ARAÇSAL TASARSIZ AĞLARDA SALDIRILARIN ANALİZİ

ANALYSIS OF ATTACKS IN VEHICULAR AD HOC NETWORKS

ÖMER MİNTEMUR

DOÇ. DR. SEVİL ŞEN AKAGÜNDÜZ

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Bilgisayar Mühendisliği Anabilim Dalı için Öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2016

ÖMER MİNTEMUR'un hazırladığı "**Araçsal Tasarsız Ağlarda Saldırıların Analizi**" adlı bu çalışma aşağıdaki jüri tarafından **BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI'**nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Yrd. Doç. Dr. Kasım ÖZTOPRAK

Başkan ……

Doç. Dr. Sevil ŞEN AKAGÜNDÜZ

Danışman ……

Yrd. Doç. Dr. Ahmet Burak CAN

Üye ……

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

Prof. Dr. Salih Bülent ALTEN

Fen Bilimleri Enstitüsü Müdürü

ETİK

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

- 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,

- Başkarlarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,

- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,

- Kullanılan verilerde herhangi bir değişiklik yapmadığımı

- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

Beyan ederim.

…/…/….

Ömer MİNTEMUR

ÖZET

ARAÇSAL TASARSIZ AĞLARDA SALDIRILARIN ANALİZİ

Ömer MİNTEMUR

Yüksek Lisans, Bilgisayar Mühendisliği

Tez Danışmanı: Doç. Dr. Sevil ŞEN AKAGÜNDÜZ

Nisan 2016, 113 Sayfa

Araçsal tasarsız ağlar, mobil tasarsız ağların bir kolu olup, gün geçtikçe gelişmektedir. Araçsal tasarsız ağlar, araçların birbirleriyle haberleşmesini sağlayan bir mobil tasarsız ağ çeşididir. Araçlar birbirleriyle haberleşerek trafik ve yol bilgisi gibi can güvenliği için önemli olan mesajları birbirleriyle paylaşabilirler. Bu avantajlarının yanı sıra, bu ağın en büyük dejavantalarından birisi güvenliktir. Araçların çok yüksek hızda seyrettiği ve topoloji değişkenliğinin çok olduğu bir ağ olduğu için söz konusu ağ, saldırılara çok açıktır.

Bu çalışmada, mobil tasarsız ağlarda da sıkça kullanılan AODV yönlendirme protokolü ve coğrafi pozisyon verilerini kullanarak paket iletimini gerçekleştiren GPSR yönlendirme protokolünün, iki farklı haritada ve farklı saldırılar altında performansları analiz edilmiştir. Benzetimlerde 35 araç kullanılmış ve bir benzetim 200 saniye gerçekleştirilmiştir. Saldırıların etkisini daha iyi görebilmek için, her tekrarda, farklı bağlantı dosyaları kullanılmıştır. İki farklı protokolde de, karadelik saldırısı, sel saldırısı, paket düşürme saldırısı ve sahte bilgi saldırısı

gerçekleştirilmiştir. Yapılan benzetimlerde saldırgan sayısı sürekli olarak artırılmıştır. Benzetimlerde araç yoğunluğu fazla olan ve fazla olmayan, iki farklı harita (Münih şehir merkezi ve İstanbul Yolu) kullanılmıştır. İki protokol de, paket iletim oranı, verimlilik, uçtan uca gecikme ve ek yük metrikleriyle analiz edilmiştir.

Benzetim sonuçlarında görülmüştür ki, saldırısız ortamda AODV yönlendirme protokolü paket iletimi metriği bakımından, GPSR yönlendirme protokolünden iki haritada da daha iyi sonuç vermektedir. Saldırı olduğu durumlarda ise, AODV yönlendirme protokolü en fazla karadelik saldırısından etkilenmiş olup, GPSR yönlendirme protokolü her saldırıdan neredeyse eşit oranda etkilenmiştir.

Sonuç olarak, yapılan benzetimlerde iki protokolün de saldırılara açık olduğu görülmüş ve iki protokolün de saldırılara karşı gelişmiş bir tespit sistemine sahip olması gerektiği sonucuna varılmıştır.

Anahtar Kelimeler: Vanet, güvenlik, saldırı, AODV, GPSR, karadelik, sel saldırısı, paket düşürme, sahte bilgi

ABSTRACT

ANALYSIS OF ATTACKS IN VEHICULAR AD HOC NETWORKS

ÖMER MİNTEMUR

Master Thesis, Department of Computer Engineering

Supervisor: Doç. Dr. Sevil ŞEN AKAGÜNDÜZ

April 2016, 113 pages

Vehicular ad hoc networks, is a subbrunch of mobile ad hoc networks, and it is an emerging area. Vehicular ad hoc network is a network type that enables cars to communicate with each other. Cars could send information about traffic and road conditions, which are critical for traffic safety. Despite of having such advantages, one of the biggest disadvantages of this network is security. The networks in which cars could travel at high speeds and the network topology change very dynamically, are exposed to attacks.

In this thesis, AODV routing protocol, that is used widely in mobile ad hoc networks and GPSR routing protocol, that uses geographic locations of nodes for packet transmission are used and their performances are analyzed in 4 different attacks. 35 cars are used for simulations and every simulation takes 200 seconds. In every simulation different connection patterns are used to get better results of simulations. Blackhole attack, flooding attack, packet dropping attack and bogus information attack are implemented for both protocols. Attackers numbers are increased in every simulation. Two different maps, which have two different density, namely

Munich city center which has a high density and İstanbul Road which has a low density are used. Packet delivery ratio, throughput, end to end delay and overhead metrics are analyzed for both protocols.

The simulation results showed that, in a network under no attack AODV routing protocol has a better performance in terms of packet delivery ratio in both maps than GPSR. Results also showed that in the network that has attackers, AODV is effected most by the blackhole attack while GPSR is effected almost equally by each attack type.

As a result, it is shown that both protocol is open to attacks and both protocol should have advanced detection sytems against attacks.

Keywords: VANETs, security, attacks, AODV, GPSR, blackhole, flooding, dropping, bogus information

TEŞEKKÜR

Tez konusunun seçiminde ve tez çalışmamda bana yön, güven, destek veren ve çalışmam boyunca bilgi ve deneyimlerini esirgemeyen danışmanım Sayın Doç. Dr. Sevil Şen AKAGÜNDÜZ'e sonsuz teşekkürlerimi sunarım.

Ayrıca değerli yorum ve önerileriyle katkıda bulunan juri üyelerim Sayın Yrd. Doç. Dr. Ahmet Burak CAN ve Sayın Yrd. Doç. Dr. Kasım ÖZTOPRAK'a teşekkür ederim.

Tez çalışmam aşamasında istatistiki konularda yardım ve bilgilerini esirgemeyen Sayın Yrd. Doç. Dr. Ufuk EKİZ'e, Sayın Öğretim Görevlisi Mücahit KURTULUŞ'a teşekkür ederim.

Son olarak hayatta beni hiçbir zaman yalnız bırakmayan, doğru yolu gösteren, cesaretlendiren aileme, arkadaşlarıma ve çalışmam boyunca beni destekleyen nişanlım Merve ÇOLAK'a tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLER

Sayfa

Sayfa

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR

Simgeler

∑	Toplam

Kısaltmalar

ACK	Acknowledgement
AODV	Ad-Hoc on Demand Distance Vector Routing Protocol
CA	Central Authority
CBR	Constant Bit Rate
CREP	Route Confirmation Reply
CREQ	Route Confirmation Request
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSDV	Destination – Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
FSR	Fisheye State Routing
GPSR	Greedy Perimeter Stateless Routing
MANET	Mobile Ad-Hoc Network
NS	Network Simulator
OBU	On Board Unit
OLSR	Optimized Link State Routing
OSM	Open Street Map

RHR	Right Hand Rule
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSU	Road Side Unit
SUMO	Simulation of Urban Mobility
TCL	Tool Command Language
TCP	Transmission Control Protocol
TORA	Temporally Ordered Routing Algorithm
UDP	User Datagram Protocol
VANET	Vehicular Ad-Hoc Network
WRP	Wireless Routing Protocol

1. GİRİŞ

Internete bağlanan cihazların sayısı gün geçtikçe artmaktadır. Artık cihazlar birbirleriyle haberleşmekte ve kendi içlerinde kendi ağlarını oluşturmakta, böylelikle birbirleri arasında veri veya bilgi alışverişi yapabilmektedirler. Bu tarz ağların en güzel örneklerinden birisi mobil tasarsız ağlardır (Mobile Ad Hoc Networks). Mobil tasarsız ağlar, mobil cihazların (cep telefonu, dizüstü bilgisayar vs.), diğer bir deyişle düğümlerin, herhangi bir sabit yapı olmadan, kendi aralarında kurdukları ağ sayesinde birbirleriyle kablosuz haberleşme aracılığıyla haberleştiği bir ağ çeşididir. Mobil tasarsız ağların en büyük avantajlarından biri, cihazlar arasındaki haberleşmenin herhangi bir sabit yapıya ihtiyaç duymadan cihazların içindeki kablosuz teknolojiyle istenilen her yerde haberleşmeye imkan vermesidir [1]. Mobil ismi, bu tür cihazların taşınabilir olmasından ve dolayısıyla belli bir hareketliliğe sahip olmasından gelmektedir. Telefondan telefona bilgi gönderimi, diz üstü bilgisayarlardan kişisel bilgilere erişim gibi özellikleri mobil tasarsız ağların haberleşmesine örnek gösterebiliriz.

Mobil tasarsız ağların gelişmesiyle birlikte bu ağların farklı türleri ortaya çıkmaya başlamıştır. Bunlardan en önemlisi araçsal tasarsız ağlardır (Vehicular Ad Hoc Networks). Mobil tasarsız ağlarda mobil cihazlar nasıl birbirleriyle haberleşebiliyorsa araçsal tasarsız ağlarda da araçlar birbirleriyle haberleşebilir, bilgi alışverişinde bulunabilirler. Araçsal tasarsız ağların mobil tasarsız ağlardan en büyük farkı, hareketliliğin mobil tasarsız ağlara göre çok daha yüksek olmasıdır. Mobil tasarsız ağlarda düğümler sabit değildir ve taşınabilirdir, ancak araçsal tasarsız ağlarda araçlar mobil tasarsız ağlara göre çok daha yüksek hızlarda hareket ederler ve ağ topolojisi sürekli değişmektedir. Araçsal tasarsız ağların bir diğer farkı ise araçların enerji sorununun olmamasıdır.

Kendi aralarında haberleşen araçlar birbirlerine trafik durumları hakkında, yol bilgisi hakkında ya da eğlence ve bilgi amaçlı veri gönderebilir (Turistik yerler, park yerleri vs.). Kullanım alanlarından bir diğeri ise sürücü güvenliğidir. Akıllı sistemle donatılan araçlar, aracı kullanan şoförü uyararak kendi güvenliği ve çevresindeki araçların güvenliği açısından önemli rol oynayabilirler.

Araçsal tasarsız ağlarda da diğer ağlarda olduğu gibi güvenlik sorunları bulunmaktadır [2,3,4]. Bu ağların kullanımı yaygınlaştıkça, bu sorunlara çözüm bulmak da önem kazanmaktadır. Diğer ağlardan farklı olarak araçsal tasarsız ağlarda ağ topolojisinin sürekli değişmesi, araçların çok hızlı hareket etmesi ve ağa araçların sürekli giriş çıkış yapması araçların takibini güçleştirmekte ve ağı saldırıya çok açık hale gelmektedir. Araçsal tasarsız ağlarda meydana gelen saldırıların sonuçları, diğer ağlara göre daha tahrip edici olabilir. Herhangi bir saldırı durumunda ağın kullanılamaz hale gelmesi can ve mal kayıplarına neden olabilir, bu nedenle ağa yapılan saldırılar doğru bir şekilde analiz edilmeli ve sonuçları iyi değerlendirilmelidir.

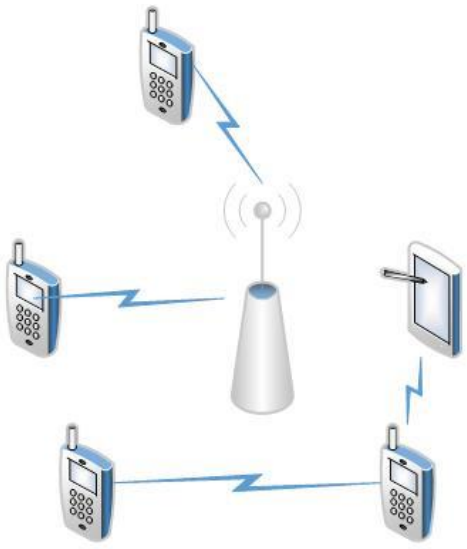
Literatürde saldırıların araçsal tasarsız ağlarda yaptığı tahribatı inceleyen çalışmalar mevcuttur. Ancak bu çalışmalarda kullanılan modellerin (araçların hızları, haritalar vs.) gerçeğe uygun olarak hazırlanmaması sonucu yapılan benzetimlerden alınan sonuçlar, saldırıların ağa vereceği tahribatı doğru şekilde yansıtmamaktadır. Ayrıca yapılan çalışmalar, genellikle bir protokolü kapsamakta ve birden fazla protokolde aynı saldırılar gerçekleştiğinde saldırıların etkisini inceleme imkânı sağlamamaktadır. Son olarak, kullanılan protokoller, genellikle belli başlı protokoller (AODV, DSDV, OLSR, TORA vs.) üzerinde olup [5,6], araçsal tasarsız ağlara uygun coğrafi tabanlı protokollerde saldırılar denenmemiştir.

Bizim bu çalışmamızda, daha önce sıkça kullanılmış olan AODV yönlendirme protokolü ve daha önce araçsal tasarsız ağlarda saldırı yapılarak benzetimi gerçekleştirilmemiş olan ve araçsal tasarsız ağlara uygun olan GPSR yönlendirme protokolü kullanılmıştır. Yaptığımız benzetimler sonucunda hem AODV protokolünün hem de GPSR protokolünün saldırısız ortamlarda bile araçsal tasarsız ağlardaki veriminin oldukça düşük olduğu görülmüştür. Saldırı yapılan durumlarda ise bu sözü geçen iki protokolün veriminin çok daha düştüğü gözlemlenmiştir. Çalışmamızda gerçeğe uygun olması açısından iki farklı harita kullanılmış ve araçsal tasarsız ağlarda AODV ve GPSR protokolünün bu iki farklı haritada nasıl sonuç verdiği, benzetim sonuçları bölümünde gösterilmiştir. Çalışmamızda kendi çıkardığımız Türkiye İstanbul yolu haritası kullanılmış ve bunun yanında Almanya Münih kent merkezinin haritası çıkarılarak aynı benzetimler tekrarlanmış ve sonuçlar elde edilmiştir. Yapılan benzetimler sonucunda, saldırıların, ağdaki paket düşürme

oranına, paket iletim oranına, verimlilik oranına, ek yük oranına ve uçtan uca gecikme oranına nasıl etki ettiği gösterilmiştir.

2. ARAÇSAL TASARSIZ AĞLAR

Mobil tasarsız ağların yaygınlaşmasıyla ve kullanım alanlarının artmasıyla birlikte, tasarsız ağların yeni modelleri ortaya çıkmıştır. Bunlardan bir tanesi de araçsal tasarsız ağlardır (Vehicular Ad Hoc Networks). Araçsal tasarsız ağların amacı, genel olarak araçların birbirleri arasında haberleşmesini sağlamaktır. Birbirleriyle haberleşen araçlar, yol durumu hakkında birbirlerine bilgi verirler ve araçların trafikteki sürüş rahatlığını arttırırlar. Her yıl yaklaşık olarak 1,2 milyon insan trafik kazalarında hayatını kaybetmektedir [7]. Araçsal tasarsız ağların ortaya çıkmasının en önemli nedeni, trafikteki can ve mal kaybını azaltacak olmasıdır. Araçsal tasarsız ağlar, kullanım olarak mobil tasarsız ağlara benzer (veri alışverişi, bilgilendirme vs.). Araçsal tasarsız ağları, mobil tasarsız ağlardan ayıran farklar araçların çok yüksek hızda hareket etmesi, yer değiştirmenin sürekli olması ve ağ topolojisinin, trafik durumu sürekli değiştiği için çok değişken olmasıdır. Mobil tasarsız ağlarda, düğümlerdeki yer değiştirme araçsal tasarsız ağlara göre daha azdır ve genellikle cihazlar hareketliliği sağlamak için pil ile çalışırlar. Bu nedenle bu ağlar için geliştirilen sistemler ve protokoller bu enerji kısıtını göz önünde bulundurmalıdır. Ancak araçsal tasarsız ağlarda, düğümler araçlar olduğu için önemli bir enerji kısıtı bulunmamaktadır.

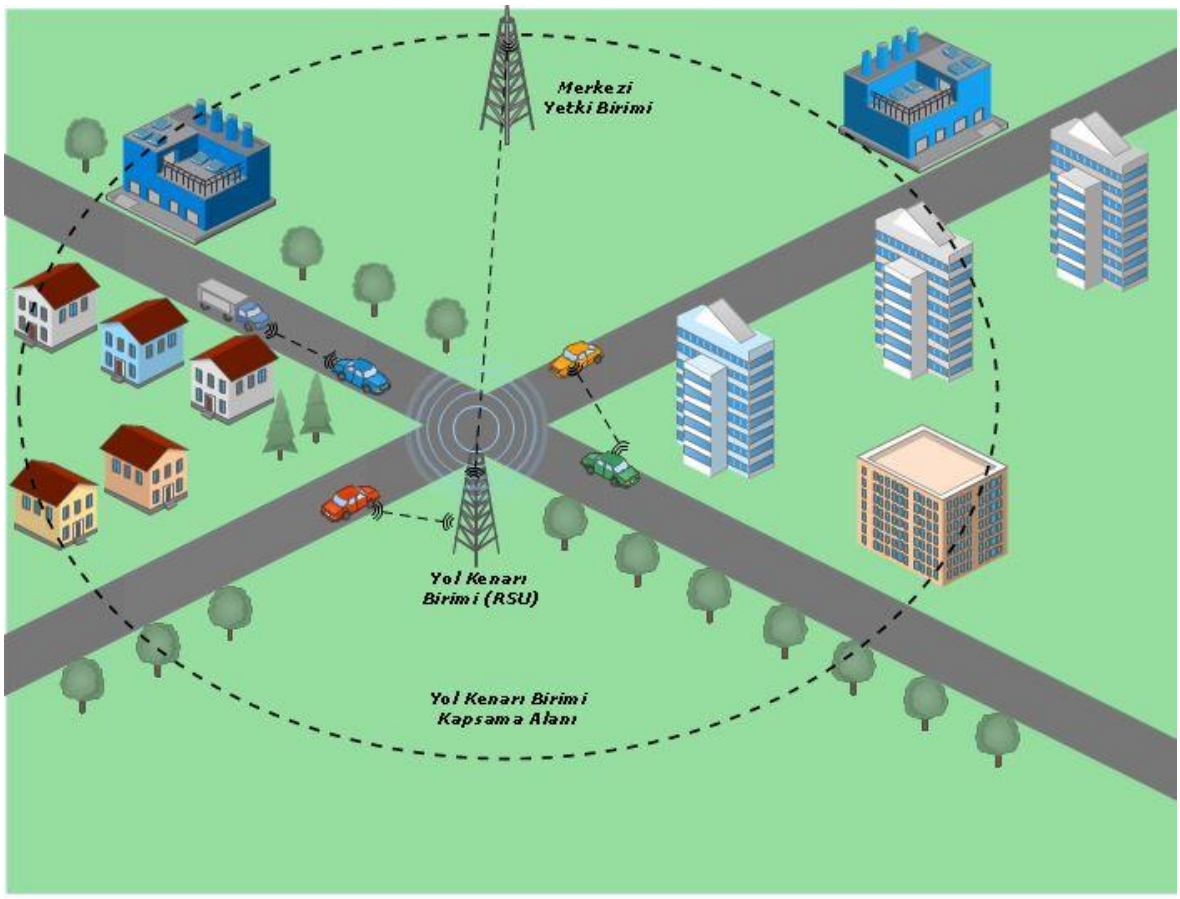


Şekil 2.1. Mobil Tasarsız Ağlar

Şekil 2.1.'de çok basit bir şekilde mobil tasarsız ağın nasıl çalıştığı ve iletişim kurduğu gösterilmiştir. Mobil tasarsız ağlardaki düğümlere örnek olarak cep

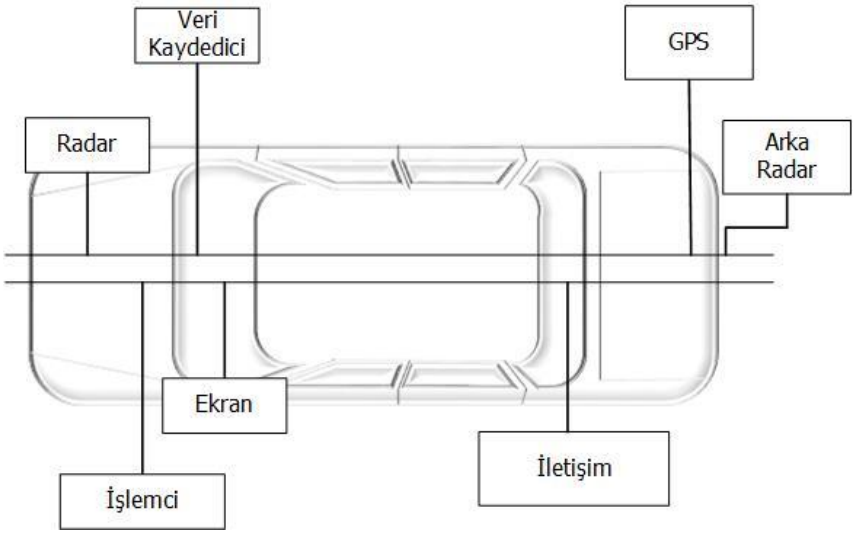
telefonlarını, cep bilgisayarlarını (PDA), diz üstü bilgisayarlarını, kısacası Internete bağlanabilen bütün cihazları örnek verebiliriz.

Araçsal tasarsız ağlar ise tamamen araçlara özel olarak düşünülmüş bir tasarsız ağ çeşididir. Araçlar ağa bağlanabilmek için Merkezi Yetki (Central Authority - CA) adı verilen bir yapıyla iletişime geçebilirler. Ağa bağlanmak isteyen araç, CA'ya mesaj göndererek ağa katılmak istediğini bildirebilir. Bu mesajı yol kenarlarındaki Yol Kenarı Birimleri (Road Side Unit - RSU) aracılığı ile gönderirler [8]. RSU'lar sabit olan birimlerdir ve belirli bir kapsama alanına sahiptirler. Mesajı RSU'lar aracılığı ile alan CA, araca ağa giriş izni verir. Burada, her zaman CA gerekli olmayabilir, bazen de CA farklı roller üstlenebilir. CA, mesajlarını RSU aracılığı ile alabilir, ya da göndereceği bir mesaj varsa yine RSU aracılığı ile gönderebilir. CA'ların nasıl farklı rol üstlenebileceğini birkaç örnekle açıklamak gerekirse, yoldaki buzlanmayı ölçen RSU'lar bu bilgiyi CA ile paylaşabilir ve CA bunu bünyesinde tutarak yolun haftalık, aylık, yıllık durumu hakkında çıkarım yapabilir. Diğer bir örnek ise şu şekilde verilebilir, RSU'lar aracılığı ile bilgi toplayan CA, bulunduğu yolun günlük trafik yoğunluğunu tespit edebilir, yolun fiziki koşulları hakkında bilgi toplayabilir ve herhangi bir bakım onarım durumunda bünyesinde topladığı bilgileri yetkililerle paylaşabilir.



Şekil 2.2. Araçsal Tasarsız Ağlar

Şekil 2.2.'de araçsal tasarsız ağların basit bir şeması verilmiştir. Şekilde görünen araçlar birbirleriyle haberleşmekte ve ister yol durumu, isterse de diğer bilgi mesajlarını paylaşabilmektedirler. Şekil 2.2.'de Yol Kenarı Birimi'nin kapsama alanı ve nasıl çalıştığı gösterilmiştir. Şekildeki araçlar arası çizgiler araçlar arası haberleşmeyi göstermektedir. Bunun yanı sıra, araçlar Yol Kenarı Birim'i ile de iletişime geçebilmektedirler. Şekilde yol kenarı biriminin kapsadığı alan da gösterilmiştir. Yol kenarı biriminin kapsadığı alan içinde, araçlar yol kenarı birimleriyle mesajlaşabilirler, bunun haricinde kendi aralarında da bilgi alışverişi yapabilirler.



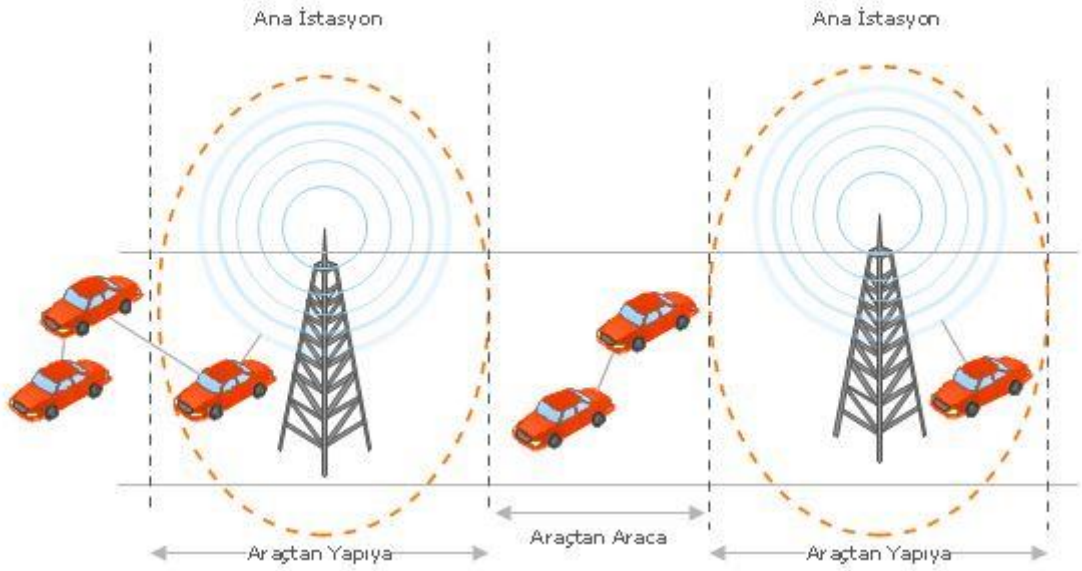
Şekil 2.3. Araç İçi Ünitesi (On Board Unit)

Bunun haricinde araçların üstünde haberleşmeyi sağlayan Araç İçi Ünitesi (On Board Unit - OBU) adı verilen bir yapı bulunmaktadır. Her araç OBU ile donatılır ve bu sayede araçların birbirleri arasında ya da yol kenarlarında bulunan RSU'lar ile haberleşmesi sağlanır [8]. OBU'lar arabanın altyapısında bulunan ve aracın kimliğini ve bilgilerini saklayan yapıdır.

Şekil 2.3.'te bir aracın içindeki Araç İçi Ünitesi örnek olarak verilmiştir. Gerçek hayatta birebir bu şekilde olmasa da örnek olarak aracın ön ve arka kısmında birer radar, motor kısmında aldığı mesajları işleyen ve hesaplayan bir bilgisayar (işlemci), aynı bölgeye yakın olarak bir adet veri kaydedici ve aracın iç göğüs kısmında bir ekran bulunmaktadır. Aracın arka kısmında ise arka radar, iletişim cihazı ve GPS bulunmaktadır.

Araçsal tasarsız ağlarda iletişimi iki kategoriye ayırabiliriz [4];

- Araçtan – Araca İletişim, iki ya da daha fazla araç birbirleriyle yol durumları veya trafik durumları için haberleşebilirler.
- Araçtan – Yapıya İletişim, herhangi bir araç, yol kenarlarında bulunan RSU'lar ile haberleşebilirler.



Şekil 2.4. Araçsal Tasarsız Ağlar Arası Haberleşme

Araçlar birbirlerine yol durumlarını, acil durumları göndermenin haricinde bulundukları bölgedeki turistik alanların, park alanlarının, restoranların, benzin istasyonlarının bilgilerini de alıp verebilirler. Araçsal tasarsız ağlar sadece araçtan araca ya da araçtan RSU'ya haberleşmekle kalmayıp, diğer haberleşme seçeneklerini de içinde barındırmaktadırlar. Bu sayede araç sürücüsü, bulunduğu bölge hakkında bilgi alabilir. Şekil 2.4.'te araçtan araca ve araçtan yapıya olan haberleşmenin bir örneği verilmiştir.

2.1. Araçsal Tasarsız Ağlarda Yönlendirme Protokolleri

Kablosuz ağlarda veri yönlendirmesi (haberleşme, mesajlaşma) çoğu açıdan kablolu ağlardaki veri yönlendirmesine benzese de, bazı noktalarda kablolu ağlardan ayrılmaktadır. Her iki ağda da gönderilen verilerin bütünlüğü korunmalı ve verinin gönderildiği yere gittiğinden emin olunmalıdır. Ancak, kablosuz ağların kablolu ağlardan en büyük farklarından biri kablosuz ağların topolojisinin çabuk değişmesidir. Kablolu ağlarda bilgisayarlar (düğümler) ağın yapısına hâkimdir ve bir veri gönderilmesi gerektiğinde araçların ağın topolojisini tekrardan keşfetmesine gerek yoktur. Ancak tasarsız ağlarda araçlar ağın yapısına hâkim değildir ve ağa yeni katılan her düğüm sisteme kendisini tanıtmalıdır. Sisteme giren araçlar ağın kullandığı yönlendirme protokolünün türüne göre ilgili kontrol paketlerini kullanarak

sisteme giriş yaptığını bildirebilir ve ağ topolojisi hakkında bilgi sahibi olur (AODV yönlendirme protokolü için RREQ, RREP, REER paketleri gibi).

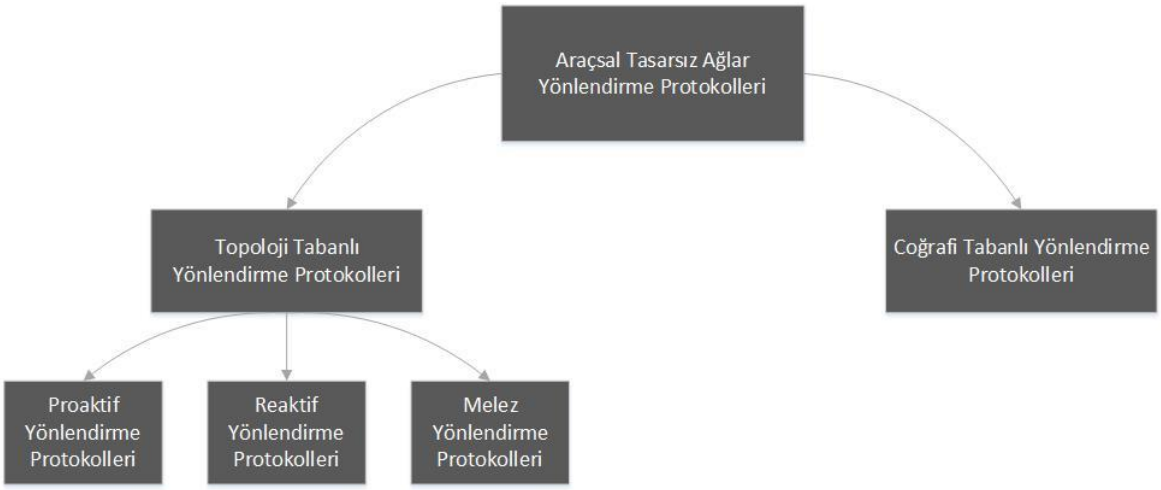
Araçsal tasarsız ağlarda iletişim zorluğu diğer mobil ağlara göre farklılık göstermektedir. Mobil ağlarda topoloji daha az değiştiği için iletişim daha rahat olmaktadır. Ayrıca diğer mobil ağlarda düğümler sabit olmadığı için, bir diğer deyişle sabit bir güç kaynağına bağlı olmadığı için güç sorunu ortaya çıkmaktadır. Araçsal tasarsız ağlara bakıldığında ise diğer mobil ağlara göre çok daha farklı zorluklar ve aynı zamanda araçsal tasarsız ağların getirdiği avantajlar da bulunmaktadır. Bu zorluklardan bir tanesi araçların hareketinin, bir diğer deyişle süratinin değişken olmasıdır. Bu durumda haberleşmenin çok hızlı ve sağlıklı bir şekilde gerçekleşmesi gerekmektedir. Araçlar çok hızlı hareket ettikleri için aralarındaki bağlantı çok kısa süreli olacaktır. Bu da beraberinde, araçsal tasarsız ağlarda araçlar arasındaki bağlantının sürekli kopması sorununu getirecektir. Araçların yüksek süratte hareket etmeleri ve bunun sonucunda RSU'ların (Yol Kenarı Birimleri) kapsama alanından çıkmaları sonucu sürekli ağ kopmaları meydana gelecektir. Bu kopma sonucu gönderilmek istenen mesaj gönderilemeyecek ve bunun sonucunda bazı sorunları beraberinde getirecektir. Bir diğer sorun ise çevresel faktörlerdir. Araçsal tasarsız ağların hızlı hareket etmelerinden dolayı çevresel faktörler sürekli değişecektir (binalar, dağlar, köprüler vs.). Kimi yerlerde haberleşme çok rahat olacakken, kimi yerlerde imkansız hale gelebilecektir. Bu durum diğer mobil ağlarda da geçerlidir, herhangi bir mobil cihaz diğer bir mobil cihazla haberleşirken elektromanyetik dalgaları kullanacağından, önüne bir engel çıkması halinde bu engeli aşamayacak ve bilgi veya mesaj iletilemeyecektir. Araçsal tasarsız ağlarda ise durum daha ciddi bir hal almaktadır. Bu tarz durumlarla karşılaşmamak için kullanılan yönlendirme protokolünün etkili olması gerekmektedir. Diğer bir deyişle kullanılan yönlendirme protokolünün bu tarz durumları göz önünde bulundurarak bir kontrol mekanizmasına sahip olması büyük önem taşımaktadır.

Araçsal tasarsız ağların diğer mobil ağlardan farklı olumlu özellikleri ise araçlarda enerji sorunu olmamasıdır. Haberleşme mekanizması aracın aküsüne bağlı olduğundan, bu sistemdeki araçlarda enerji kısıtı olmayacaktır.

Yönlendirme protokolünün tanımı yapılacak olursa, yönlendirme protokolü, iletişim yapmak isteyen iki aracın, iletişimi yaparken nasıl bir yol izleyeceğini belirler.

Yönlendirme protokolü, iletişim yolunun nasıl oluşturulacağı ve yönlendirme için gerekli kararların alınması, kurulan yolun devamlı aktif olması, kurulan yoldaki herhangi bir bozukluğun giderilmesi ile ilgilenir.

Araçsal tasarsız ağlardaki yönlendirme protokollerini iki ana başlık altında inceleyebiliriz. Örnek sınıflandırma aşağıdaki gibidir [9].



Şekil 2.5. Araçsal Tasarsız Ağlar için Önerilen Yönlendirme Protokollerinin Sınıflandırılması

2.1.1. Topoloji tabanlı yönlendirme protokolleri

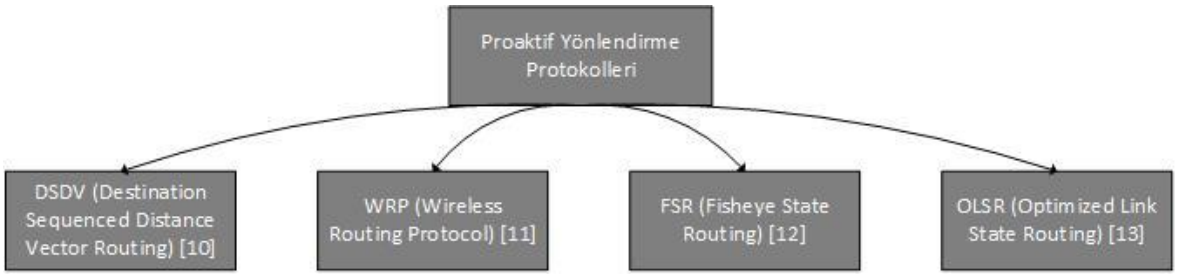
Bu tarz yapıyı kullanan yönlendirme protokolleri sistemde bulunan bağlantı durumlarına göre hareket ederler. Veri gönderimini sistemdeki bağlantı durumuna göre yaparlar. Topoloji tabanlı yönlendirme protokolleri ise Proaktif, Reaktif ve Melez olmak üzere üç başlık altında incelenebilirler.

Proaktif Yönlendirme Protokolleri

Bu tarz yönlendirme protokollerinde her düğümün kendi içinde bir tablosu vardır. Bu tablo içinde diğer düğümlerin bilgileri tutulur ve bu tablo sürekli olarak güncellenir. Bu yönlendirme protokollerinde tablonun güncel olabilmesi için düğümler sürekli olarak belli aralıklarla birbirlerine kontrol paketleri gönderirler. Kontrol paketleri düğümler arası bağlantının durumunu kontrol etmek amacıyla sistemdeki tüm düğümlere gönderilir. Sürekli gönderilen kontrol paketleri sayesinde herhangi bir paket gönderilmesi gerektiğinde yol keşfine gerek olmaz. Bu protokollerin avantajlarından biri de gerçek zamanlı uygulamalarda gecikme yaşamamasıdır.

Ancak tablonun sürekli güncel kalması gerektiğinden, düğümlerin işlem kapasitelerinin yüksek olması gerekmektedir.

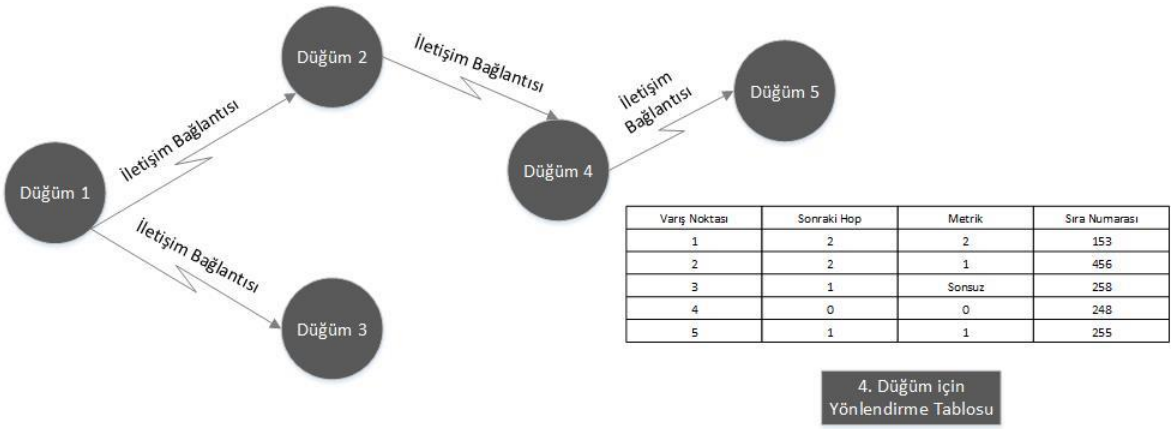
Şekil 2.6.'da kablosuz tasarsız ağlarda bulunan, örnek proaktif yönlendirme protokolleri verilmiştir.



Şekil 2.6. Örnek Proaktif Yönlendirme Protokolleri

DSDV (The Destination-Sequenced Distance Vector Routing) [10]

DSDV yönlendirme protokolünde [10], ağdaki her düğüm kendi içinde, bütün olası yolları, bir sonraki düğümü (next hop) ve hedef düğüm tarafından yaratılan sıra numarasını tutan bir tablo bulundurmaktadır. Düğümler, periyodik olarak ya da ağ topolojisi değiştiğinde, ağa, ağdaki düğümlerin tablolarını güncellemesi için, içinde yeni sıra numarası barındıran tablo güncelleme paketleri gönderirler. Bu sayede ağdaki değişimden bütün düğümler haberdar olmuş olurlar. Tablo güncelleme paketleri her yaratıldığında sıra numaraları bir yükseltilerek yayınlanır. Böylece paketi alan düğüm eski paket bilgilerini silmesi gerektiğini anlar. Ancak DSDV yönlendirme protokolündeki dezavantaj, ağdaki düğüm sayısı artınca güncelleme paketlerinin kontrolünün zor olmasıdır. Düğümler, tablo güncelleme paketlerini birbirlerinden bağımsız olarak, farklı zaman aralıklarında ağdaki düğümlere göndermektedir. Bu durumda ağdaki düğüm sayısı arttıkça, düğümlerin göndereceği tablo güncelleme paketleri de artacaktır. Bu sebeple, farklı zamanlarda, birden fazla tablo güncelleme paketi alan düğüm, sürekli olarak tablosunda bulunan sonraki düğüm (next hop) sıra numarasını değiştirmek zorunda kalacaktır. Sürekli sıra numarası değişmesi, ağda dalgalanma problemine sebep olacaktır. Hedef düğüm, en son sıra numarasını alsa da, çok fazla güncelleme paketi alacağı için, söz konusu düğüm sürekli işlem halinde olacaktır.



Varış Noktası	Sonraki Hop	Metrik	Sıra Numarası
1	2	2	153
2	2	1	456
3	1	Sonsuz	258
4	0	0	248
5	1	1	255

4. Düğüm için Yönlendirme Tablosu

Şekil 2.7. DSDV için Örnek Yönlendirme Tablosu

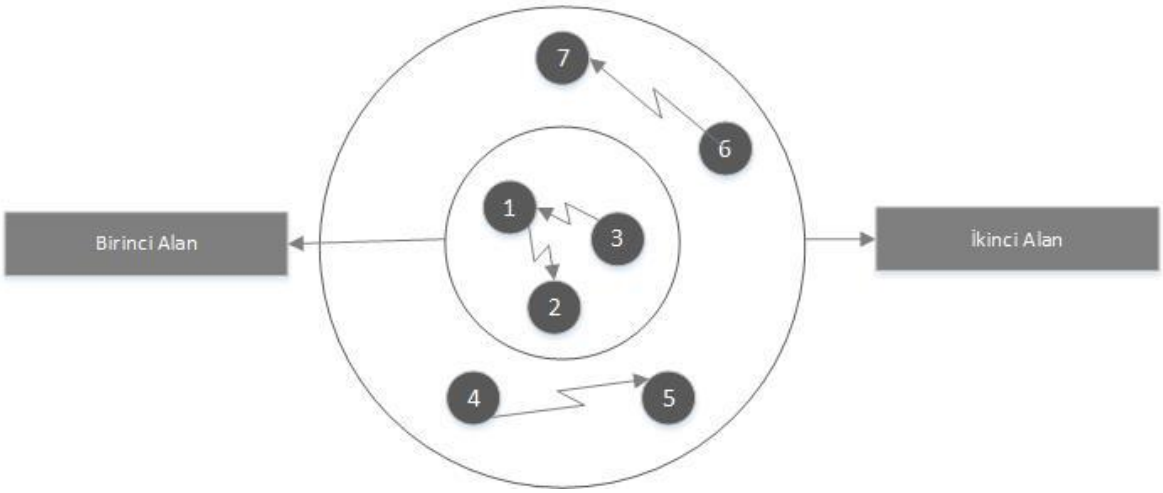
Şekil 2.7.'de DSDV protokolü için örnek bir yönlendirme tablosu verilmiştir bu tablo 4. düğümün yönlendirme tablosudur. Tabloda 4. düğümün komşuları ve bu komşulara kaç hopta ulaşabileceği gösterilmiştir. Örnek olarak 4. düğüm, 1. düğüme mesaj göndermek istediğinde ilk ulaşacağı düğüm, bir hop uzağındaki düğüm iki olacaktır. Tabloda bu durum Varış Noktası ve Sonraki Hop bölümünde sayısal olarak gösterilmiştir (Varış Noktası 1, Sonraki Hop 2, Metrik 2). Ayrıca düğümlerin tablosunda Sıra Numarası sütunu vardır. Sıra numarası protokolde varış noktası tarafından oluşturulur ve ağ içinde döngüyü önlemek amaçlıdır. Yeni bir mesaj gönderilmek istenildiğinde düğümler tablolarındaki en son sıra numarasını kullanırlar. İki tane aynı sıra numarası varsa, düğüm daha iyi metriğe sahip olan düğümü seçer ve iletim bu şekilde devam eder. Örnek vermek gerekirse, mesaj göndermek isteyen düğüme aynı sıra numaralı iki (örn. 180) güncelleme paketi gelirse, kaynak düğüm, hop sayısına göre karar verebilir. Hangi düğümün hop sayısı daha az ise, kaynak düğüm o düğümü seçecektir.

WRP (Wireless Routing Protocol) [11]

Kablosuz yönlendirme protokolü, DSDV yönlendirme protokolünün geliştirilmiş versiyonudur. WRP [11], DSDV gibi en güncel rota bilgilerini saklar. Bu algoritma DSDV'den farklı olarak, bünyesinde daha doğru bir veri iletimi sağlamak için birden fazla tablo tutar. Birden çok yönlendirme tablosu sakladığı için, bir düğüme olan en kısa yol bilgisini de saklar.

FSR (Fisheye State Routing) [12]

Bu protokolde de, diğer protokollerde olduğu gibi, her düğüm ağın topolojisini saklayan tablolara sahiptir. Her düğüm kendi yerel komşularına Hello mesajları göndererek ağ topolojisi hakkında bilgi sahibi olur. Her düğümde, benzer protokollerde olduğu gibi komşu listesi, ağ topolojisi tablosu, sonraki hop (next hop) tablosu bulunur. Düğüm sayısının fazla olduğu ağlarda güncelleme mesajlarının sayısını düşürmek için FSR [12] protokolü, tablosundaki her bir girdi için farklı mesaj periyodları kullanır, bir başka deyişle her bir girdi için farklı aralıklarla mesaj gönderir. Bu protokolün diğer protokollerden farkı, düğümlere göre ağ farklı genişliklere ayrılmıştır.Şekil 2.8.'de Fisheye State yönlendirme protokolünün basit bir şekli verilmiştir.Şekil 2.8.'de de görüldüğü gibi, ağ hop sayısına göre iki bölgeye ayrılmıştır. Burada birinci bölgedeki düğümler (1 hop uzağındakiler) 1., 2. ve 3. düğümler kendi ağlarında haberleşmektedirler. Ancak 1. düğüm 4.düğüme mesaj göndermek istediğinde, bunu yerel komşuları üstünden yani birinci alandaki düğümler üstünden yapacaktır. 4. düğüm 2. veya 3. düğümün yerel komşusu ise mesaj iletilecektir.



Şekil 2.8. Fish Eye State Yönlendirme Protokolü

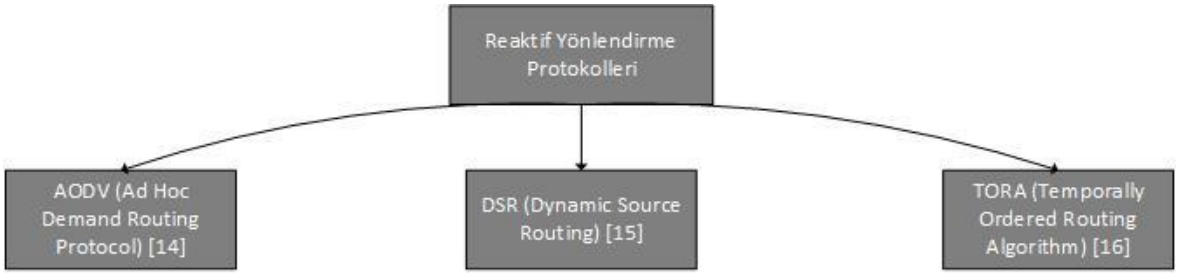
OLSR (Optimized Link State Routing) [13]

OLSR [13] yönlendirme protokolü, normal Link State yönlendirme protokolünün geliştirilmiş halidir. Bu protokolün geliştirilme amaçlarından bir tanesi, ağa gönderilen kontrol mesajlarının sayısını düşürmektedir. Kontrol mesajları bütün ağa gönderilmek yerine sadece seçilen düğümlere gönderilir. Bu düğümlere MPR (Multipoint relay) denir. Burada MPR, düğümün bir hop uzağındaki düğümü ya da düğümleri temsil eder. Bu seçim yapılma şartı şu şekilde açıklanabilir, eğer bir düğüm, diğer bir düğümü ya da düğümleri MPR olarak seçiyorsa, seçilen MPR düğüm ya da düğümler de, kendine bir hop uzağındaki düğümü, asıl düğümün iki hop uzağındaki düğümleri kapsamalıdır. Protokolün içindeki diğer bir özellik ise, yayın (Broadcast) mesajlarını sadece MPR seçilen düğümler yayınlar. Bu sayede diğer protokollere göre, ağda gönderilen yayın mesajlarının sayısı azalmakta ve dolayısıyla ağdaki yük miktarı azalmaktadır. Aynı şekilde, ağa gönderilen kontrol mesajları da MPR olarak seçilen düğümler tarafından gönderilir ve bu sayede kontrol mesajlarının ağa getirdiği yük de azalmış olur. Son olarak OLSR yönlendirme protokolünün getirdiği yenilik, bağlantı bilgilerinin sadece MPR seçilen düğümler ile o düğümleri MPR seçen düğüm arasında olmasıdır. Bu da, ağda bütün düğümlerin bağlantı bilgisini paylaşması yerine belirli düğümlerin bilgi paylaşmasını sağlar ve bu durum yine ağdaki yükü azaltır. Ancak OLSR yönlendirme protokolü bağlantı kopmalarına karşı herhangi bir mesaj üretmemektedir. Bu da sistemde bir bağlantı kopması durumunda sisteme herhangi bir mesaj gönderilmemesi demektir. Rota korumasının olmaması OLSR'in önemli dezavantajlarından birisidir.

Reaktif Yönlendirme Protokolleri

Bu tarz yönlendirme protokollerinin, proaktif yönlendirme protokollerinden farkı herhangi bir paket üretildiğinde yol keşfinin önceden yapılmamış olmasıdır. Adından da anlaşılabileceği gibi, yol keşfi talep üzerine gerçekleştirilir. Paket üretilir ve yol keşfi paket üretildiği zaman yapılır. Bu yönlendirme protokolünün amaçlarından biri proaktif yönlendirme protokollerinde tabloda tutulan gereksiz ve kullanılmayan yolların bilgisini ortadan kaldırmaktır. Reaktif yönlendirme protokolü bu yönden avantaj sağlasa da, paket oluşturulduktan sonra yol keşfi için gönderilen kontrol paketleri, dolayısıyla yolun oluşturulması, veri paketlerinin iletiminin gecikmesine

neden olacaktır. Şekil 2.9.'da mobil tasarsız ağlarda bulunan popüler reaktif yönlendirme protokollerine bir örnek gösterilmektedir.



Şekil 2.9. Örnek Reaktif Yönlendirme Protokolleri

AODV (Ad Hoc On Demand Routing Protocol) [14]

Yönlendirme protokollerinde, iki çeşit yönlendirme vardır: Tek yönlü yönlendirme ve çok yönlü yönlendirme. Tek yönlü yönlendirmede tek bir mesaj gönderici ve tek bir mesaj alıcı vardır. Çok yönlü yönlendirmede ise tek bir mesaj gönderici vardır, ancak mesajı alan birden fazla alıcı vardır. AODV [14] yönlendirme protokolü hem tek yönlü yönlendirmeye hem de çok yönlü yönlendirmeyi destekleyen bir protokoldür. AODV protokolünde ağdaki her yolun bir ömrü vardır. Belirlenen süre içinde yol kullanılmazsa o yol ağdan kaldırılır.

AODV protokolünde yol keşfi için iki tür mesaj (RREQ ve RREP), yol onarımı için ise bir tür mesaj (RERR) tanımlanmıştır;

- Yol İstek Paketleri (*Route Request (RREQ)*)
- Yol Cevap Paketleri (*Route Reply (RREP)*)
- Yol Hata Paketleri (*Route Error (RERR)*)

AODV protokolünde yol keşfi sırasında keşfedilen yolların listesini tutmak için sıra numarası kullanılır (*Sequence Number*). Yeni mesaj göndermek isteyen araç, yeni bir sıra numarası kullanarak mesajını gönderir.

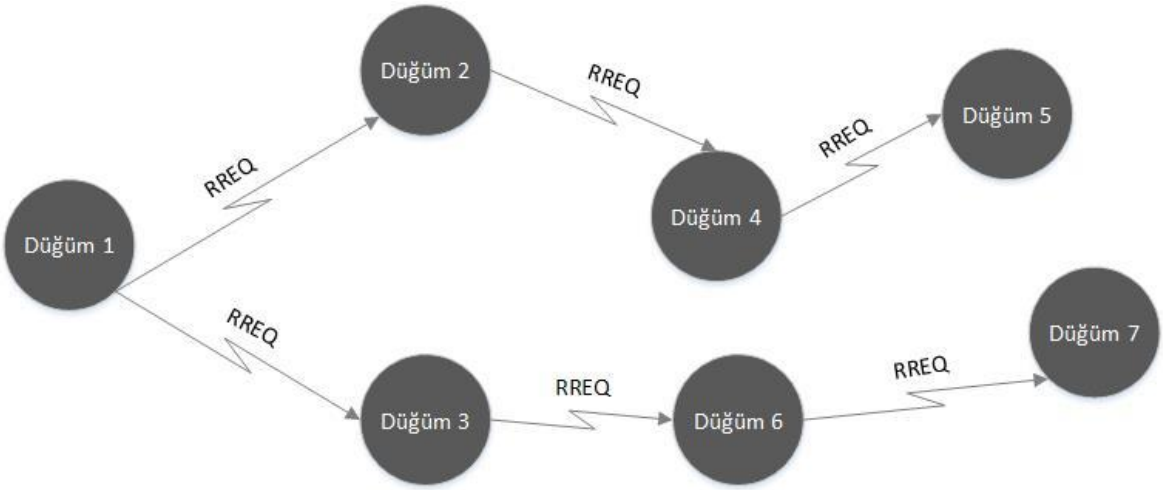
A aracı F aracına mesaj göndermek istediğinde ilk önce kendi tablosunda F aracına herhangi bir yol olup olmadığına bakar. Eğer A'nın tablosunda F aracına ait bir yol yoksa A aracı ağa Yol İstek Paketi (*RREQ*) gönderir. Bu paketi F aracına özel olarak yaratacağından gönderdiği pakete kendi IP adresini ve göndereceği aracın IP

adresini ekler. Bunun yanında A kendi sıra numarasını (*Sequence Number*) ve A'nın, F aracı ile ilgili bildiği F'in en son sıra numarasını gönderir. Son olarak mesaj göndermek isteyen A, bir yayın numarasını da mesaja ekler (*Broadcast ID*). A her Yol İstek Paketi göndermek istediğinde yayın mesajındaki yayın numarasını bir arttırır. Böylelikle yayın mesajlarının güncelliği kontrol edilebilir.

A'nın yayınladığı Yol İstek Paketini alan araçların (örneğimizde C) ilk olarak bakacağı durum, bu Yol İstek Paketi'ni daha önce alıp almadığıdır. Ağdaki araçlar, kendilerine gelen Yol İstek Paket'lerini saklarlar ve bünyelerindeki paketlerle, aldıkları paketleri karşılaştırırlar. Eğer paketi alan C, bu Yol İstek Paketi'ni daha önce görmüşse, paketi dikkate almaz ve düşürür.

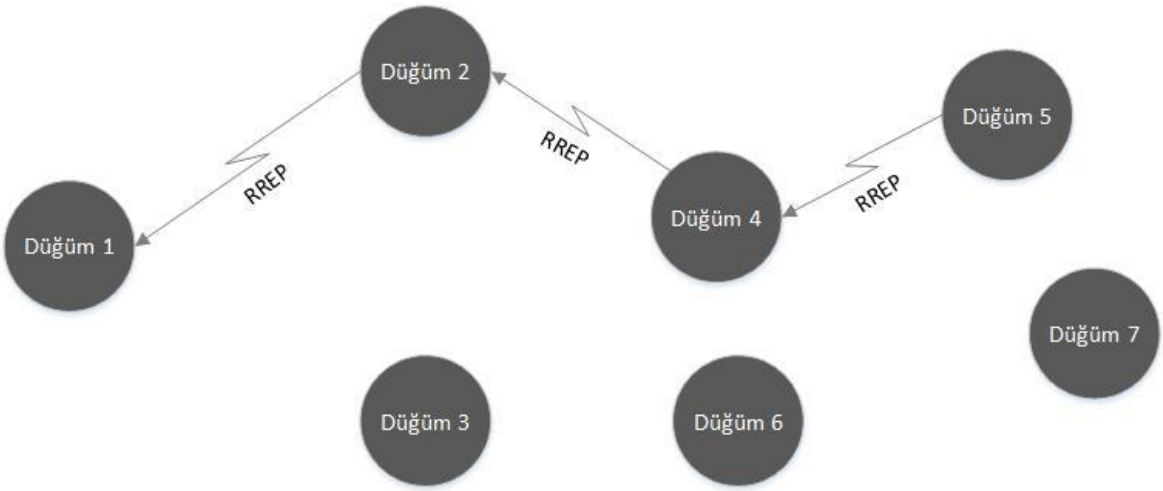
C aracı paketi ilk defa gördüyse, kendi tablosuna kendi konumundan A konumuna ulaşılabilecek şekilde bir tersine yol (*Reverse Route*) girdisi girer. Bu girdinin içinde A'nin IP adresi, A'nın hali hazırdaki sıra numarası, A'ya giderken ne kadar araç geçtiği (*Hop Count*) ve C'nin Yol İstek Paketini aldığı komşusunun IP adresi vardır. Tabloya girilen girdilerin önceden belirlenmiş bir yaşam süresi vardır. Yukarıda da bahsedildiği gibi, yaşam süresi dolan girdi tablodan silinir ve geçerliliğini kaybeder.

C aracının yönlendirme tablosunun içinde F aracı için henüz yaşam süresi dolmamış bir girdi varsa A'nın gönderdiği Yol İstek Paketi'ne cevap döner. C'nin Yol İstek Paketi'ne cevap dönmesinin diğer bir şartı ise, C'nin tablosundaki F için sakladığı sıra numarasının, C'nin A'dan aldığı Yol İstek Paketi'ndeki sıra numarasından daha küçük olmamasıdır. Bu sayede sistemde herhangi bir döngü oluşması da engellenmiş olur. Yol İstek Paket'ini alan C bu durumları sağlıyorsa A'ya Yol Cevap Paketi döner. Eğer C Yol Cevap Paketi dönemeyecek durumdaysa Hop sayısını bir arttırarak Yol İstek Paketi'ni komşusuna iletir. Aynı işlemler, varış düğümüne ulaşıncaya dek ana düğümler tarafından tekrar edilecektir. Yol İstek Paketinin kaybolduğu durumlarda ise A, tekrar Yol İstek Paketi oluşturup ağdaki komşularına gönderecektir.



Şekil 2.10. AODV'de RREQ Paketlerinin Gönderimi

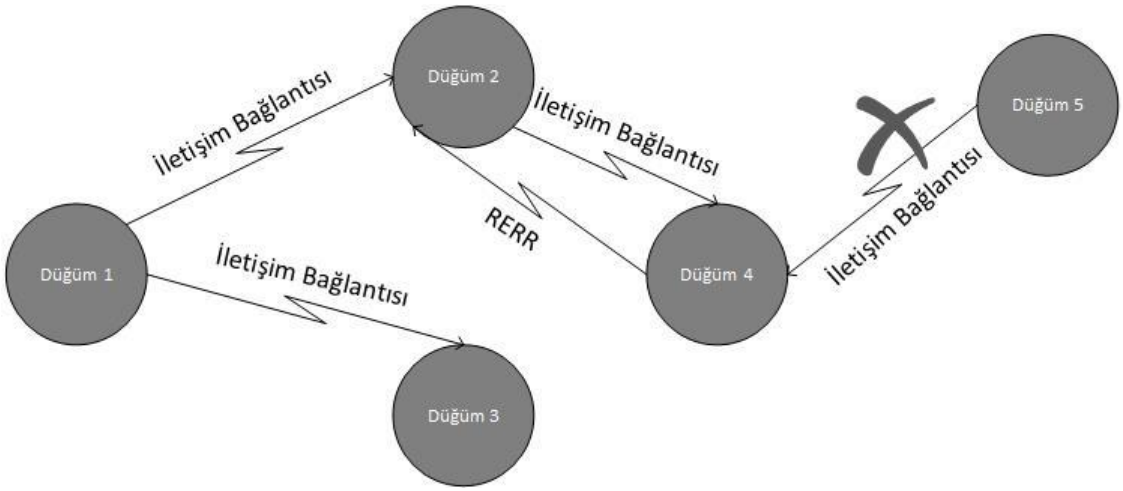
Şekil 2.10.'da AODV'de yol keşfine bir örnek verilmektedir. Bu örnekte 1. düğüm, 5. düğüme mesaj göndermek istemektedir ancak 5. düğüme ulaşılacak yolu bilmediği için ağa RREQ paketleri göndermektedir. RREQ paketi alan diğer düğümler, kendileri hedef düğüm değillerse, RREQ paketi göndermeye devam ederler. Düğüm 5 RREQ paketi aldığında kendisi hedef düğüm olduğu için kendisinden bir önceki düğüme (RREQ aldığı en son düğüme: Düğüm 4) RREP mesajı gönderir.



Şekil 2.11. AODV RREP Paketleri ile Yolun Kurulması

Şekil 2.11.'de 5. düğümün kendisine RREQ mesajının geldiği en kısa yoldan RREP mesajını gönderdiği gösterilmiştir. RREP mesajı alan düğümler, kendilerinden bir önceki düğümlere RREP mesajı dönerler. RREP mesajı düğüm 1'e ulaştığında, veri paketleri gönderilmeye başlanır. Bu durumda, veri paketleri 1-2-4. düğümler üzerinden 3 hop ile 5. düğüme ulaşacaktır.

AODV protokolünün kullandığı bir diğer mesaj türü de Yol Hata Paketleri'dir. Bu mesaj paketi ağda bir hata meydana geldiğinde ilgili diğer düğümlere gönderilmektedir. Yol Hata Paketleri'nin amacı sistemdeki artık aktif olmayan ve yaşam süresi dolmuş yolları sistemden çıkarmaktır. Şekil 2.12.'de görüldüğü üzere, düğüm 4 ile düğüm 5 arasındaki iletişim bağlantısının kopması durumunda, düğüm 4 komşu düğümlerine RERR mesajı göndererek kendi üzerinden 5. düğüme ulaşılamayacağını bildirir.



Şekil 2.12. AODV'de Yol Tamirleri

DSR (Dynamic Source Routing) [15]

Dynamic Source Routing algoritması, AODV algoritmasına benzer olarak istek üzerine yol keşfi yaparak paket iletimini gerçekleştirir. DSR [15] algoritması, AODV algoritmasından farklı olarak kaynak yönlendirme mekanizmasını kullanmaktadır. AODV paketin gideceği noktayı her düğümde tablodan öğrenmektedir, ancak DSR yol keşfi sırasında gönderilen paket içerisinde gidilecek yolu saklamaktadır. Her düğüm, bu yolları saklayarak herhangi bir paket iletimi olacağı zaman kullanmaktadır. Bu algoritmanın avantajı, tablo tabanlı algoritmalarda kullanılan tablo güncelleme mesajlarının kullanılmıyor olmasıdır. Dezavantajı ise yol bilgileri güncellenmediğinden, sistemde tutarsızlıklar oluşabilmektedir. Diğer bir dezavantajı ise yol için bağlantı kurulma süresinin tablo tabanlı algoritmalara göre daha yavaş

olmasıdır. Algoritma, düğüm sayısının az olduğu ağlarda düzgün çalışsa da, düğüm sayısının fazla olduğu, yoğun ağlarda yüksek bir başarım göstermemektedir.

TORA (Temporally Ordered Routing Algorithm) [16]

TORA [16] yönlendirme protokolü, dinamik ağlarda kontrol mesajlarının fazla sayıda olmasını engellemek için geliştirilmiş bir algoritmadır. TORA yönlendirme protokolü, diğer yönlendirme protokollerinin aksine, kaynak düğümden hedef düğüme olan en kısa yol mantığını kullanmaz. Bunun yerine TORA yönlendirme algoritması bir sonraki düğümün bilgisini saklar. Bu sayede kaynak düğümün paketi göndermek için, düğüm olarak, birden fazla ihtimali vardır. Bunun haricinde TORA yönlendirme protokolü, sadece kaynak düğüm hedef düğüme mesaj göndermek istediğinde düğümlerin yol oluşturmasına izin verir. Bu protokol 3 şekilde ağı kontrol eder:

- Hedef düğümden kaynak düğüme yol oluşturma,
- Oluşturulan yolu denetleme,
- Geçersiz yolları silme.

Protokolün dezavantajlarından birisi ölçeklenebilir olmamasıdır.

Melez Yönlendirme Protokolleri

Bu protokolü kullanan yönlendirme protokolleri, hem proaktif yönlendirme protokolünün özelliklerini hem de reaktif yönlendirme protokolünün özelliklerini kullanır.

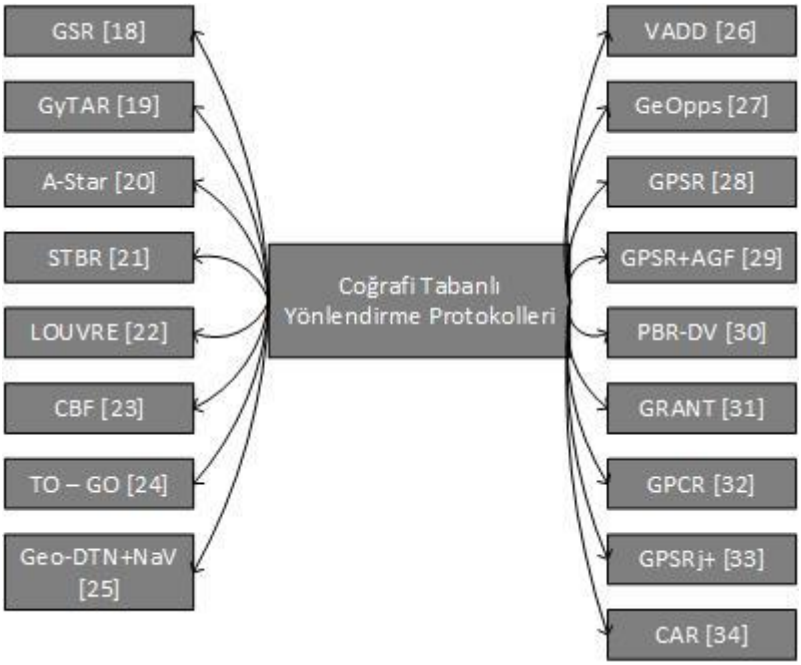
ZRP (Zone Routing Protocol) [17]

İki farklı yönlendirme algoritmasını bir arada barındıran bir protokoldür. Bu nedenle melez (Hybrid) yönlendirme protokolü olarak adlandırılır. Bu protokolde ağ bölgelere ayrılır ve gönderilecek mesaja göre hangi algoritma tipinin kullanılacağına karar verilir. Gönderilecek olan paket aynı bölge içindeyse, proaktif bir yönlendirme protokolü kullanılarak, mesaj gönderilmek istenen düğüme gönderilir. Mesaj gönderen ve mesajı alacak olan düğüm aynı bölgede olacağı için tekrar bir yol keşfine gerek olmayacaktır. Mesajı alacak olan düğüm, mesajı gönderecek olan düğümle aynı bölgede değilse, yol keşfi gerekeceği için reaktif bir yönlendirme protokolü kullanılacaktır.

2.1.2. Coğrafi Tabanlı Yönlendirme Protokolleri

Araçsal tasarsız ağlar için kullanılan bir diğer tür yönlendirme protokolü ise coğrafi tabanlı yönlendirme protokolleridir. Bu protokol, diğer protokollerden farklı olarak araçlarda herhangi bir yönlendirme tablosu saklamaz. Bu protokolde, adından da anlaşılacağı gibi her düğüm kendi pozisyonu GPS yardımıyla bilmektedir. Mesaj gönderilmek istenildiğinde yol bilgisi, araçlarda bulunan GPS sinyalinden alınmaktadır. Bu tarz algoritmaların avantajı diğer yönlendirme protokollerinde olduğu gibi herhangi bir tablo, ya da yol keşfi için ekstra bir mesaj gönderimi gerçekleştirmemesidir. Diğer bir avantajı ise, bu protokollerin ölçeklenebilir olmasıdır. Kaynak düğüm, hedef düğüme mesaj göndermek istediğinde, topoloji tabanlı protokollerde olduğu gibi yol oluşturma işlemleri gerçekleşmeyecektir, bu durum sayesinde düğümlerin bünyelerinde, herhangi bir tablo saklama ihtiyacı da olmayacaktır. Sonuç olarak kontrol paketlerinin hazırlanması için geçen hazırlık süresi, coğrafi tabanlı protokollerde ortadan kalkmış olacaktır.

Bu sınıftaki protokollere örnek, Şekil 2.13.'te verilmiştir.



Şekil 2.13. Örnek Coğrafi Tabanlı Yönlendirme Protokolleri

GPSR (Greedy Perimeter Stateless Routing) [28]

GPSR yönlendirme protokolü [28], diğer yönlendirme protokollerinin aksine düğümlerin coğrafi konumlarını dikkate alarak yönlendirmeyi yapmaktadır. Algoritmada bütün düğümlerin GPS ile kendi pozisyonlarını bildiği varsayılmaktadır. Yönlendirme protokolünde her düğümün sinyal alanı, bir başka deyişle kapsama alanı vardır ve paket iletimini bu kapsama alanı içinde gerçekleştirir. GPSR yönlendirme protokolündeki düğümler birbirlerine belirli aralıklarla yayın mesajları (beacon) göndererek yerlerini haber verirler. Her düğüm sadece kendi komşularının yerlerini bilmektedir. Bu da GPSR yönlendirme protokolünü diğer protokollerden (topoloji tabanlı) ayıran önemli özelliklerdendir. GPSR yönlendirme protokolünde, kaynak düğümün, sadece hedef düğümü ve bir hop uzağındaki (next hop) düğümü bilmesi yeterli olacaktır. GPSR yönlendirme protokolü iki farklı yöntemle mesaj iletimini gerçekleştirmektedir. Bunlardan bir tanesi Aç Gözlü Yönlendirme (*Greedy Forwarding)*, diğeri ise Çevresel Yönlendirme'dir *(Perimeter Forwarding).*

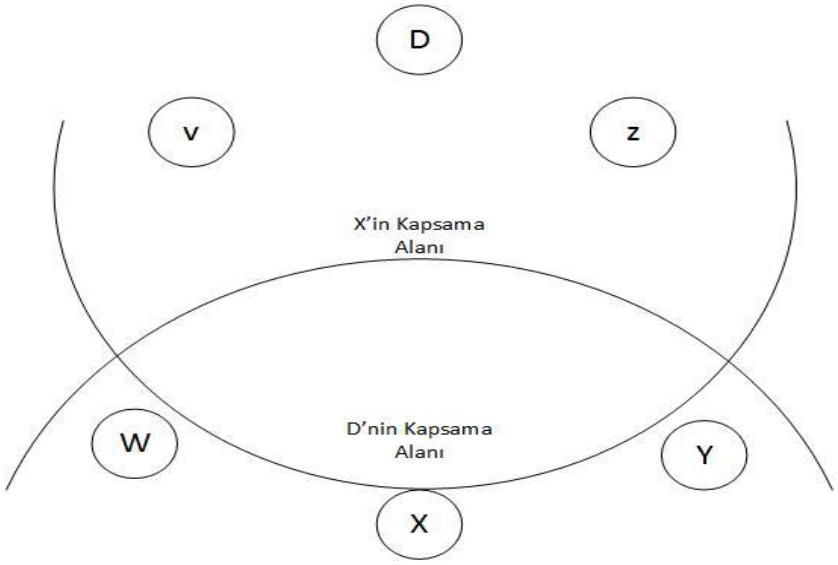
Aç Gözlü Yönlendirme (Greedy Forwarding)

Sistemde mesaj göndermek isteyen düğüm, mesajı yayınlarken mesajın içine hedef düğümün adresini yazarak yaratır. Mesajı alan düğüm, komşularının içinden coğrafi olarak hedef düğüme en yakın olan düğüme paketi göndermektedir. Bu işleyiş paket hedef düğüme ulaşana kadar devam etmektedir. Aç Gözlü Yönlendirme'nin en büyük avantajlarından birisi, mesaj gönderecek düğümün sadece en yakın düğümün coğrafi yerini bilmesinin yeterli olmasıdır. Fakat Aç Gözlü Yönlendirme seçeneğinin her zaman çalışmadığı durumlar vardır. Bazı topolojilerde paketin geçici olarak hedef düğümden daha uzağa gönderilmesi gerekebilir. Bu, Aç Gözlü Yönlendirme seçeneğine ters düştüğü için GPSR'da bu durumda Çevresel Yönlendirme seçeneği devreye girmektedir.

Çevresel Yönlendirme (Perimeter Forwarding)

Çevresel Yönlendirme seçeneği, Aç Gözlü Yönlendirme seçeneğinin başarısız olduğu zaman devreye girmektedir. Bu seçenek, paket gönderen düğümün kapsama alanında, hedef düğüme yakın olan hiçbir düğümün bulunmadığı durumda devreye girer. Düğüm, ağa çizge gibi davranıp, paket iletimini bu şekilde

gerçekleştirir. GPSR'da mesaj yaratılırken, iki seçenekten biri mesajın içine yazılarak yaratılır. Mesaj iletimi sırasında Aç Gözlü Yönlendirme ya da Çevresel Yönlendirme seçenekleri arasında geçiş yapabilir. Yukarıda belirtildiği gibi Aç Gözlü Yönlendirme'nin gerçekleştirilemediği durumda Çevresel Yönlendirme devreye girer. Mesajın Çevresel Yönlendirme'ye geçtiği noktada mesaj içine, mesajın hangi noktada Çevresel Yönlendirme'ye girdiği, bir başka deyişle hangi noktada Aç Gözlü Yönlendirme'nin başarısız olduğu kaydedilir. Bu noktadan sonra düğüm sağ el kuralına göre (*Right Hand Rule*) düğümleri gezerek (*Traverse*) iletimi gerçekleştirmeye çalışır. Burada ağa, bir çizge gibi davranılır. Örnek vermek gerekirse, düğümlerin sinyal güçlerine *r* (kapsama alanı), örnek düğümlere de *a* ve *b* dersek, eğer *a* ve *b* düğümleri arasında bu iki düğüme birbirlerinden daha yakın bir *x* düğümü yoksa, *a* ile *b* (Edge) birleşiktir denebilir. Mesaj hedef düğüme iletilene ya da Aç Gözlü Yönlendirmeye dönene kadar, mesaj iletimi saat yönünün tersine doğru devam eder.



Şekil 2.14. GPSR Çevresel Yönlendirme Örnek [28]

Şekil 2.14.'te GPSR yönlendirme protokolünün hangi durumda çevresel yönlendirmeye düştüğü gösterilmiştir. Şekil üstünde görüldüğü gibi X, Y->Z->D yolunu seçebilecekken protokol mantığı gereği X burada D' ye olan uzaklığında yerel maksimum olmakta ve çevresel yönlendirmeye geçmektedir [28].

3. ARAÇSAL TASARSIZ AĞLARDA GÜVENLİK

Araçsal tasarsız ağlar her ne kadar araçlar arasında haberleşmeyi sağlayıp hem trafik güvenliğini, hem de sürüş konforunu arttırsa da, bu ağların güvenlik problemleri de bulunmaktadır. Bu bölümde, bu ağların güvenlik gereksinimleri tartışılmaktadır.

3.1. Araçsal Tasarsız Ağların Güvenlik Gereksinimleri

Araçsal tasarsız ağlar mobil ağlardan farklı oldukları için, güvenlik gereksinimleri de farklıdır. Bu gereksinimlerden herhangi biri eksik olduğunda sistem saldırılara daha açık hale gelecektir. Araçsal tasarsız ağlardaki güvenlik gereksinimlerini şu şekilde belirtebiliriz [4];

Şekil 3.1. Araçsal Tasarsız Ağların Gereksinimleri

3.1.1. Kimlik Doğrulama (Authentication)

Ağdaki araçlar, çok yüksek hızda veya düşük hızda hareket edebilirler, bu yüzden mesajlaşmanın hızını tahmin edebilmek mümkün olmamaktadır. Bu durumda hangi aracın ağ içinde olup hangi aracın ağ dışında olduğunu tahmin etmek için araçların hepsinin kimlik doğrulamasının yapılması gerekmektedir. Ağa giren her araç, ağ tarafından tanınmalıdır. Ağa girmeyen herhangi bir aracın mesaj göndermesine veya almasına izin verilmemelidir. Kimlik doğrulaması olmadan ağa giren bir araç

gerçek olmayan mesajlar gönderebilir ve ağa zarar verebilir. Bu nedenlerden dolayı ağa giren her aracın kimlik doğrulaması yapılması zorunludur.

3.1.2. Yetki (Authorization)

Sisteme giren araçların neler yapıp neler yapamayacağını belirleyen bir gereksinimdir. Araçların ne tür mesajlar gönderip ne tür mesajlar alacağı, hangi yönlendirme protokolü ile mesaj göndereceği tarzı yetkiler ağ tarafından araçlara bildirilmelidir. Ağda bir bütünlük olması açısından önemlidir.

3.1.3. Veri Tutarlılığı (Data Integrity)

Ağa gönderilen mesajların doğruluğu takip edilmelidir. Mesaj gönderen aracın doğru bilgiyi verip vermediği önemlidir. Buradaki veri tutarlılığı kimlik doğrulama ile ilişkili değildir. Kimliği doğrulanan araçlar her zaman doğru mesaj göndermeyebilir, diğer bir deyişle kimliği doğrulansa bile iç saldırganlar her zaman olabilir. Gönderilen mesajların zaman ve mekan açısından tutarlı olması gereklidir.

3.1.4. Gizlilik (Confidentiality)

Ağda bulunan araçların birbirleriyle yol, trafik, acil durum gibi bilgileri paylaşması gerektiği için ağda bulunan bütün araçların bütün mesajlara ulaşması gerekmektedir. Bu yüzden sistemde herhangi bir bilgi gizliliği, şifreleme vb. uygulamaya gidilmesine gerek yoktur. Ancak gelen mesajların kimlik doğrulaması yapılmış araçlardan geldiğinden emin olunmalıdır.

3.1.5. İçerik Değişimi (Data Alteration)

Ağda gönderilen mesajların gönderileceği yere kadar değişmeden gitmesi gerekmektedir. Mesaj göndermek isteyen araçtan gönderilmek istenen araca gidene kadar mesaj değişebilir ve bu da istenmeyen durumlar ortaya çıkarabilir. Bu nedenle ağdaki mesajların bütünlüğü önemlidir. Buradaki içerik değişiminin veri tutarlılığından farkı, veri tutarlılığında ilk mesajı yaratan aracın doğru mesaj yaratıp yaratmaması sorunken, içerik değişiminde araçtan araca iletilen mesajın herhangi bir araç tarafından değiştirilmemesidir.

3.1.6. Erişilebilirlik (Accesibility)

Araçsal tasarsız ağlar gerçek zamanlı ve hareketliliğin yüksek olduğu bir ağ çeşidi olduğundan sürekli mesajlaşma ve bir iletişim olacaktır. Bu yüzden araçlar için ağın her zaman erişilebilir olması gerekmektedir. Değişken topolojiye sahip bir ağ olduğu için araçlar arasında iletişim ağlarının sürekli açık olması gerekmektedir. Herhangi bir saldırı durumunda araçların haberleşememesi istenmeyen durumları ortaya çıkarabilir.

3.1.7. İnkar Edememe (Non Repudiation)

Ağda, mesajların sayısını tahmin etmek mümkün değildir ve mesajlaşmada herhangi bir sınır yoktur. Ağda mesaj gönderen herhangi bir araç, sonradan bu mesajı göndermediğini iddia edemez. Herhangi bir kazada ya da sorunda mesajı gönderen aracın kolayca belirlenebilmesi gerekmektedir.

3.1.8. Mahremiyet (Privacy)

Araçlar arasındaki mesajların gizliliği gerekli değilken, araçları kullanan şahısların kimliklerinin açığa çıkmaması çok önemlidir. Ağa bağlanan araçların şoförleri kimliklerini ve kişisel bilgilerini açığa çıkarmak istemezler. Ayrıca herhangi bir aracın nereye gittiği, nasıl bir yol izlediği de mahremiyete girmektedir.

3.1.9. Anonimlik (Anonymity)

Araçlar sisteme kendilerini tanıtmak zorundadır, ancak ağ içindeki araçlara kendilerini tanıtmayabilirler. Bu durum yukarıda bahsedilen gizlilikten farklı olarak araçların kendi içlerinde bilgilerini saklamasıyla ilgilidir.

3.1.10. Gerçek Zaman Kısıtlaması (Real Time Constrained)

Araçsal tasarsız ağlardaki en önemli konulardan biri sistemin gerçek zamanlılığının sürdürülebilir olmasıdır. Burada gerçek zaman kısıtlaması olan bir olayın hemen gönderilip işlenmesi olarak açıklanabilir. Tarihi geçmiş bir olayın, özellikle trafikte, bir etkisi olmayacaktır. Tarihi geçmiş bilgilerin ağdan kaldırılması ya da tarihi geçmiş

bir bilginin tekrar gönderilmesine engel olunması gibi önlemlerin ağ tarafından sağlanması gerekmektedir.

3.2. Araçsal Tasarsız Ağlardaki Güvenlik Sorunları

Mobil tasarsız ağlar, kablolu bilgisayar ağlarından farklı güvenlik sorunlarını da beraberinde getirmiştir [35,36]. Açık alandaki araçların batarya sorunu, taşınabilmeleri, sabit bir noktanın olmaması gibi sorunlar, bu araçlara yapılan saldırılara karşı alınacak önlemleri de zorlaştırmaktadır. Mobil tasarsız ağlarda araçların çalışmasını engelleyecek, geciktirecek veya bilginin yanlış gönderilmesini sağlayacak şekilde saldırılar yapılmaktadır. Aynı durum araçsal tasarsız ağlarda da geçerlidir. Bu ağ tipinde, araçların hareketli olması sonucunda ağdaki araçlar, saldırılara çok daha fazla maruz kalmakta ve bu saldırıların sonucunda onarılması imkânsız sonuçlar ortaya çıkmaktadır.

Saldırı yapan saldırgan araçlar tek başlarına ya da ekipçe çalışabilirler. Tek aracın yaptığı saldırı limitli olsa da, saldırgan araçların bir arada yaptıkları saldırılar daha kötü sonuçlar doğurabilir. İki veya daha fazla saldırgan aracın yapacağı saldırı, araçların birlikte hareket ederek tek bir araç ya da RSU seçerek, ona karşı birlikte yönlendirecekleri saldırı şeklinde olacaktır.

Saldırıyı gerçekleştiren araçlar, saldırıyı bilgi edinmek amacı ile ya da sadece sisteme zarar vermek için yapabilirler. Bu saldırı çeşidini aktif ve pasif olarak ikiye ayırabiliriz. Saldırı yapan zararlı araçların saldırıları doğrudan bir düğümü ya da ağı kullanılamaz hale getirmek şeklinde olabilir, örneğin zararlı bir düğüm tek bir düğüme ya da RSU'ya direkt saldırı düzenleyebilir (örn. Hizmet Engelleme Saldırısı). Bu şekil yapılan saldırılar doğrudan sistemi kullanılamaz hale getirmek için yapılan saldırılar olduğu için aktif olarak değerlendirilebilir.

Pasif saldırıda ise zararlı araç ya da araçlar, saldırı yapacağı araca doğrudan saldırmayıp, saldırısını aracı takip ederek aracın gittiği yoldan, davranışlarından bir yorum çıkararak yapabilir [4]. Bu durumda saldırı yapacağı aracı sessiz bir şekilde dinleyip takip edeceği için bu tarz saldırıların tespiti imkansızdır.

Araçsal tasarsız ağlarda, saldırılar ikinci bir sınıflandırma yöntemi ile araç içi saldırı ve araç dışı saldırıdır. Ağa bağlanan araçlar, birbirleriyle haberleşebildiği için

birbirlerinden yol durumu, trafik durumu gibi bilgileri alabilirler. Saldırgan olan araçlar, bu bilgileri alarak diğer araçları yanlış yönlendirerek saldırılarını gerçekleştirebilirler.

Araç içi saldırılar ise aracın OBU (On Board Unit) sistemine yapılan modifikasyonlardır. Örneğin saldırgan, saldırı yapacağı aracın GPS sistemini yanıltarak, GPS'ten gönderilen veriyi yanlış göndererek saldırısını gerçekleştirebilir.

Araçsal tasarsız ağlarda araçların yüksek hızda hareket etmesi saldırıların tespitini güçleştirmektedir. Bu, saldırganın hareketlilik ile kendini gizleyebilmesinden kaynaklanmaktadır.

3.3. Araçsal Tasarsız Ağlardaki Saldırılar

Araçsal tasarsız ağlar, mobil tasarsız ağlardan farklı bir yapıya sahiptir. Mobil tasarsız ağlardan en büyük farkı düğümlerin daha yüksek hızlarda hareket etmesidir. Ancak mobil tasarsız ağlardaki güvenlik açıkları araçsal tasarsız ağlarda da devam etmektedir. Mobil tasarsız ağlardaki saldırı çeşitleri araçsal tasarsız ağlarda da gerçekleştirilebilmektedir. Bunun yanında, araçsal tasarsız ağlara özgü yeni saldırı çeşitleri de bulunmaktadır.

Bu bölümde araçsal tasarsız ağlara karşı yapılabilecek saldırılar açıklanmıştır. Bu saldırılardan bazıları mobil tasarsız ağlara da uygulanabilir fakat etkileri daha farklı olacaktır.

3.3.1. Kimlik Değiştirme Saldırısı (Sybil Attack)

Kimlik Değiştirme Saldırısı, araçsal tasarsız ağlardaki saldırılar içindeki en tehlikeli saldırı olarak değerlendirebilir. Bu saldırıda, saldırgan düğüm birden fazla düğümmüş gibi davranabilir. Sisteme giren her araca bir kimlik verildiği için, ağa bağlanan araçların yalnızca bir kimliği olmaktadır [37]. Kimlik değiştirme saldırısında, saldırgan araç diğer araçların da kimliklerine ulaşarak diğer araçların kimliklerini kendinde toplayarak ağa mesaj gönderebilir [38].

Bu durumda diğer araçların, gelen mesajın bir arabadan mı yoksa birden fazla arabadan mı geldiğini anlaması mümkün olmamaktadır. Bu saldırıdaki asıl amaç saldırgan aracın ağı şekillendirmesidir. Bu saldırı türü, tespit edilmesi en zor

saldırılardan biridir. Ayrıca saldırgan araç, GPS sistemini de yanıltarak, kendini birden fazla pozisyondaymış gibi gösterebilir, ya da herhangi bir kazayı başka bir yerde gerçekleşmiş gibi gösterebilir. Bu tür bir saldırı sistemde ölümcül sonuçlar doğurabilir.

Kimlik Değiştirme Saldırısı altında sınıflandırabileceğimiz bir saldırı türü de Araç Taklit Etme Saldırısıdır (*Node Impersonation Attack*) [39]. Sisteme bağlanan her aracın kendine özel bir kimliği bulunmaktadır. Diğer araçlarla haberleşmek isteyen bir araç, bu kimliği kullanarak haberleşmeyi gerçekleştirir. Bu saldırı türünde saldırgan araç, kendi kimliğini sisteme haber vermeden değiştirebilir. Bu durumda sistem, saldırgan olan düğümü başka bir araçmış gibi görecek ve asıl saldırganın kimliğini bilemeyecektir.

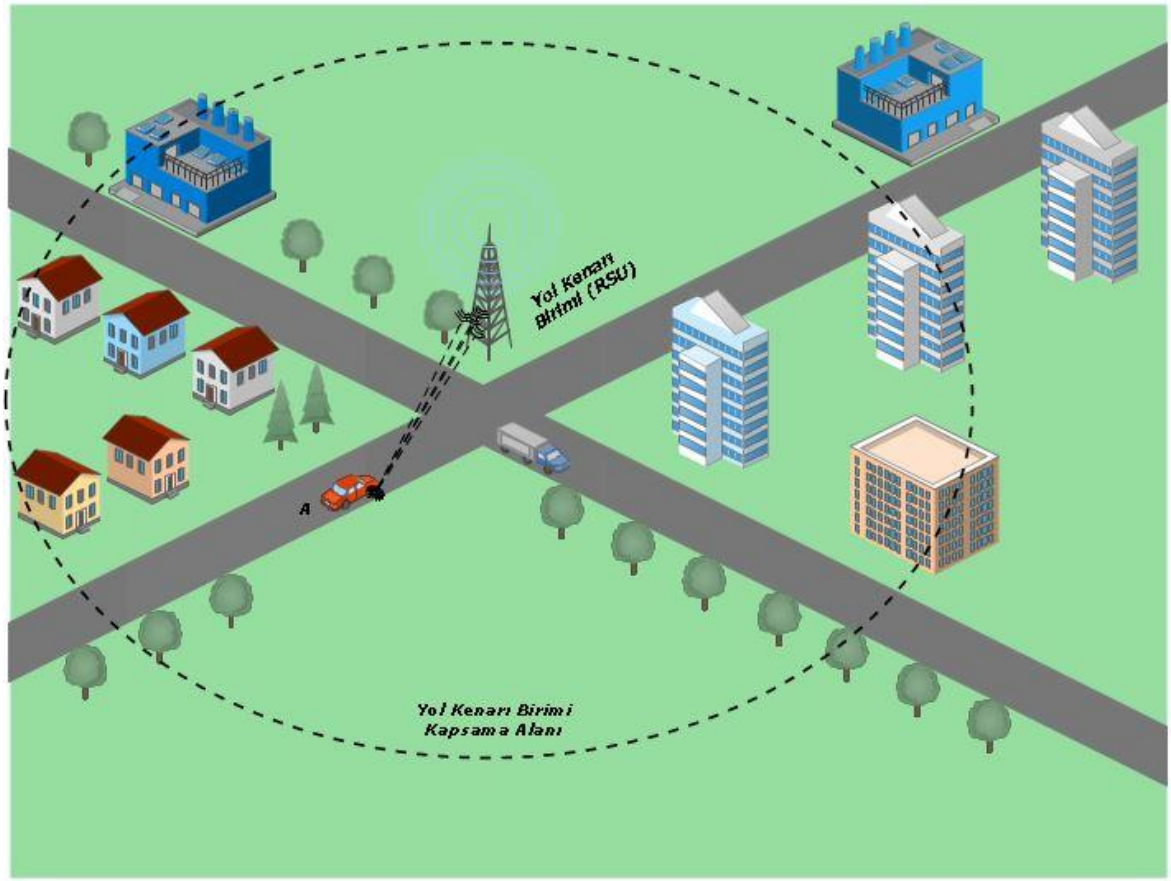
Şekil 3.2. Sybil Saldırısı

Şekil 3.2.'de kimlik değiştirme saldırısının bir örneği gösterilmektedir. Burada A aracı, B ve D araçlarının kimliklerini çalarak C aracına onların yerine mesaj gönderebilir. Yani A aracı birden fazla araçmış gibi davranıp C aracına gönderdiği mesajla, C aracını mesajın birden fazla araçtan geldiğine ikna edebilir. Böylelikle C aracı gelen mesajın gerçekliğine inanacak ve ona göre davranacaktır.

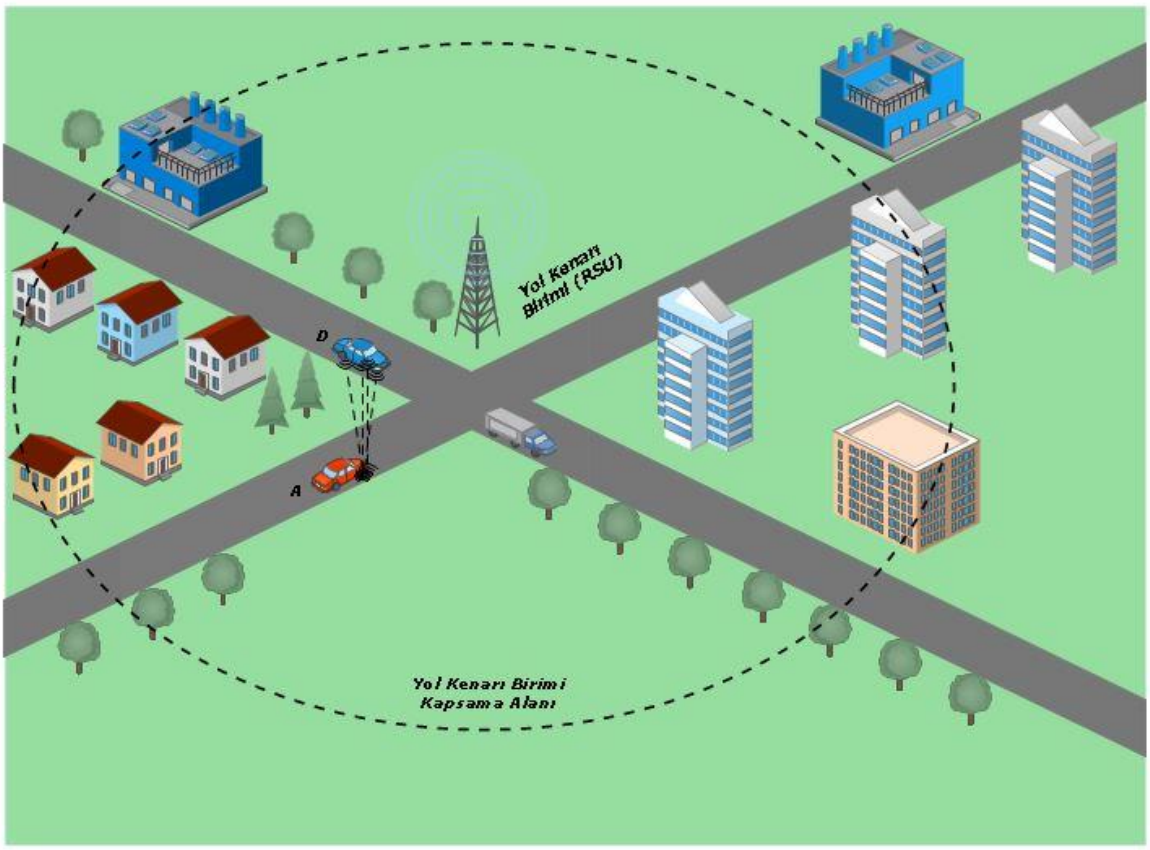
3.3.2. Hizmet Engelleme Saldırısı (Denial Of Service Attack: DoS)

Hizmet Engelleme Saldırısının amacı, kablolu ağlarda olduğu gibi sistemin çalışmasını engellemektir. Hizmet engelleme saldırıları genelde sisteme, sistemin kaldıramayacağı miktarda istek göndererek gerçekleştirilmektedir. Bu sayede sistem belirli bir noktadan sonra gelen isteklere cevap veremeyecek ve çalışamayacak duruma gelecektir [40]. Araçsal tasarsız ağlarda saldırgan düğüm DoS saldırısını bir araca ya da RSU'ya yapabilir. Saldırı yapmak isteyen araç fazla sayıda istek göndererek diğer aracı veya sistemi etkisiz hale getirebilir. Bu atağın bir diğer çeşidi ise, Dağıtık Hizmet Engelleme Saldırısı'dır (Distributed Denial of Service: DDoS) [40]. Bu saldırı mantığı Hizmet Engelleme Saldırısı ile aynı olmakla birlikte, bu saldırıda saldırıyı gerçekleştiren birden fazla saldırgan araç vardır. Saldırıya başlayan araçlar kendilerine bir araç ya da RSU'yu seçerek farklı noktalardan aynı anda saldırılarını gerçekleştirebilirler. DoS saldırısı veya DDoS saldırısı gerçekleştiren saldırgan araçlar sadece araçlara değil RSU'ya da zarar verebildikleri için sistemin çalışmasını durdurabilirler.

Şekil 3.3.'te görüldüğü gibi, A aracı yol kenarı birimine, birimin işlem kapasitesinin üstünde mesaj göndererek yol kenarı biriminin dolayısıyla bütün sistemin çalışmasını engellemiş olacaktır. Şekil 3.3.'te, yol kenarı birimine mesaj gönderecek araçlar mesajlarını gönderecek, ancak sistem bunları işleyemeyeceği için araçların gönderdiği mesajlara sistem tarafından bir tepki verilemeyecektir.

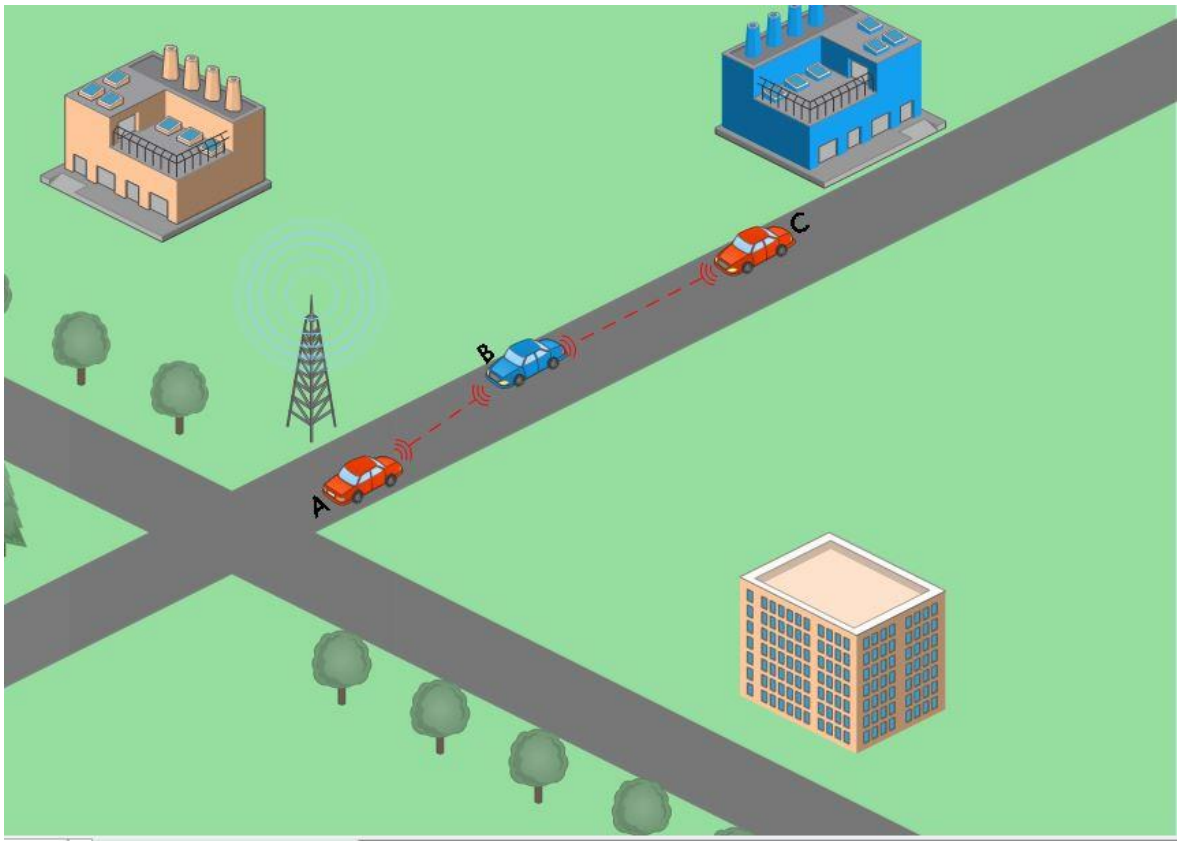


Şekil 3.3. Hizmet Engelleme Saldırısı



Şekil 3.4. Hizmet Engelleme Saldırısı – 2

Şekil 3.4.'te ise hizmet engelleme saldırısının yol kenarı birimi haricinde, ağdaki araçlar üstünde de gerçekleştirilebileceği gösterilmiştir. Şekil 3.4.'te A aracı D aracına aracın işlem kapasitesinin üstünde mesaj göndererek aracı ağda işlevsiz hale getirecektir. Bu durumda D aracına gelen herhangi bir bilgi işlenemeyecektir. Aynı şekilde D aracı gelen mesajları işleyemediği gibi, kendi de mesaj gönderemeyecektir.



Şekil 3.5. Dağıtık Hizmet Engelleme Saldırısı

Şekil 3.5.'te yukarıda da tanımı verilen dağıtık hizmet engelleme saldırısının bir örneği gösterilmiştir. Burada A ve C araçları, B aracına B aracının işlem gücünün kaldırabileceğinden daha fazla mesaj göndererek B aracının hem yol kenarı birimleriyle hem de diğer araçlarla iletişimini kesmektedirler.

Hizmet engelleme saldırısının altında sınıflayabileceğimiz saldırılardan biri de Sel Saldırısıdır (Flooding Attack). Sel saldırısı en bilinen DoS saldırılarından birisidir. Sel Saldırısı kendi içinde iki kısımda incelenebilir. Bunlardan birincisi RREQ sel saldırısıdır. Saldırgan araç ağa çok sayıda RREQ göndererek sistemin kaynaklarını sömürebilir ve sistemi yavaşlatabilir, hatta tamamen durdurabilir. Bu saldırı, RREQ gibi ağdaki bütün düğümlere giden yayın paketlerini kullanan reaktif protokollerine karşı yapılmaktadır. İkinci çeşidi ise veri seli saldırısıdır (Data Flooding) [41]. Bu saldırıda ağda bulunan saldırgan araç, araçlarla arasında bağlantı kurar ve bağlantı kurduğu araçlara kendi ürettiği boş paketleri, sık aralıklarla göndererek araçları meşgul eder ve hem sistemin hem de araçların kaynaklarını sömürerek, ağda yoğunluğa neden olur.

3.3.3. Paket Düşürme Saldırısı (Packet Dropping Attack)

Hem mobil tasarsız ağlarda hem de araçsal tasarsız ağlarda oldukça bilinen bir saldırı çeşididir. Bu saldırı çeşidinde zararlı araçlar kendilerine gelen paketleri düşürerek saldırıyı gerçekleştirirler. Zararlı araçlar gelen paketin türüne bakmaksızın (RREQ, RREP, veri paketi vs.) paketi düşürerek, paketi iletilmesi gereken yere göndermeyerek saldırıyı gerçekleştirmektedirler.

3.3.4. Karadelik Saldırısı (Blackhole Attack)

Araçsal tasarsız ağlarda, ağın yapısında değişikliği amaçlayan saldırılardan birisi de Karadelik Saldırısıdır. Tasarsız ağ protokollerinde düğümler arasında iletişim genelde en kısa yoldan yapılmaktadır. Bu saldırı, ağ protokollerinin bu özelliğini istismar eder. Bu saldırıda saldırgan olan araç, kendisinin, gönderilecek mesajı en kısa yoldan ulaştırabileceğini iddia eder ve diğer araçlara bu yönde bilgi gönderir. Sistemdeki herhangi bir araca bilgi göndermek isteyen araç, kendisine gelen bu bilgiye dayanarak bilgi paketini saldırgan araç aracılığıyla daha çabuk ulaştırabileceğini sanarak paketi saldırgan araca gönderir.

Paketi kendisine doğru çeken saldırgan araç sonrasında başka saldırılar gerçekleştirebilir, örneğin ona gelen paketleri düşürerek paketleri, gitmesi gereken yere göndermez. Normal bilgi mesajlarında sadece paket kaybı olurken, hayati önem taşıyan bilgi mesajlarında saldırı sonucu düşen paketler, daha kötü sonuçlar doğurabilir.

Bu saldırı türünde saldırgan araçlar sadece paketi düşürmekle kalmayıp, birbirleri arasında kendi ağlarını da oluşturabilirler. Herhangi bir araca bilgi göndermek isteyen düğüm, bilgiyi gönderdiği aracın saldırgan düğüm olduğundan habersiz bir şekilde bilgiyi iletir. Saldırgan düğüm bilgiyi aldıktan sonra, bu bilgiyi diğer bir saldırgan düğüme gönderebilir. Bu durumda söz konusu olan bilgi, iletilmesi gereken yere gitmeyip, bir saldırgan düğümden diğer bir saldırgan düğüme iletilecektir. Bu durumda iki saldırgan düğüm arasında olan araçlar, hiçbir şekilde mesaj alamayacak ya da gönderemeyecektir.

3.3.5. Solucan Deliği Saldırısı (Wormhole Attack)

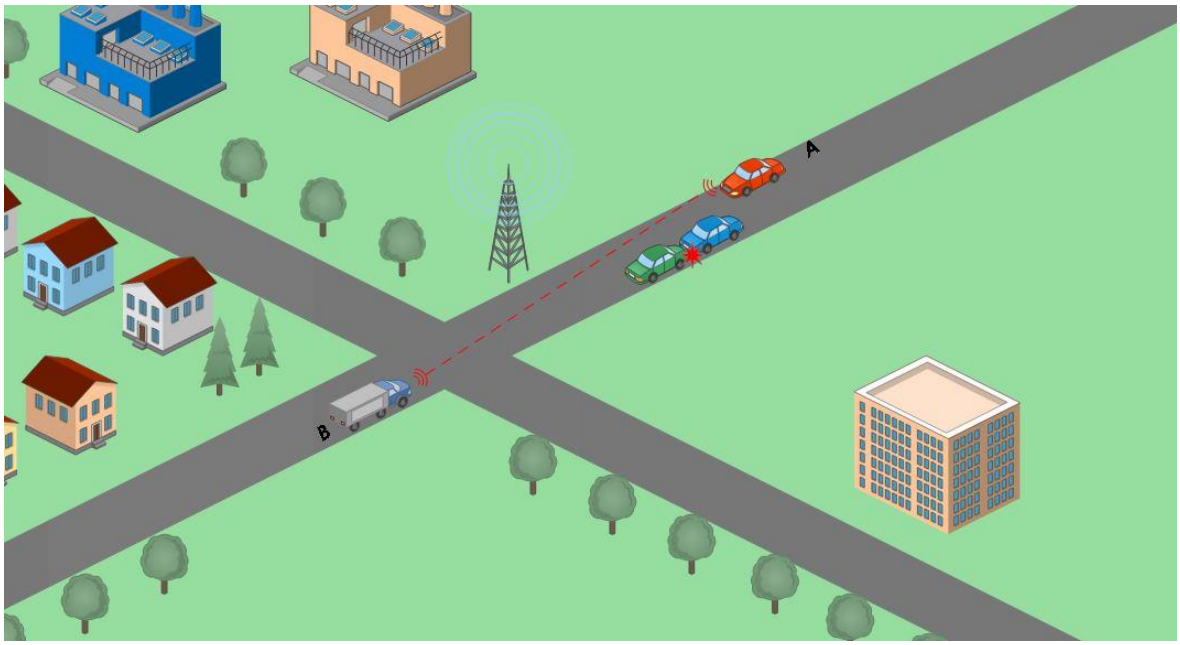
Solucan deliği saldırısı, karadelik saldırısına benzer bir saldırıdır. Ancak burada birden fazla araç saldırıyı gerçekleştirir. İki ya da daha fazla saldırgan araç kendi aralarında özel bir ağ kurarlar (kablolu ağ da olabilir) ve kendilerine gelen paketleri gönderilmesi gereken yere göndermeyip kendi kurdukları özel ağda birbirleri arasında gönderirler. Bu durumda iletilmesi gereken yere iletilmeyen paketler, bir süre saldırgan araçların arasında dolaşacak ve sonuçta düşecektir.

3.3.6. Sahte Bilgi Saldırısı (Bogus Information Attack)

Araçsal tasarsız ağlarda araçlar bir mesaj üretir ve bunu diğer araçlara gönderir. Diğer araçlar üretilen bu mesajı ya iletirler ya da kendileri için kullanırlar. Ama bu senaryo, araçların her zaman doğru bir mesaj göndereceği varsayımına dayanmaktadır. Diğer araçların aldığı bilgi her zaman doğru bilgi olmayabilir. Ağda bulunan saldırgan araçlardan biri gerçek olmayan bir bilgi üretebilir ve bu bilgiyi diğer araçlara gönderebilir [40]. Gerçek olmayan bir bilgi üreten araç diğer araçlara kaza olduğu haberini ya da gittiği yolda trafiğin yoğun olduğu bilgisini yayabilir ve mesajı alan araçların farklı yöne gitmesini sağlayabilir. Bu saldırıda, ağ içinde o bilgiyi doğrulayacak ya da yanlış olduğunu ifade edecek bir araç yoksa saldırının etkisi daha da büyüyecektir. Bunlardan yola çıkarak, ortamda mesajı değerlendirecek başka bir araç yoksa saldırıyı tespit etmek imkânsız olacaktır. Ayrıca saldırgan sürekli yer değiştiriyor ve her girdiği ağda yalan mesaj yayıyorsa, saldırının sonuçları daha kötü olacaktır. Saldırgan hızlı bir şekilde ağ değiştirdiği için yeni girdiği ağda aracın saldırgan olduğu bilinmeyecek ve saldırgan tespit edilmeden çok sayıda aracı etkileyecektir. Bu saldırı türüne ise literatürde otoyol saldırısı denmektedir [42].

Sahte bilgi saldırısı altında sınıflayabileceğimiz bir diğer saldırı türü de Sahte Pozisyon Bilgisi Saldırısı'dır (False Position Information Attack). Bu saldırı türünde saldırgan düğüm, ağa gerçek yerini göndermez. Özellikle can güvenliğinin önemli olduğu araçsal tasarsız ağlarda saldırgan araç, gerçek yerini göndermediği zaman ağda herhangi bir problem yaşanırsa, aracın tespiti mümkün olmadığı için geri dönülmez sonuçlar oluşabilir.

Şekil 3.6.'da sahte bilgi saldırısının bir örneği verilmiştir. Şekilde A aracı B aracına, B aracının yolunun üstünde kaza olduğu halde yolun açık olduğu bilgisini göndererek B aracının güzergahından sapmamasına neden olacak ve daha fazla tahribata neden olacaktır.



Şekil 3.6. Sahte Bilgi Saldırısı

3.3.7. Sensör Tahrifatı Saldırısı (Sensor Tampering Attack)

Araçsal tasarsız ağlarda her aracın içinde Araç İçi Ünitesi (On Board Unit) bulunur. Bu ünite normalde ulaşılması zor bir yerde bulunur. Bu durumda saldırgan ünitenin yapısını değiştirmektense ünitenin sensörünü bozarak kendi istediği mesajı yaratabilir. Bu durumda da saldırı tespit edilemeyecektir [43].

3.3.8. İllüzyon Saldırısı (Illusion Attack)

Sahte Bilgi Saldırısına çok benzeyen bir saldırıdır. Burada saldırgan düğüm yine diğer araçların inanacağı şekilde yalan bir mesaj yayınlar. Bu saldırıdaki fark saldırgan aracın yaydığı yalan mesajı hali hazırdaki trafik durumuna göre belirlemesidir. Buradaki asıl amaç bir trafik durumuna göre diğer araçları yanlış yönlendirecek bir mesaj yayınlamaktır [43].

Bir örnekle açıklamak gerekirse, sıkışık bir trafikte, saldırgan bir araç ileride trafik kazası olduğu bilgisini diğer araçlara gönderebilir, sıkışık trafikte bekleyen diğer araçların, bu yalan bilgiye diğer durumlara göre inanması daha kolay olacaktır.

Saldırgan bu atağı Sensör Tahrifatı saldırısında olduğu gibi aracın içinde bulunan sensörü kandırarak yapabilir. Bu durumda saldırının yalan mesaj içerdiğini tespit etmek daha zor olacaktır.

3.3.9. Tekrar Saldırısı (Replay Attack)

Sistemde sürekli mesaj üretmek gerekli değildir. Saldırgan araçlar kendilerine zaman içinde gönderilen mesajları saklayabilirler. Bu sayede geçmiş zamanda yaratılan bir mesajı saklayıp ileriki bir zamanda tekrar ağa gönderebilirler [44]. Bu saldırıyı saldırgan araç, gelen mesajları saklamasına gerek olmadan, kendisinin geçmiş zamanda ürettiği bir mesajı saklayıp başka zamanda tekrar göndererek de gerçekleştirebilir.

3.3.10. Pasif Gizli Dinleme Saldırısı (Passive Eavesdropping Attack)

Araçsal tasarsız ağlarda saldırgan araçların, her zaman aktif bir saldırı yapmasına gerek yoktur. Bu saldırı türünde saldırgan araç, ağı dinleyerek kendine yararlı bilgiyi çıkarabilir ya da araçlar arasındaki haberleşmeyi dinleyebilir. Burada aktif bir saldırı söz konusu olmadığı için bu atağın tespiti imkansızdır. Bu saldırı, genelde aktif bir saldırıdan önce, bilgi almak amacıyla gerçekleştirilir.

3.3.11. Bizans Saldırısı (Byzantine Attack)

Bu saldırı türünde saldırgan araç, bir veya birden fazla düğümü kontrol etmelidir. Saldırgan araç, kendisine gelen bilgiyi, gitmesi gereken yerden çok uzak bir yere gönderebilir ya da mesajı yok edebilir. Birden fazla saldırgan düğüm olması durumunda ise saldırgan araçlar mesajı kendi içlerinde döngü içine sokabilirler. Bu durumda mesaj gitmesi gereken yere asla ulaşamayacaktır.

3.4. Araçsal Tasarsız Ağlardaki Saldırılara Karşı Çözüm Önerileri

Araçsal tasarsız ağlar, kablosuz tasarsız ağlar içinde hareketliliğin en yüksek olduğu ağ çeşididir. Araçsal tasarsız ağlarda araçların hızlı hareket etmesi, trafik topolojisinin sürekli olarak değişmesi, saldırganların saldırılarını gerçekleştirmesini kolaylaştırmaktadır. Ayrıca bu durum sonucunda, ağda saldırganları tespit etmek de zor olmaktadır.

Bu saldırıların kötü sonuçlarını engellemek için her saldırı için özel, hızlı çözümler sunulması gerekmektedir. Araçların hızlı hareket etmesi, trafiğin akışına göre hızlı ya da yavaş olması, bu çözümlerin saldırılara özel ve gerektiğinde çok çabuk karar mekanizmasına sahip olmayı gerektirmektedir. Bu nedenle, var olan saldırılara literatürde birden fazla çözüm getirilmeye çalışılmıştır. Bu kısımda, literatürdeki saldırılara getirilen çözümler saldırı isimlerine göre sınıflandırılıp incelenmiştir.

3.4.1. Kimlik Değiştirme Saldırısı

Kimlik Değiştirme Saldırısı ilk olarak 2002 yılında Doucuer [45] tarafından literatüre kazandırılmıştır. Doucuer, Kimlik Değiştirme Saldırısına çözüm olarak sisteme giren araçlara Merkezi Yetki tarafından kesinlikle tek bir kimlik verilmesi koşulunu getirmiştir. Ancak bu çözüm, düğüm sayısının çokluğu nedeniyle ölçeklenebilir olmayabilir.

Golle ve arkadaşları [46] ise Kimlik Değiştirme Saldırısının çözümüne muhalif sezgisellik adını verdikleri bir çözüm bulmuştur. Bu çalışmada, Kimlik Değiştirme Saldırısının tespit edilebilmesi için arabanın içindeki sensörlerin kabiliyetlerinin artırılması gerekmektedir. Sensör kabiliyetleri artırıldıktan sonra hangi arabanın gerçekte var olup olmadığı öğrenilebilir.

Park ve arkadaşları [47] ise araçların kimliğini açığa çıkarmadan zaman pulu ile Kimlik Değiştirme Saldırısına çözüm bulmaya çalışmıştır.. Bu çözümde aracın, diğer araçlara mesaj göndermeden önce RSU'lardan zaman pulu alması gerekmektedir. Bu zaman pulları, aracın hangi zamanda mesaj gönderdiğini ve yakın zamandaki hareketini tespit etmek için kullanılabilir. Eğer araçlar, aynı RSU'dan belli bir süre içinde aynı zaman pulunu tekrar tekrar alıyorlarsa, saldırgan aracın Kimlik Değiştirme Saldırısı gerçekleştirdiği kabul edilecektir. Grover ve arkadaşları da [48]

bu çözüme benzer bir çözüm bulmuşlardır ve iki aracın belli bir süre içinde aynı komşulara sahip olamayacağı varsayımıyla yola çıkmışlardır.

Xiao ve arkadaşları [49] ise Sybil saldırısının tespitini üç aşamada gerçekleştirmektedir. Bu çözümde, araçlar değişik zaman aralıklarında üç değişik rol üstlenmektedirler. Bu roller sırasıyla sistemde komşularını bulmak için yayın (Beacon) mesajları gönderen araç (Claimer), bu mesajları alan araçlar (Witness) ve son olarak bu mesajları alıp işleyen araçlar (Verifier) olarak adlandırılırlar. Sistem şu şekilde çalışmaktadır; A aracı belirli aralıklarla düğümlere yayın mesajları göndermekte ve belirli aralıklarla komşu araçlardan yayın mesajı almaktadır. Her aldığı yayın mesajının sinyal gücünü kendi hafızasında saklamaktadır. A aracı B aracından yeteri kadar sinyal gücü aldığında, A aracı B aracı üstünde pozisyon doğrulama algoritmasını çalıştırmaktadır. B aracının ikinci aşamada Sybil araç olduğu kanıtlanırsa, A aracı yakındaki diğer araçlar üstünde de aynı sistemi uygulayarak birden fazla Sybil araç olup olmadığına bakar. Bu sayede, sistemdeki Sybil araçlar bulunmuş olacaktır.

3.4.2. Hizmet Engelleme Saldırısı

Sinha ve arkadaşları [50] hizmet engelleme saldırısına çözüm olarak birbirine mesaj gönderen araçların belli bir süre içinde ne kadar mesaj gönderdiğini takip eden bir mekanizma geliştirmişlerdir. Mekanizma şu şekilde çalışmaktadır; sistemdeki herhangi bir araç diğer bir araca mesaj gönderdiğinde, mesajı alan araç mesaj gönderen araç için bir sayaç başlatır. Bu sayaç belli bir sınır değerine kadar sayar ve bu sınır değerini de gelecek olan mesaj sayısına göre karar verir. Örneğin A aracı B aracına mesaj gönderdiğinde, B aracı A aracı için bir sayaç başlatır ve IP adresini kaydeder. Belli bir süre içinde A aracından B aracına, B aracının belirlediği mesaj sınır değerinden daha fazla mesaj gelirse, B aracı A aracını ağdan çıkarma isteği yollar ve Hizmet Engelleme Saldırısını tespit etmiş olur.

Yi ve arkadaşları [51], Hizmet Engelleme Saldırısının bir türü olan Sel Saldırısına çözüm getirmeye çalışmışlardır. Bu saldırı türünde saldırgan birden fazla RREQ mesajı göndererek ağ kaynaklarını sömürmeye çalışmaktadır. Bu saldırının çözümü olarak her düğüm komşu araçları izler ve gönderdikleri RREQ mesajları belirli bir

sınır değerin üstünde mi değil mi kontrol ederler. Eğer gönderilen RREQ mesajları sınır değerin üstündeyse, RREQ mesajı gönderen araçlar kara listeye alınırlar.

Desilva ve arkadaşları [52], yukarıdaki çözüme benzer bir çözüm sunmuşlardır, bu çözümde getirdikleri yenilik yukarıdaki gibi sabit bir sınır değer olmaması, sınır değerin sistemdeki RREQ mesajları analiz edilerek sistem tarafından kendiliğinden yeniden belirlenmesidir.

3.4.3. Karadelik Saldırısı

Lee ve arkadaşları [53] RREP ve RREQ mesaj paketlerini kullanarak karadelik saldırısına çözüm getirmişlerdir. Ağda mesaj göndermek isteyen herhangi bir araç, ilk önce RREQ mesaj paketi göndererek, mesaj göndereceği araçla arasında bağlantı kurmak istediğini belirtir. Yol bulunduğunda RREQ mesajını alan araçlar, mesaj göndermek isteyen düğüme RREP mesajını geri döndürür. RREP mesajını dönen araç, kendinden sonraki araca CREQ (Yol Teyit İsteği) mesajı gönderir. Bundan sonra CREQ mesajını alan düğüm, mesaj göndermek isteyen kaynak araca CREP mesajı gönderir. Kaynak araç CREP mesajını almazsa ya da CREP mesajları ile RREP mesajları uyuşmaz ise, sistemde saldırı olduğu konusunda alarm verilir.

Hortelano ve arkadaşları [54] ise, araçların gönderdiği mesajları izleyen bir mekanizma geliştirmişlerdir (Takipçi - Watchdog). Bu öneri, takip edilen aracın, takip eden aracın kapsama alanı içinde olduğu sürece uygulanabilir. Sistemde bulunan A aracı, B aracına mesaj gönderdiğinde, A aracı B aracının mesajı iletip iletmediğini takip edebilir. Geliştirilen çözümde, her araç komşu araçları için komşu listesi tutar ve bu listede güven değerleri vardır. Bu güven değeri, araca gelen ve gönderilmesi gereken paketlerin gerçekten gönderilen paketlere oranıyla belirlenir. Ve belirlenen sınır değerin altına düşen araçlar, sistemde saldırgan olarak kabul edilirler.

Al-Shurman ve arkadaşları [55] kara delik saldırısına farklı bir çözüm getirmişlerdir. Bu çözümde mesaj göndermek isteyen araç, en az ikiden fazla araçtan RREP mesajı beklemek zorundadır. Kaynak araç birden fazla RREP mesajı alıp birden fazla yol elde ettikten sonra bu yolların bir yerde kesişmesi gerektiği mantığına dayanmaktadır. Eğer ortak bir yol yoksa, kaynak araç farklı RREP mesajı bekleyecektir. Aksi halde sistemde kara delik saldırısı olduğu bilgisi gönderilecektir.

3.4.4. Solucan Deliği Saldırısı

Qian ve arkadaşları [56], solucan deliği saldırısına Çoklu Yolun İstatistiksel Analizi adını verdikleri bir çözüm getirmişlerdir. Solucan deliği saldırısının mantığı gereği sistemde diğer yollardan daha çok tercih edilen bir yol olmak zorundadır. Bu durumda keşfedilen yolların çoğunluğu solucan deliği saldırısına maruz kalmış yol olacaktır. Sistem üç aşamada çalışmaktadır. Birinci aşamada, sistem ağdaki yol keşiflerinden elde edilen yolların istatistiksel analizini yapar. İkinci aşamada, birinci aşamadaki istatistiksel aşamada yüksek değeri alan yol şüpheli olarak işaretlenir. Şüpheli olan yol sistem tarafından veri paketleri gönderilerek teste tabi tutulur ve gönderilen veri paketlerine cevap olarak ACK (Acknowledgement – Teyit) paketleri beklenir. Eğer teste tabi tutulan yol gerçekten etkilenmişse, sistemde saldırı olduğu uyarısı verilir.

Safi ve arkadaşları [57] ise, gönderilen paketlere ek bilgiler ekleyerek solucan deliği saldırısına çözüm bulmaya çalışmışlardır. Getirdikleri çözümde tasma (Leash) adını verdikleri ve gönderdikleri veri paketine, gidebileceği maksimum uzaklığı ve izin verilen iletişim uzaklığını belirten ek bilgiler eklemişlerdir. Yazarlar bu çözümde coğrafi tasma adını verdikleri sistemi kullanmışlardır. Yazarların bu sistemi kullanmasının amacı mesajı gönderen araçla, mesajı alacak aracın arasındaki mesafeyi kesin olarak ölçmeyi istemeleridir. Bu durumda bütün araçlar kendi konumlarını bilmekte ve aralarında senkronize olmuş bir zaman bulunmaktadır. Mesaj göndermek isteyen araç, göndereceği mesajın içine konumunu ve gönderdiği zamanı da koyar, mesajı alan araç, mesaj gönderen aracın gönderdiği konum bilgisini ve zaman bilgisini kendi konumu ve zamanı ile karşılaştırır. Mesajı alan araç, mesajı gönderen araçla aralarındaki uzaklığı ölçebileceğinden sistemde herhangi bir saldırının olup olmadığına karar verebilir. Eğer paketin gittiği yol (y) iki araç arasındaki mesafeden daha kısaysa, ya da paketin belirlenen hızdan daha hızlı gittiği tespit edilirse mesajı alan araç saldırı uyarısı verebilir.

3.4.5. Tekrar Saldırısı

Adjih ve arkadaşları [58] tekrar saldırısına çözüm için gönderilen mesajlara tarih damgası koymuşlardır. Basit bir şekilde mesajı alan araç, gelen mesajın tarihine bakarak eski ya da geçerli bir mesaj olduğuna karar vermektedir.

3.4.6. Byzantine Saldırısı

Baras ve arkadaşları [59], Byzantine saldırısına sistemde bir aracın gözlemci olarak davranmasıyla çözüm getirmişlerdir. Getirilen çözümde sistemde sürekli olarak bir aracın gözlemci olması gerekmektedir ve belirlenen sınır değere göre sistemde bir saldırının olup olmadığına karar vermektedir.

Literatürdeki çözüm önerileri genel olarak tek tür saldırının çözümü üzerine odaklanmışlardır. Ağda aynı anda farklı saldırılar olduğundaki çözümler ve sistemin bu saldırılara gerçek anlamda nasıl bir tepki vereceği araştırılmamıştır. Ayrıca, saldırı çözümlerinin denenmesi genellikle tek bir topoloji üstünde olmaktadır. Gerçek hayatta topolojinin ve araç sayısının bu kadar sık değiştiği bir ortamda saldırı çözümlerinin ne derecede etkili olduğu incelenmelidir. Çözüm önerilerindeki eksikliğin bir nedeni de bu saldırıların gerçek anlamda analizinin yapılmamış olmasıdır. Bu çalışmada, araçsal tasarsız ağlarda saldırgan olması durumunda, saldırganların ağa yaptığı etki gözlemlenmiş ve yorumlanmıştır. Çalışmada, 4 adet saldırı, iki farklı yönlendirme protokolünde (AODV ve GPSR) gerçekleştirilmiş ve benzetimleri yapılmıştır.

4. ARAÇSAL TASARSIZ AĞLARA KARŞI YAPILAN SALDIRILARIN ANALİZİ

Araçsal tasarsız ağlarda hareketliliğin çok fazla olması, araçların değişken hızlarda ilerlemesi, trafik topolojisinin çabuk değişmesi, sistemi saldırılara karşı çok açık bir konuma getirmektedir. Sistemde gerçekleştirilecek olan ciddi bir saldırı hayati öneme sahip olabilir. Gerçek hayatta, trafikte yaşanacak olan herhangi bir gecikme, ya da herhangi bir saldırı zaman kaybına, para kaybına ve daha önemlisi can kaybına neden olabilir. Araçsal tasarsız ağlardaki araç sayısının belli olmaması, hangi aracın saldırgan olup olmadığının tespitini neredeyse imkansız hale getirmektedir. Ayrıca sürekli hareket halindeki bir yapı olduğu için ve zamanlama hayati öneme sahip olduğu için, herhangi bir saldırı olduğunda zamanında tespit edilmesi çok önemlidir.

Sistemin henüz gerçek hayata uyarlanamaması sonucu bu saldırıların gerçekleştirilmesinin benzetim ortamında yapılması gerekmektedir. Benzetim ortamlarında gerçek hayattaki gibi trafik yoğunlukları kullanılmalı ve saldırıların ne gibi sonuçlar ortaya çıkardığı görülmelidir. Saldırılar benzetim ortamlarında gerçekleştirilirken can kaybı gibi veriler alınamayacağı için saldırgan sayısıyla orantılı olarak paket kaybı, sistemdeki yükün ne kadar arttığı vb. gibi sonuçlar gözlemlenip ona göre çıkarımlar yapılmalıdır.

Bu çalışmada AODV ve GPSR protokolünü kullanarak dört tane saldırıyı gerçekleştirip sistemde paket düşmesi, ağdaki yoğunluğun ne kadar etkilendiği ve paket iletim sürelerinin ne kadar geciktiği gözlemlenmiştir. Bu analizlerde mobil tasarsız ağlarda ve araçsal tasarsız ağlardaki benzetimlerde sıkça kullanılan protokollerden biri olduğu için AODV [60,61] protokolünün ve bunun yanı sıra coğrafi sistemi kullandığı ve pozisyona göre gönderim yaptığı için GPSR protokolünün kullanılmasına karar verilmiştir.

AODV ve GPSR protokollerinde gerçekleştirdiğimiz saldırılar sırasıyla paket düşürme saldırısı (Dropping Attack), sel saldırısı (Flooding Attack), karadelik saldırısı (Blackhole Attack) ve son olarak sahte bilgi saldırısıdır (Bogus Information Attack).

4.1. Paket Düşürme Saldırısı

Paket düşürme saldırısı, yukarıda da tanımı yapıldığı gibi, saldırgan düğümün aldığı paketi düşürmesi ve iletmesi gereken düğüme iletmemesidir. Burada düğüm ağa normal bir düğüm olarak katılır ve aldığı mesajları düşürür. Mesajı gönderen düğüm paketin saldırgan düğüme gelip gelmediğini bilmemektedir. Paketi saldırgan düğüme gönderen araç, paketin iletime devam edeceğini varsaymaktadır.

AODV protokolünde RREQ, RREP ve RERR paketlerinin yanı sıra asıl veriyi içeren paketler vardır. Yaptığımız paket düşürme saldırısında, veri paketini alan saldırgan araç, paketi sebepsiz yere düşürmektedir. İstediğimiz sayıda aracı saldırgan düğüm yaparak sisteme verilen zarar ölçülebilmektedir.

GPSR protokolünde ise söz konusu saldırı, AODV protokolüne benzer olarak gerçekleştirilmiştir. Mesajı alan saldırgan düğüm paketi sebepsiz yere düşürmektedir. Aynı şekilde GPSR protokolünde de saldırgan sayısı istenilen düzeye getirilerek saldırının şiddeti artırılmakta ve sisteme verdiği zarar ölçülmektedir.

4.2. Sel Saldırısı

Sel saldırısı sistemin işlevini kaybetmesine yol açacak şekilde gerçekleştirilen bir saldırı türüdür. Sel saldırısını Hizmet Engelleme Saldırısı'nın (DoS) altında sınıflayabiliriz. Sel saldırı, saldırgan düğümün sisteme çok fazla sayıda mesaj, istek mesajı göndererek sistemi yorması ve bunun sonucunda da sistemi işlevsiz hale getirmesidir.

Her ağda olduğu gibi araçsal tasarsız ağlarda da ağa gönderilen mesajlar her zaman bilgi içermeyebilir. Saldırgan araçlar ağı yormak için kendi ürettikleri RREQ mesajlarını göndererek sistemi meşgul edebilirler. Bu saldırıda, saldırgan araçlar bizim belirleyebildiğimiz bir aralıkla sürekli olarak RREQ mesajı göndermektedir. Paket düşürme saldırısında olduğu gibi burada da bir ya da birden fazla araç saldırgan yapılabilmekte ve sisteme verdiği zarar ölçülebilmektedir.

GPSR protokolünde, AODV protokolündeki RREQ mesajına benzer olarak gönderilen yayın mesajları (beacon) vardır. Bu mesajlarda düğümler birbirlerine

yerlerini haber ederek, mesaj göndermek isteyen düğümleri ve ağı bilgilendirmektedirler. Saldırıda ise AODV protokolüne benzer şekilde saldırgan araç düğümlere, düğümlerin işlem kabiliyetinden daha fazla yayın mesajı göndererek hem sistemi hem de düğümleri meşgul etmektedirler. Yapılan saldırıdıda saldırgan düğüm 0.2 saniye aralıklarla sistemde olmayan bir düğüm için RREQ paketi göndermektedir. GPSR'da ise saldırgan araç, yine AODV'de olduğu gibi 0.2 saniye aralıklarla beacon paketi göndermektedir.

4.3. Karadelik Saldırısı

Saldırılar kısmında da belirtildiği gibi kara delik saldırısı, saldırgan aracın mesajın gideceği araca en kısa yola sahip olduğu bilgisini ağa yayması sonucu ortaya çıkan bir saldırıdır. En uygun yolun kendisinde olduğunu ağa söyleyip bütün iletilmek istenen mesajları kendine alan saldırgan araç, sonrasında bu mesajları düşürmektedir. Yapılan saldırı açıklanmak istenirse; ağda, düğümler RREQ paketleri göndererek mesaj göndermek için en uygun düğümü öğrenmek isterler. RREQ paketi alan düğümler, en uygun yolun kendisinde olduğunu RREP mesajları ile RREQ aldığı düğümlere söylemektedirler. Yol için uygun olmayan düğümler RREP mesajı dönmezler. Ancak karadelik saldırısında RREQ alan paket RREP mesajının içine uygun yol olarak kendi sıra numarasını yazar ve paketi üstüne çeker. Tabii burada yapılan saldırı, paketi göndermek isteyen düğümün komşuları ve bu komşuların ulaşabildiği diğer düğümler arasında gerçekleşir. Paket göndermek isteyen düğümün bağlantı alanı dışında olan düğümler saldırıda o an için aktif rol alamazlar. RREQ paketi, ağdaki tüm düğümlere gitse de, bazı durumlarda RREQ paketinin ulaşamadığı düğümler olabilir. Bu durumda, RREQ paketi alamayan araç, RREP dönemeyecek ve söz konusu araç, saldırgan olsa da etkisi olmayacaktır. Diğer iki saldırıda olduğu gibi burada da saldırgan sayısı istenilen şekilde ayarlanmış ve sistemde yaptığı tahribat gözlemlenmiştir.

GPSR protokolü yapı gereği AODV protokolünden farklı olduğu için karadelik saldırısında farklı bir yol izlenmiştir. Gönderilen yayın mesajlarına (beacon) dönülen cevap paketleri kullanılmıştır. Mesaj göndermek isteyen araç yayın mesajı göndererek komşularını bilmek istediğini sisteme haber verir, bunun karşılığında komşuları cevap paketi kullanarak mesaj göndermek isteyen düğümün komşusu olduğunu haber verir. Bu saldırıda saldırgan düğüm uzakta bile olsa, mesaj

göndermek isteyen düğüme, hedef düğüme en yakın komşu olduğunu haber verir ve mesajı kendi üstüne çeker. Saldırgan araç mesaj göndermek isteyen düğümün komşu tablosunda ise, kendini hedef düğüme en yakın düğüm olarak gösterir ve paketi kendi üstüne çeker. AODV protokolünde olduğu gibi burada da saldırgan sayısı istenilen şekilde ayarlanmış ve ağa verdiği tahribat gözlemlenmiştir.

4.4. Sahte Bilgi Saldırısı

Benzetimlerde, iki protokolde de gerçekleştirilen bir diğer saldırı ise sahte bilgi saldırısıdır. Sahte bilgi saldırısı, saldırgan düğümlerin diğer düğümlere gerçek olmayan bir bilgiyi gönderip, onları yanlış yönlendirmeyi amaçlayan bir saldırı türüdür. Gerçek hayatta bu saldırılar, yanlış trafik bilgisi gönderme, olmayan bir olayı olmuş gibi gösterme şeklinde gerçekleştirilebilir. Ancak benzetim ortamında bu tarz durumların gerçekleştirilmesi mümkün olmadığından, sahte bilgi saldırısının farklı yollardan gerçekleştirilmesi gerekmektedir. Sahte bilgi saldırısı, AODV ve GPSR yönlendirme protokolünde, RREQ ve yayın (beacon) mesajları kullanılarak kontrol paketleri ile yanlış yönlendirme bilgisi gönderilmiştir.

AODV yönlendirme protokolünde sahte bilgi saldırısı, RREQ kontrol paketleri kullanılarak gerçekleştirilmiştir. Saldırgan düğüm, bir tane düğüm seçip (kurban düğüm), onun adına başka düğümlere RREQ (5 saniye aralıklarla) paketi göndermektedir. Ayrıca saldırgan düğüm, seçtiği kurban düğümleri ilerleyen zamanlarda kullanmak için hafızasında saklar. RREQ paketini alan düğüm, kurban düğüme, saldırgan düğüm aracılığı ile ulaşacağını varsayar ve saldırgan düğümü tablosuna kaydeder. Bu durumdan sonra, kurban düğüme mesaj göndermek isteyen düğüm, mesajı saldırgan düğüm üzerinden gönderecektir. Mesajı alan saldırgan düğüm, paketin içindeki hedef düğümün, önceden saldırı amaçlı gönderdiği RREQ paketi için seçtiği düğüm olup olmadığına bakar, eğer hedef düğüm, saldırgan düğümün kurban olarak seçtiği düğümse, paketi düşürür. Aksi durumda paketi iletir. GPSR yönlendirme protokolünde de sahte bilgi saldırısı, AODV protokolüne benzer şekilde gerçekleştirilmiştir. Ancak burada RREQ paketleri yerine, GPSR yönlendirme protokolü gereği yayın mesajları (beacon) kullanılmıştır.

Mesaj göndermek isteyen araç beacon gönderirken sahte beacon göndererek kurban düğümü hafızasına kaydeder ve kendisine o düğüme iletilecek bir veri paketi geldiğinde söz konusu veri paketini düşürür.

4.5. Saldırılarda Ağda Görünen Etkiler

Gerçekleştirilen üç saldırıda da ağda görünen etkiler şu başlıklar altında incelenmiştir. Gerçek hayatta araçlar üstünde saldırılar tespit edilemeyeceği için saldırıların etkileri paket iletim ve paket düşürme oranı, uçtan uca gecikme, ek yük ve verimlilik başlıkları altında incelenmiştir.

4.5.1. Paket İletim Oranı (Packet Delivery Ratio)

Ağdaki paketler saldırgan sayısı arttıkça gidecekleri yere gitmeden saldırganlar tarafından düşürülürler. Paket iletim oranını;

$$\text{Paket İletim Oranı} = \frac{\text{Başarıyla Gönderilen Paket Sayısı}}{\text{Gönderilen Toplam Paket Sayısı}} \quad (1)$$

şeklinde bulabiliriz.

Saldırgan sayısının artmasına ve azalmasına göre paket iletim oranının değişimleri gözlenmiştir.

4.5.2. Verimlilik (Throughput)

Ağdaki verimlilik, bir iletişim kanalında iletilen başarılı mesaj sayısıdır. Saldırgan sayısının durumuna göre ağdaki verimlilik değişkenlik göstermektedir. Ağın verimliliğini (V) aşağıdaki formülle gösterebiliriz;

$$V = \frac{Toplam\ \text{İ}letilen\ byte}{Sim\ddot{u}lasyon\ S\ddot{u}resi} X\ \frac{8}{1000}\ Kbps \quad (2)$$

4.5.3. Uçtan Uca Gecikme (End to End Delay)

Uçtan uca gecikme, herhangi bir ağda, yaratılan bir paketin hedef düğüme gidene kadar geçen süre şeklinde ifade edilebilir. Herhangi bir ağda, uçtan uca gecikme, paketlerin toplam gönderilme zamanlarının, toplam bağlantı sayısına bölümü olarak bulunabilir.

$$Uç\tan Uca\ Gecikme = \frac{\sum Paket\ Gönderim\ Zamanı - \sum Paket\ Alım\ Zamanı}{\sum Bağlantı\ Sayısı} \quad (3)$$

4.5.4. Ek Yük (Overhead)

Ek yük, herhangi bir ağda normal mesaj paketlerinin dışında kullanılan paketlerin sisteme getirdiği yük olarak ifade edilebilir. Bir örnekle açıklamak gerekirse, TCP/IP protokolünde normal bilgi içeren mesajların haricinde, protokolün kendi içinde bulunan el sıkışma (Handshake) için kullanılan paketler vardır. Bu durum TCP/IP protokolüne ek yük getirecektir. UDP protokolünde ise TCP/IP protokolüne göre, el sıkışma mesajları vs. olmadığı için, ek yük daha azdır. Benzetimler sonucunda UDP protokolünde ek yük, yönlendirme paketlerinin (Routing Packets), alınan bilgi paketlerine (CBR) oranıyla bulunmuştur.

$$Ek\ Yük = \frac{Yönlendirme\ Paketleri\ (Routing\ Packets)}{Bilgi\ Paketleri\ (CBR)} \quad (4)$$

5. DENEY SONUÇLARI

Bahsettiğimiz saldırıları gerçekleştirebilmek için literatürdeki benzetim araçlarını inceledikten ve diğer benzetim araçlarının literatürdeki kullanım durumlarına da baktıktan sonra, bizim istediğimiz sonuçları verebileceğine inandığımız NS'i (Network Simulator) kullanmayı uygun bulduk.

5.1. Network Simulator (NS-2)

Network Simulator, ağ deneylerini gerçekleştirebildiğimiz, ağ araçlarını istediğimiz gibi modelleyebildiğimiz ve içinde çok sayıda yönlendirme protokolü barındıran C++ ve Python yazılım dilini kullanan bir benzetim programıdır. Açık kaynak olması nedeniyle, diğer kullanıcıların da ekleme ve geliştirme yapabildiği, hem de zaman geçtikçe, gelişmelere uygun sürümlerin çıkması Network Simulator programını literatürde en çok tercih edilen benzetim programı yapmaktadır.

Network Simulator Linux işletim sistemlerine (Fedora, Ubuntu, Debian vs.) göre hazırlanmış ve en verimli sonucu bu işletim tabanlı sistemlerde veren bir benzetim programıdır.

Benzetim programı, Tool Command Language (TCL) isminde bir yazılım diliyle birlikte çalışmaktadır. Sistem, yapacağımız benzetimleri TCL dosyasında hazırlayıp, NS-2'ye girdi olarak verip istediğimiz deneyi çalıştırmamıza olanak vermektedir.

```
#Initialization

#Create a ns simulator
set ns [new Simulator]

#Setup topography object
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)

#Open the NS trace file
set tracefile [open Result.tr w]
$ns trace-all $tracefile

#Open the NAM trace file
set namfile [open Result.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel
```

Şekil 5.1. Örnek TCL Dosyası

TCL dosyasının içinde, benzetimde kullanacağımız araç sayısını, benzetim ortamımızın büyüklüğünü, yapacağımız benzetimin ne kadar süreceğini, benzetim sonucunda sonuç verilerinin nerede saklanacağını, hangi aracın saldırgan araç olacağını, saldırgan aracın hangi süre zarfında saldırgan rolünü üstleneceğini belirleyebiliyoruz. Şekil 5.1.'de örnek bir TCL dosyası verilmiştir.

Araçların birbirleriyle haberleşmesini sağlamak amacıyla otomatik olarak hazırladığımız bağlantı dosyasını oluşturduk. Burada, süresini ve araç sayısını, hangi tür veri paketi göndereceğini parametre olarak vererek, araçların haberleşme zamanının, hangi aracın hangi araçla haberleşeceğinin rastgele oluşturulduğu bir veri dosyası elde ettik. Burada araçsal tasarsız ağların yapısına uygun olarak UDP paketi göndermeyi tercih ettik.

```
#
# nodes: 35, max conn: 15, send rate: 1.0, seed: 1.0
#
#
# 25 connecting to 7 at time 100.05852885547026
#
set udp_(0) [new Agent/UDP]
$ns attach-agent $node_(25) $udp_(0)
set null_(0) [new Agent/Null]
$ns attach-agent $node_(7) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 512
$cbr_(0) set interval_ 1.0
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 10000
$cbr_(0) attach-agent $udp_(0)
$ns connect $udp_(0) $null_(0)
$ns at 100.05852885547026 "$cbr_(0) start"
```

Şekil 5.2. Örnek Bağlantı Dosyası

Benzetim için gerekli TCL dosyasının haricinde, düğümler arası bağlantıları gösteren bağlantı dosyalarımızı ve hareketliliği belirleyen TCL dosyamızı da NS-2 programına parametre olarak vererek benzetimlerimizi gerçekleştirdik.

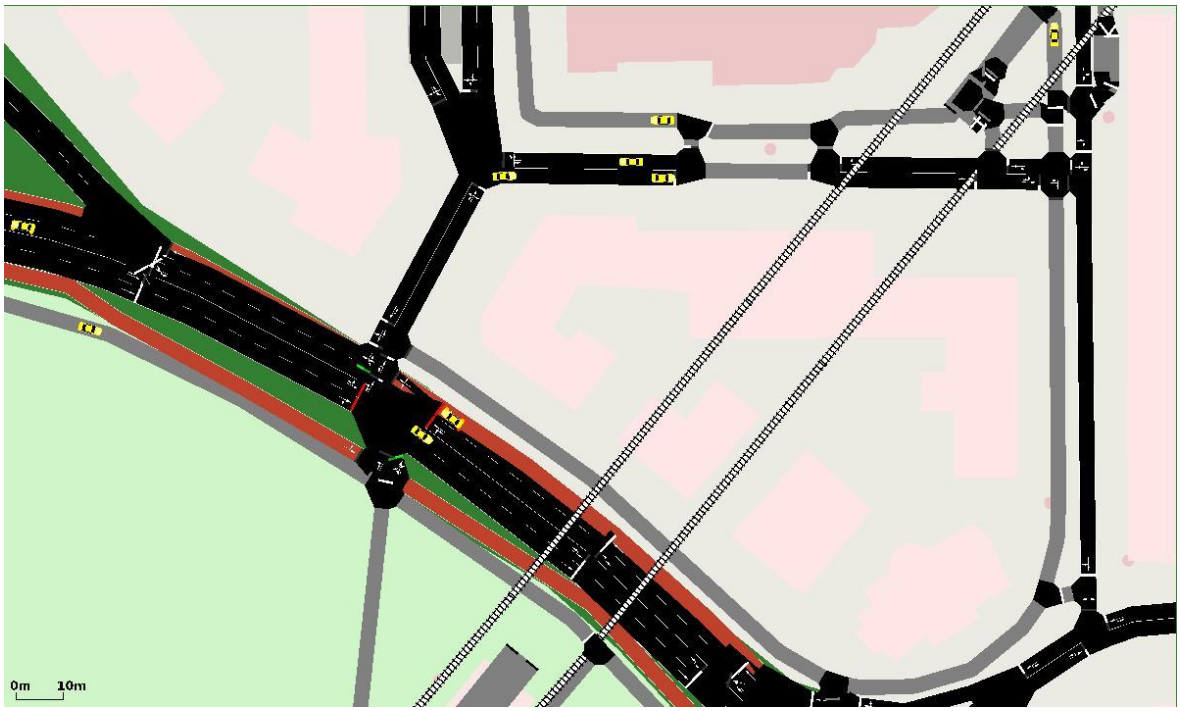
Benzetimlerimizi her saldırı için İstanbul Yolu ve Münih şehir merkezi olmak üzere iki farklı haritada gerçekleştirdik. Her iki haritayı da OpenStreetMap [62] ve SUMO Mobility Simulator'ü [63] kullanarak benzetim ortamımız olan NS-2'ye aktardık. Benzetim parametrelerimiz aşağıdaki tabloda verilmiştir.

Çizelge 5.1.Benzetim Parametreleri

Simulator	ns-2
Süre	200 Saniye
Haritalar	İstanbul Yolu – Münih
Araç Sayısı	35
Paket Türü	UDP
Yayılma Modeli	Nakagami [64]
Paket Boyutu	512 Kb
Paket Gönderim Aralığı	1 Saniye
Hız	0-70 m/s
Maksimum Bağlantı Sayısı	15

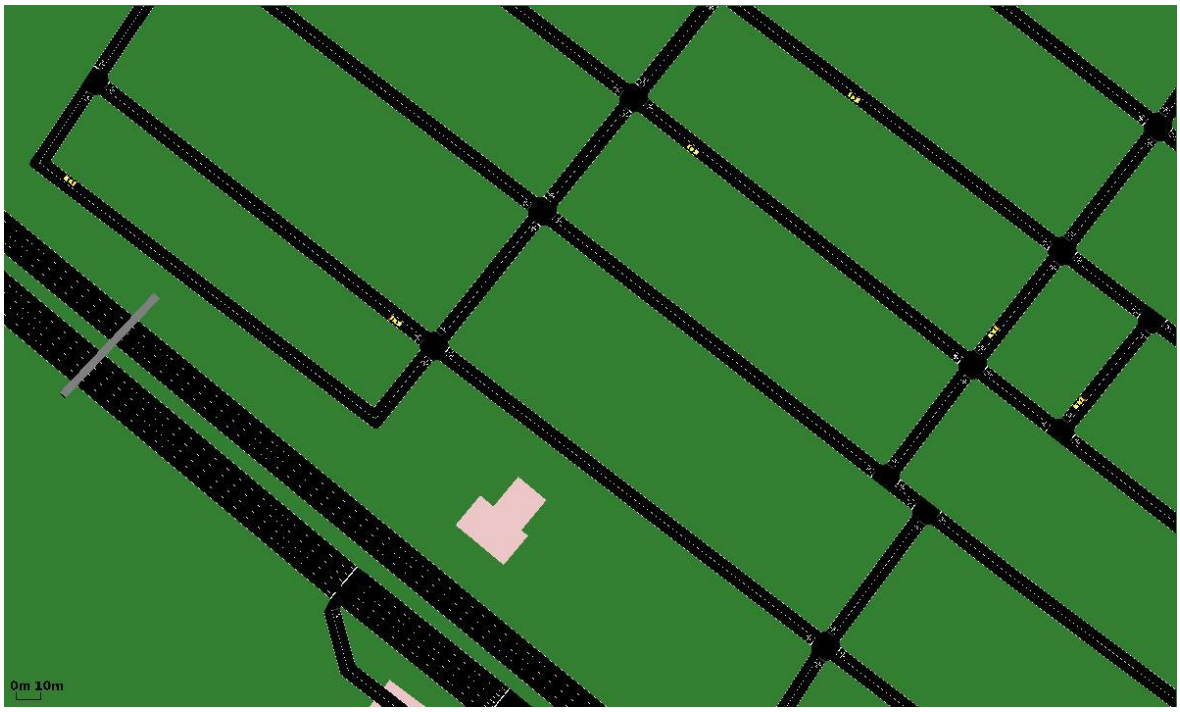
5.2. İstanbul Yolu Haritası ve Münih Şehir Merkezi Haritası

İstanbul Yolu haritası ve Münih Şehir Merkezi haritası OpenStreetMap [62] ve SUMO Mobility Simulator'ü [63] kullanılarak çıkarılmıştır. Haritalar, iki farklı yoğunluğu göstermesi açısından yoğun ve seyrek trafik olacak şekilde ayarlanmıştır.



Şekil 5.3. Münih Şehir Merkezi Haritası

Şekil 5.3.'te Münih şehir merkezinin haritası gösterilmiştir. Harita OpenStreetMap kullanılarak Münih kentinin merkezinden çıkarılmıştır.



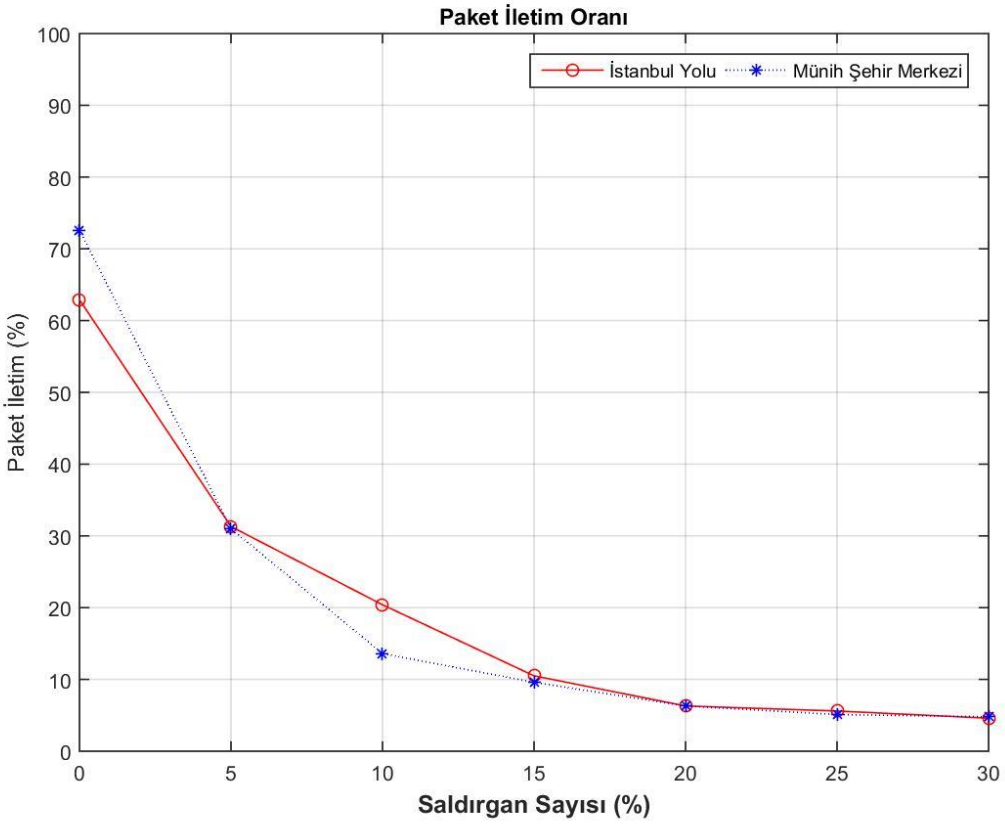
Şekil 5.4. İstanbul Yolu Haritası

Şekil 5.4.'te İstanbul Yolu haritasının SUMO Mobility Simulator'deki görüntüsü verilmiştir. Münih haritasının aksine İstanbul Yolu haritası, trafik daha seyrek olacak şekilde çıkarılmıştır.

5.3. AODV Yönlendirme Protokolü Saldırı Sonuçları

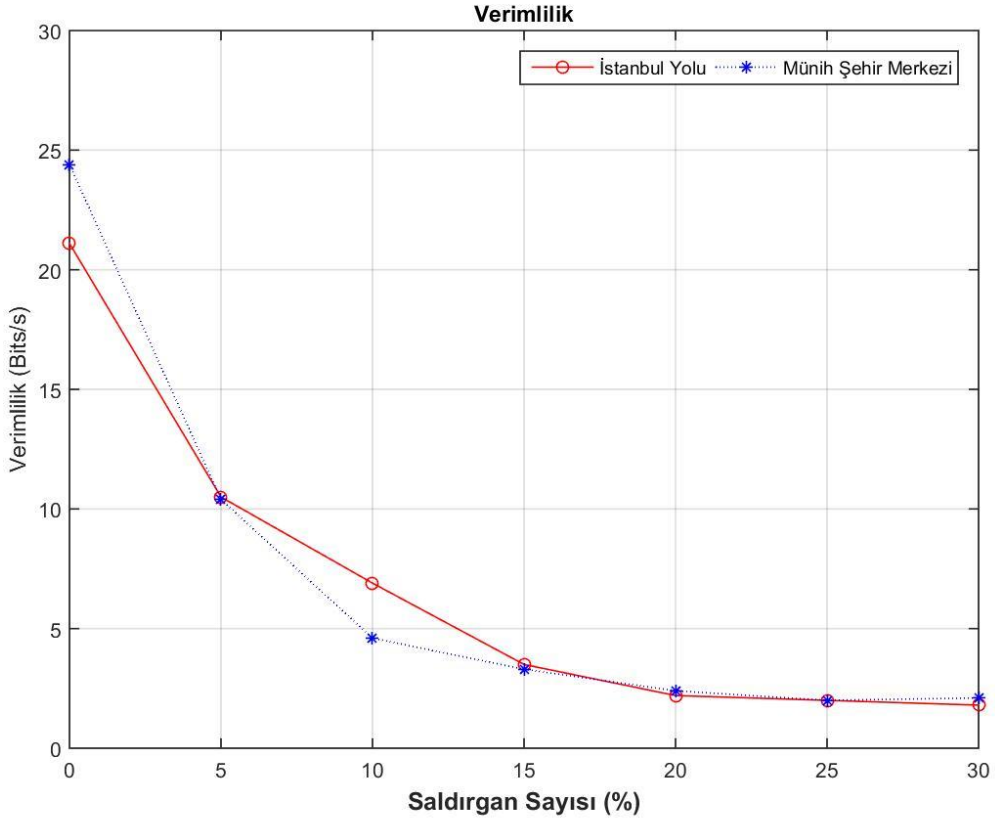
AODV protokolünde hem İstanbul Yolu için hem de Münih kenti için saldırılar yukarıda verilen parametrelere uygun olarak gerçekleştirilmiştir. Benzetimler gerçeğe uygun olması açısından her seferinde değişik bağlantı modelleriyle denenmiştir. Toplamda 10 farklı bağlantı dosyası kullanılmış ve seçilen her bir saldırgan 10 bağlantı dosyası üstünde tek tek çalıştırılmıştır. Her bir saldırgan grubu için (%0, %5, %10, %15, %20, %30) 10 bağlantı dosyası tek tek çalıştırılmıştır. Örnek vermek gerekirse, %5'lik saldırgan grubu için her 10 seferde bir saldırganın yeri değiştirilmiş ve bağlantı dosyaları tekrar çalıştırılmıştır. Toplamda bir saldırgan grubu için (örn. %5) 100 tekrar yapılmıştır. Bir saldırı için toplam 700 simülasyon tekrarı yapılmış ve bir protokol için toplam 2800 simülasyon tekrarı yapılmıştır.

5.3.1. AODV Karadelik Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



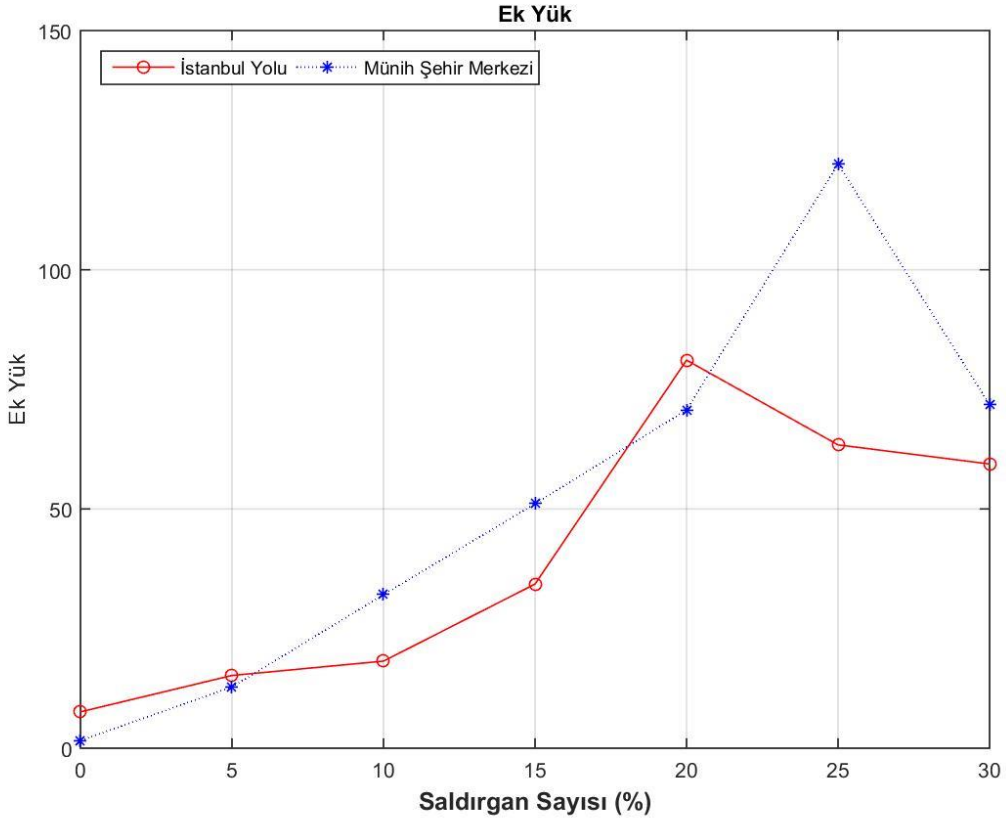
Şekil 5.5. AODV Karadelik Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.5.'te AODV protokolünde karadelik saldırısı sonucu ortaya çıkan paket iletim oranı sonuçları grafiksel olarak verilmiştir. Karadelik saldırısı, saldırgan düğümün kendisini hedef düğüme en yakın düğüm olduğunu iddia etmesine dayanır. Bu sayede paketleri kendine çekerek düşürür. Benzetim sonuçları da bu durumu desteklemektedir. İki haritada da paket iletim oranları birbirine yakın olup saldırgan sayısı arttıkça düşmektedir. Örneğin, saldırgan sayısı %20 iken paket iletim oranı Münih haritasında %10'un altındadır. Yukarıda verilen grafik yorumlandığında paket iletim oranının ağdaki saldırgan sayısı %5 olduğunda bile %30 civarında olduğu görülmektedir.



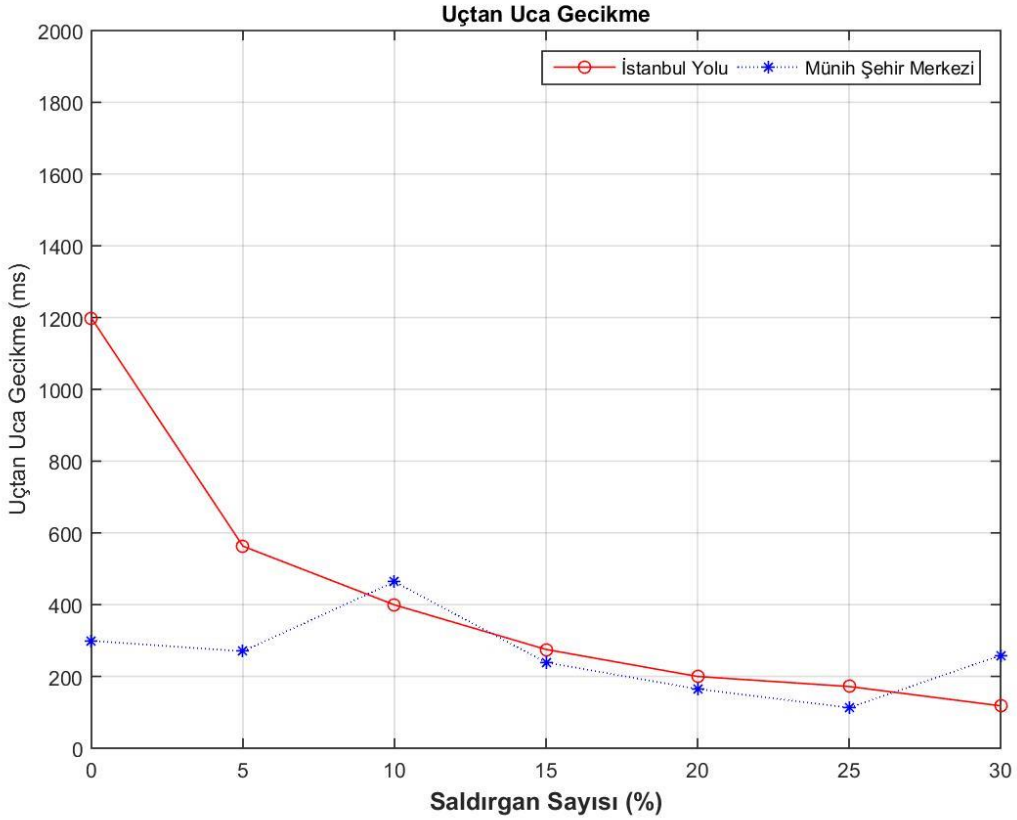
Şekil 5.6. AODV Karadelik Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.6.'da ise iki haritanın benzetimler sonucunda ortaya çıkan verimlilik grafiği verilmiştir. Ağdaki verim, saniyede gönderilen bit sayısı olarak ifade edilir. Ağda, Şekil 5.5.'in yorumlamasında belirtildiği üzere paket iletim oranının düşmesi ağda verimliliğin de düşmesine neden olmuştur.



Şekil 5.7. AODV Karadelik Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.7.'de AODV yönlendirme protokolünü kullanarak iki haritada gerçekleştirilen karadelik saldırısı sonucu ortaya çıkan ek yük oranları verilmiştir. Münih haritasında en fazla artış saldırgan sayısı %25 iken gerçekleşirken, İstanbul Yolu haritasında en fazla artış saldırgan sayısı %20 iken gerçekleşmiştir.



Şekil 5.8. AODV Karadelik Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.8.'de AODV yönlendirme protokolünde gerçekleştirilen Karadelik saldırısı sonucu iki haritada da ortaya çıkan uçtan uca gecikme oranı verilmiştir.

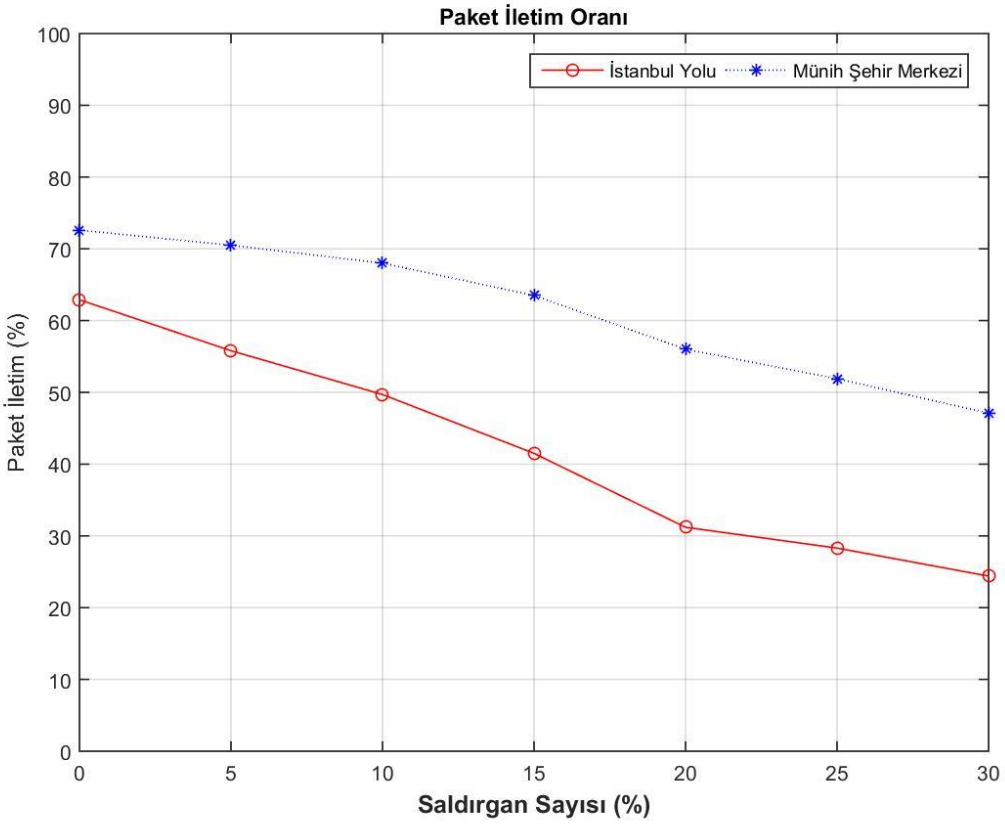
Hiçbir saldırganın olmaması durumunda, İstanbul Yolu haritasında uçtan uca gecikme zamanı, Münih haritasına göre daha fazladır.

Her iki haritada da saldırgan sayısı %5'e ulaştığında Münih haritasında, İstanbul Yolu haritasına göre daha az gecikme görülmektedir. Ancak, saldırgan sayısı %30'a ulaştığında bu durumun tersi meydana gelmektedir. Saldırgan sayısı %30 olduğunda İstanbul Yolu'ndaki uçtan uca gecikme, Münih haritasına göre daha düşüktür. Saldırgan sayısı %10 ile %25 arasında iken her iki haritada da düşüş meydana gelmiştir.

Münih haritasında araç yoğunluğuna, araçların zaman zaman hareketsiz olmalarına ve İstanbul Yolu haritasına göre daha yavaş hızda seyretmelerine bağlı olarak uçtan uca gecikme değişkenlik göstermektedir.

Münih haritasında, düğümlerin birbirlerine daha yakın olması, saldırganın olması durumunda bile mesajlaşmayı mümkün kılmaktadır. Ancak bu durum İstanbul Yolu haritası için geçerli değildir. Araçların hızlı hareket etmeleri, aralarındaki bağlantının daha sık kopması gibi nedenler uçtan uca gecikmenin azalmasına neden olmuştur. Bu durum, iletilen paketlerin daha yakın paketlere iletilebildiğini göstermektedir. Bunun sonucu olarak, iki haritada da uçtan uca gecikme azalma göstermiştir.

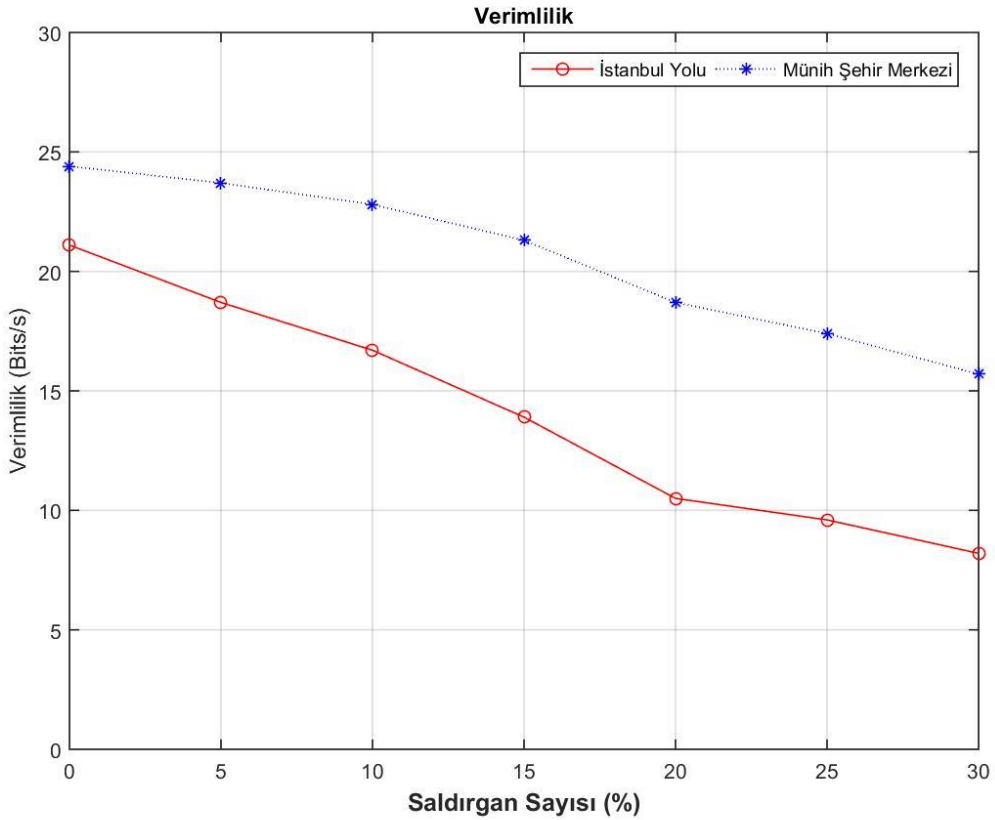
5.3.2. AODV Paket Düşürme Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



Şekil 5.9. AODV Paket Düşürme Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

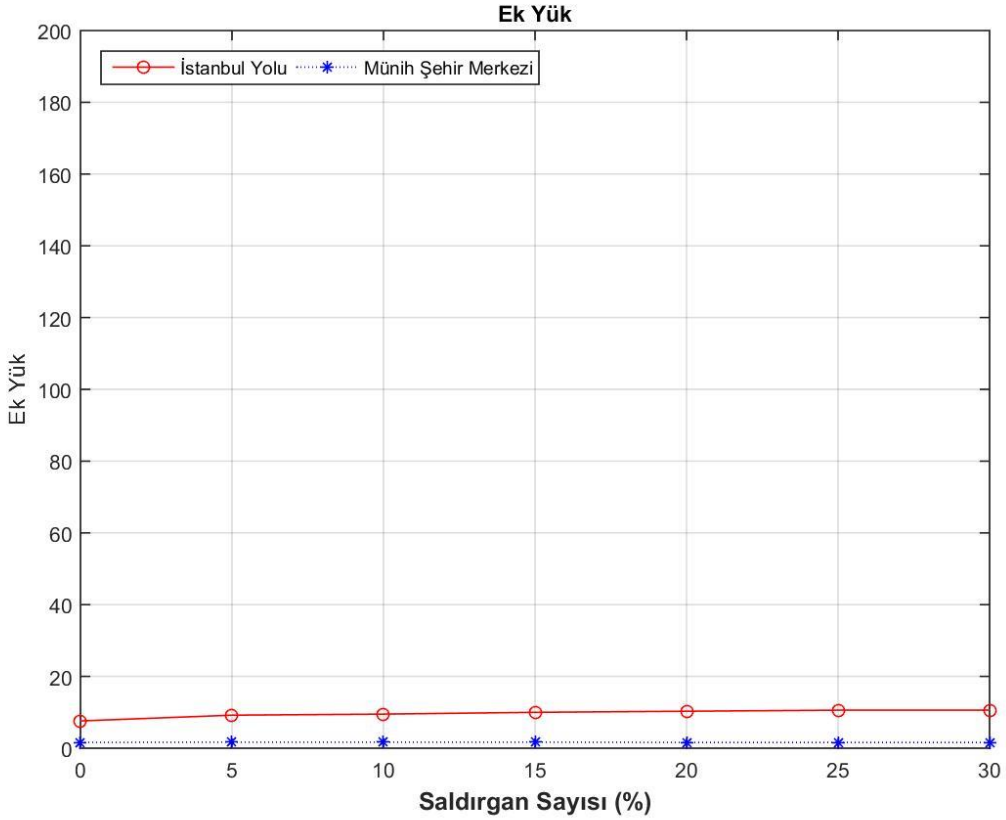
Şekil 5.9.'da AODV protokolünde paket düşürme saldırısının sonucunda ortaya çıkan paket iletim oranları verilmiştir. Grafikte görüldüğü gibi, her iki haritada da saldırgan sayısı arttıkça paket iletim oranı düşmektedir. Kullanılan iki haritanın farkı bu grafikte açıkça görülmektedir. Münih haritasında düğümler birbirlerine daha yakın olduğu için paket iletimi, İstanbul Yolu haritasına göre daha yavaş düşmektedir. Paket düşürme saldırısında, saldırgan düğüm kendine gelen paketleri düşürmekte ve paketin iletimini gerçekleştirmemektedir.

Paket düşürme saldırısı, paket yok etme açısından karadelik saldırısına benzemektedir. Ancak paket düşürme saldırısında, saldırgan düğüm, karadelik saldırısında olduğu gibi paketleri üstüne çekmemektedir. Bu saldırı türünde sadece saldırgan düğüme gelen paketler düşürülmektedir. Bu da paket iletim oranının, karadelik saldırısından daha yavaş bir düşüş gösterdiğini açıklamaktadır.



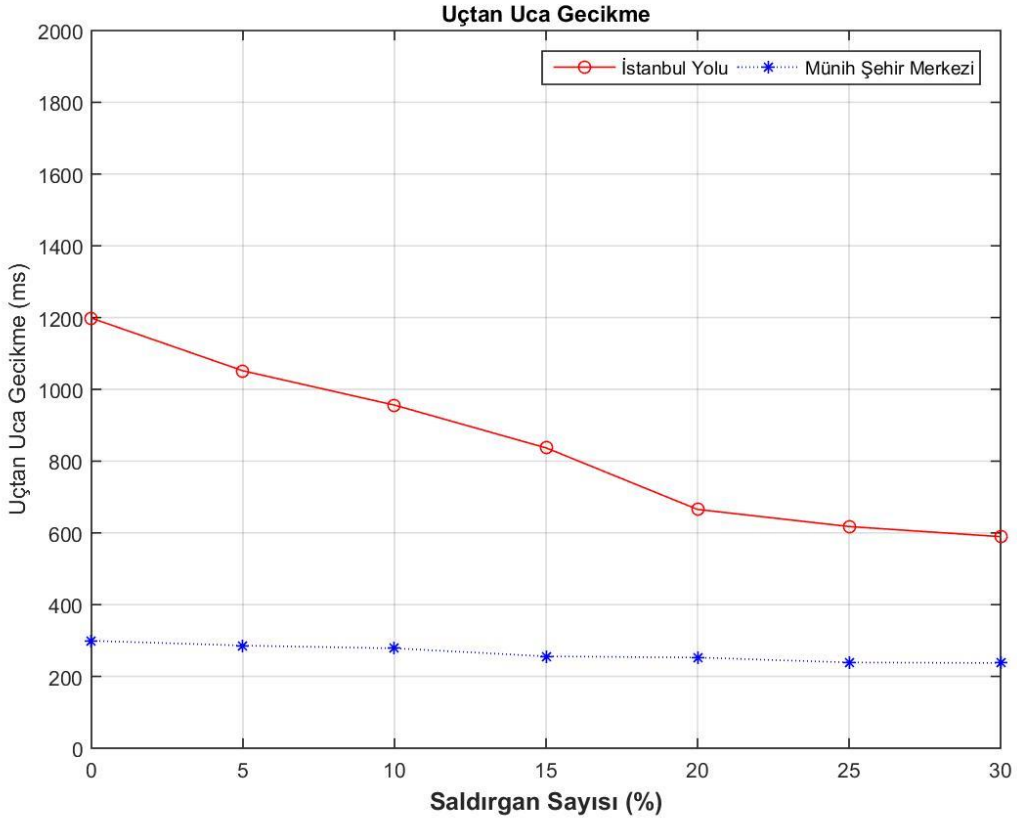
Şekil 5.10. AODV Paket Düşürme Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.10.'da AODV paket düşürme saldırısının iki harita için verimlilik oranı verilmiştir. Saldırgan sayısı %20 iken İstanbul Yolu haritası için verimlilik saniyede 10 bite kadar düşmüştür. Ancak bu oran Münih haritası için saniyede 19 bit civarındadır.



Şekil 5.11. AODV Paket Düşürme Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

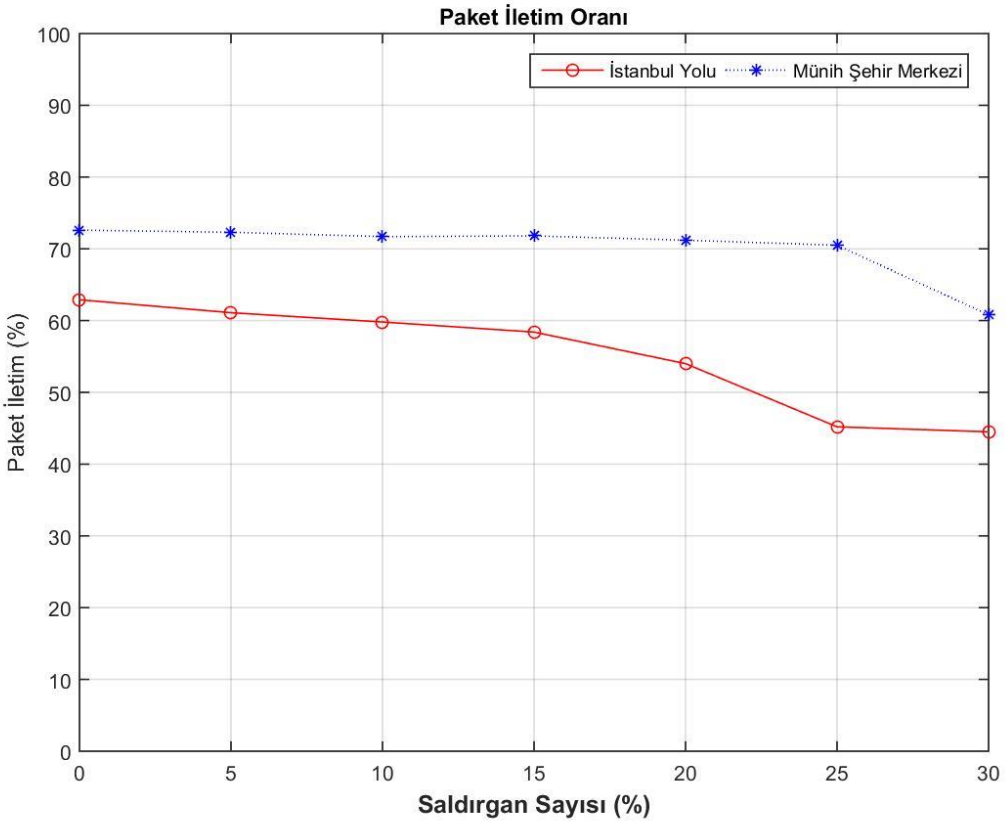
Şekil 5.11.'de AODV protokolünde gerçekleştirilen paket düşürme saldırısı sonucunda iki haritada da ortaya çıkan ek yük oranları verilmiştir. Saldırı sonucunda ek yük oranında iki haritada da ciddi bir yükselme olmamaktadır.



Şekil 5.12. AODV Paket Düşürme Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

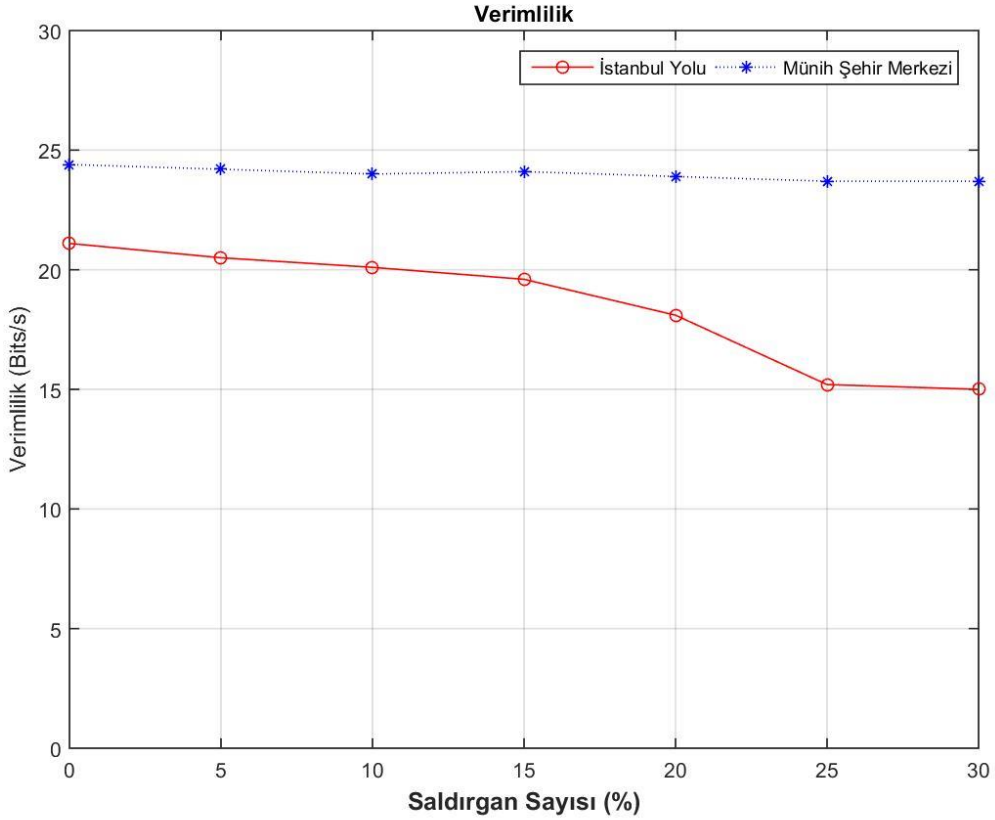
Şekil 5.12.'de AODV yönlendirme protokolünde gerçekleştirilen paket düşürme saldırısının uçtan uca gecikme oranı verilmiştir. Verilen grafikte, İstanbul Yolu için uçtan uca gecikmenin sert bir şekilde azaldığı görülmektedir. Ancak bu durum Münih haritası için geçerli değildir. Münih haritasında daha yavaş bir düşüş olmuştur. Münih haritasında, düğümler paketler düşse bile paketi iletebilecek diğer düğümler bulmaktadır. Bu da uçtan uca gecikmenin Münih haritası için sabit olmasını açıklamaktadır. Ancak İstanbul Yolu'ndaki hızlılık ve seyreklik, paket iletimi için o an saldırgan dışında alternatif düğümlerin olmaması paket iletimini etkilemektedir.

5.3.3. AODV Sel Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



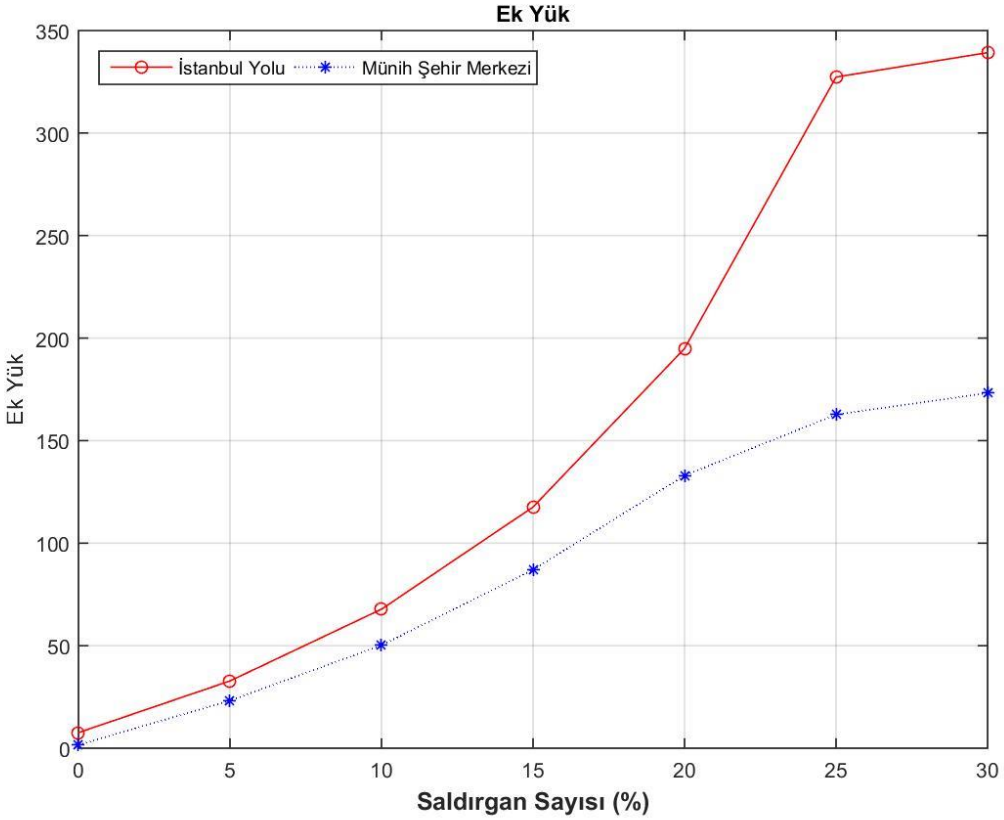
Şekil 5.13. AODV Sel Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.13.'te AODV protokolünde sel saldırısının hem İstanbul Yolu hem de Münih kenti haritası için benzetim sonuçları verilmiştir. Grafik yorumlandığında iki haritada da yaklaşık olarak aynı seviyede paket iletim oranının düştüğü görülmektedir. Bu durum, sel saldırısında iki haritada da düşük sayıda saldırganın bir etkisi olmadığını göstermektedir. Grafikte de görüldüğü gibi, paket iletim oranı İstanbul Yolu'nda daha fazla bir düşüşe sahiptir. Bu da, yukarıda açıklandığı gibi iki haritanın yoğunluk durumuyla ilişkilidir.



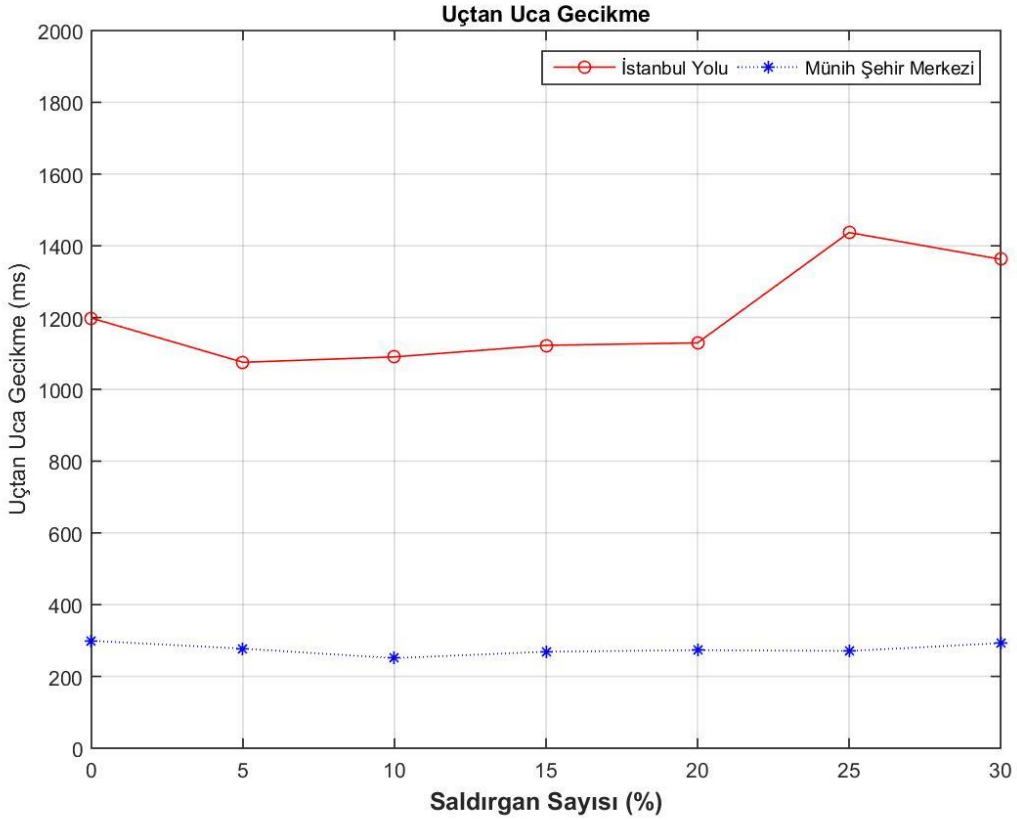
Şekil 5.14. AODV Sel Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.14.'te AODV protokolündeki sel saldırısının iki harita için verimlilik oranı verilmiştir. Diğer saldırılarda olduğu gibi, İstanbul Yolu haritası saldırıdan daha fazla etkilenmiş ve verimlilik oranında Münih haritasına göre daha fazla düşüş olmuştur.



Şekil 5.15. AODV Sel Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

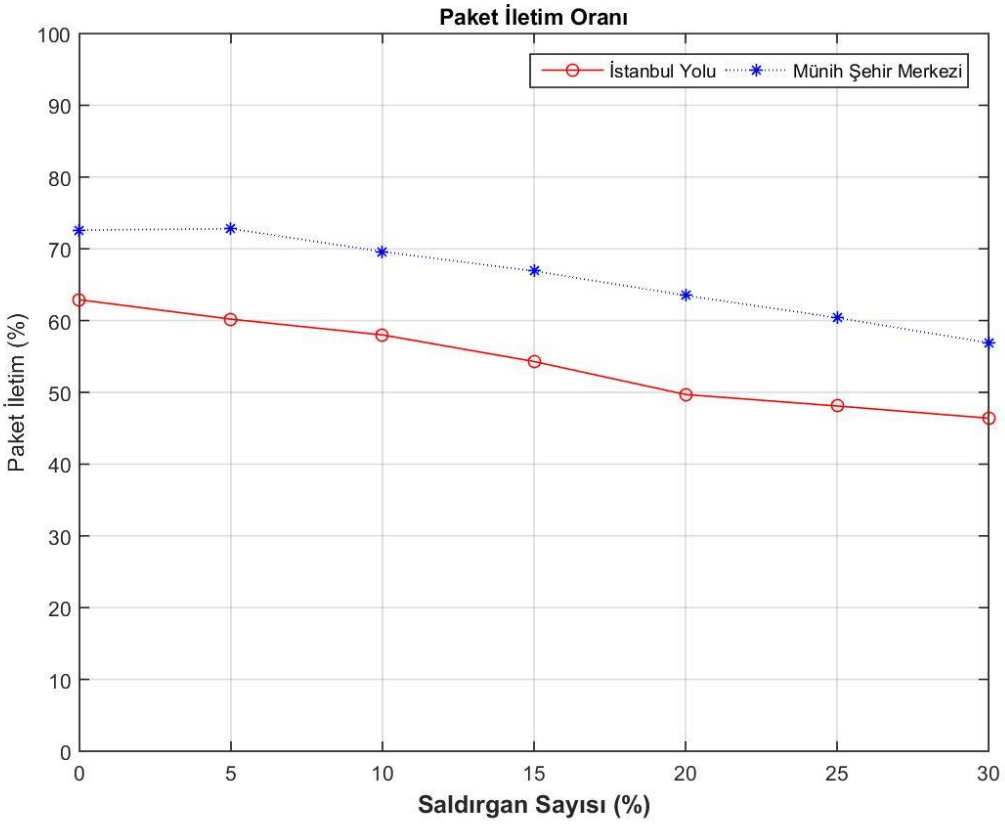
Şekil 5.15.'te AODV yönlendirme protokolünde gerçekleştirilen sel saldırısının yapılan benzetimler sonucu ortaya çıkan ek yük sonuçları grafiksel olarak verilmiştir. Ağa çok sayıda kontrol paketi gönderildiği için, ağdaki ek yük oranı yükselme göstermiştir. Saldırgan sayısı arttıkça, ek yük oranında da keskin bir yükseliş olmuştur.



Şekil 5.16. AODV Sel Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.16.'da AODV yönlendirme protokolünde gerçekleştirilen sel saldırısının uçtan uca gecikmeye olan etkisi verilmiştir. Saldırı sonucunda iki haritada da uçtan uca gecikme oranı farklılık göstermiştir. Saldırgan düğümler tarafından çok fazla sayıda RREQ paketi alan düğümler, kendilerine gelen diğer paketleri, ön belleklerinde (buffer) bekletirler. Ancak uzun zaman sonra paket iletimini gerçekleştirebilirler. Bu uzun süre bekleme, uçtan uca gecikmeyi artırmaktadır. Düğümlerin yoğunluğu bekletilen paketlerin iletiminin gerçekleşme oranını etkilemektedir.

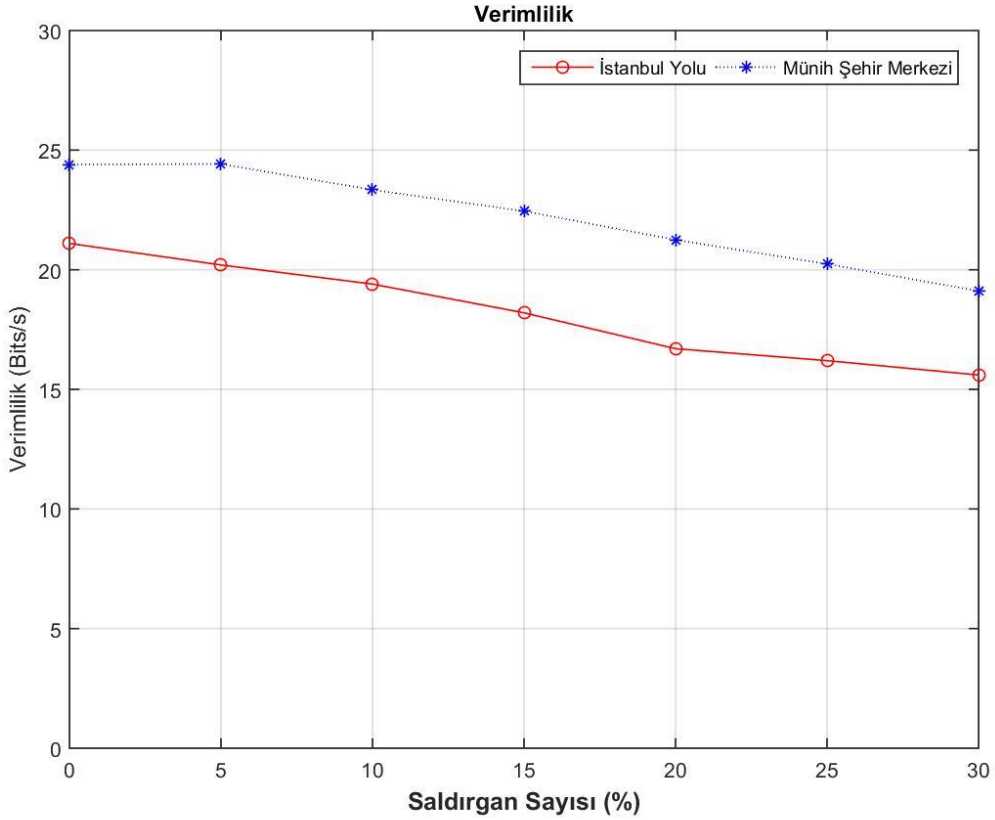
5.3.4. AODV Sahte Bilgi Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



Şekil 5.17. AODV Sahte Bilgi Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

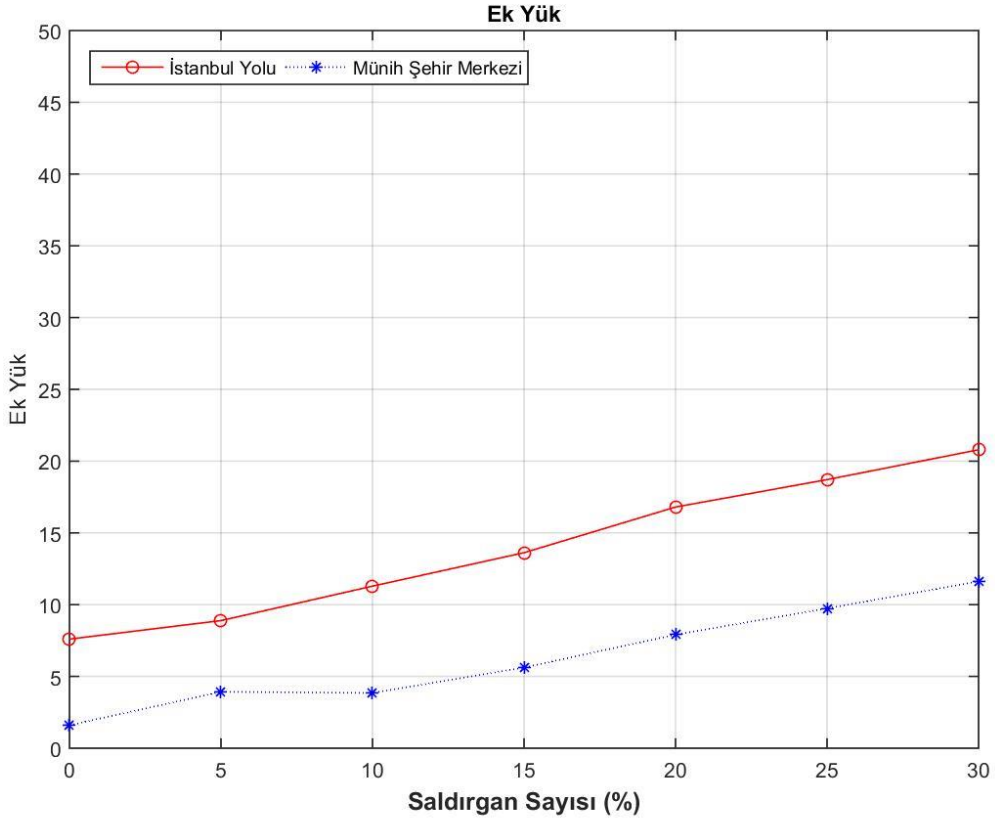
Şekil 5.17.'de AODV yönlendirme protokolünde gerçekleştirilen sahte bilgi saldırısının paket iletim oranı verilmiştir. Grafikte görüldüğü gibi, iki haritada da paket iletim oranı düşmektedir.

Sahte bilgi saldırısında asıl amaç, kurban olarak seçilen düğümü sistemden izole etmektir. Seçilen saldırganlar kendilerine gelen paketleri düşürdükleri için bir süre sonra iki haritada da paket iletim oranı düşmektedir.



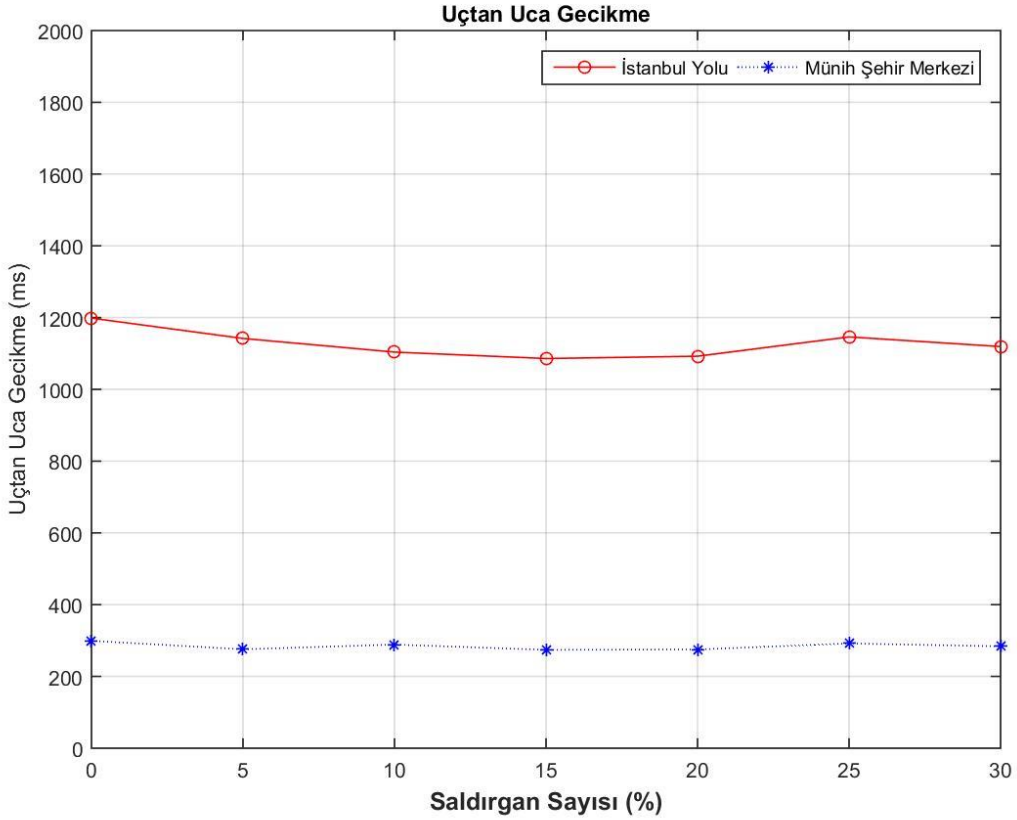
Şekil 5.18. AODV Sahte Bilgi Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.18.'de AODV protokolünde gerçekleştirilen sahte bilgi saldırısının verimlilik oranları verilmiştir. Saldırı sonucu, paket iletim oranı düştüğü için, iki haritada da ağın verimliliği düşmüştür. Verimliliğin düşüşü, haritaya bağlı olarak değişmektedir.



Şekil 5.19. AODV Sahte Bilgi Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.19.'da AODV yönlendirme protokolünde gerçekleştirilen sahte bilgi saldırısının iki haritaya da getirdiği ek yük oranları verilmiştir. Saldırgan düğüm, 5 saniye aralıklarla RREQ paketi gönderdiği için sistemde fazladan RREQ paketleri olacaktır. Saldırgan sayısı arttıkça sistemde dolaşan sahte RREQ paketleri de artacağından ek yük artmıştır.



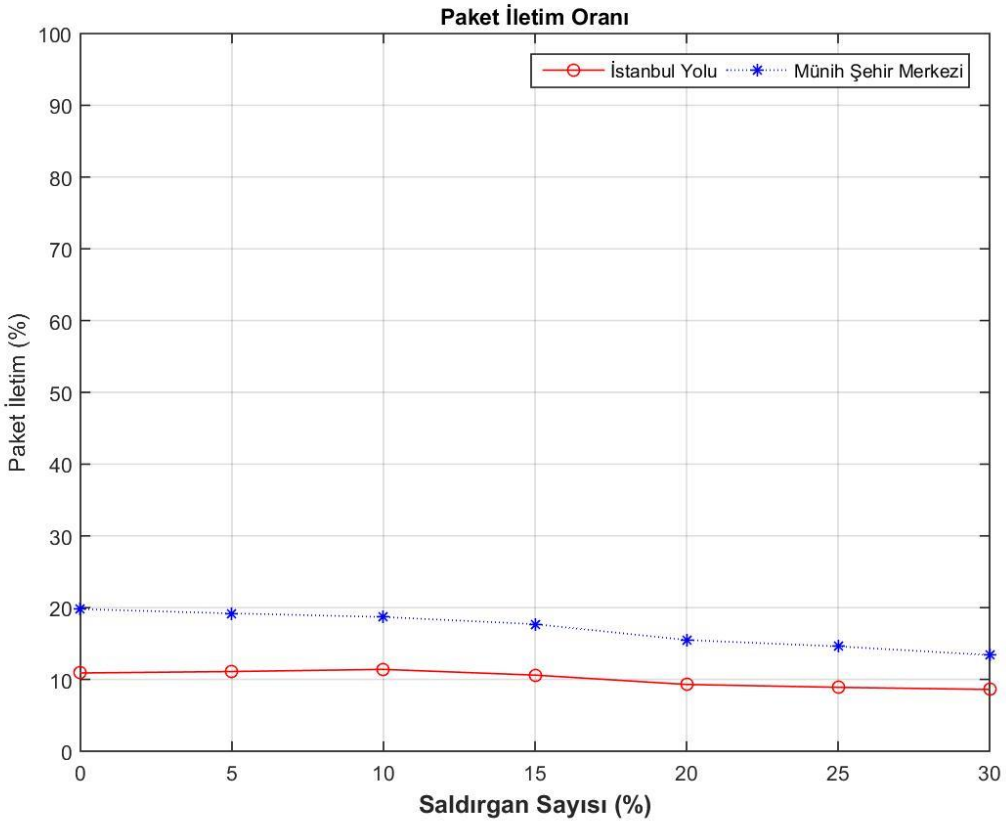
Şekil 5.20. AODV Sahte Bilgi Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.20.'de AODV yönlendirme protokolündeki sahte bilgi saldırısının ağdaki uçtan uca gecikmeye olan etkisi grafiksel olarak gösterilmiştir. Saldırgan düğüm, seçtiği kurban düğümü sistemden izole etmeye çalıştığı için, paket iletimini geciktirmeye çalışmıştır. Ancak atağın etkisi çok fazla olmadığı için uçtan uca gecikme iki harita da fazla etkilenmemiştir.

5.4. GPSR Yönlendirme Protokolü Saldırı Sonuçları

GPSR yönlendirme protokolünde de AODV yönlendirme protokolünde olduğu gibi dört saldırı da denenmiş ve sonuçları aşağıda verilmiştir. Gerçeğe yakın sonuçlar elde edilebilmesi için birden fazla bağlantı modelinde denenmiş ve her bir saldırgan farklı bağlantı modellerinde denenerek sonuçlar elde edilmiştir.

5.4.1. GPSR Karadelik Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



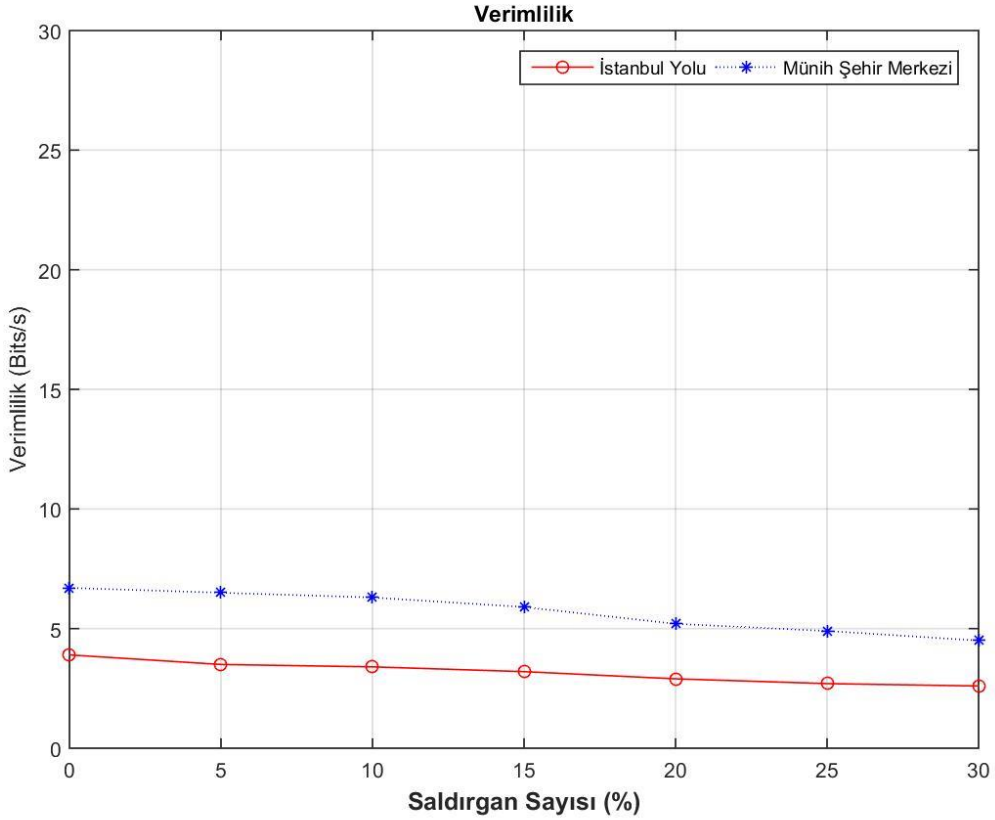
Şekil 5.21. GPSR Karadelik Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.21.'de GPSR yönlendirme protokolünde her iki haritada da gerçekleştirilen paket düşürme saldırısının sonuçları verilmiştir. AODV yönlendirme protokolünde olduğu gibi GPSR yönlendirme protokolünde de saldırgan sayısı arttıkça paket iletim oranında düşme olmuştur. Benzetimler sonucunda GPSR protokolünün saldırısız bir ortamda ortalama paket iletimi İstanbul Yolu haritasında %11 ve Münih haritasında %20 civarında olduğu görülmüştür.

GPSR protokolünde saldırı olması durumunda benzetimler sonucunda GPSR protokolünün ortalama paket iletimi İstanbul Yolu haritasında %10 iken bu oran

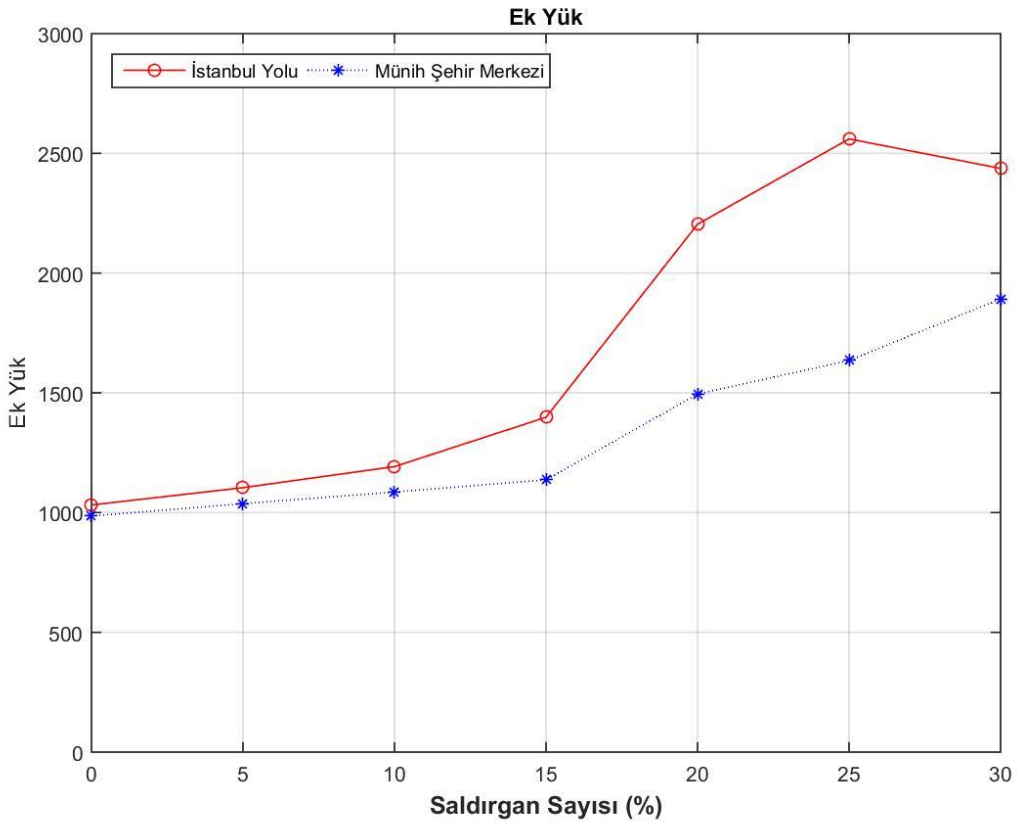
Münih haritasında %16 civarındadır. Münih haritasının daha yoğun olmasından dolayı saldırgan olması durumunda paket iletim oranı İstanbul Yolu haritasından daha yüksek çıkmıştır.

Burada GPSR yönlendirme protokolünün yeterli bir kontrol mekanizmasına sahip olmaması, mesaj ileten düğümün sadece komşu düğümlerinden bir tanesine mesaj iletip, mesaj iletim mekanizmasından çekilmesi, hedef düğümle mesaj gönderen düğüm arasında önceden bir yolun oluşturulmaması bu paket iletim oranının düşüklüğünü açıklamaktadır. Burada bu düşüklük sadece saldırgan araçların paket düşürmesiyle değil, paketin ulaşacağı yere ulaşamaması sonucu TTL (Time to Live) sayısının sıfıra ulaşmasıyla da bağlantılıdır. GPSR yönlendirme protokolünün aç gözlü yönlendirmeden çevresel yönlendirmeye geçmesi paketlerin döngüye girmesine ve düşmesine neden olmaktadır. Grafikten çıkarılacak nihai yorum, karadelik saldırısı GPSR yönlendirme protokolü uygulayan bir ağda, AODV protokolünde de olduğu gibi iletişimi ciddi şekilde etkilemekte, neredeyse durma noktasına getirmiştir.



Şekil 5.22. GPSR Karadelik Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

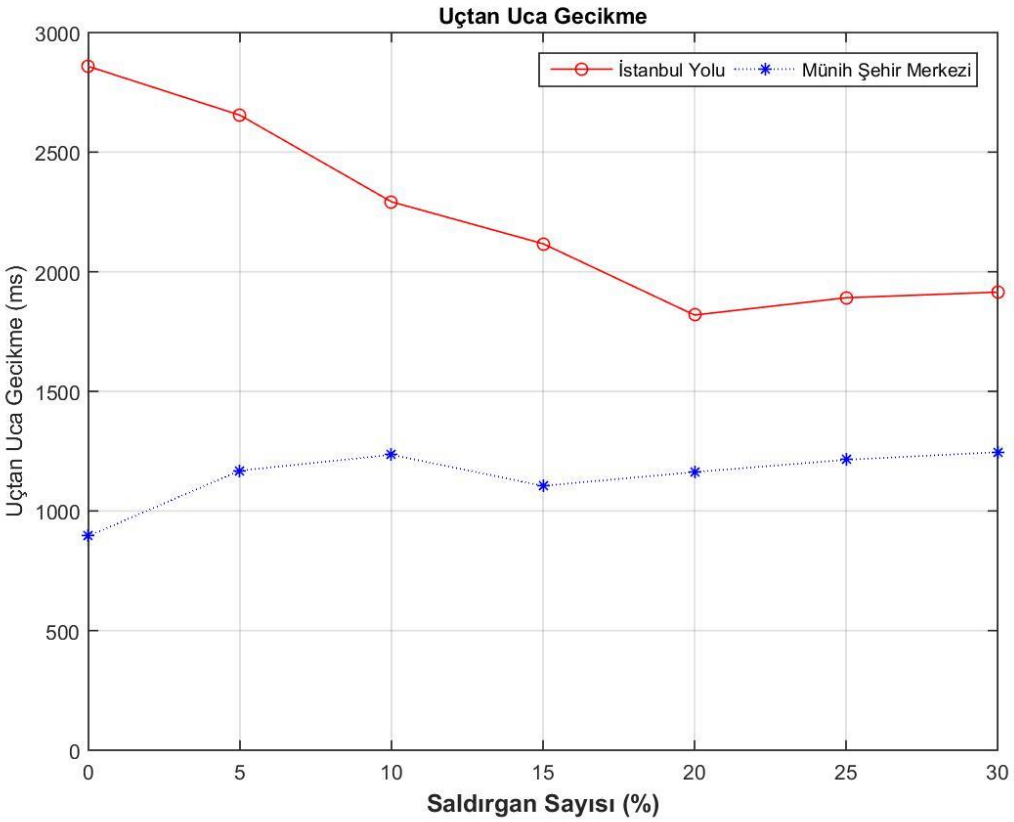
Şekil 5.22.'de GPSR protokolünde paket düşürme saldırısının iki haritada da benzetim sonucu ortaya çıkan verimlilik grafiği verilmiştir. Şekil 5.22.'de verilen paket iletim grafiğiyle doğru orantılı olarak iki haritada da verimlilik, saldırgan sayısının artmasıyla durma noktasına gelmiştir. Burada, Şekil 5.21.'in açıklamasında da bahsedildiği gibi, saldırgan sayısının artmasının yanı sıra, mesajların iletilmesi gereken yere iletilememesi sonucu (burada saldırgan harici TTL sayısı devreye girmektedir) verimlilik de düşmüştür. İstanbul Yolu haritasında saldırgan sayısı %5 iken verimlilik oranı 3.5 bit/s iken, bu oran Münih haritasında 6.5 bit/s'dir. Saldırgan sayısı %30 iken İstanbul Yolu'nda verimlilik 2.6 bit/s, Münih haritasında ise 4.5 bit/s'dir.



Şekil 5.23. GPSR Karadelik Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.23.'te GPSR yönlendirme protokolünde iki haritada da gerçekleştirilen karadelik saldırısı sonucunda ortaya çıkan ek yük oranı verilmiştir. Grafik incelendiğinde İstanbul Yolu haritasındaki haberleşmenin getirdiği ek yükün Münih haritasına göre daha yüksek olduğu görülmektedir. Saldırgan sayısı arttıkça iki haritada da ek yük oranı yükselmektedir. İstanbul Yolu haritasında saldırgan sayısı

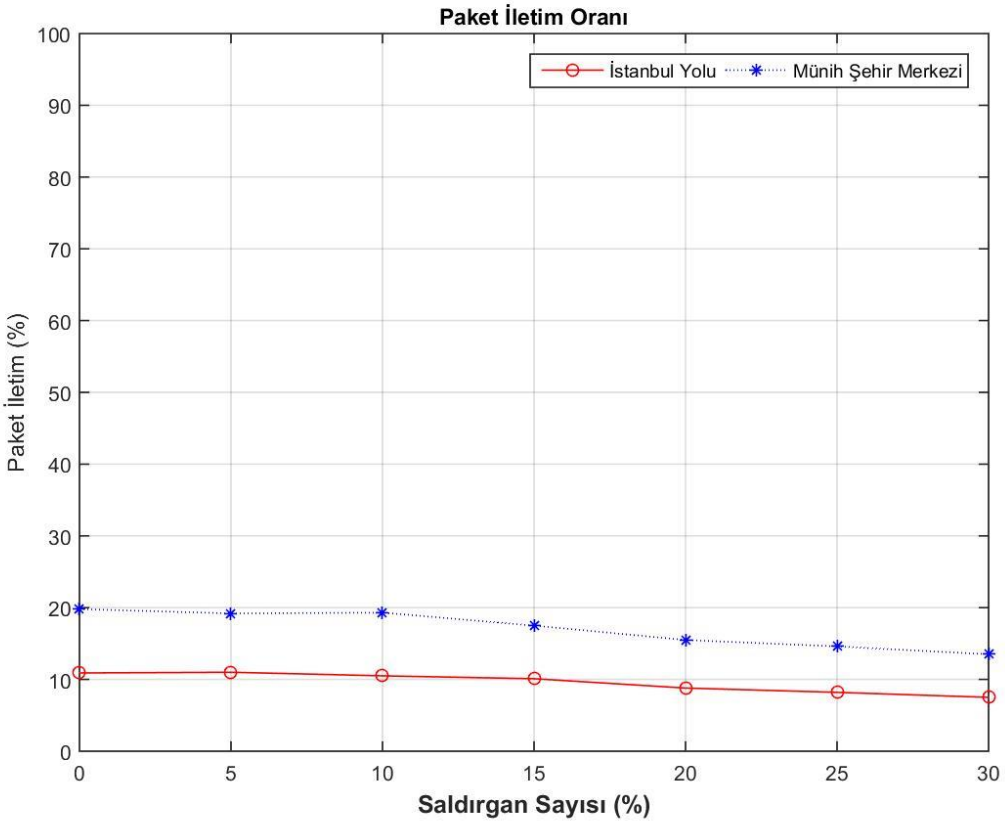
%25 iken veri paketi başına gönderilen yönlendirme paketi 2500 civarındadır. Bu durum GPSR yönlendirme protokolünün aç gözlü yönlendirme yapamadığı yerlerde çevresel yönlendirmeye geçerek ağı daha fazla gezmesine ve bunun sonucunda daha fazla kontrol paketi göndererek ek yükü artırmasına neden olmuştur.



Şekil 5.24. GPSR Karadelik Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

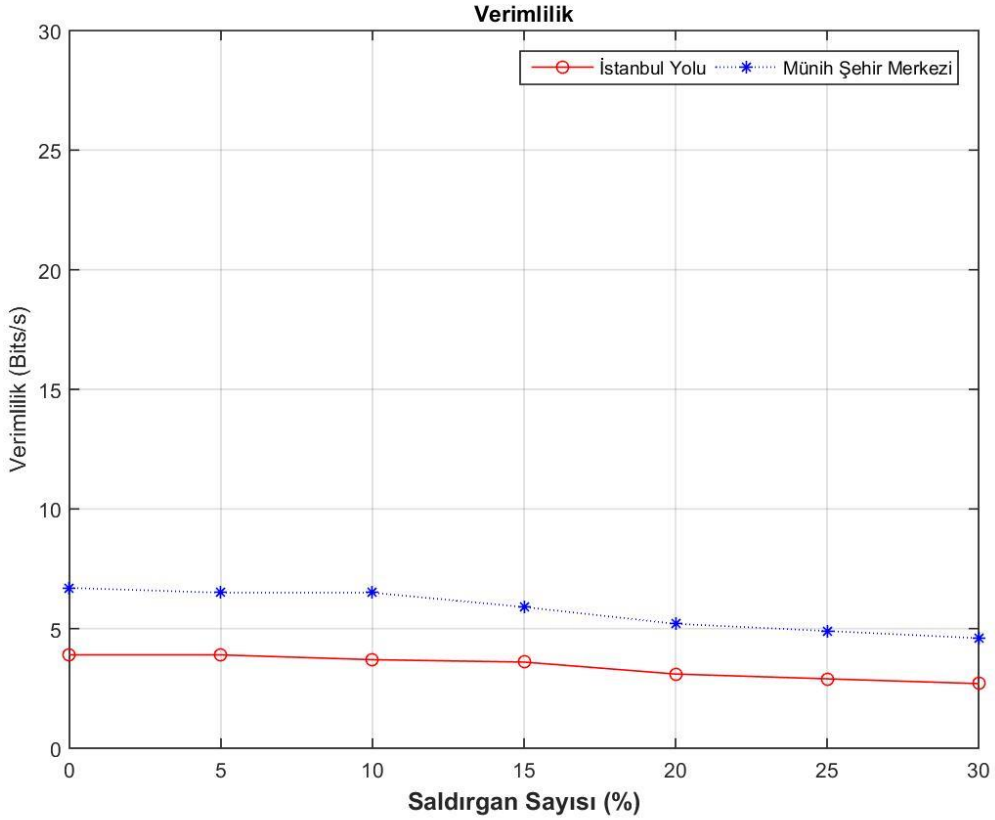
Şekil 5.24.'te GPSR yönlendirme protokolünde gerçekleştirilen karadelik saldırısı sonucu ortaya çıkan uçtan uca gecikme oranları verilmiştir. Münih haritasında uçtan uca gecikme saldırgan sayısı arttıkça sabit gibi görünmektedir. İstanbul Yolu haritasında ise, uçtan uca gecikme oranı düşmektedir.

5.4.2. GPSR Paket Düşürme Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



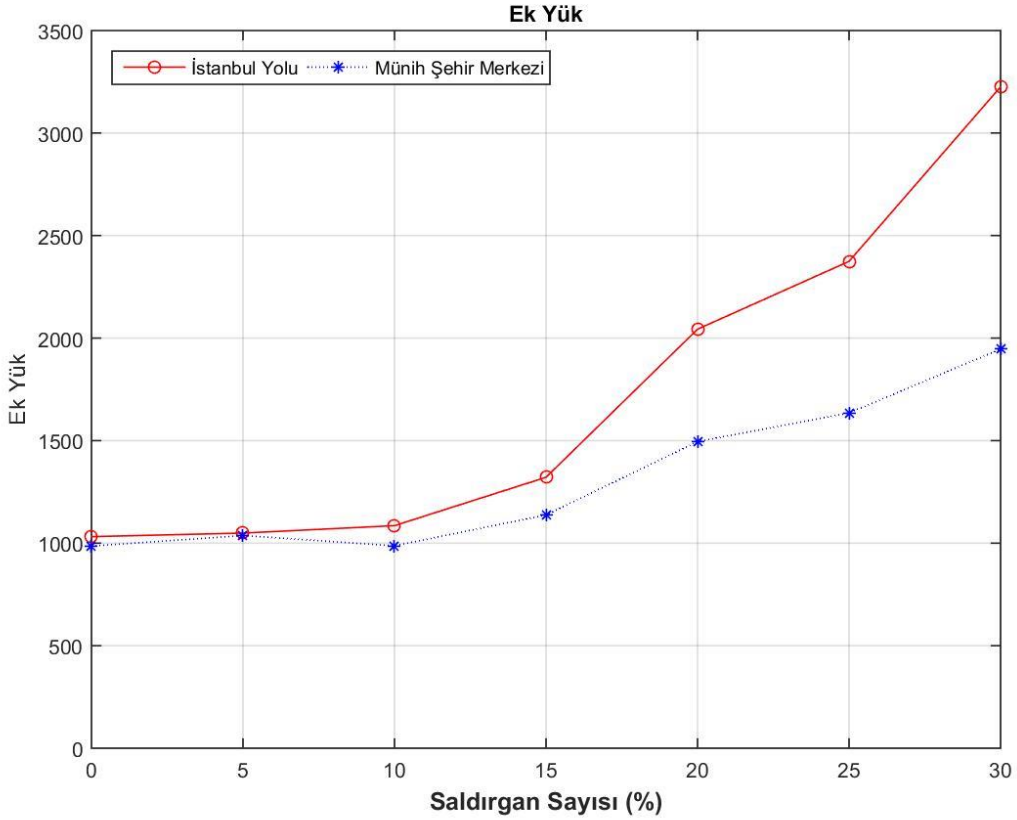
Şekil 5.25. GPSR Paket Düşürme Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.25.'te GPSR yönlendirme protokolünde hem İstanbul Yolu hem de Münih haritasında gerçekleştirilen paket düşürme saldırısının grafiksel sonuçları verilmiştir. Grafikte İstanbul ve Münih haritaları için saldırgan sayısı arttıkça paket iletim oranı da düşmektedir. Saldırgan sayısı %30'a ulaştığında Münih haritasındaki paket iletim oranı %13.5'dir. Bu durum İstanbul Yolu haritasında %7.5'dir. Münih haritasındaki düğüm yoğunluğu paket iletim oranındaki düşüşte farklılığa sebep olmuştur.



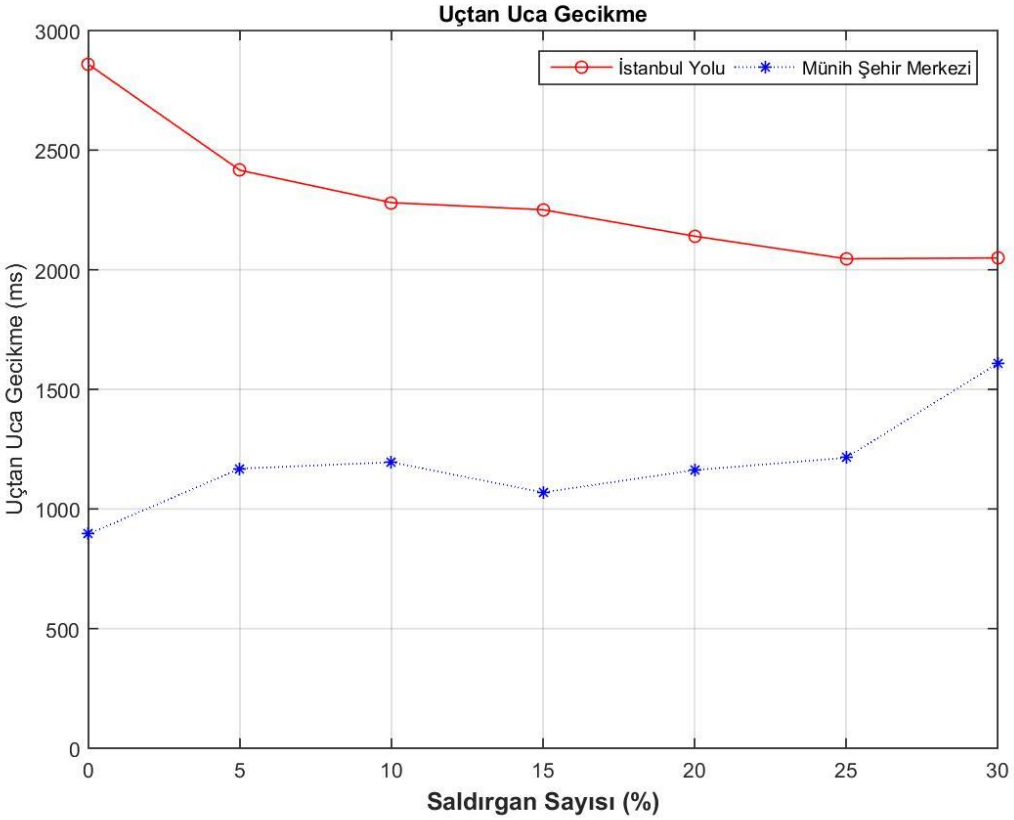
Şekil 5.26. GPSR Paket Düşürme Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.26.'da GPSR yönlendirme protokolünde gerçekleştirilen paket düşürme saldırısının verimliliğe olan etkisi gösterilmiştir. İki haritada da ağdaki verimliliğin saldırgan sayısının artmasıyla düştüğü görülmüştür. Saldırgan sayısı iki haritada da %30'a ulaştığında verimlilik İstanbul Yolu haritasında 2.7 bit/s'dir. Bu oran Münih haritasında 4.6 bit/s'dir.



Şekil 5.27. GPSR Paket Düşürme Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

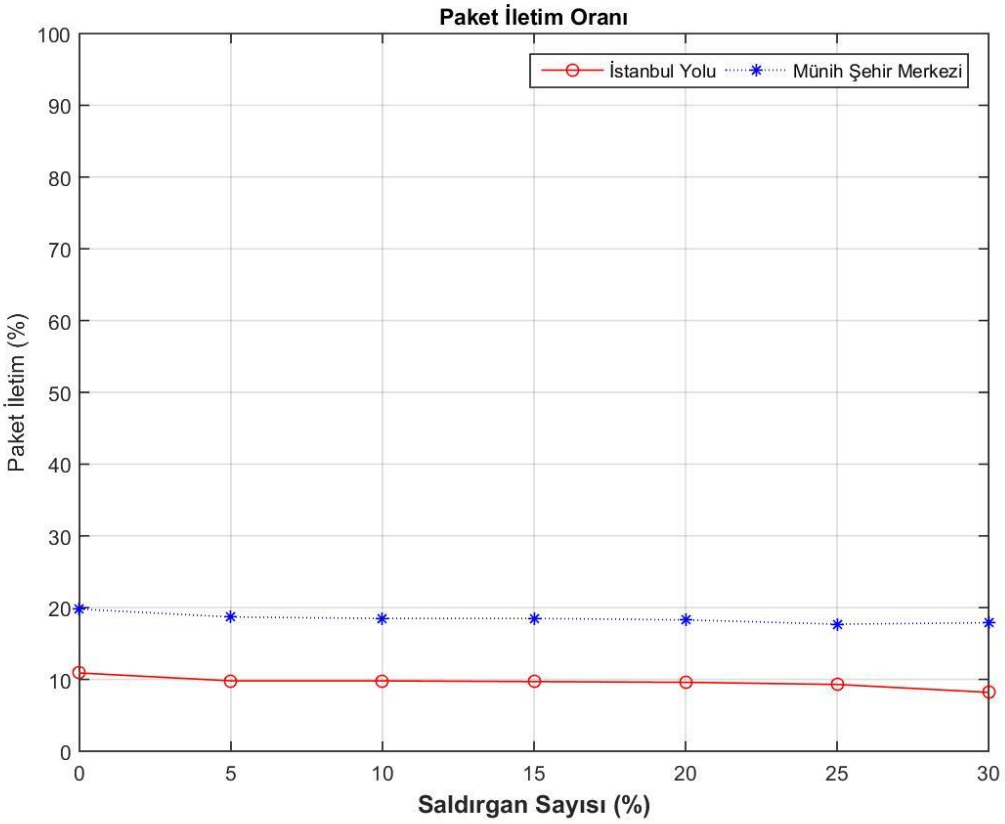
Şekil 5.27.'de GPSR protokolünde her iki haritada da gerçekleştirilen paket düşürme saldırısının ek yük oranları grafiksel olarak verilmiştir. Grafikte görüldüğü gibi iki haritada da ek yük oranı saldırgan sayısı arttıkça yükselmiştir. Saldırgan sayısı %15'i geçtiğinde her iki haritada da ek yük oranları daha fazla artış göstermiştir.



Şekil 5.28. GPSR Paket Düşürme Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

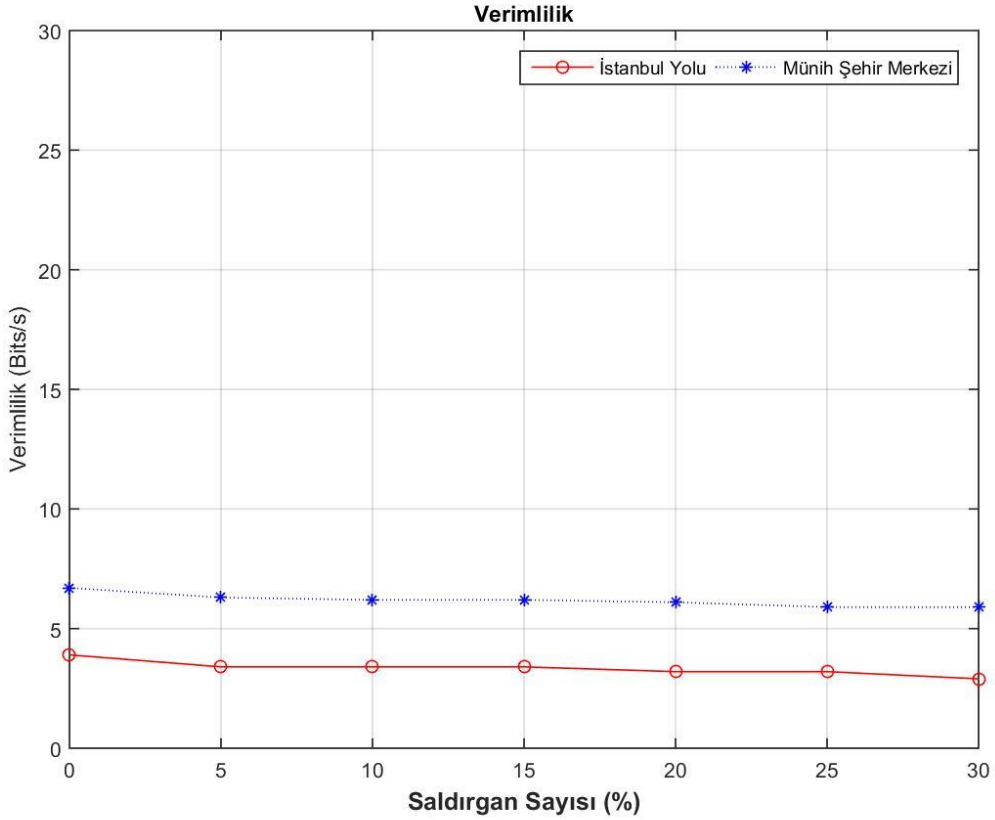
Şekil 5.28.'de GPSR yönlendirme protokolünde gerçekleştirilen paket düşürme saldırısının uçtan uca gecikmeye olan etkisi verilmiştir. Düğüm yoğunluğu daha fazla olan Münih haritasında saldırgan sayısı arttıkça uçtan uca gecikme yükselmektedir. Ancak İstanbul Yolu haritasında uçtan uca gecikme saldırgan sayısı arttıkça hafif bir azalma göstermektedir. Saldırgansız ortamda uçtan uca gecikme, Münih haritası için 895,4 ms iken, bu durum İstanbul Yolu haritasında 2858,3 ms'dir. Ancak saldırgan sayısı %30 olduğunda Münih haritasındaki uçtan uca gecikme 1608,1 ms iken İstanbul Yolu haritasında 2049,2 ms'dir.

5.4.3. GPSR Sel Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



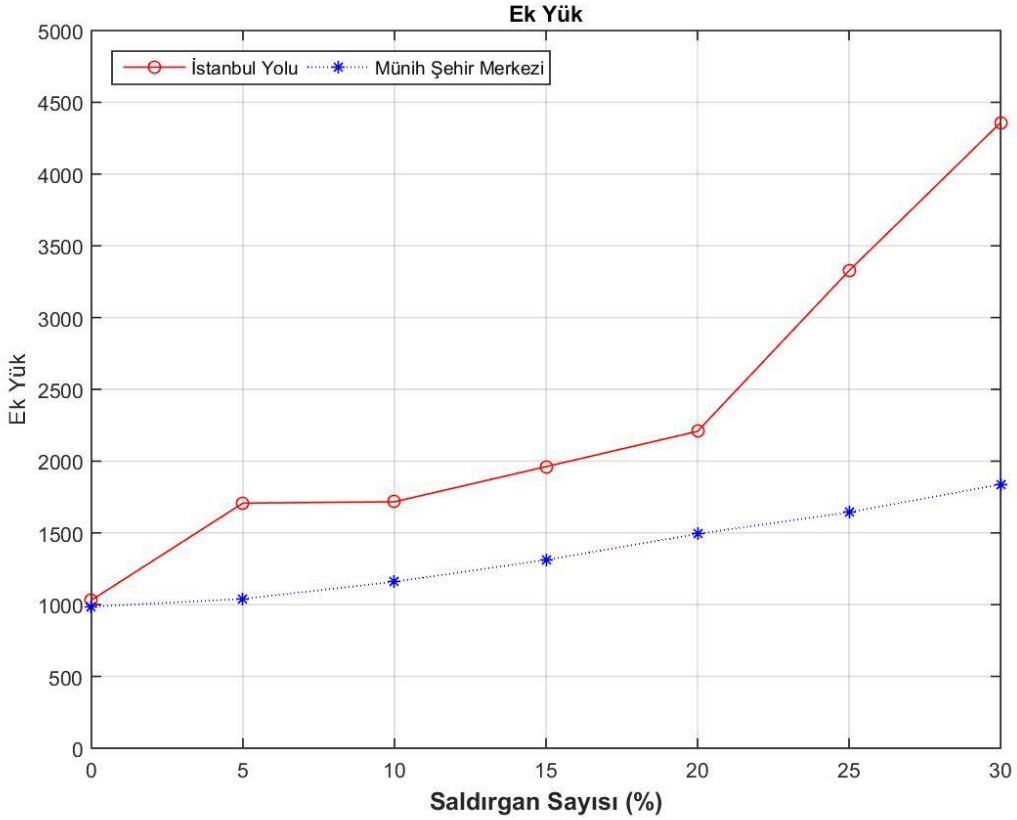
Şekil 5.29. GPSR Sel Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.29.'da GPSR yönlendirme protokolünde gerçekleştirilen sel saldırısının benzetim sonuçlarının grafiksel gösterimi verilmiştir. Saldırı, paket iletim oranında İstanbul Yolu haritasında saldırgan sayısı %20 ve üstüne ulaştığında etkili olmuştur. Ancak bu durum Münih haritası için geçerli değildir. Münih haritasında az da olsa sabit bir düşüş görülmektedir. İstanbul Yolu haritasında saldırgan sayısı %30'a ulaştığında paket iletim oranı %8.2'dir.



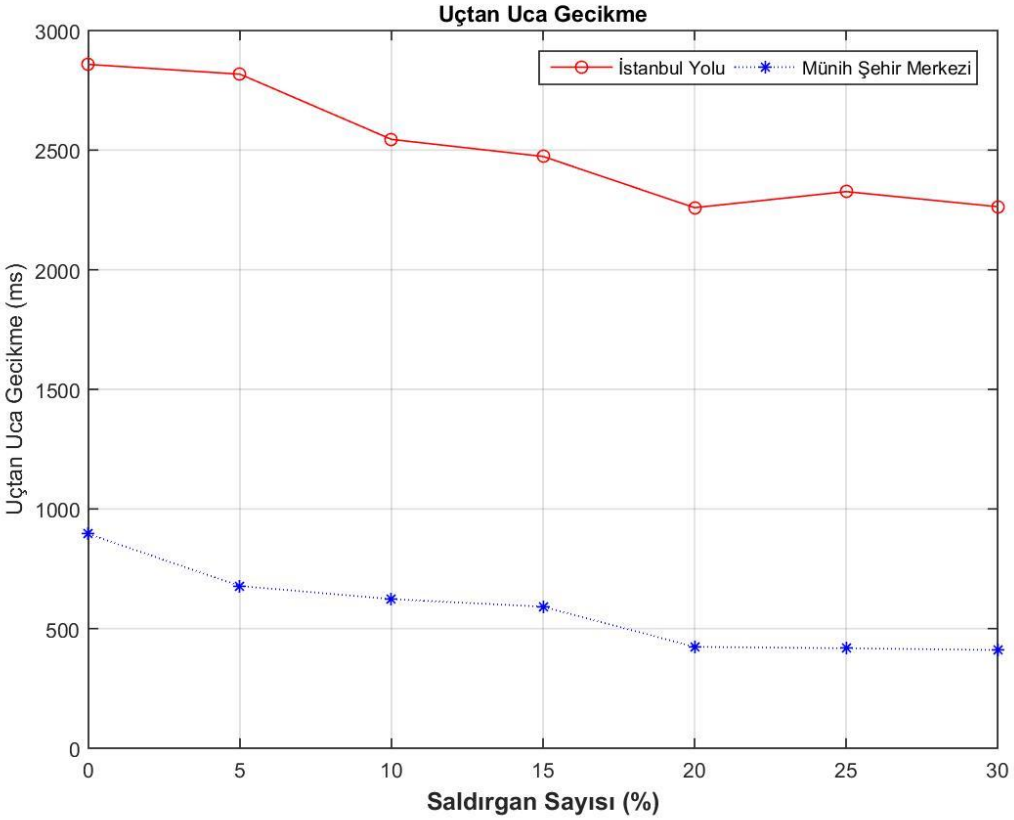
Şekil 5.30. GPSR Sel Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.30.'da GPSR yönlendirme protokolünde gerçekleştirilen sel saldırısının iki haritada da ortaya çıkan verimlilik sonuçları verilmiştir. İki haritada da verimlilikte, saldırgan sayısı arttıkça düşme gözlenmiştir. Münih haritasında saldırgan sayısı %30'a çıktığında verimlilik 5.9 bit/s'dir. Bu oran İstanbul Yolu haritasında 2.90 bit/s'dir.



Şekil 5.31. GPSR Sel Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

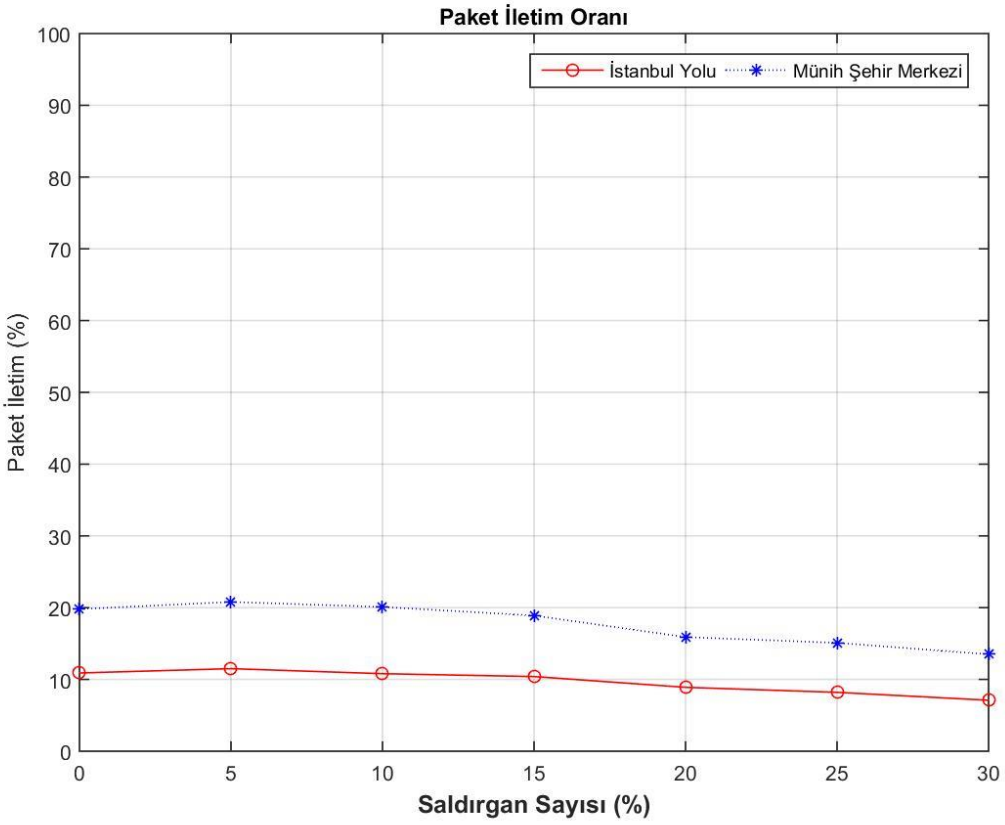
Şekil 5.31.'de GPSR yönlendirme protokolünde gerçekleştirilen sel saldırısı sonucu ortaya çıkan ek yük oranları verilmiştir. Ağda sürekli beacon istek paketleri gönderildiğinden, sisteme bindirilen ek yük iki haritada da artmıştır. Saldırgan sayısı %30 olduğu durumda İstanbul Yolu haritasında ek yük oranı 4358 iken, bu oran Münih haritasında 1837'dir.



Şekil 5.32. GPSR Sel Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

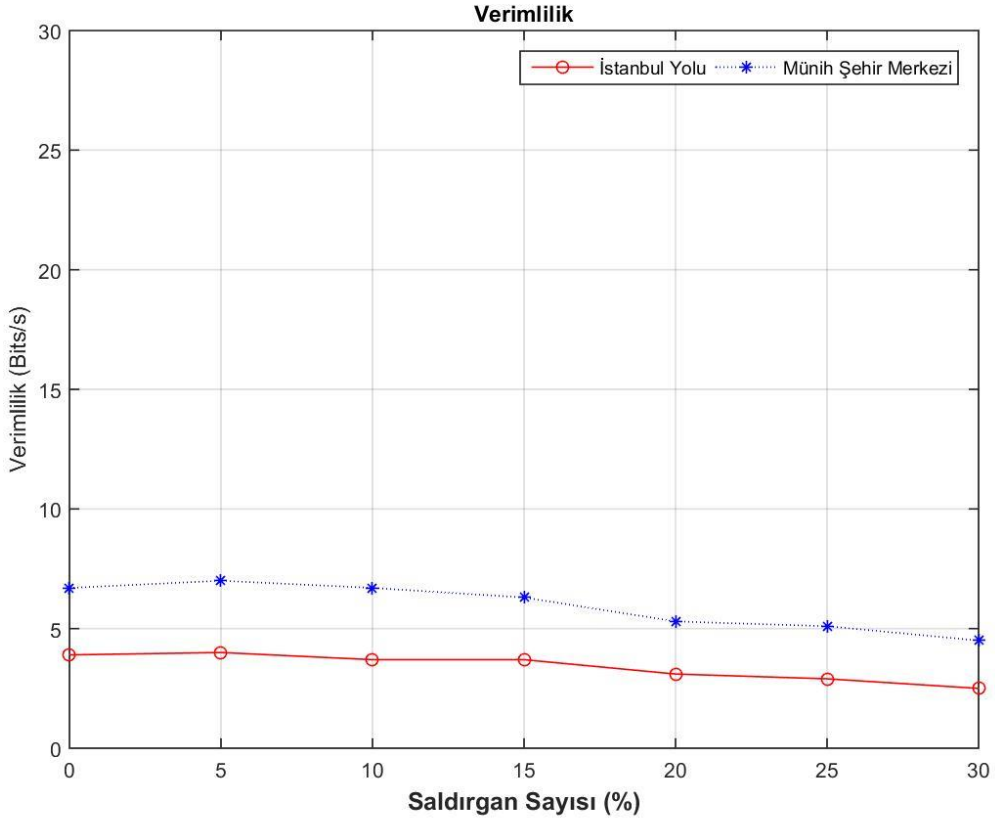
Şekil 5.32.'de GPSR yönlendirme protokolünde gerçekleştirilen sel saldırısının uçtan uca gecikmeye yaptığı etki grafiksel olarak gösterilmiştir. Saldırgan sayısı arttıkça iki haritada da uçtan uca gecikme az bir azalma göstermiştir. Saldırgan sayısı %15 olduğunda İstanbul Yolu haritasındaki uçtan uca gecikme 2473 ms'dir. Ancak bu durum Münih'te 591 ms'dir. Uçtan uca gecikme metriğinde de, iki haritadaki düğüm yoğunluğu farkının etkisi görülmektedir.

5.4.4. GPSR Sahte Bilgi Saldırısı Sonuçları (İstanbul Yolu – Münih Şehir Merkezi)



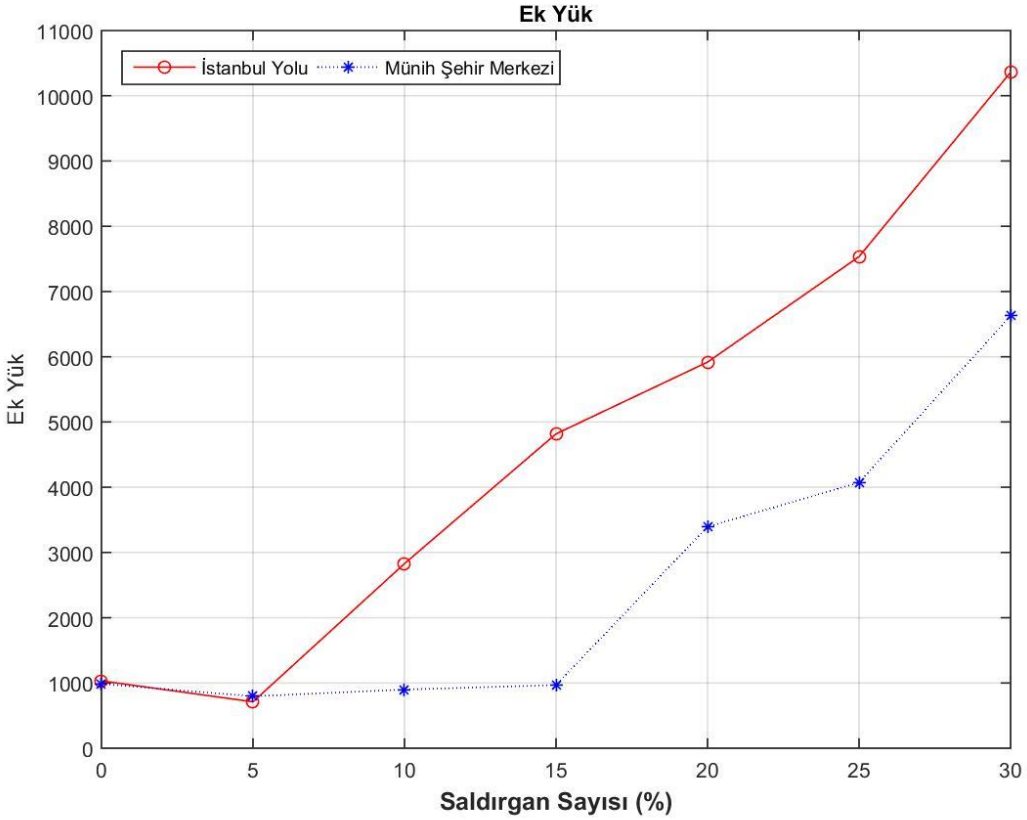
Şekil 5.33. GPSR Sahte Bilgi Saldırısı Paket İletim Oranı (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.33.'te GPSR yönlendirme protokolünde gerçekleştirilen sahte bilgi saldırısının iki haritada da ortaya çıkan paket iletim oranları verilmiştir. Gerçekleştirilen saldırı sonucunda Münih haritası, İstanbul Yolu haritasına göre daha fazla etkilenmiştir. Saldırgan sayısı %30'a ulaştığında Münih haritasında paket iletim oranı %13.5'tir. Bu oran İstanbul Yolu haritasında %7.1'dir. Bu durum Münih haritasında, sahte bilgi saldırısının İstanbul Yolu haritasına göre daha etkili olduğunu göstermektedir. Münih Şehir Merkezindeki arabaların birbirlerine daha yakın olması bu durumda etkili olmuştur.



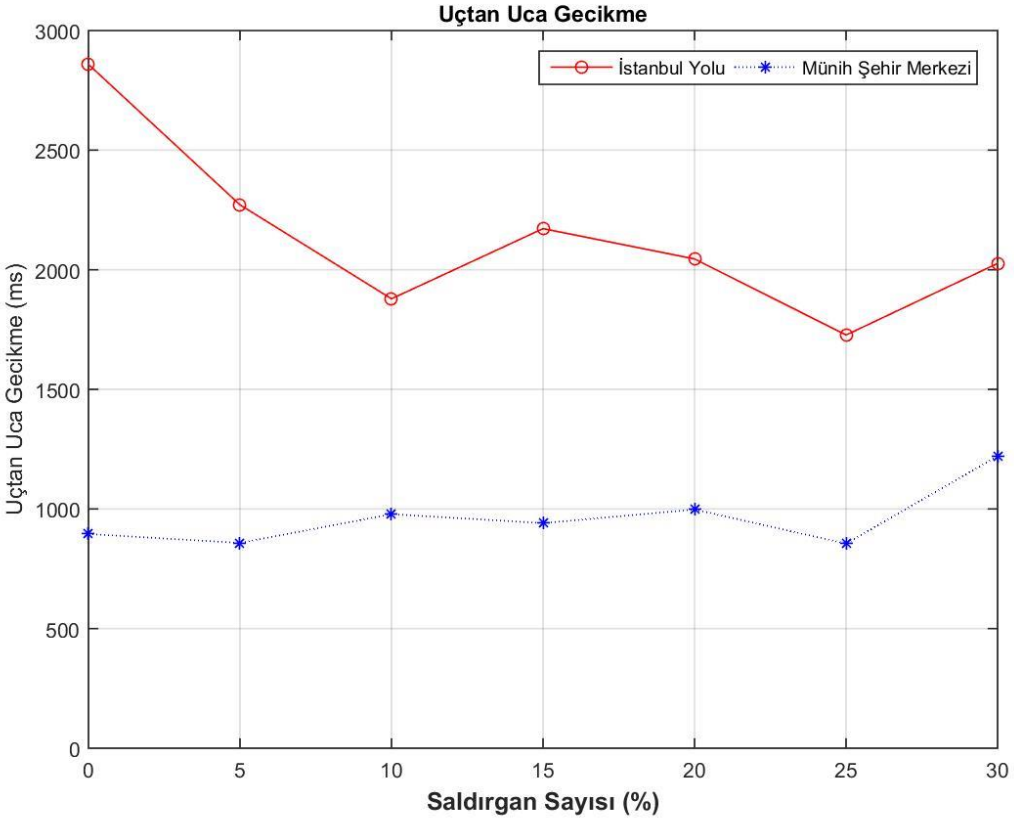
Şekil 5.34. GPSR Sahte Bilgi Saldırısı Verimlilik (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.34.'te GPSR'da gerçekleştirilen sahte bilgi saldırısının, iki haritada da ortaya çıkan grafiksel oranları verilmiştir. İki haritada da, saldırgan sayısı arttıkça verimlilik düşmüştür. Saldırgan sayısı %30'a ulaştığında Münih haritasındaki verimlilik 4.5 bit/s'dir. Bu oran İstanbul Yolu'nda 2.5 bit/s'dir.



Şekil 5.35. GPSR Sahte Bilgi Saldırısı Ek Yük (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.35.'te GPSR yönlendirme protokolünde gerçekleştirilen sahte bilgi saldırısının iki haritadaki ek yük oranı verilmiştir. İki haritada da saldırgan sayısının %5'i aşmasıyla birlikte ek yük oranı yükselmiştir. Grafik incelendiğinde İstanbul Yolu haritası saldırıdan, ek yük anlamında Münih haritasından daha fazla etkilenmiştir.



Şekil 5.36. GPSR Sahte Bilgi Saldırısı Uçtan Uca Gecikme (İstanbul Yolu – Münih Şehir Merkezi)

Şekil 5.36.'da ise GPSR yönlendirme protokolünde yapılan sahte bilgi saldırısının uçtan uca gecikme oranı verilmiştir. Grafikte, İstanbul Yolu haritasında saldırgan sayısı arttıkça uçtan uca gecikmede düşüş gözlenmiştir. Ancak, bu durum Münih haritasında farklılık göstermiş ve Münih haritası dalgalı bir seyir izlemiştir. Saldırgan sayısı %20 olduğunda Münih haritasındaki uçtan uca gecikme 997,68 ms'dir. Bu oran İstanbul Yolu'nda 2045 ms'dir. İki haritanın yoğunluk farkı uçtan uca gecikmede farklılık görülmesine neden olmuştur.

Fonseca ve arkadaşları [65], kullanılan hareketlilik modelinin, araçların hızlarının paket iletimini ve diğer metrikleri etkilediğinden bahsetmiştir. Ayrıca yine aynı çalışmada, GPSR'ın aç gözlü yönlendirmesinden bahsedilmiş ve bu sistemin her zaman paket iletimi için doğru düğüm seçemeyeceği söylenmiştir. Bu durum yapılan benzetimlerde GPSR yönlendirme protokolünün az bir iletim oranına sahip olduğunu desteklemektedir. Ayrıca sözü geçen çalışmada, çevresel yönlendirmeye geçiş yapan GPSR yönlendirme protokolünün sağ el kuralına göre iletimi sırasında paketi döngüye sokabileceği belirtilmiştir.

5.4.5. Saldırılar Hakkında Genel Yorum

Protokoller, düğüm yoğunluğu açısından iki farklı haritada denenmiş ve beklenildiği gibi, iki protokolün de saldırısız ortamda, düğüm yoğunluğu daha fazla olan haritada daha iyi sonuç verdiği görülmüştür. Düğüm yoğunluğu daha fazla olan Münih haritasında AODV yönlendirme protokolünün paket iletim oranı %72'dir. Bu durum İstanbul Yolu haritasında %63'tür. AODV yönlendirme protokolünün, rota tespit mekanizmasına sahip olması ve, hataları daha çabuk tespit etmesi bu oranın yüksek çıkmasında etkili olmuştur. Ancak, yönlendirme protokolü saldırıya maruz kaldığında bu oran ciddi şekilde düşmektedir. Örneğin karadelik saldırısında, saldırgan sayısı %5 olduğunda bile AODV yönlendirme protokolünde Münih haritasında ve İstanbul Yolu haritasında paket iletim oranı %31'e kadar düşmektedir. AODV protokolünde sel saldırısı hariç diğer saldırılar, paket iletimini ciddi oranda etkilemektedir.

GPSR yönlendirme protokolüne bakıldığında ise, AODV yönlendirme protokolünde olduğu gibi, düğüm yoğunluğu daha fazla olan haritada paket iletiminin daha fazla olduğu görülmüştür. Ancak paket iletimi AODV kadar yüksek olmamıştır. Bu durum, GPSR yönlendirme protokolünün anlık karar vermesi ve mesajı tek bir düğüme iletmesiyle ilişkilendirilebilir. Saldırısız ortamda GPSR yönlendirme protokolünün paket iletim oranı Münih haritasında %20, İstanbul Yolu haritasında ise %10'dur. Aynı şekilde veriler incelendiğinde, GPSR yönlendirme protokolünün ek yük oranı AODV yönlendirme protokolüne göre çok daha yüksek çıkmıştır. Bu durum GPSR yönlendirme protokolünün kendi içinde iki farklı yönlendirme kullanmasıyla ilişkilendirilebilir. GPSR yönlendirme protokolü, Aç Gözlü Yönlendirme yapamadığı yerlerde Çevresel Yönlendirmeye geçmekte ve bu da sistemde daha fazla kontrol paketinin dolaşmasına neden olmaktadır. Saldırılara bakıldığında, AODV protokolünde olduğu gibi, GPSR yönlendirme protokolü de saldırılardan ciddi oranda etkilenmiştir. Saldırıların türlerine bakıldığında, GPSR saldırılardan büyük ölçüde etkilenmiştir.

Kullanılan iki farklı protokol genel olarak incelenirse, araçsal tasarsız ağlar için kullanılan yönlendirme protokolünde kontrol mekanizmasının olması avantaj sağlamaktadır. İletilecek paket için önceden yol oluşturulması, hata kontrol paketlerinin olması protokolün verimliliğine etki etmektedir. Bu bilgiler ışığında

AODV yönlendirme protokolü, bu bahsedilen özellikleri barındırdığı için GPSR yönlendirme protokolünden saldırısız ortamda daha iyi sonuç vermiştir.

Benzetimlere, kullanılan hareketlilik ve kullanılan bağlantı dosyaları açısından da bakılmalıdır. Kullanılan bağlantı dosyasında, hangi düğümün hangi düğümle haberleşeceği, paket gönderimini ne zaman başlatacağı gibi bilgiler rastgele oluşturulduğundan, benzetim sonuçlarına etki etmektedir. Ayrıca kullanılan hareketlilik (harita, düğümlerin hızları vs.) benzetim sonuçlarında büyük rol oynamaktadır. Bu durum yukarıda da bahsedildiği gibi, AODV ve GPSR protokolündeki paket iletim oranının Münih haritasında ve İstanbul Yolu haritasında farklı çıkmasını desteklemektedir.

AODV ve GPSR yönlendirme protokolünün saldırısız ve saldırılı ortamdaki verileri Çizelge 5.2., Çizelge 5.3., Çizelge 5.4. ve Çizelge 5.5.'te ayrıntılı bir şekilde verilmiştir.

Çizelge 5.2. AODV ve GPSR Paket İletim Oranları

Paket İletim Oranları (%)																
Saldırgan Sayısı	Karadelik Saldırısı				Paket Düşürme Saldırısı				Sel Saldırısı				Sahte Bilgi Saldırısı			
	Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu	
	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV
0	19,8	72,6	10,9	62,9	19,8	72,6	10,9	62,9	19,8	72,6	10,9	62,9	19,8	72,6	10,9	62,9
5%	19,2	31,0	11,1	31,3	19,2	70,5	11,0	55,8	18,7	72,3	9,8	61,1	20,8	72,8	11,5	60,2
10%	18,7	13,6	11,4	20,4	19,3	68,0	10,5	49,7	18,5	71,7	9,8	59,8	20,1	69,6	10,8	58,0
15%	17,7	9,6	10,6	10,5	17,5	63,5	10,1	41,5	18,5	71,8	9,7	58,4	18,9	66,9	10,4	54,3
20%	15,5	6,3	9,3	6,3	15,5	56,0	8,8	31,2	18,3	71,2	9,6	54,0	15,9	63,5	8,9	49,7
25%	14,6	5,1	8,9	5,6	14,6	51,9	8,2	28,3	17,7	70,5	9,3	45,2	15,1	60,4	8,2	48,1
30%	13,4	4,8	8,6	4,6	13,5	47,1	7,5	24,4	17,9	60,8	8,2	44,5	13,5	56,9	7,1	46,4

Çizelge 5.3. AODV ve GPSR Ek Yük Değerleri

Ek Yük																
Saldırgan Sayısı	Karadelik Saldırısı				Paket Düşürme Saldırısı				Sel Saldırısı				Sahte Bilgi Saldırısı			
	Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu	
	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV
0	985,74	1,60	1031,81	7,60	985,74	1,60	1031,81	7,60	985,74	1,60	1031,81	7,60	985,74	1,60	1031,81	7,60
5%	1037,13	12,80	1104,05	15,20	1037,13	1,70	1049,18	9,20	1040,60	23,20	1707,42	32,80	795,81	3,93	710,62	8,89
10%	1085,91	32,10	1192,00	18,20	987,05	1,70	1085,30	9,50	1159,45	50,20	1716,75	67,80	898,94	3,85	2829,17	11,29
15%	1136,87	51,10	1397,87	34,30	1137,56	1,70	1321,16	10,00	1311,67	87,00	1961,48	117,60	968,05	5,62	4817,77	13,62
20%	1495,00	70,70	2204,02	81,10	1495,11	1,60	2043,38	10,30	1492,78	133,00	2207,50	194,90	3394,57	7,91	5917,75	16,80
25%	1635,00	122,10	2560,14	63,40	1635,01	1,60	2374,18	10,60	1644,04	162,70	3326,57	327,30	4071,78	9,74	7533,66	18,71
30%	1892,02	71,80	2437,22	59,40	1946,32	1,60	3225,33	10,60	1837,24	173,20	4358,17	339,20	6624,23	11,62	10359,74	20,79

Çizelge 5.4. AODV ve GPSR Verimlilik Değerleri

Verimlilik (Bit/s)																
Saldırgan Sayısı	Karadelik Saldırısı				Paket Düşürme Saldırısı				Sel Saldırısı				Sahte Bilgi Saldırısı			
	Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu	
	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV
0	6,7	24,4	3,9	21,1	6,7	24,4	3,9	21,1	6,7	24,4	3,9	21,1	6,7	24,40	3,9	21,1
5%	6,5	10,4	3,5	10,5	6,5	23,7	3,9	18,7	6,3	24,2	3,4	20,5	7,0	24,42	4,0	20,2
10%	6,3	4,6	3,4	6,9	6,5	22,8	3,7	16,7	6,2	24,0	3,4	20,1	6,7	23,34	3,7	19,4
15%	5,9	3,3	3,2	3,5	5,9	21,3	3,6	13,9	6,2	24,1	3,4	19,6	6,3	22,45	3,7	18,2
20%	5,2	2,4	2,9	2,2	5,2	18,7	3,1	10,5	6,1	23,9	3,2	18,1	5,3	21,25	3,1	16,7
25%	4,9	2,0	2,7	2,0	4,9	17,4	2,9	9,6	5,9	23,7	3,2	15,2	5,1	20,24	2,9	16,2
30%	4,5	2,1	2,6	1,8	4,6	15,7	2,7	8,2	5,9	23,7	2,9	15,0	4,5	19,11	2,5	15,6

Çizelge 5.5. AODV ve GPSR Uçtan Uca Gecikme Değerleri

Uçtan Uca Gecikme Zamanı (Milisaniye)																
Saldırgan Sayısı	Karadelik Saldırısı				Paket Düşürme Saldırısı				Sel Saldırısı				Sahte Bilgi Saldırısı			
	Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu		Münih Şehir Merkezi		İstanbul Yolu	
	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV	GPSR	AODV
0	895,36	299,20	2858,26	1198,40	895,36	299,20	2858,26	1198,40	895,36	299,20	2858,26	1198,40	895,36	299,20	2858,26	1198,40
5%	1168,84	270,00	2654,34	562,90	1168,84	286,00	2415,75	1051,70	678,06	277,50	2817,39	1075,40	858,03	275,54	2271,25	1141,87
10%	1234,82	463,70	2292,22	399,40	1195,27	278,30	2280,32	956,00	623,32	250,90	2544,82	1090,50	978,20	288,82	1878,56	1103,87
15%	1105,18	239,00	2117,10	275,20	1069,25	256,00	2250,86	837,00	591,46	268,90	2473,61	1122,60	940,84	274,04	2171,83	1085,97
20%	1162,55	164,90	1818,93	199,90	1162,55	252,60	2140,30	665,40	423,57	273,20	2259,39	1129,60	997,68	275,15	2045,21	1092,40
25%	1214,00	112,90	1891,31	171,90	1214,00	238,90	2045,87	617,70	417,82	270,90	2326,58	1437,00	855,23	291,92	1727,24	1146,14
30%	1245,89	258,50	1914,63	118,10	1608,13	237,40	2049,23	589,50	410,39	292,80	2263,46	1362,60	1221,24	283,84	2026,38	1119,19

6. SONUÇ

Araçsal tasarsız ağların kullanımı gün geçtikçe artmaktadır. Araçların kendi aralarında ve yol kenarlarındaki yol kenarı birimleri ile haberleşmesini sağlayan yapı, trafikte can güvenliğini, araçların daha güvenli bir şekilde yol almasını sağlamaktadır. Birbirleriyle haberleşebilen araçlar kendi aralarında yol bilgilerini, trafik bilgilerini paylaşabilirler. Trafikte herhangi bir kaza ya da sıkışıklık olduğu zaman diğer araçlara haber gönderen araç, diğer araçların daha güvenli bir yolculuk yapmasını sağlayabilir. Bu bilgilerin yanında sistem araçlara park yerlerini yakındaki benzin istasyonlarını, eğlence yerlerinin de bilgisini vererek sürüşü daha keyifli bir hale getirebilir.

Sisteme giren saldırgan araçlar yaptıkları saldırılar sonucunda sistemin çalışmasına veya diğer araçlara zarar verebilirler. Araçsal tasarsız ağlara karşı yapılan saldırılar sonucunda ağda sadece veri kaybı olmayacak, can ve mal kaybı söz konusu olacaktır. Saldırıyı gerçekleştiren araç (örn; sahte bilgi saldırısı) gönderdiği gerçek olmayan bilgilerle trafikteki araçları yanlış yönlendirerek trafikte kazaya ve daha da fazlası can kaybına neden olabilir.

Araçsal tasarsız ağlar mobil tasarsız ağların hızla gelişen bir kolu olmakta ve gün geçtikçe de kullanımı artmaktadır. Ancak mobil tasarsız ağlardaki güvenlik sorunu burada çok daha büyük bir önem kazanmaktadır. Araçların hızlı hareket etmesi, sürekli yer değiştirmesi araçsal tasarsız ağları saldırıya çok açık hale getirmektedir. Araçsal tasarsız ağlardaki saldırıların analizi gerçekçi olmalı ve bu bağlamda getirilen çözümlerin de uygulanabilir olması gerekmektedir.

Araçsal tasarsız ağlardaki saldırıların sınıflandırılmasının düzgün bir şekilde yapılıp, saldırıların iyice analiz edilmesi gerekmektedir. Saldırıların sisteme verecekleri zararlar iyice anlaşılıp ona göre yorumlanması, sistemin daha güvenli kullanılmasına ve daha iyi güvenlik çözümlerinin gerçekleştirilmesine olanak sağlayacaktır. Literatürde, böyle kapsamlı bir analiz bulunmamaktadır.

Saldırıların analizi sonucunda yapılacak olan benzetimlerin gerçek hayata uygun ve gerçek hayata en yakın trafik şartlarında yapılması saldırıların vereceği zararı anlamak açısından sağlıklı olacaktır. Yapılan benzetimlerin gerçeğe uygun olması

açısından, İstanbul yolu haritası ve Münih kent merkezi haritası çıkarılmış ve benzetimler bu haritalar üstünden gerçekleştirilmiştir. Yine, gerçeğe uygun olması açısından, benzetimler sırasında farklı bağlantı dosyaları kullanılmıştır. Bu nedenle bu çalışmada 4 adet saldırı analiz edilmiştir. Bu saldırılar; karadelik saldırısı, sel saldırısı, düşürme saldırısı ve sahte bilgi saldırısıdır. Ağda saldırgan düğümün yaptığı etki 4 farklı başlık altında incelenmiştir;

- Paket İletim Oranı
- Verimlilik
- Ek Yük
- Uçtan Uca Gecikme

Ağda gerçekleştirilen saldırılar sonucunda ortaya çıkan verilerde paket iletim oranının ve verimliliğin saldırgan sayısıyla doğru orantılı olarak, saldırgan sayısı arttıkça düştüğünü gözlemlenmiştir. Gerçekleştirilen 4 farklı saldırıda ve seçilen protokollerde gerçekleştirilen saldırılar sonucunda saldırının ağda nasıl bir tahribat yaptığı grafiklerle gösterilmiştir. Ayrıca yapılan benzetimler sonucunda açıkça görülmüştür ki, seçilen parametreler (Trafik örüntüleri, topoloji vs.) benzetim sonuçlarında ciddi oranda etki etmektedir.

Bu çalışmada, araçsal tasarsız ağlarda sıkça kullanılan AODV yönlendirme protokolü ile coğrafi tabanlı GPSR yönlendirme protokolü kullanılarak 4 farklı saldırı gerçekleştirilmiştir. Bu saldırılar; karadelik saldırısı, paket düşürme saldırısı, sel saldırısı ve sahte bilgi saldırısıdır. Benzetim sonuçları göstermiştir ki, iki yönlendirme protokolü de saldırgansız bir ağda, yüksek bir performans göstermemiştir. Bunun yanında, ağdaki saldırgan oranı arttıkça, iki protokolde de verim düşmektedir. Araçsal tasarsız ağlarda, coğrafi protokollerin kullanımı daha uygun görünse de, yapılan benzetimler sonucu ağda, kontrol mekanizmasına sahip bir yönlendirme protokolü kullanılması, ağın verimliliği açısından daha sağlıklı olacaktır.

Yapılan benzetimler sonucunda, AODV yönlendirme protokolünün, GPSR yönlendirme protokolünden daha iyi sonuç verdiği görülmüştür. Ancak AODV yönlendirme protokolü de, düğüm yoğunluğu daha az olan haritada (İstanbul Yolu), diğer haritaya (Münih Şehir Merkezi) göre daha kötü bir sonuç vermiştir. AODV yönlendirme protokolünün paket iletim oranı düğüm yoğunluğu fazla olan Münih haritasında %72, İstanbul Yolu haritasında ise %62'dir. Bu durum GPSR

yönlendirme protokolünde sırasıyla %20 ve %11'dir. Bu sonuçlardan açıkça görülmektedir ki, kullanılan haritalarda ve parametrelerde, saldırısız bir ortamda AODV yönlendirme protokolü, GPSR yönlendirme protokolünden daha iyi bir sonuç vermektedir. Ancak saldırı durumunda iki protokolde de paket iletim oranı ciddi anlamda düşmektedir. Örneğin karadelik saldırısında AODV yönlendirme protokolünde Münih haritasında paket iletimi %4.8'e kadar düşerken, İstanbul Yolu haritasında %4.6'ya kadar düşmüştür. Aynı durum GPSR yönlendirme protokolünde sırasıyla %13.4 ve %8.6'dır. Bu da iki protokolün, saldırılara çok açık protokoller olduğunu göstermektedir.

Bu bilgiler ışığında araçsal tasarsız ağlarda iki protokolden biri kullanılmak istenirse AODV yönlendirme protokolü daha verimli bir protokol olacaktır. Ancak her iki protokol de ağdaki düğümlerin iyi niyetli oldukları varsayımına dayanmaktadır. Durum böyle olmadığında, ağda ciddi performans düşüşüne neden olmaktadır. Bu nedenle güvenlik sistemelerinin geliştirilmesi kaçınılmazdır. Bu tezde yapılan çalışma, gelecek çalışmalar için temel olacaktır.

KAYNAKLAR

[1] Conti, M., Boldrini, C., Kanhere, S. S., Mingozzi, E., Pagani, E., Ruiz, P. M., Younis, M., From MANET to people-centric networking: Milestones and open research challenges. *Computer Communications,* 71, 1-21, **2015**.

[2] Pietro, R. D., Guarino, S., Verde, N. V., Domingo-Ferrer, J., Review: Security in wireless ad-hoc networks - A survey, *Computer Communications,* 51, 1-20, **2014**.

[3] Mokhtar, B., Azab, M., Survey on Security Issues in Vehicular Ad Hoc Networks. *Alexandria Engineering Journal,* 54(4), 1115-1126, **2015**.

[4] Raya, M., Hubaux, J.-P., Securing vehicular ad hoc networks, *Journal of Computer Security.,* 15(1), 39-68, **2007**.

[5] Bibhu, V., Kumar, R., Kumar, B. S., Singh, D. K., Performance Analysis of black hole attack in VANET. *International Journal Of Computer Network and Information Security,* 4(11), 47, **2012**.

[6] Ahmed, E. F., Abouhogail, R. A., Yahya, A., Performance Evaluation of Blackhole Attack on VANET's Routing Protocols, *International Journal of Software Engineering and Its Applications,* 8(9), 39-54, **2014**.

[7] Bala, A., Bansal, M., Singh, J., Performance Analysis of MANET under Blackhole Attack, *Networks and Communications*, 27-29 December, **2009**.

[8] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., Zedan, H., A comprehensive survey on vehicular Ad Hoc network, *Journal of Network and Computer Applications, 37*, 380-392, **2014**.

[9] Paul, B., Ibrahim, M., Bikas, M., Naser, A., VANET Routing Protocols: Pros and Cons, *International Journal of Computer Applications***,** 20 (1), 28-34, **2011**.

[10] He, G., Destination-sequenced distance vector (DSDV) protocol. *Networking Laboratory, Helsinki University of Technology*, 1-9, **2002**.

[11] Murthy, S., Garcia-Luna-Aceves, J. J., An efficient routing protocol for wireless networks. *Mobile Networks and Applications, 1*(2), 183-197, **1996**.

[12] Guangyu, P., Gerla, M., & Tsu-Wei, C., Fisheye state routing: a routing scheme for ad hoc wireless networks*, IEEE International Conference on Communications*, **2000**.

[13] Jacquet, P., Mühlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., Viennot, L., Optimized link state routing protocol for ad hoc networks*, In Proceedings of The Multi Topic Conference,* (pp. 62 - 68)*,* **2001**.

[14] Perkins, C. E., Royer, E. M., Ad-hoc on-demand distance vector routing*, In Proceedings of The Mobile Computing Systems and Applications,* 25-26 February, New Orleans, LA, 90-100*,* **1999**.

[15] Johnson, D. B., Maltz, D. A. Dynamic source routing in ad hoc wireless networks, *Mobile computing,* 153-181, **1996**.

[16] Park, V. D., Corson, M. S., A highly adaptive distributed routing algorithm for mobile wireless networks*, In Proceedings of the IEEE Computer and Communications Societies. Driving the Information Revolution*, 7-12 April, Kobe, **1997**.

[17] Haas, Z. J., A new routing protocol for the reconfigurable wireless networks*, In Proceedings of The Universal Personal Communications Record*, 12-16 October, San Diego, CA, **1997**.

[18] Tsu-Wei, C., Gerla, M., Global state routing: a new routing scheme for ad-hoc wireless networks*, In Proceedings of IEEE International Conference on The Communications,*7-11 June, Atlanta, GA, 171-175, **1998**.

[19] Jerbi, M., Senouci, S. M., Ghamri-Doudane, Y., Towards efficient routing in vehicular Ad Hoc networks*, 3rd IEEE international workshop on Mobile Computing and Networking*, **2006**.

[20] Seet, B.-C., Liu, G., Lee, B.-S., Foh, C.-H., Wong, K.-J., Lee, K.-K., A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications, *In Proceedings of The Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks,* 9–14 May, 898-999, **2004**.

[21] Forderer, D., Street-Topology Based Routing, Master's thesis, University of Mannheim, Mannheim, **2005**.

[22] Lee, K. C., Le, M., Harri, J., Gerla, M., LOUVRE: Landmark Overlays for Urban Vehicular Routing Environments*, In Proceedings of The Vehicular Technology Conference,* 21-24 September, Calgary, BC, 1-5, **2008**.

[23] Füßler, H., Widmer, J., Käsemann, M., Mauve, M., Hartenstein, H., Contention-based forwarding for mobile ad hoc networks. *Ad Hoc Networks, 1*(4), 351-369, **2003**.

[24] Lee, K. C., Lee, U., Gerla, M., TO-GO: TOpology-assist geo-opportunistic routing in urban vehicular grids, In Proceedings of The *Sixth International Conference on Wireless On-Demand Network Systems and Services,* 2-4 February, Snowbird, UT, 11-18, **2009**.

[25] Cheng, P.-C., Weng, J.-T., Tung, L.-C., Lee, K. C., Gerla, M., Haerri, J., GeoDTN+ Nav: a hybrid geographic and DTN routing with navigation assistance in urban vehicular networks, *MobiQuitous/ISVCS*, **2008**.

[26] Zhao, J., Cao, G., VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks, *In Proceedings of the 25th IEEE International Conference on Computer Communications,* April,Barcelona, Spain, 1-12, **2006**.

[27] Leontiadis, I., Mascolo, C., GeOpps: Geographical Opportunistic Routing for Vehicular Networks, *In Proceedings of The IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks,* 18-21 June, Espo, Finland, 1-6, **2007**.

[28] Karp, B., Kung, H.-T., GPSR: Greedy perimeter stateless routing for wireless networks, *In Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 20-24 September, Chicago, USA, **2000**.

[29] Naumov, V., Baumann, R., Gross, T., An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces*, In Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, 22-25 May, Florence, Italy, 108-119, **2006**.

[30] Schnaufer, S., Füßler, H., Transier, M., Effelsberg, W., Unicast Ad-hoc routing in vehicular city scenarios, **2008**.

[31] Schnaufer, S., Effelsberg, W., Position-based unicast routing for city scenarios, In Proceedings of the *International Symposium on Mobile and Multimedia Networks,* 23-26 June, Newport Beach, CA, 1-8, **2008**.

[32] Lochert, C., Mauve, M., Füßler, H., Hartenstein, H., Geographic routing in city scenarios, *Mobile Computing and Communications Review,* 9(1), 69-72, **2005**.

[33] Lee, K. C., Haerri, J., Lee, U., Gerla, M., Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios, *In Proceedings of the Globecom Workshops,* 26-30 November, Washington, DC, 1-10, **2007**.

[34] Naumov, V., Gross, T. R., Connectivity-Aware Routing (CAR) in Vehicular Ad-hoc Networks, In Proceedings of the *26th IEEE International Conference on Computer Communications*, 6-12 May, Anchorage, AK, **2007***.*

[35] Sen, S., Clark, J. A., Tapiador, J.E., Security Threats in Mobile Ad Hoc Networks, In *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Auerbach Publications, CRC Press, **2010**.

[36] Clark, J.A., Murdoch, J., McDermid, J.A., Sen, S., Chivers, H.R., Worthington, O., Rohatgi, P., Threat modelling for mobile ad hoc sensor networks, In Proceedings of the *Annual Conference of ITA*, **2007**.

[37] Yan, G., Olariu, S., Weigle, M. C., Providing VANET security through active position detection. *Computer Communications, 31*(12), 2883-2897, **2008**.

[38] Mutaz, M. A., Malott, L., Chellappan, S., Leveraging platoon dispersion for Sybil detection in vehicular networks, In Proceedings of The *Eleventh Annual International Conference on Privacy, Security and Trust (PST),* 10-12 July, Tarragona, 340-347, **2013**.

[39] Dak, A. Y., Yahya, S., Kassim, M., A literature survey on security challenges in VANETs, *International Journal of Computer Theory and Engineering, 4*(6), 1007, **2012**.

[40] Sumra, I. A., Ahmad, I., Hasbullah, H., Manan, J.-l. B. A., Classes of attacks in VANET, *In Proceedings of the Saudi International Electronics, Communications and Photonics Conference, Riyadh, 1-5,* **2011**.

[41] Mohd, N., Annapurna, S., Bhadauria, H., Taxonomy on Security Attacks on Self Configurable Networks, *World Applied Sciences Journal, 31*(3), 390-398, **2014**.

[42] Moore, T., Raya, M., Clulow, J., Papadimitratos, P., Anderson, R., Hubaux, J. P., Fast Exclusion of Errant Devices from Vehicular Networks, *In Proceedings of the 5th Annual IEEE Communcations Society Conference on Sensor, Mesh and Ad Hoc Communications,* 16-20 June, San Franciso, CA, 135-143, **2008**.

[43] Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., Leinmüller, T., Attacks on inter vehicle communication systems-an analysis. *In Proceedings of the 3rd International Workshop on Intelligent Transportation,* 189-194, **2006**.

[44] Samara, G., Al-Salihy, W. A., Sures, R., Security analysis of vehicular ad hoc nerworks (VANET)*, In Proceedings of The 2nd International Conference on Network Applications Protocols and Services*, 22-23 September, Kedah, 55-60, **2010**.

[45] Douceur, J. R., The sybil attack, Peer-to-peer Systems, 7-8 March, MA, USA, 251-260, **2002**.

[46] Golle, P., Greene, D., Staddon, J., Detecting and correcting malicious data in VANETs, *In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 26 September-1 October, Philadelphia, Pennsylvania, 29-37, **2004**.

[47] Park, S., Aslam, B., Turgut, D., Zou, C. C., Defense against sybil attack in vehicular ad hoc network based on roadside unit support, In Proceedings of The IEEE *Military Communications Conference*, Boston, MA, 1-7, **2009**.

[48] Grover, J., Gaur, M. S., Laxmi, V., Prajapati, N. K., A sybil attack detection approach using neighboring vehicles in VANET, *In Proceedings of the 4th international conference on Security of information and networks*, Sydney, Australia, 151-158, **2011**.

[49] Xiao, B., Yu, B., Gao, C., Detection and localization of sybil nodes in VANETs, *In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks,*29 September, Los Angeles, CA, 1-8, **2006***.*

[50] Aditya, S., Santosh, K. M., Preventing VANET From DOS & DDOS Attack, *International Journal of Engineering Trends and Technology (IJETT)*, 4(10), 4373-4376, **2013**.

[51] Yi, P., Dai, Z., Zhang, S., Zhong, Y., A new routing attack in mobile ad hoc networks, *International Journal of Information Technology, 11*(2), 83-94, **2005**.

[52] Desilva, S., Boppana, R. V., Mitigating malicious control packet floods in ad hoc networks, *In Proceedings of the Wireless Communications and Networking Conference,* 13-17 March, 2112-2117*,* **2005**.

[53] Seungjoon, L., Bohyung, H., Minho, S., Robust routing in wireless ad hoc networks*, In Proceedings of The International Parallel Processing Workshops,* 73-78**, 2002***.*

[54] Hortelano, J., Ruiz, J. C., Manzoni, P., Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs, *Communications Workshops (ICC), 2010 IEEE International Conference*, 23-27 May, **2010**.

[55] Al-Shurman, M., Yoo, S.-M., Park, S., Black hole attack in mobile Ad Hoc networks, *Proceedings of the 42nd annual Southeast regional conference*, **2004**.

[56] Lijun, Q., Ning, S., Xiangfang, L., Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path, *In Proceedings of The Wireless Communications and Networking Conference,* 13-17 March, **2005**.

[57] Safi, S. M., Movaghar, A., Mohammadizadeh, M., A Novel Approach for Avoiding Wormhole Attacks in VANET, *In Proceedings of The 2nd International Workshop on Computer Science and Engineering,* 28-30 October, Qinqdao, 160-165, **2009**.

[58] Adjih, C., Raffo, D., Mühlethaler, P., Attacks against OLSR: Distributed key management for security*, In Proceedings of the 2nd OLSR Interop and Workshop*, Palaiseau, France, 28-29 July, 28-35 **2005**.

[59] Baras, J. S., Radosavac, S., Theodorakopoulos, G., Sterne, D., Budulas, P., Gopaul, R., Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR*, In Proceedings of The IEEE Military Communications Conference,* Orlando, FL, 29-31 October, 1-7, **2007***.*

[60] Sen, S., Clark, J. A., Intrusion Detection in Mobile Ad Hoc Networks, Chapter 17, pp. 427-454, *Guide to Wireless Ad Hoc and Sensor Networks*, Springer, **2009**.

[61] Ning, P., & Sun, K., How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols, *Ad Hoc Networks*, *3*(6), 795-819. **2005**

[62] Haklay, M., & Weber, P., OpenStreetMap: User-Generated Street Maps. *IEEE Pervasive Computing, 7*(4), 12-18, **2008**.

[63] Behrisch, M., Bieker, L., Erdmann, J., Krajzewicz, D., Sumo–simulation of urban mobility*, In Proceedings of The Third International Conference on Advances in System Simulation*, Barcelona, Spain, 23-29 October, 63-69, **2011**.

[64] Singh, P. K., Influences of TwoRayGround and Nakagami propagation model for the performance of adhoc routing protocol in VANET. *International Journal of Computer Applications, 45*, **2012**.

[65] Fonseca, A., Vazão, T., Applicability of position-based routing for VANET in highways and urban environment. *Journal of Network and Computer Applications, 36*(3), 961-973, **2013**.

ÖZGEÇMİŞ

Kimlik Bilgileri

Adı Soyadı : Ömer MİNTEMUR

Doğum Yeri : ANKARA

Medeni Hali : Bekar

E-Posta : omermintemur@gmail.com

Adresi : Akın Caddesi Sevgi Sokak 5/5 Yenimahalle / ANKARA

Eğitim

Lisans : Çankaya Üniversitesi

Yüksek Lisans :

Doktora :

Yabancı Dil ve Düzeyi

İngilizce – Çok İyi

İş Deneyimi

Yıldırım Beyazıt Üniversitesi Bilgisayar Mühendisliği Araştırma Görevlisi 2013 -

Deneyim Alanları

C, C++, C#, Java, Network

Tezden Üretilmiş Projeler ve Bütçesi

Tezden Üretilmiş Yayınlar

Tezden Üretilmiş Tebliğ ve/veya Poster Sunumu ile Katıldığı Toplantılar