. Pearson Korelasyon Katsayısı Değerleri

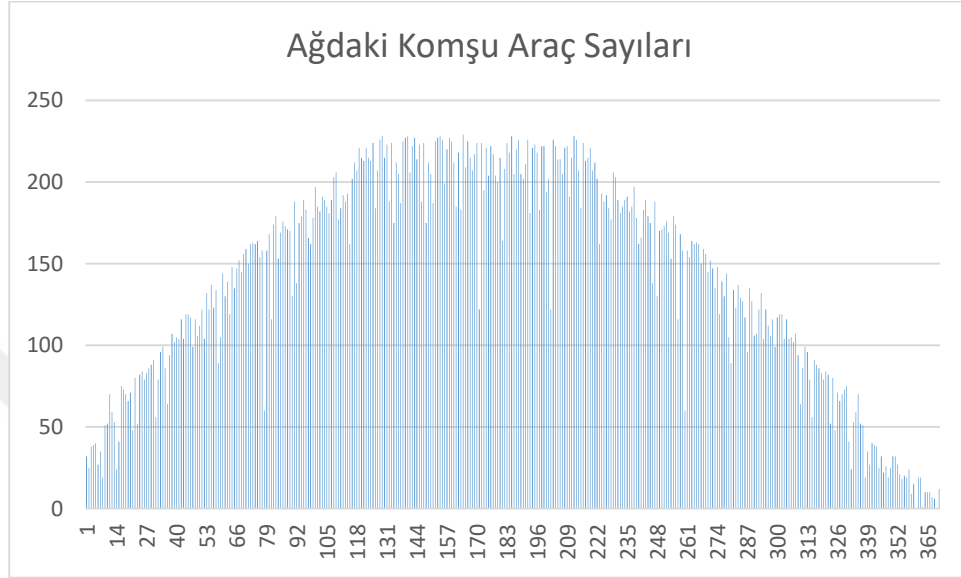
R	İlişkinin derecesi	İlişkinin Yönü
(-0,90) – (-1,00)	Çok Yüksek	Negatif
(-0,70) – (-0,89)	Yüksek	
(-0,50) – (-0,69)	Orta	
(-0,49) – (-0,26)	Zayıf	
(-0,25) - 0	Çok Zayıf	
0 – 0,25	Çok Zayıf	Pozitif
0,26 – 0,49	Zayıf	
0,50 – 0,69	Orta	
0,70 – 0,89	Yüksek	
0,90 – 1,00	Çok Yüksek	

3.1.2. Pearson Korelasyon Katsayısının Saldırı Tespitine Uygulanması

Pearson korelasyon katsayısı (r), iki değişken arasındaki ilişkinin yönünü ve anlam düzeyini göstermektedir. Bu ilişki pozitif veya negatif yönde değişim gösterebilmektedir. Bu tez çalışmasında, uygulanan iki farklı sahte bilgi saldırısının tespiti için kritik görülen iki değişken belirlenmiştir: düğümlerin komşu sayısı ve bu komşuların kazaya olan uzaklıkları. Saldırı olmayan ortamda, bu iki değişken arasındaki ilişkinin yönü referans değer olarak kabul edilmektedir. Eğer, bu referans değerinin zıt yönünde bir değer elde edilirse, ağda bir anomali olduğu kabul edilmektedir.

Komşu sayısı ile komşu araçların kazaya olan uzaklıkları arasındaki Pearson katsayısı değerini bulmak için, 370 aracın olduğu bir ağ benzetimi yapılmış ve bu araçlar arasındaki iletişimler incelenmiştir. Bu inceleme sonucunda her araç için komşu araç sayısında farklılıklar ortaya çıkarılmıştır. Şekil 3-1’de görüldüğü gibi, araçların her saniyede iletişime

geçtikleri komşu araç sayısının normal dağılım gösterdiği tespit edilmiştir. Ayrıca her araçtan toplanan, kazaya olan konum farklılıkları da incelenmiş ve bu değerlerin de normal dağılıma uygunluk gösterdiği görülmüştür.



Şekil 3-1. Komşu Araç Sayılarının Normal Dağılım Grafiği

Ağda kazanın var olduğu ancak saldırı olmayan ortamda normal dağılım gösteren bu iki değişken arasındaki ilişki incelendiğinde, Pearson korelasyon değeri -0.291 olarak ölçülmüştür. Bu sonuca göre komşu sayıları ve bu komşuların kazalara olan uzaklıkları arasında negatif yönlü, fakat zayıf bir ilişki bulunmaktadır. Bu tez çalışmasında, bu ilişkinin, ağda sahte bilgi saldırısı olması durumunda korunup korunmadığı incelenerek, iki farklı yöntem önerilmiştir. Buradaki temel varsayım, sahte bilgi saldırısı sonucu, saldırgan tarafından kazanın konumu hakkındaki gönderilen yanlış bilgiler, komşu sayısı ile komşuların kazaya olan uzaklıkları arasındaki ilişkiyi etkileyecektir. Özellikle, kaza olması durumunda araçların yer değiştirmesi ile bu değişimin daha da belirgin olacağı düşünülmektedir. İleriki bölümlerde, bu tez çalışmasında önerilen kümülatif ve çoğunluk tabanlı Pearson analizi yöntemleri detayları ile açıklanmaktadır.

3.1.2.1. Kümülatif Tabanlı Pearson Analizi

Uyguladığımız istatistiksel tabanlı saldırı tespit yöntemlerinden birisi, kümülatif tabanlı Pearson analizi olarak adlandırılmaktadır. Bu yöntemde, öncelikle kazanın olduğu, fakat saldırısız ağlarda, komşu araç sayısı ile bu komşu araçların kazaya olan uzaklık bilgilerinin ortalaması arasındaki ilişkinin yönü tespit edilmiştir. Bu yöntemdeki temel varsayım, yakın çevremizde olan komşu araçlar ile kazaya olan uzaklığımızı doğrulayabileceğimizdir. Yapılan benzetimler sonucu, bu iki değişken arasındaki ilişkinin zayıf ve negatif yönde olduğu görülmüştür. Saldırı olan ağlarda, her araç için bu değişkenlerin yönü hesaplanmış ve negatif zayıf yönde olan bu ilişki ile kıyaslanmıştır.

Kümülatif tabanlı Pearson analizi yönteminde, her aracın kendi başına saldırı tespiti yaptığı varsayılmıştır. Dolayısıyla her araç, bir kaza olması durumunda, komşu araçlarından onların kazaya uzaklıklarını toplamakta ve kazaya olan ortalama uzaklık değerini hesaplamaktadır. Saldırı olmayan ortamda, her araç, komşu sayısı ile komşularının kazaya olan ortalama uzaklıkları arasındaki ilişkiyi bilmektedir. Saldırı olan ortamda, bu değişkenler arasındaki Pearson korelasyon katsayısının yönü değişirse ağdaki anomali saldırı olarak ele alınmaktadır. Tablo 3-2’de önerilen kümülatif tabanlı saldırı tespiti algoritmasının temel adımları gösterilmiştir.

Tablo 3-2. Kümülatif Tabanlı Saldırı Tespit Algoritmasının Temel Adımları

```
for Benzetim Sonuna Kadar Her 1 Saniyede do
    Komşulardan Gelen Kaza Mesajlarını Kaydet
    Komşu Araç Sayısını (Değişken 1) Kaydet
    Her Aracın Kazaya Olan Uzaklığın (Değişken 2) Ortalamalarını Kaydet
    İki değişken Arasındaki Pearson Korelasyon Katsayısını Hesapla
    Pearson Korelasyon Katsayısının Yönünü Belirle
    if Pearson Korelasyon Katsayısının Yönü != Saldırısız Ortamdaki Pearson
    Korelasyon Katsayısının Yönü then
        Saldırı Olduğunu Rapor Et
    end if
end for
```

3.1.2.2. Çoğunluk Tabanlı Pearson Analizi

Kullanılan diğer yöntem ise çoğunluk tabanlı Pearson analizi olarak adlandırılmaktadır. Bu yöntem, dağıtık ve işbirlikçi bir mimariye dayanmaktadır. Yine kazaların olduğu, fakat saldırıların olmadığı ağlarda, komşu araç sayısı ile bu araçlardan gelen mesajlarda iletilen bu araçların kazaya uzaklıkları arasındaki ilişkinin yönü, Pearson korelasyon katsayısı yöntemi ile belirlenmiştir. Saldırlı ortamda, her araç bu ilişkinin yönünü hesaplamakta ve diğer komşu düğümlere göndermektedir. Komşu düğümlerden gelen ilişkinin yönü, çoğunluk tarafından saldırısız ortamdaki temel alınan ilişki yönünden farklı ise, ağdaki kaza konum bilgilerinin saldırgan tarafından değiştirildiği varsayılır ve saldırı olarak etiketlenir.

Kümülatif tabanlı Pearson analizinde, her araç tekil olarak saldırı tespiti yaparken, komşularının kazaya olan uzaklıklarının ortalama değeri üzerinden Pearson korelasyon katsayısını hesaplamaktadır. Fakat çoğunluk tabanlı yöntemde, her araç kendi katsayısını hesaplayarak, komşu düğümlere ayrıca bu bilgiyi göndermektedir.

Bu nedenle, hem hesaplama, hem de iletişim açısından daha maliyetli bir yöntemdir. Tablo 3-3’de önerilen çoğunluk tabanlı saldırı tespiti algoritmasının temel adımları verilmiştir.

Tablo 3-3. Çoğunluk Tabanlı Saldırı Tespit Algoritmasının Temel Adımları

```
for Benzetim Sonuna Kadar Her 1 Saniyede do
    Saldırı Tespit Eden Komşu Sayısını sıfırla
    for Tüm Komşular do
        Komşulardan Gelen Kaza Mesajlarını Kaydet
        if Mesajlardaki Pearson Korelasyon Katsayısının Yönü != Saldırısız Ortamdaki
        Pearson Korelasyon Katsayısının Yönü then
            Saldırı Tespit Eden Komşu Sayısı arttır
        end if
    end for
    if Saldırı Tespit Eden Komşu Sayısı >= (Komşu Araç Sayısı / 2) then
        Saldırı Olduğunu Rapor Et
    end if
end for
```

3.2. Benzetim Ortamı

Araçsal tasarsız ağlar, gün geçtikçe yaygınlaşmaktadır. Bu ağlar üzerindeki standartlaşma çalışmaları hala devam etmektedir. Bu nedenlerden dolayı araçsal tasarsız ağlara ilişkin büyük ölçekli uygulamaların gerçek ortamda denenmesi zordur. Dolayısıyla, bu tez çalışmasında, bu ağlar için önerilen saldırı tespiti yöntemleri benzetim ortamında hazırlanan ağlarda değerlendirilmiştir. Benzetim ortamında gerçek trafik bilgilerinin kullanılması mümkün olmakta, bu da saldırılar ve önerilen tespit sistemlerinin ağ üzerindeki etkilerinin gerçekçi bir şekilde değerlendirilmesine izin vermektedir.

Bu tez çalışmasında, literatürde varolan ağ benzetim araçlarının kullanım oranları incelenmiş ve bu inceleme sonucunda Ns-3 aracı tercih edilmiştir.

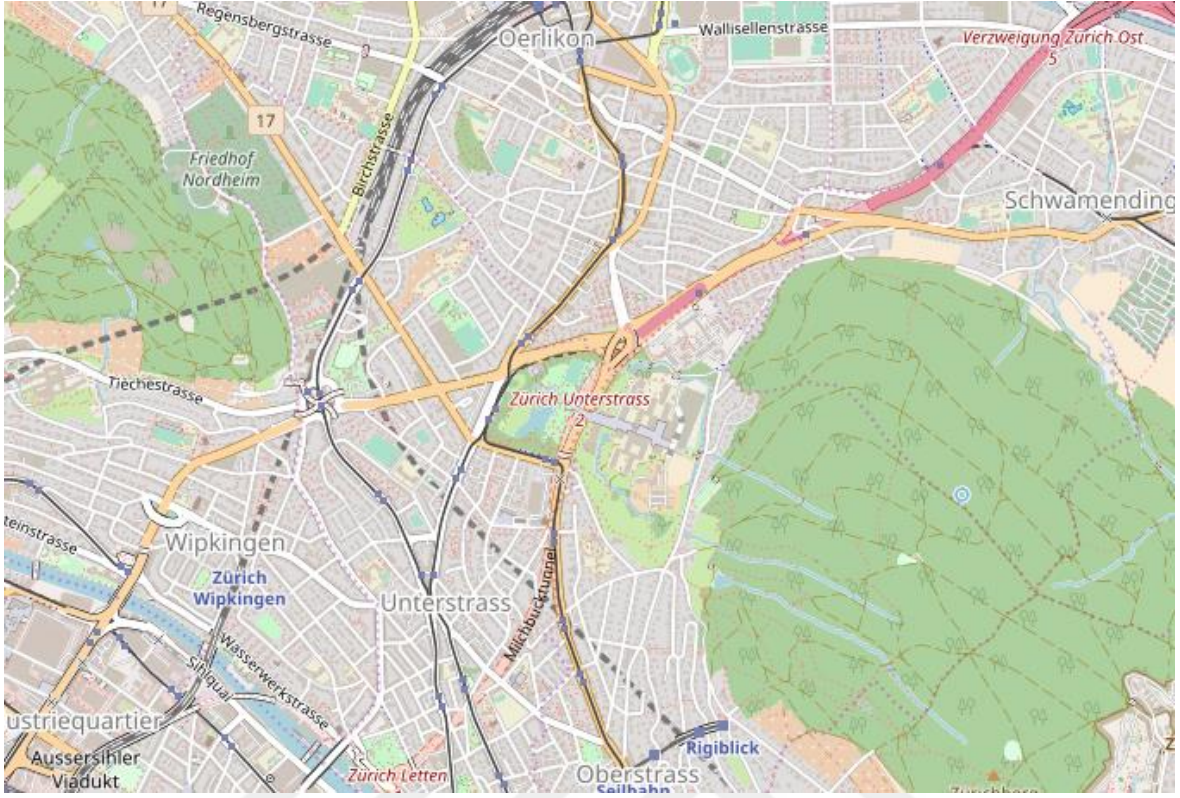
Bu tez çalışmasında, lüteratürde varolan ağ benzetim araçlarının kullanım oranları incelenmiş ve bu inceleme sonucunda Ns-3 aracı tercih edilmiştir. Ns-3 ve diğer versiyonlarının tercih edilme nedenlerinden en önemlisi; açık kaynak kodlu bir benzetim aracı olması ve bu araç ile ilgili bilgi paylaşımının yüksek olmasıdır. Bu benzetim aracını kullanan ve gelişmesi için katkı sağlayan birçok kullanıcısı bulunmaktadır [67]. Günümüzde tasarımı devam eden, açık kaynak kodlu bir ağ benzetim aracı olan Ns-3, kablolu, kablosuz, hareketli tasarsız ağlar vb. gibi birçok türde ağın modellemesinin yapılmasına izin vermektedir. Bu araç, Linux işletim sistemi üzerinde çalışmaktadır. Cygwin programı ile Windows tabanlı sistemlerde de kullanıma olanak sağlamaktadır. Bu araç, C++ ve Python dilleri kullanılarak geliştirilmiştir [68].

Ns-3.26 [69] kullanarak, Zürih 6. Bölgesi Unterstrass haritası üzerinde gerçekleştirdiğimiz ağ benzetimlerine ilişkin parametreler Tablo 3-4. Benzetim Parametreleri’te gösterilmiştir.

Tablo 3-4. Benzetim Parametreleri

Simulasyon	NS-3.26
Simulasyon süresi	300 Saniye
Harita	Unterstrass / Zürih / İsviçre
Araç Sayısı	370
Topoloji	4.6 km x 3.0 km
Protokol	-
Veri Paketi Gönderim Aralığı	1 Saniye

Benzetimlerin temel aldığı haritanın görüntüsü Şekil 3-2’de gösterilmiştir. Her benzetimde, bu haritada rasgele bir kaza yeri belirlenmiş ve bu kaza yerine 100 metreden yakın olan araçların bu kaza ile ilgili mesaj almaları üzerine bir senaryo kurulmuştur.



Şekil 3-2. Unterstrass/Zurih/İsviçre

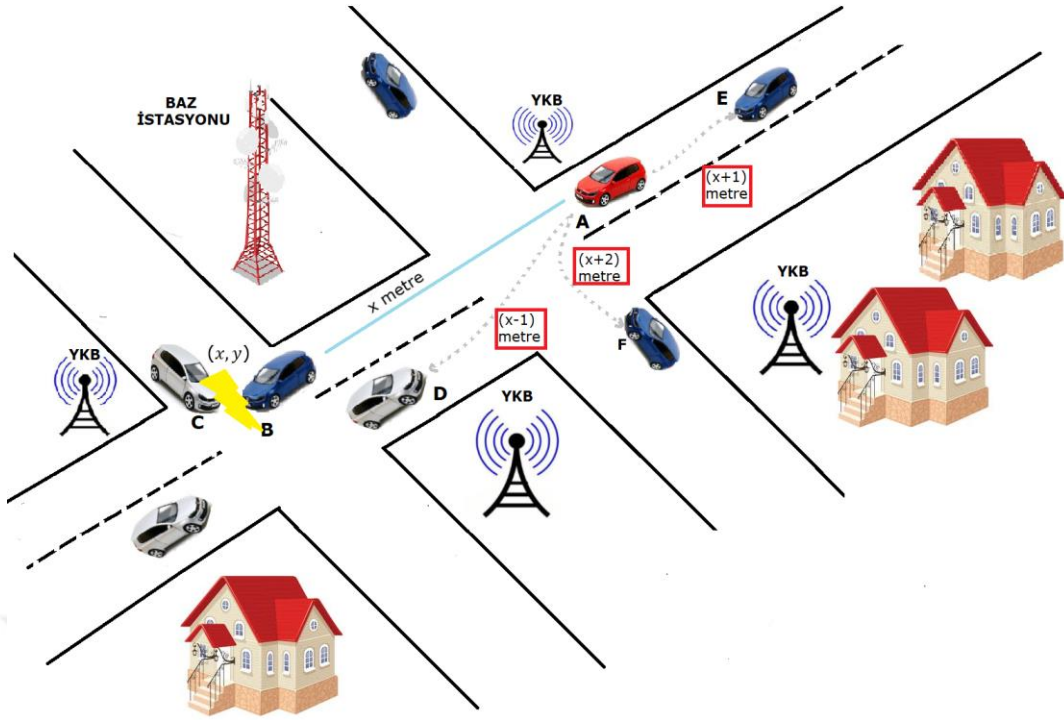
3.1. Uygulanan Saldırıların Analizi

Uygulanan saldırılar, ağda tahribata sebep olmakta ve ağı kullanılamaz hale getirmeyi amaçlamaktadırlar. Bu bölümde gerçekleştirdiğimiz saldırılar açıklanmıştır.

3.1.1. Sahte Bilgi Saldırısı – Kaza Uzaklığı Değiştirme

Sahte bilgi saldırısında, saldırgan araç ağda bulunan diğer araçlara gerçek olmayan bilgi veya mesajlar göndererek, ağda yanlış yönlendirmelere sebep olmaktadır. Bu saldırıların gerçek hayatta görülmesi, trafik durumunun yanlış gönderilmesi, var olan bir olayın olmamış gibi gösterilmesi veya olmamış bir olayın olmuş gibi gösterilmesi şeklindedir.

Sahte bilgi saldırısında saldırgan araç, ağdaki diğer araçlara yanlış veya eksik bilgi göndermektedir. Çalışmamızda araçlar birbirleri ile ağdaki kaza bilgileri ve bu kazaya olan uzaklıklarını paylaşmaktadır. Saldırgan araç, gelen mesajlardaki kazaya olan ortalama uzaklık bilgisi üzerinde değişiklikler yaparak araçların kazaya doğru gitmesine ve ağ trafiğinde yoğunluğa sebep olmaktadır. Saldırgan araç, kazaya olan uzaklığı rastgele olarak değiştirmektedir. Saldırgan araç, olan kazayı daha uzak gösterdiğinde, araçları kazaya doğru gitmesine izin vermektedir. Kazaya olan mesafeyi daha yakın göstermesi durumunda ise, araçların daha erken yol değiştirme planlaması yapmasına sebep olmaktadır. Ancak, literatürde kabul gören bir uygulama protokolü olmadığından, gelen mesajlara göre araçların yol değiştirmesi benzetim ortamında bulunmamaktadır. Senaryonun bu şekilde değiştirilmesi ile, komşu sayısı ile uzaklık bilgisi arasında daha büyük bir değişim olması ve bu değişikliğin yöntemimizi olumlu etkilemesi beklenmektedir. Bu nedenle, araçsal tasarsız ağlarda standart protokollerin belirlenmesi ile önerilen yöntemin tekrar değerlendirilmesi, ileriki çalışmalara bırakılmıştır.



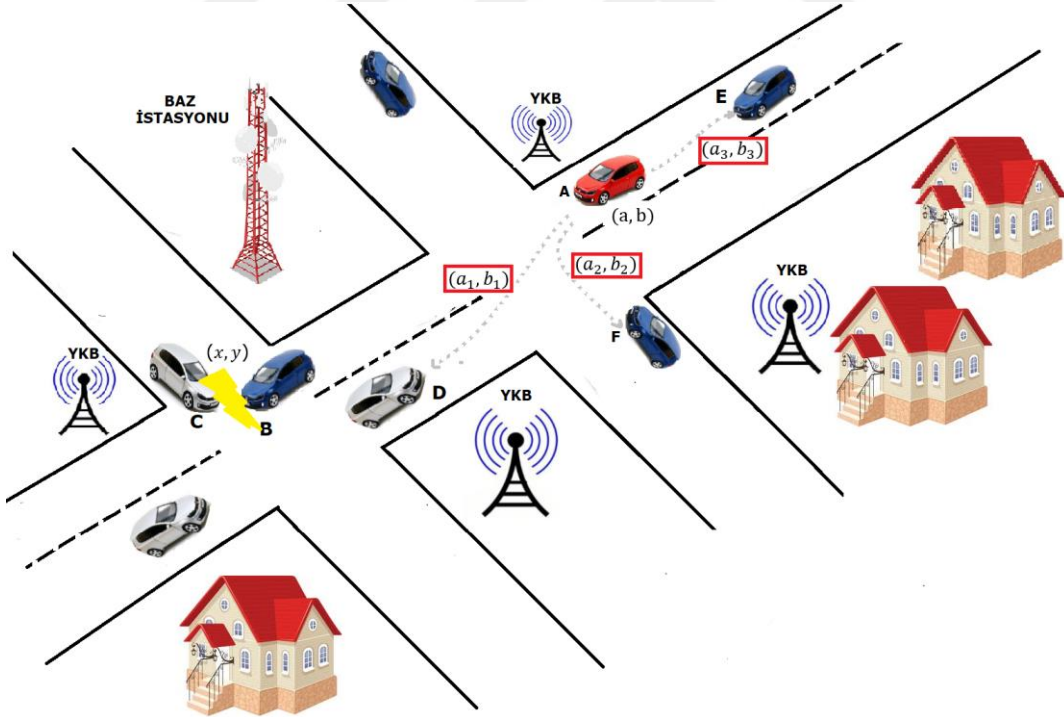
Şekil 3-3. Sahte Bilgi Saldırısı – Kaza Uzaklığı Değiştirme

Şekil 3-3'te bu saldırı için bir örnek gösterilmiştir. Saldırgan A aracı, komşu düğümlerine kazaya olan uzaklığını farklı göndermektedir.

Bu çalışmada ağda farklı oranlarda saldırgan araç olduğu varsayılmıştır. Ağdaki tüm araç sayısının, %1, %5 ve %10'u kadarının saldırgan olması durumu incelenmiştir. Her durum için, benzetim ortamı, farklı saldırgan ve kaza yeri seçimleri ile onar kez çalıştırılmıştır. Bu saldırganlar, her benzetimde rastgele seçilmiştir. Aynı şekilde, kaza yeri de rastgele seçilmekte, fakat etkisinin olabilmesi için trafiğin yoğun olduğu bölgelere öncelik verilerek yerleştirilmiştir. Saldırı, kaza mesajları saldırgan araca geldiğinde gerçekleşmektedir. Kaza bildirimini yapan paketler haricinde, araçlar arasındaki diğer iletişim paketleri değişikliğe uğramamaktadır.

3.1.2. Sahte Bilgi Saldırısı – Saldırgan Konumu Değiştirme

Sahte bilgi saldırısında saldırı araç, ağdaki diğer araçlara yanlış veya eksik bilgi göndermektedir. Çalışmamızda araçlar birbirlerine ağdaki kaza bilgileri ve bu kazaya olan uzaklıklarını iletmektedir. Saldırgan araç, komşu araçlara gönderdiği mesajda kendi konum bilgisinde değişiklikler yaparak araçların kazaya olan uzaklıklarını hatalı olarak göndermektedir. Saldırgan araç, kendi konumunu rastgele olarak değiştirmekte ve kendini farklı yerlerde gibi diğer araçlara göstermektedir. Bu çalışmada, her benzetimde farklı oranlarda saldırı araçlar ağda iletişimi yanlış yönlendirmektedir. Bu saldırı araçlar her benzetimde rastgele seçilmiştir. Kaza bilgisi içeren paketler, saldırı araca geldiğinde saldırılar gerçekleşmektedir.



Şekil 3-4. Sahte Bilgi Saldırısı - Saldırgan Konumunu Değiştirme

Şekil 3-4'te görüldüğü üzere saldırgan A aracı, komşu düğümlerine kendi konumunu farklı göstermektedir. Saldırgan aracın gönderdiği mesaj içeriğinde kazaya olan uzaklığı da bulunmaktadır, dolayısıyla aracın kazaya uzaklığı da değişmektedir.

3.2. Değerlendirme Metrikleri

Bu çalışmada, Unterstrass – Zürih haritası kullanılarak, yönlendirme protokolünden bağımsız iki farklı sahte bilgi saldırısı gerçekleştirilmiştir. Her saldırı, 370 aracın olduğu bir trafikte, farklı oranlarda saldırgan (%1, %5, %10) ile denenmiştir. 300 saniye süren ağ benzetimlerinde, bir milyona yakın trafik verisi elde edilmiş, veriler Oracle veri tabanında saklanmıştır. Bu veriler üzerinde analiz, Excel ve Spss [70] araçları ile gerçekleştirilmiştir.

Bu çalışmada, önerilen saldırı tespit sistemlerinin başarımını değerlendirmek için literatürdeki iki temel değerlendirme metriği kullanılmıştır: doğru pozitif oranı (tespit oranı) ve yanlış pozitif oranı.

3.2.1. Tespit Oranı (TO)

Tespit oranı, benzetim ortamında doğru olarak tespit edilen saldırıların, tüm saldırılara oranı olarak tanımlanmaktadır [3]. Bu değer yüksek olması istenmektedir.

$$TO = \frac{\text{Saldırının doğru tespit edildiği durumlar}}{\text{Saldırının olduğu tüm durumlar}}$$

3.2.2. Yanlış Pozitif Oranı (YPO)

Yanlış pozitif oranı; saldırının olmadığı durumlarda saldırı olarak tespit edilen durumların, saldırının olmadığı tüm durumlara oranıdır.

$$YPO = \frac{\text{Yanlış olarak saldırının tespit edildiği durumlar}}{\text{Saldırısız tüm durumlar}}$$

Yanlış tespit oranının düşük olması, tespit oranının büyük olması kadar önemlidir. Çok sayıda yanlış tespit oranı, bu yanlış alarmların değerlendirilmesi için zaman kaybına neden olur ve saldırı tespit sistemlerinin güvenilirliğini azaltmaktadır [3]

4. ÖNERİLEN SALDIRI TESPİT SİSTEMİNİN DEĞERLENDİRİLMESİ

Bu tez çalışmasında, araçsal tasarsız ağlar için istatistiksel anomali tabanlı bir saldırı tespit yöntemi önerilmiştir. Kaza uzaklığını değiştirme ve saldırgan konumunu değiştirme olmak üzere iki farklı saldırı türü için benzetim ortamında uygulamalar yapılmıştır. Benzetim ortamında farklı saldırgan oranları dikkate alınarak değerlendirmeler yapılmıştır. Elde edilen sonuçlar saldırıların tespit oranı ve yanlış pozitif oranı ile değerlendirilmiş ve bu bölümde elde edilen bu sonuçlar incelenmiştir.

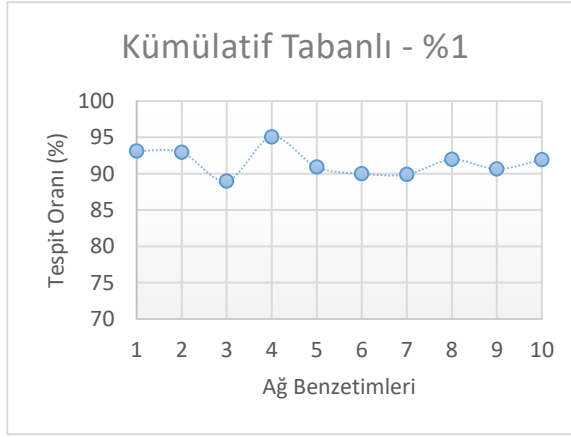
4.1. Sahte Bilgi – Kaza Uzaklığı Değiştirme Saldırısının Tespiti

Araçsal tasarsız ağlarda uyguladığımız kaza uzaklığını değiştirme saldırısı, Zürih kentinde Tablo 3-4'te verilen benzetim parametrelerine uygun olarak gerçekleştirilmiştir. Ağda farklı oranlarda saldırgan araç olduğu varsayılmıştır. Bu saldırganlar, her benzetimde rastgele seçilmiştir. Ağdaki tüm araç sayısının, %1, %5 ve %10'u kadarının saldırgan olması durumu incelenmiştir. Her durum için, on farklı benzetim ortamı oluşturulmuştur. Her benzetimde, saldırganın kimliği ve kaza yeri değişmekte, bu parametreler rastgele seçilmektedir. Kümülatif tabanlı Pearson analizi ve çoğunluk tabanlı Pearson analizi yöntemlerinin başarımları, bu benzetim ortamları kullanılarak değerlendirilmiştir. Dolayısıyla, her yöntemin bu saldırı türünü tespit etmesindeki başarımını değerlendirmek için, toplam 30 farklı benzetim oranı kullanılmıştır.

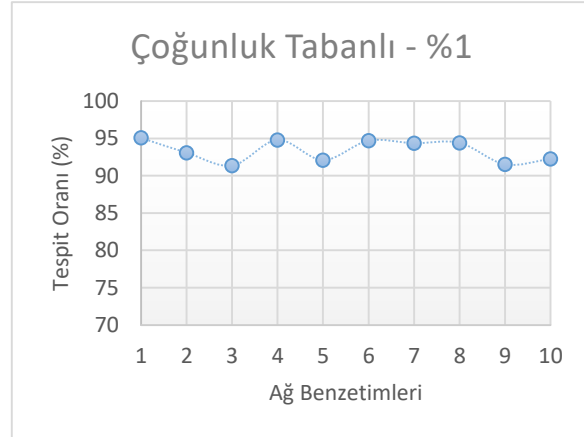
Kümülatif tabanlı Pearson analizi yöntemi ile kaza uzaklığı değiştirme tabanlı sahte bilgi saldırısının tespit oranları Şekil 4-1, Şekil 4-3 ve Şekil 4-5'te gösterilmiştir. Şekilde görüldüğü ve beklendiği üzere, ağdaki saldırgan oranı arttıkça, saldırının tespit oranında düşüş gözlenmektedir.

Çoğunluk tabanlı Pearson analizi yöntemi ile ilgili sahte bilgi saldırısının tespit oranları Şekil 4-2, Şekil 4-4 ve Şekil 4-6’da gösterilmiştir. Ağıdaki saldırgan oranı arttıkça, saldırının tespit oranında yine düşüş gözlenmektedir.

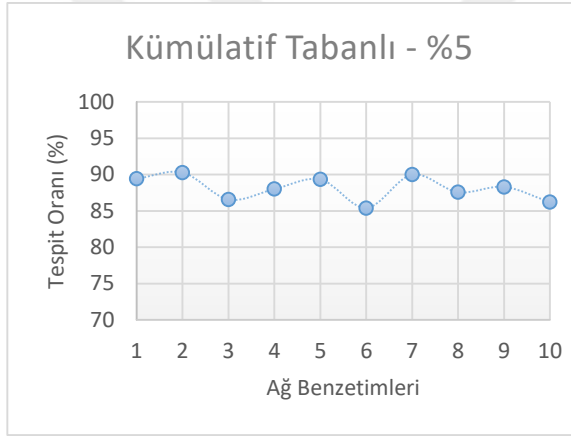




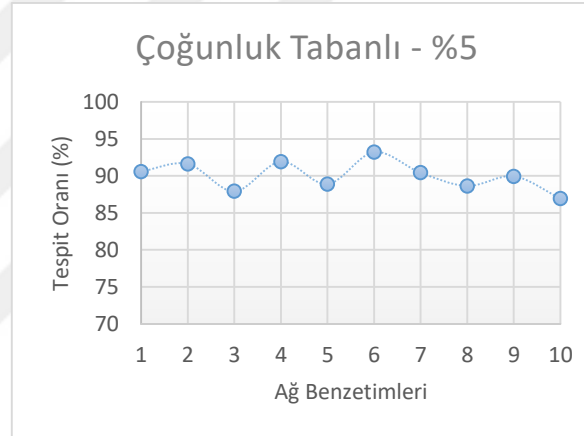
Şekil 4-1. Ağda %1 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



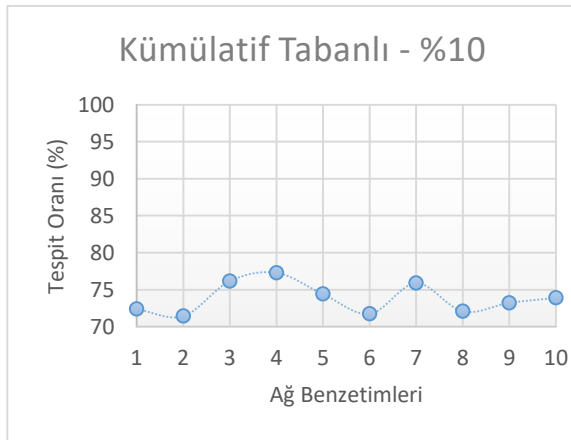
Şekil 4-2. Ağda %1 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



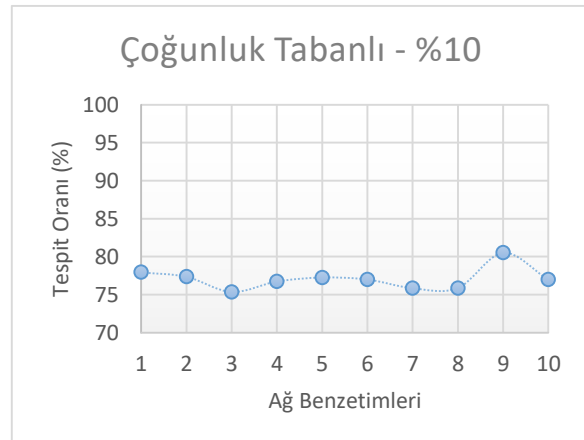
Şekil 4-3. Ağda %5 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



Şekil 4-4. Ağda %5 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı

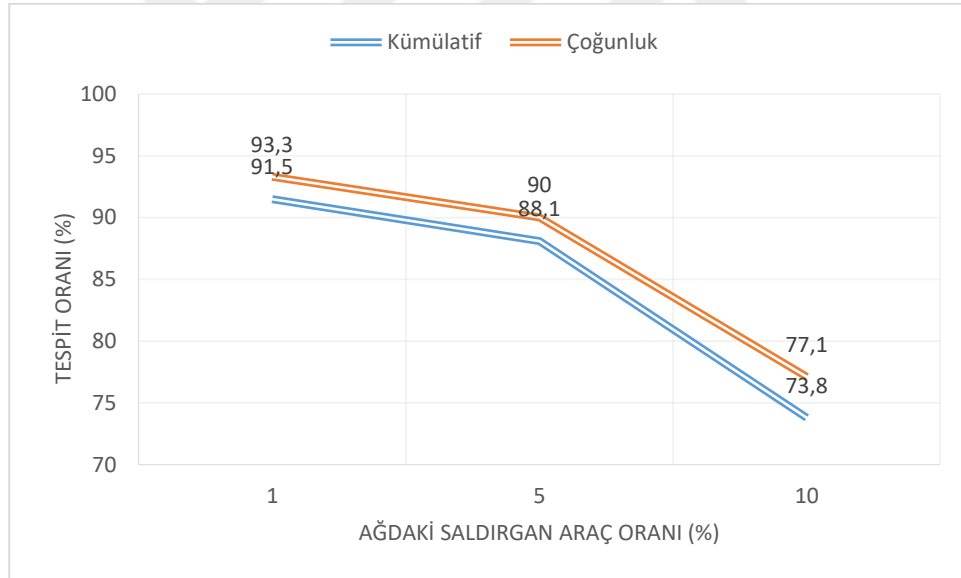


Şekil 4-5. Ağda %10 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı

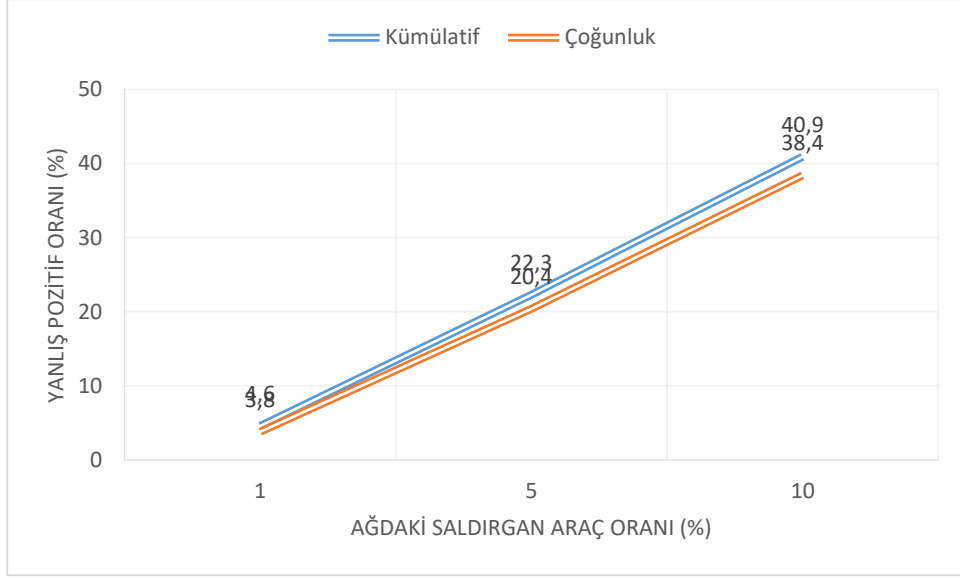


Şekil 4-6. Ağda %10 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı

Bu saldırı, ağdaki araçların %1'inin saldırgan olduğu durumda, kümülatif tabanlı Pearson analizi yöntemi ile ortalama %91.5 oranında tespit edilirken, çoğunluk tabanlı Pearson analizi yöntemi ile ortalama %93.3 oranında tespit edilmektedir. Saldırgan araç oranı ağdaki tüm araçların %5'i olduğunda, tespit oranı kümülatif tabanlı Pearson analizi yöntemi için %88.1, çoğunluk tabanlı Pearson analizi yöntemi için ise %90 olarak hesaplanmıştır. Ağdaki saldırgan araç oranı, 370 aracın %10'u olarak ayarlanıp benzetim ortamında kümülatif tabanlı saldırı tespit yöntemi uygulandığında ise tespit oranı ortalama %73.8 iken çoğunluk tabanlı Pearson analizi yönteminde ortalama %77.1 olarak hesaplanmıştır (Şekil 4-7).



Şekil 4-7. Kaza Uzaklığı Değiştirme Saldırı için Ortalama Tespit Oranları

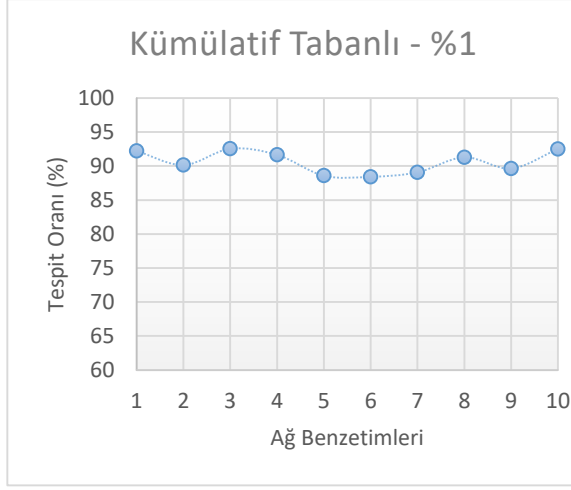


Şekil 4-8. Sahte Bilgi - Kaza Uzaklığı Değiştirme Saldırısı için Yanlış Pozitif Oranları

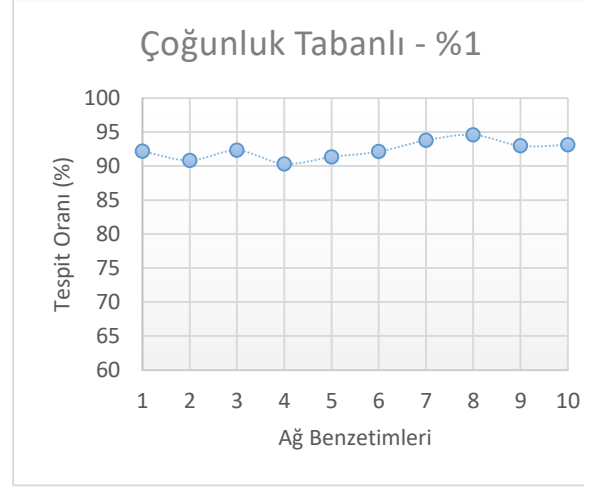
Şekil 4-8’de bu saldırıların tespiti için önerilen saldırı tespit yöntemlerinin, yanlış pozitif oranları gösterilmiştir. Ağdaki araçların %1’inin saldırgan olduğu durumda, kümülatif tabanlı saldırı tespit yönteminin yanlış pozitif oranı ortalama % 4.6, çoğunluk tabanlı saldırı tespit yönteminin ise %3.8 olarak hesaplanmıştır. Ağdaki saldırgan oranı artış gösterdiğinde, yanlış pozitif oranı da yükselmektedir. Bu şekile göre, çoğunluk tabanlı Pearson analizi yönteminin, kümülatif tabanlı Pearson analiz yöntemine kıyasla, saldırı olmayan durumları, saldırı olan durumlardan biraz daha iyi ayırdettiği görülmektedir.

4.2. Sahte Bilgi – Saldırgan Konumu Deęiřtirme Saldırısının Tespiti

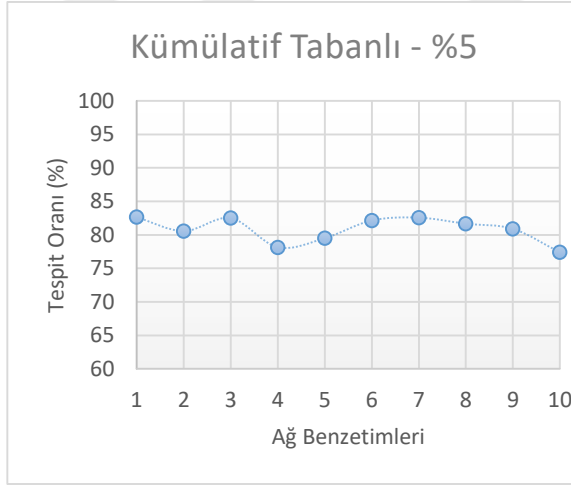
Saldırgan konumunu deęiřtirme sahte bilgi saldırısı, Zrih kentinde Tablo 3-4'te verilen benzetim parametrelerine uygun olarak gerekleřtirilmiřtir. Aęda farklı oranlarda saldırgan ara olduęu varsayılmıřtır. Bu saldırganlar, her benzetimde rastgele seilmiřtir. Aędaki tm ara sayısının, %1, %5 ve %10'u kadarının saldırgan olması durumu incelenmiřtir. Bu saldırı iin tm ara sayısının, %1, %5 ve %10'u kadarının saldırgan ara olması senaryoları, iki farklı yntem iin toplam 60 benzetim yapılarak deęerlendirilmiřtir.



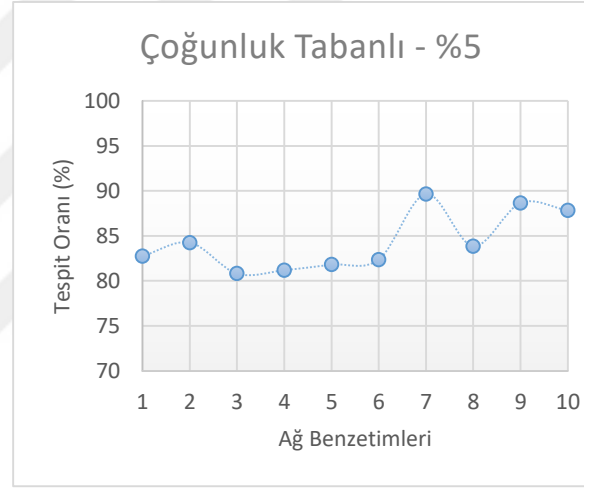
Şekil 4-9. Ağda %1 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



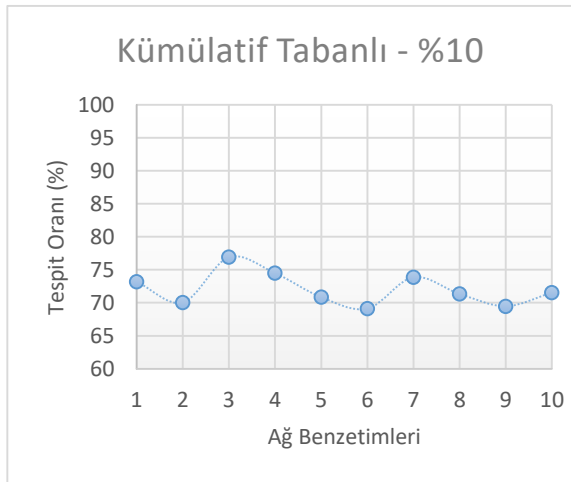
Şekil 4-10. Ağda %1 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



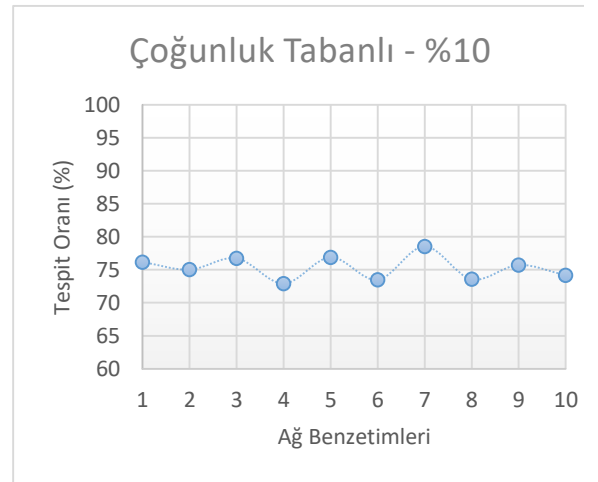
Şekil 4-11. Ağda %5 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



Şekil 4-12. Ağda %5 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



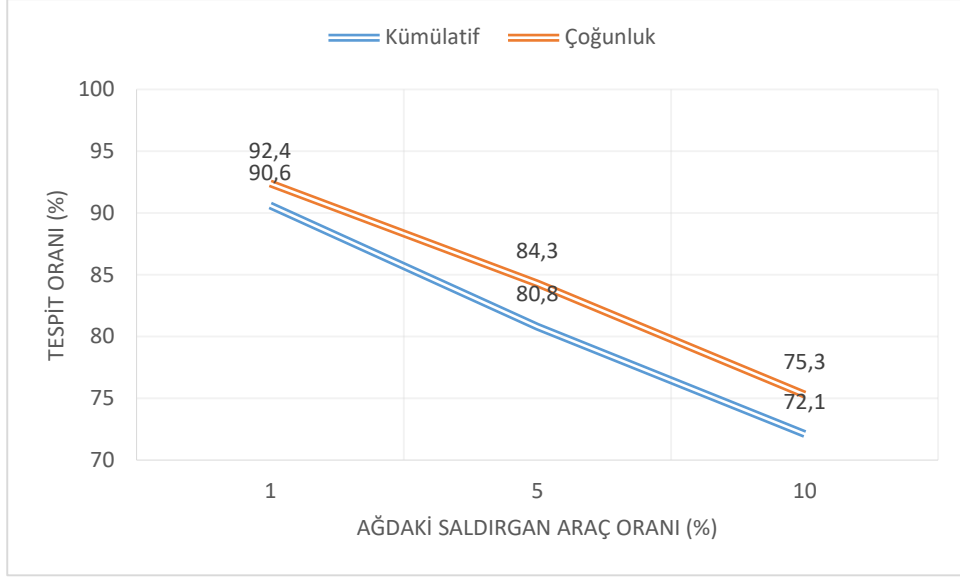
Şekil 4-13. Ağda %10 Oranında Saldırgan Olduğunda, Küümülatif Tabanlı Saldırı Tespit Yönteminin Tespit Oranı



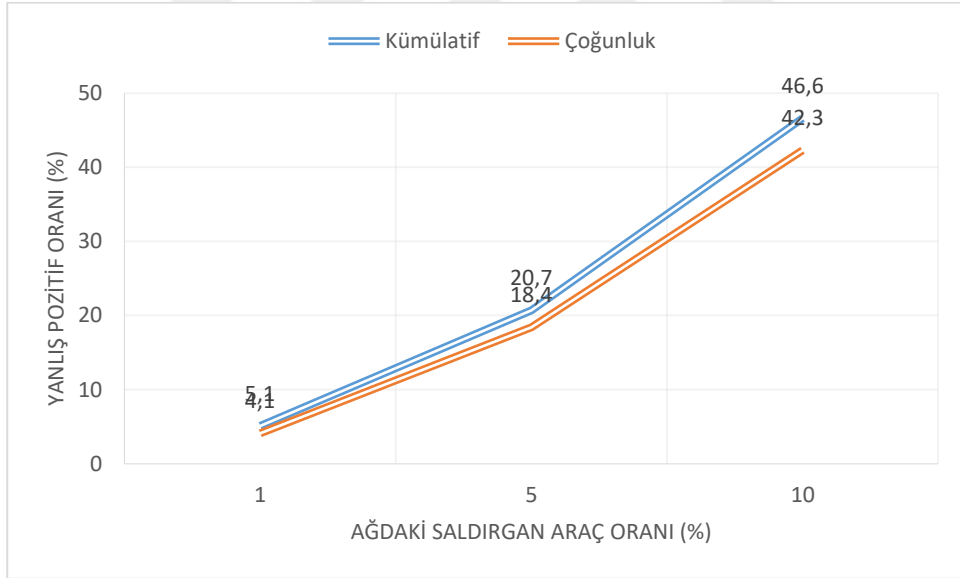
Şekil 4-14. Ağda %10 Oranında Saldırgan Olduğunda, Çoğunluk Tabanlı Saldırı Tespit Yönteminin Tespit Oranı

Kümülatif tabanlı Pearson analizi yöntemi ile saldırgan konumu değiştirme sahte bilgi saldırısının tespit oranları Şekil 4-9, Şekil 4-11 ve Şekil 4-13’de gösterilmiştir. Ağdaki saldırgan oranı arttıkça, saldırının tespit oranında düşüş gözlenmektedir. Çoğunluk tabanlı Pearson analizi yöntemi ile ilgili sahte bilgi saldırısının tespit oranları Şekil 4-10, Şekil 4-12 ve Şekil 4-14’te gösterilmiştir.

Bu saldırı, ağdaki araçların %1’inin saldırgan olduğu durumda, kümülatif tabanlı Pearson analizi yöntemi ile ortalama %90.6 oranında tespit edilirken, çoğunluk tabanlı Pearson analizi yöntemi ile ortalama %92.4 oranında tespit edilmektedir. Saldırgan araç oranı ağdaki tüm araçların %5’i olduğunda, tespit oranı kümülatif tabanlı Pearson analizi yöntemi için %80.8, çoğunluk tabanlı Pearson analizi yöntemi için ise %84.3 olarak hesaplanmıştır. Ağdaki saldırgan araç oranı, 370 aracın %10’u olarak ayarlanıp benzetim ortamında kümülatif tabanlı saldırı tespit yöntemi uygulandığında ise tespit oranı ortalama %72.1 iken çoğunluk tabanlı Pearson analizi yönteminde ortalama %75.3 olarak hesaplanmıştır (Şekil 4-15). Her iki tür saldırı için de, ağdaki saldırgan oranı %10’un üzerine çıktığında, tespit oranında hızlı bir düşüş görülmektedir.



Şekil 4-15. Saldırgan Konumu Değiştirme Saldırı için Tespit Oranları



Şekil 4-16. Sahte Bilgi Saldırısı - Saldırgan Konumu Değiştirme Saldırısı için Yanlış Pozitif Oranları

Şekil 4-16'te bu saldırı için önerilen saldırı tespit yöntemlerinin ortalama yanlış pozitif oranları gösterilmiştir. Bu grafiğe göre çoğunluk tabanlı Pearson analizinin çok az bir farkla bile olsa daha verimli olduğu ortaya çıkmaktadır. Ağdaki araçların %1'inin saldırgan olduğu durumda,

kümülatif tabanlı saldırı tespit yönteminin yanlış pozitif oranı ortalama yüzde 5.1, çoğunluk tabanlı saldırı tespit yönteminin ise yüzde 4.1 olarak hesaplanmıştır. Ağdaki saldırgan oranı tüm araçların %5 ve %10'u olduğunda, yanlış pozitif oranı da yükselmektedir.

4.3. Sonuçların Genel Değerlendirilmesi

Araçsal tasarsız ağlarda güvenlik, üzerinde çalışılan ve çözülmesi gereken önemli bir konudur. Gizlilik, bütünlük ve kullanılabilirlik bir sistemin sağlaması gereken temel güvenlik gereksinimleridir. Ağdaki gizliliği veya iletişimdeki bütünlüğü ve kullanılabilirliği bozmaya çalışan saldırılara karşı, etkili saldırı tespit ve önleme sistemleri geliştirilmelidir.

Bu tez kapsamında önerilen istatistiksel anomali tabanlı saldırı tespit sisteminde, ağdaki komşu sayısı ve komşuların kazaya olan uzaklıkları arasındaki ilişkiyi incelemek için Pearson korelasyon katsayısı yöntemi uygulanmıştır. Ağdaki tüm araç sayısının, %1, %5 ve %10'u kadarının saldırgan araç olduğu üç farklı benzetim senaryosu Unterstrass - Zürih haritasında test edilmiştir. Bu senaryoların her birinde ağda kaza bulunmaktadır. Araçların kazaya olan uzaklıklarını ve saldırganın konumunu değiştirdiğimiz iki farklı sahte bilgi saldırısının tespiti için iki saldırı tespit yöntemi önerilmiştir.

Kümülatif tabanlı Pearson analizi ve çoğunluk tabanlı Pearson analizi olarak adlandırılan saldırı tespit yöntemlerinde, komşu sayısı ve komşuların kazaya olan uzaklıkları arasındaki ilişki incelenmektedir. Bu iki değişken arasındaki ilişkinin yönü, saldırı olmayan ortamdaki değer ile kıyaslanarak, birbirleri ile ilişkileri gözlemlenmiştir. Saldırı olmayan ortamda komşu sayısı ve komşuların kazaya olan uzaklıkları arasında negatif yönlü zayıf bir ilişki tespit edilmiştir. Bu iki saldırı tespiti, ağda

herhangi bir saldırı olması durumunda, komşu sayısı ve komşuların kazaya olan uzaklıkları arasındaki ilişkinin yön değiştirdiği varsayımına dayanmaktadır.

Önerilen kümülatif tabanlı saldırı tespit sisteminde, araçların komşularından aldıkları komşularının kazaya olan uzaklık bilgilerinin ortalaması kullanılmaktadır. Ortalama yanlış pozitif oranı, ağdaki saldırgan oranının artması ile hızlı olarak artmaktadır. Saldırgan oranı %5'i geçtiğinde, önerilen yöntem yönetilemeyecek seviyede yanlış alarm üretmektedir. Bu yöntem ile ağdaki saldırgan oranı %1'den %10'a çıkarıldığında, ortalama tespit oranı da %91.5'ten %73.8' düşmektedir.

Çalışmamızda önerdiğimiz diğer saldırı tespit yöntemi, çoğunluk tabanlı saldırı tespit sisteminde ise araçlar, komşularından aldıkları Pearson korelasyon katsayısını değerlendirmektedir. Komşularından gelen Pearson korelasyon değerinin yönü, komşu sayısı ve komşuların kazaya olan uzaklıkları arasında hesaplanan Pearson korelasyon katsayısı ile kıyaslanmaktadır. Komşularının çoğunluğu, bu iki değer arasında fark buluyorsa bu durum saldırı olarak değerlendirilmektedir. Bu değerlendirme sonucunda ortalama tespit oranı, ağdaki saldırgan oranına göre %93.3 ve %75.3 arasında değişiklik göstermektedir.

Komşulardan alınan kazaya olan uzaklık bilgisi her iki önerilen saldırı tespit yönteminde de önemli bir faktördür. Komşu araçlar, kazaya daha yakın olduğu varsayımıyla, kazanın konumu hakkında bilgi vermektedirler. Kümülatif tabanlı Pearson analizi yönteminde, bu uzaklık bilgisinin ortalamasının alınması ile, konum ile ilgili toplanan verileri normal dağılıma uygun hale getirdiği ve nötrleştirdiği gözlenmiştir. Verilerde bulunan pozitif ve negatif uç değerler, ortalama alındığında normale yakın sonuçlar vermektedir. Bu sebeple çalışmalarımız

sonucunda, komşuların çoğunluğunun kararına göre saldırıyı tespit eden çoğunluk tabanlı Pearson analizi, tespit oranı ve yanlış pozitif oranında daha verimli sonuçlar ortaya çıkarmıştır. Dağıtık ve işbirlikçinin mimarının, tekil mimariden daha çok bilgi içermesi ile daha yüksek bir başarımla elde edilmiştir. İleride, benzetim senaryolarına, gelen kaza mesajlarına göre araçların yol değiştirmesi ve/veya yeni rota oluşturmaları özelliklerinin eklenmesi ile, yöntemimizin sonuçlarının gelişeceği düşünülmektedir. Çünkü bu özellikler, komşu sayısı ile konum arasındaki ilişki üzerinde daha belirgin bir değişime neden olacaktır. İleride, araçsal tasarsız ağlardaki uygulama protokollerinin standartlaşması ile bu tür özelliklerin benzetim senaryolarında ele alınacağı umulmaktadır.

5. SONUÇ

Günümüzde, birçok cihaz ve uygulama kablosuz iletişim ile bağlantı sağlamaktadır. Farklı cihaz türleri ve iletişim teknolojileri kullanarak, hareketli ortamda dahi bilgiye erişilebilmektedir. Araçlar arasında iletişime ihtiyaç duyulması, hareketli tasarsız ağların bir türü olan araçsal tasarsız ağların ortaya çıkmasını sağlamıştır.

Hareketli tasarsız ağlar kendinden yapılı, mobil düğümler ile telsiz bağlantıların bir araya gelmesi ile oluşan ağlardır. Bu ağlar önceden kurulmuş, sabit bir yapıya sahip değildirler. Bu özellikleri, onları birçok uygulama için çekici kılmakla beraber, saldırılara karşı da dayanıksız hale getirmektedir.

Araçsal tasarsız ağlarda, cihazların hareketliliği hareketli tasarsız ağlardaki cihazlara göre çok daha fazladır. Bu ağlardaki araçların hızları ve yüksek hareketliliği nedeniyle, ağ topolojisi sürekli değişim göstermektedir. Sürekli değişen ağ topolojisi ise, ağda kopmalara ve paket iletim oranının düşmesine sebep olmaktadır. Ayrıca bu dinamik topoloji, ağ trafiğinin kontrolünün yapılmasını zorlaştırmakta, dolayısıyla ağ tehditlere ve saldırılara açık hale getirmektedir. Araçsal tasarsız ağlar ile trafikteki araçlar arasında gerçek zamanlı ve anlık iletişimin sağlanması ile ağdaki olası kazalar önlenmektedir. Bu sebeple, araçsal tasarsız ağlarda birbirleriyle haberleşen araçların, trafikteki durum bilgisini doğru ve eksiksiz göndermeleri, ağda oluşabilecek tahribatı önlemek ve saldırıları doğru tespit edebilmek için gerekli görülmektedir.

Literatür araştırmaları sonucunda, istatistiksel yöntemlerin araçsal tasarsız ağlarda saldırı tespit için kullanımının çok nadir olduğu görülmüştür. Var olan yöntemler ise kimlik değiştirme saldırısına karşı

uygulanan normal dağılımı içeren istatistiksel yöntemlerdir. Bunun sebebi ise, araçlar arasındaki iletişimde gönderilen mesajlarda araçların hız ve konum bilgilerinin gönderilmesidir. Bu bilgiler ile araçların ağdaki bir sonraki saniyede bulunacağı konum bilgilerinin tahmin edilebilir olması sebebiyle, normal dağılım analizi kullanılarak saldırı tespiti yapılmıştır. Ancak sahte bilgi saldırısı için herhangi bir tahmin verisi elde edilemeyeceğinden dolayı, bu saldırı için incelenen araştırmalarda istatistiksel tabanlı saldırı tespit yönteminin kullanımına rastlanmamıştır. Bu sebeple, çalışmamızda iki farklı sahte bilgi saldırısına karşı istatistiksel tabanlı bir saldırı tespit yöntemi önerilmiştir. Pearson korelasyon katsayısı ile komşu sayısı ve komşuların kazaya olan uzaklığı arasındaki ilişkinin analiz edilmiştir. Pearson korelasyon katsayısı ile komşu sayısı ve komşuların kazaya olan uzaklığı arasındaki ilişkinin yönü ve derecesi analiz edilmiş, bu durumdan sapmalar anomali, yani saldırı olarak etiketlenmiştir. Pearson katsayısı tabanlı iki yöntem önerilmiştir: kümülatif tabanlı Pearson analizi ve çoğunluk tabanlı Pearson analizi.

Önerilen saldırı tespit yöntemleri, ağda herhangi bir saldırı olması durumunda, komşu sayısı ve komşuların kazaya olan uzaklıkları arasındaki ilişkinin yön değiştirdiği varsayımına dayanmaktadır. Pearson korelasyon katsayısı kullanılarak, saldırı olmayan ortamda komşu sayısı ve komşuların kazaya olan uzaklıkları arasında negatif yönlü, fakat zayıf bir ilişki tespit edilmiştir. Kümülatif tabanlı saldırı tespit yöntemi, komşulardan alınan uzaklık bilgilerinin ortalamasını alıp, komşu sayısı ile bu ortalama arasındaki korelasyon değerini ve bu değer yönünü hesaplamaktadır. Çoğunluk tabanlı saldırı tespit yönteminde ise, Pearson korelasyon katsayısı yönü ve değeri komşu araçların çoğunluğuna göre değerlendirilmektedir.

Bu çalışmada önerilen saldırı tespit sistemleri, Zürih Unterstrass haritası üzerinde oluşturulan benzetimler üzerinde değerlendirilmiştir. Yapılan

alıřmalar sonucunda, kaza uzaklıđına karřı yapılan sahte bilgi saldırısının ađda tespit edilme oranları elde edilmiřtir. Bu saldırının tespitinde kullanılan k m latif tabanlı Pearson analizine g re, ađdaki araların %1'inin saldırgan olduđu durumda saldırının tespit oranı ortalama %91.5, %5'inin saldırgan olduđu durumda %88.1 ve %10'u saldırgan ara olduğunda ise %73.8 olarak hesaplanmıřtır. Bu saldırıya karřı  nerdiđimiz bir diđer saldırı tespit y ntemi olan ođunluk tabanlı Pearson analizinin sonuları ise, saldırgan ara sayısı ađdaki araların %1'i olduğunda saldırının tespit oranı ortalama %93.3 oranında tespit edilmektedir. Saldırgan ara oranı ađdaki t m araların %5'i olduğunda ise bu oran %90 olarak hesaplanmıřtır. Ađdaki 370 aracın %10'u saldırgan olduğ  varsayılp, benzetim ortamında ođunluk tabanlı Pearson analizi y ntemi uygulandıđında tespit oranı ortalama %77.1 olarak hesaplanmıřtır. Ayrıca, kullanılan k m latif tabanlı Pearson analizine g re ađdaki saldırgan oranı araların %1, %5 ve %10'u olduğ  durumlarda sırasıyla yanlış pozitif oranı ortalama %4.6, %22.3 ve %40.9 olarak hesaplanmıřtır. ođunluk tabanlı Pearson analizinin sonularına g re yanlış pozitif oranının ortalaması sırasıyla %3.8, %20.4 ve %38.4't r.

Saldırgan konumunu deđiřtirmeye y nelik sahte bilgi saldırısının tekrarlı olarak benzetim ortamlarında uygulanması sonucu, k m latif tabanlı Pearson analizine g re ađdaki araların %1'inin saldırgan olması durumunda tespit oranının %90.6, %5 olduğunda %80.8 ve %10 olduğunda %72.1 olduğ  g zlenmiřtir. ođunluk tabanlı Pearson analizine g re ađdaki saldırgan ara oranı, 370 aracın %1'i olduğunda %92.4 olarak hesaplanmıřtır. Ađdaki saldırgan oranı %5'e y kseldiđinde, saldırgan konumunu deđiřtirmeye y nelik olan sahte bilgi saldırısının tespit oranı %84.3'e d řm řt r. Saldırgan oranı %10 olduğunda ise, %75.3 olarak hesaplanmıřtır. Kaza uzaklıđı deđiřtirme saldırısında g zlendiđi gibi, saldırgan oranı %10'a d řt đ nde saldırının tespit oranı

da düşüş göstermektedir. Saldırgan konumunu değiştirmeye yönelik sahte bilgi saldırısının tespiti sonucunda elde edilen yanlış pozitif oranı ortalamaları ise, kullanılan kümülatif tabanlı Pearson analizine göre ağdaki saldırgan oranı araçların %1, %5 ve %10'u olduğu durumlarda sırasıyla %5.1, %20.7 ve %6.6 olarak hesaplanmıştır. Çoğunluk tabanlı Pearson analizinin sonuçlarına göre yanlış pozitif oranının ortalaması aynı saldırgan oranı sırasıyla %4.1, %18.4 ve %42.3 olarak hesaplanmıştır. Ağdaki saldırgan oranı %5'in üzerinde olduğunda yanlış pozitif oranının kontrol edilemeyecek değerlerde olduğu gözlenmiştir.

Bu çalışma sonucunda, araçsal tasarsız ağlarda aracın konumuna yönelik yapılan iki sahte bilgi saldırısının tespiti iki farklı istatistiksel yöntem ile yapılmıştır. Benzetim sonuçları, araçsal tasarsız ağlarda komşuların çoğunluğunun kararı ile uygulanan çoğunluk tabanlı pearson analizinin, daha iyi bir başarımla sağladığını göstermektedir. Dağıtık ve işbirlikçi mimariye sahip bu yöntem, komşulardan alınan daha çok bilgi ile saldırı tespitinin olumlu yönde etkilendiğini göstermiştir.

Bu tez çalışmasında, benzetim senaryoları, literatürde kabul görmüş ya da standartlaşmış bir uygulama protokolü olmadığı için temel varsayımlar baz alınarak gerçekleştirilmiştir. Uygulama protokolüne, kaza olması durumunda araçların yeni rota oluşturması ve/veya yol değiştirmesi özelliklerinin eklenmesi ile, bu tez kapsamında incelenen komşu sayısı ve komşuların kazaya olan uzaklıkları değişkenleri arasındaki ilişkiyi etkileyeceği düşünülmektedir. Bu etkinin, önerilen saldırı tespit sisteminin başarımlarını arttıracak beklenmektedir.

Bu tez çalışması ile önerilen saldırı tespit sistemleri, sahte bilgi saldırısı için istatistiksel tespit yöntemlerinin uygulanabilirliğini araştırmış, ileride yapılacak çalışmalar için bir temel oluşturmuştur.

6. KAYNAKÇA

- [1] There will be 24 billion IoT devices installed on Earth by 2020 - Business Insider. <http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5>. (Ocak, **2018**).
- [2] S. Mohapatra and P. Kanungo, Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 simulator, *Procedia Engineering*, vol. 30, no. 2011, pp. 69–76, **2012**.
- [3] S. Şen and J. A. Clark, Mobil Tasarsız Ağlarda Saldırı Tespiti, in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, no. October, **2010**.
- [4] V. Viswacheda Duduku, A. Chekima, F. Wong, and J. A. Dargham, A study on vehicular Ad Hoc networks, *Proceedings - AIMS 2015, 3rd International Conference on Artificial Intelligence, Modelling and Simulation*, pp. 422–426, **2016**.
- [5] J. J. Haas, Y. Hu, and K. P. Laberteaux, Real-World VANET Security Protocol Performance, *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–7, **2009**.
- [6] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, Security in wireless ad-hoc networks - A survey, *Computer Communications*, vol. 51, pp. 1–20, **2014**.
- [7] M. Tiwari, Intrusion Detection System, *International Journal of Technical Research and Applications*, vol. 5, no. 2, pp. 38–44, **2017**.
- [8] S. Axelsson, Intrusion Detection Systems : A Survey and Taxonomy, http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf, **2000**.
- [9] M. S. I. Mamun and A. F. M. S. Kabir, Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc, *International Journal of Network Security & Its Applications (IJNSA)*, vol. 2, no. 3, pp. 102–117, **2010**.
- [10] H. H. Soliman, N. A. Hikail, and N. A. Sakr, A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks, *Egyptian Informatics Journal*, vol. 13, no. 3, pp. 225–238, **2012**.
- [11] M. Erritali and B. El Ouahidi, A review and classification of various

VANET Intrusion Detection Systems, *2013 National Security Days - 3eme Edition Des Journees Nationales de Securite, JNS3*, **2013**.

- [12] P. Brutch and C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, *Proceedings - 2003 Symposium on Applications and the Internet Workshops, SAINT 2003*, pp. 368–373, **2003**.
- [13] Y. Zhang and W. Lee, Intrusion detection in wireless ad-hoc networks, *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00*, pp. 275–283, **2000**.
- [14] B. Sun, K. Wu, and U. W. Pooch, Towards adaptive intrusion detection in mobile ad hoc networks, *Global Telecommunications Conference, GLOBECOM '04*, vol. 6, **2004**.
- [15] F. Anjum, D. Subhadrabandhu, and S. Sarkar, Signature based intrusion detection for wireless ad-hoc networks: a comparative study of various routing protocols, *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, vol. 3, p. 2152–2156 Vol.3, **2003**.
- [16] F. N. Bhatti, R. B. Ahmad, H. M. Bhatti, C. Engineering, and C. Technology, Classification of Anomaly Based Intrusion Detection Systems in VANET, *Australian Journal of Basic and Applied Sciences*, vol. 9, no. 25, pp. 24–29, **2015**.
- [17] A. Pharate, Classification of Intrusion Detection System, *International Journal of Computer Applications*, vol. 118, no. 7, pp. 23–26, **2015**.
- [18] G. Nascimento and M. Correia, Anomaly-based intrusion detection in software as a service, *2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 19–24, **2011**.
- [19] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, *Computers and Security*, vol. 28, no. 1–2, pp. 18–28, **2009**.
- [20] P. Uppuluri and R. Sekar, Experiences with Specification-Based Intrusion Detection, *International Workshop on Recent Advances in Intrusion Detection*, pp. 172–189, **2001**.
- [21] S. Sen and J. A. Clark, Evolutionary computation techniques for intrusion detection in mobile ad hoc networks, *Computer Networks*, vol. 55, no. 15, pp. 3441–3457, **2011**.

- [22] C. Tseng, C. Ko, J. Rowe, and K. Levitt, A Specification-based Intrusion Detection System for AODV, *SASN '03 Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 125–134, **2003**.
- [23] S. Sharma and E. S. Sharma, A review: Analysis of various attacks in VANET, *International Journal of Advanced Research in Computer Science*, vol. 7, no. 3, pp. 249–253, **2016**.
- [24] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, A comprehensive survey on vehicular Ad Hoc network, *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380–392, **2014**.
- [25] R. Brendha and V. S. J. Prakash, A survey on routing protocols for vehicular Ad Hoc networks, *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1–7, **2017**.
- [26] C. Paper, Attack Analysis in Vehicular Ad Hoc Networks, *Proc. of the 9th International Conference on Wireless, Mobile Network & Applications (WiMoA)*, no. September, **2017**.
- [27] S. Singh and S. Agrawal, VANET routing protocols: Issues and challenges, *2014 Recent Advances in Engineering and Computational Sciences, RA ECS 2014*, pp. 6–8, **2014**.
- [28] A. Rawat, S. Sharma, and R. Sushil, VANET : Security attacks and its possible solutions VANET : SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS, *Journal of Information and Operations Management*, vol. 3, no. 1, pp. 301–304, **2012**.
- [29] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, Recent Advances in VANET Security: A Survey, *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, **2015**.
- [30] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. L. Bin Ab Manan, Classes of attacks in VANET, *Saudi International Electronics, Communications and Photonics Conference 2011, SIEPC 2011*, **2011**.
- [31] F. Sakiz and S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, *Ad Hoc Networks*, vol. 61, pp. 33–50, **2017**.
- [32] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks : Analysis & Defenses ., *Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN '04)*, pp. 259–268, **2004**.

- [33] M. Al Mutaz, L. Malott, and S. Chellappan, Leveraging platoon dispersion for Sybil detection in vehicular networks, *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013*, pp. 340–347, **2013**.
- [34] B. Xiao and B. Yu, Detection and Localization of Sybil Nodes in VANETs Categories and Subject Descriptors, *DIWANS '06 Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8, **2006**.
- [35] P. A. N. Upadhyaya, Attacks on Vanet Security, *International journal of Computer Engineering & Technology (IJCET)*, vol. 9, no. 1, pp. 8–19, **2018**.
- [36] J. Grimaldo and R. Marti, Performance comparison of routing protocols in VANETs under black hole attack in Panama City, *2018 28th International Conference on Electronics, Communications and Computers, CONIELECOMP 2018*, vol. 2018-Janua, pp. 126–132, **2018**.
- [37] K. Kalaiselvan and G. Singh, Detection and Isolation of Black Hole Attack in Wireless Sensor Networks, *International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT)*, vol. 4, no. 5, pp. 3516–3524, **2015**.
- [38] S. Lachdhaf and M. Mazouzi, Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol, *9th International Conference on Networks & Communications*, no. December, **2017**.
- [39] S. Lachdhaf and M. Mazouzi, Secured AODV Routing Protocol for the Detection and Prevention of Black Hole, *Advanced Computing: An International Journal (ACIJ)*, vol. 9, no. January, **2018**.
- [40] L. He and W. T. Zhu, Mitigating DoS attacks against signature-based authentication in VANETs, *CSAE 2012 - Proceedings, 2012 IEEE International Conference on Computer Science and Automation Engineering*, vol. 3, pp. 261–265, **2012**.
- [41] K. Deepa Thilak and A. Amuthan, DoS attack on VANET routing and possible defending solutions-A survey, *2016 International Conference on Information Communication and Embedded Systems, ICICES 2016*, no. Icices, **2016**.
- [42] K. Edemacu, M. Euku, and R. Ssekibuule, Packet Drop Attack Detection Techniques in Wireless Ad hoc Networks: A Review, *International Journal of Network Security & Its Applications (IJNSA)*, vol. 6, no. 5, pp. 75–86, **2014**.

- [43] L. K. Bysani and A. K. Turuk, A survey on selective forwarding attack in wireless sensor networks, *2011 International Conference on Devices and Communications, ICDeCom 2011 - Proceedings*, **2011**.
- [44] S. Verma, Impact of Gray Hole Attack in V ANET, *1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India*, no. September, pp. 4–5, **2015**.
- [45] V. Mittal, Prevention of Gray Hole Attack in Vehicular Ad-hoc Network by Enhanced Multipath Approach, *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 4, no. 5, pp. 2459–2466, **2015**.
- [46] Ş. Sevil, J. A. Clark, and J. E. Tapiador, Security Threats in Mobile Ad Hoc Networks, in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, **2010**.
- [47] S. Shrivastava and W. S. Email, Rushing Attack and its Prevention Techniques, *International Journal of Application or Innovation in Engineering & Management (IJAIEEM)*, vol. 2, no. 4, pp. 453–456, **2013**.
- [48] P. R. Londhe, Analysis of Security Attack on VANET, *National Conference on Advancements in Alternate Energy Resources for Rural Applications*, pp. 23–27, **2015**.
- [49] B. Yu, C. Z. Xu, and B. Xiao, Detecting Sybil attacks in VANETs, *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, **2013**.
- [50] K. Zaidi, M. B. Milojevic, V. Rakocovic, A. Nallanathan, and M. Rajarajan, Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, **2016**.
- [51] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks, *Expert Systems with Applications*, vol. 50, no. December, pp. 40–54, **2016**.
- [52] H. Sedjelmaci and S. M. Senouci, An accurate and efficient collaborative intrusion detection framework to secure vehicular networks, *Computers and Electrical Engineering*, vol. 43, pp. 33–47, **2015**.
- [53] K. Ali Alheeti, A. Gruebler, and K. McDonald-Maier, Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks, *Computers*, vol. 5, no. 3, p. 16,

2016.

- [54] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars, *Proceedings - 2015 6th International Conference on Emerging Security Technologies, EST 2015*, pp. 86–91, **2016**.
- [55] V. Farid, P. S. S. S, and K. Harshad, Design and Analysis of AODV Routing Protocol in VANET Using NS-2, *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 2, no. IX, pp. 318–322, **2014**.
- [56] X. Yao, X. Zhang, H. Ning, and P. Li, Using trust model to ensure reliable data acquisition in VANETs, *Ad Hoc Networks*, vol. 55, pp. 107–118, **2017**.
- [57] L. Hu, Z. Ding, and H. Shi, An improved GPSR routing strategy in VANET, *2012 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2012*, pp. 1–4, **2012**.
- [58] M. P. Leckie, Christopher Chong Eik Loo, Mun Yong Ng, Christopher Leckie, Intrusion Detection for Routing Attacks, *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, **2006**.
- [59] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, Data-centric rogue node detection in VANETs, *Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 398–405, **2015**.
- [60] R. Jadhav, Security Issues and Solutions in Wireless Sensor Networks, *International Journal of Computer Applications*, vol.162, no.2, **2017**.
- [61] S. S. Kulkarni, M. G. Gouda, and A. Arora, Secret instantiation in ad-hoc networks, *Computer Communications*, vol. 29, no. 2, pp. 200–215, **2006**.
- [62] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, A sybil attack detection approach using neighboring vehicles in VANET, *Proceedings of the 4th international conference on Security of information and networks - SIN '11*, no. November, p. 151, **2011**.
- [63] A. A. Waskita, H. Suhartanto, P. D. Persadha, and L. T. Handoko, A simple statistical analysis approach for intrusion detection system, *Proceedings - 2013 IEEE Conference on Systems, Process*

and Control, ICSPC 2013, pp. 193–197, **2013**.

- [64] P. H. Gordon, Performance Evaluation of VANET with EDCA Access Scheme using Gauss- Markov Mobility Model, *International Journal of Simulation: Systems, Science & Technology*, pp. 1–7, **2017**.
- [65] M. E. Renda, G. Resta, P. Santi, F. Martelli, and A. Franchini, IEEE 802.11p VANets: Experimental evaluation of packet inter-reception time, *Computer Communications*, vol. 75, pp. 26–38, **2016**.
- [66] T. K. Koo and M. Y. Li, A Guideline of Selecting and Reporting Intraclass Correlation Coefficients for Reliability Research, *Journal of Chiropractic Medicine*, vol. 15, no. 2, pp. 155–163, **2016**.
- [67] R. Chaudhary, S. Sethi, R. Keshari, and S. Goel, A study of comparison of Network Simulator -3 and Network Simulator -2, *International Journal of Computer Science and Information Technologies*, vol. 3, no. 1, pp. 3085–3092, **2012**.
- [68] What is ns-3 « ns-3. <https://www.nsnam.org/overview/what-is-ns-3/>. (Eylül, **2018**).
- [69] Ns-3.26 - Nsnam. <https://www.nsnam.org/wiki/Ns-3.26>. (Eylül, **2018**).
- [70] IBM SPSS Software | IBM. <https://www.ibm.com/analytics/spss-statistics-software>. (Ağustos, **2018**).

ÖZGEÇMİŞ

Kimlik Bilgileri

Adı Soyadı : Fehime AYDIN
Doğum Yeri : Bulgaristan
Medeni Hali : Evli
E-posta : fehimecann@gmail.com
Adresi : Bağlıca Mah. 1061. Sok. No: 5/11 Etimesgut/Ankara

Eğitim

Lisans : Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri
Yüksek Lisans :

Yabancı Dil ve Düzeyi

İngilizce : Çok iyi

İş Deneyimi

Hacettepe Üniversitesi
Öğrenci İşleri Daire Başkanlığı Bilgi Sistemleri Birimi
Akademik Uzman 2014 -

Deneyim Alanları

C++, Java, PHP, Oracle, Network

Tezden Üretilmiş Projeler ve Bütçesi

Yok.

Tezden Üretilmiş Yayınlar

Şu an yok.

Tezden Üretilmiş Tebliğ ve Poster Sunumla Katıldığı Toplantılar

Yok.



HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 29/11/2018

Tez Başlığı / Konusu: **Araçsal Tasarsız Ağlar için İstatistiksel Tabanlı Bir Saldırı Tespit Yöntemi**

Yukarıda başlığı/konusu gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler d) Sonuç kısımlarından oluşan toplam **85** sayfalık kısmına ilişkin, **29/11/2018** tarihinde **tez danışmanım** tarafından *Turnitin* adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı **% 8** 'dir.

Uygulanan filtrelemeler:

- 1- Kaynakça hariç
- 2- Alıntılar hariç
- 3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.


Tarih ve İmza

Adı Soyadı: FEHİME AYDIN
Öğrenci No: N13222112
Anabilim Dalı: BİLGİSAYAR MÜHENDİSLİĞİ
Programı: BİLGİSAYAR MÜHENDİSLİĞİ
Statüsü: ☒ Y.Lisans ☐ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

Doç.Dr. Sevil ŞEN AKAGÜNDÜZ



(Unvan, Ad Soyad, İmza)