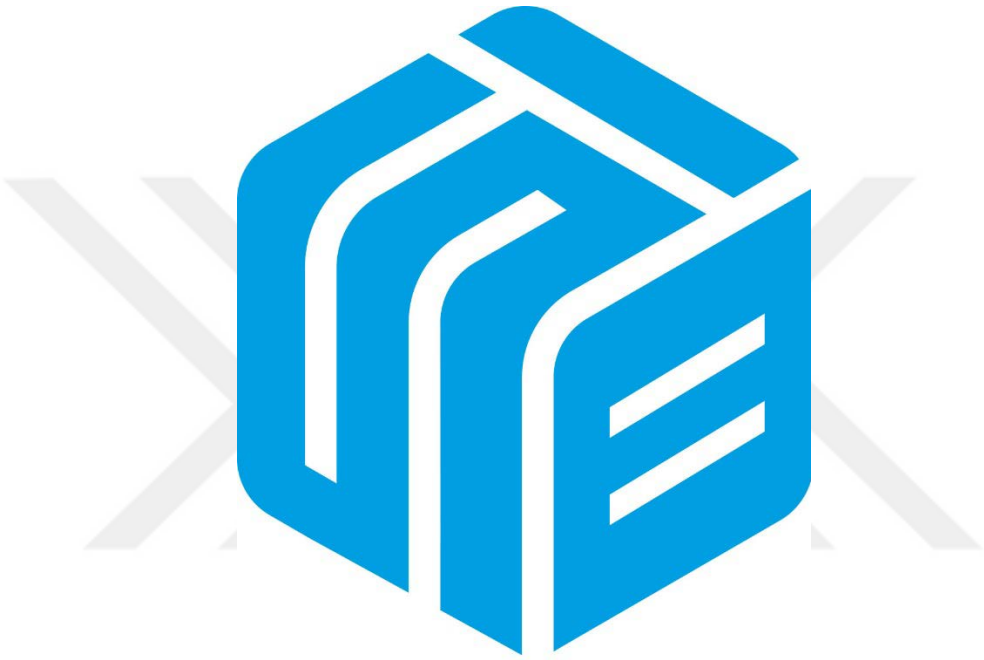


UÇAN TASARSIZ AĞLARA (FANET) YÖNELİK YÖNLENDİRME SALDIRILARININ ANALİZİ VE TESPİTİ

Özlem CEVİZ

YÜKSEK LİSANS TEZİ
SAVUNMA TEKNOLOJİLERİ ANA BİLİM DALI

SİVAS BİLİM VE TEKNOLOJİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ŞUBAT 2022

ETİK BEYAN

Sivas Bilim ve Teknoloji Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Özlem CEVİZ
07/02/2022

UÇAN TASARSIZ AĞLARA (FANET) YÖNELİK YÖNLENDİRME SALDIRILARININ ANALİZİ VE TESPİTİ

(Yüksek Lisans Tezi)

Özlem CEVİZ

SİVAS BİLİM ve TEKNOLOJİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Şubat 2022

ÖZET

Günümüzde İnsansız Hava Araçları (İHA), askeri ve endüstriyel uygulamalar başta olmak üzere çok çeşitli alanlarda yaygın olarak kullanılmaktadır. Teknolojik gelişmelerle birlikte görevlerde, tek İHA'lar yerini çoklu İHA'lara bırakmaktadır. Bu gibi durumlarda, birden fazla İHA'nın ortak bir ağa katılmasına ve karmaşık görevlerin organize bir şekilde yürütülmesine izin veren Uçan Tasarsız Ağlar (FANET'ler) önerilir. Ancak FANET'ler kritik uygulamalarda kullanıldığı için saldırıların hedefidir. Buna ek olarak, yapıları ve kullandıkları ortak yönlendirme protokolleri nedeniyle çeşitli saldırılara karşı savunmasızdırlar. FANET'ler, MANET'lerden çok daha yüksek hareketliliğe sahip olduğundan, yeni güvenlik çözümlerinin önerilmesini veya Mobil Tasarsız Ağların (MANET'ler) mevcut güvenlik çözümlerinin uyarlanmasını gerektirir. Yüksek hareketlilik, güvenliği farklı şekillerde etkileyebileceğinden, öncelikle FANET'lere yönelik saldırılar analiz edilmelidir. Bu çalışmanın temel amacı budur. Bu çalışmada, FANET'lere yönelik düşme, kara delik, düden, taşma saldırıları gibi çeşitli saldırılar analiz edilmektedir. Bu, İHA'ların gerçek hayatta olduğu gibi 3 boyutlu olarak hareket ettiği gerçekçi ağ senaryolarını simüle ederek FANET'lerde kapsamlı bir saldırı analizi sunan ilk çalışmadır. Bununla birlikte, yapılan çalışmalarının sonucunda bir veri kümesi oluşturulmuştur. Veri kümesi çeşitli ağ simülasyonları (saldırılı ve saldırısız) çalıştırılarak toplanmıştır. Daha sonra bu veri kümesi kullanılarak, FANET'lere yönelik saldırıların tespiti için yapay sinir ağlarının uygulanması araştırılmıştır. Sonuçlar, önerilen yöntemin değişik türde saldırıları başarı ile tespit edebildiğini göstermektedir.

Bilim Kodu : 10428375

Anahtar Kelimeler : FANET, İHA, AODV, yönlendirme saldırıları, kara delik saldırısı, düşürme saldırısı, sel saldırısı, obruk saldırısı, saldırı tespiti, yapay sinir ağı

Sayfa Adedi : 84

Danışman : Doç. Dr. Sevil Şen Akagündüz

ANALYSIS AND DETECTION OF ROUTING ATTACKS ON FLYING AD HOC NETWORKS

(M. Sc. Thesis)

Özlem CEVİZ

SIVAS UNIVERSITY OF SCIENCE AND TECHNOLOGY

INSTITUTE OF GRADUATE STUDIES

February 2022

ABSTRACT

Unmanned Aerial Vehicles (UAV) are widely used in a variety of fields, especially in military and industrial applications. However, the usage of a single UAV has begun to be insufficient in most missions. In such cases, Flying Ad Hoc Networks (FANETs) that allow more than one UAV to participate in a common network and execute complex tasks in an organized manner is recommended. However, FANETS are target of attacks due to being used in critical applications. Moreover, they are vulnerable to a variety of attacks due to their very nature and the cooperative routing protocols they use. Moreover, FANETs requires new security solutions or adaptation of existing security solutions of Mobile Ad Hoc Networks (MANETs), since it has much higher mobility than MANETs. Since mobility could affect security in different ways, at first attacks against FANETs should be analyzed. This is the main aim of this study. In this paper, various attacks against FANETs, namely dropping, blackhole, sinkhole, flooding attacks are analyzed. This is the first study that presents a comprehensive attack analysis in FANETs by simulating realistic network scenarios, where UAVs move in 3D as in real life. In addition, a dataset is created as a result of this study. The dataset is collected by running various network simulations (with and without attack). Afterwards, using this dataset, the application of artificial neural networks to detect attacks against FANETs is investigated. The results show that the proposed method can successfully detect different types of attacks.

Science Code : 10428375

Key Words : FANET, UAV, AODV, routing attack, blackhole attack, dropping attack, flooding attack, sinkhole attack, intrusion detection, neural networks.

Page Number : 84

Supervisor : Assoc. Prof. Sevil Şen Akagündüz

TEŞEKKÜR

Tez danışmanım Doç. Dr. Sevil Şen'e danışmanlığı kabul ettiği, bilgi ve tecrübesini benimle paylaştığı ve bu süreci yürüttüğü için teşekkür ederim.

Bu çalışmayı yapmamıza ilham olan Pınar Sadioğlu'na çalışmanın alt yapısını benimle paylaştığı için ve desteği için teşekkür ederim.

Bütün hayatım boyunca benim yanımda olan, beni ben yapan, hiçbir zaman fedakarlıktan çekinmeyen, bu zamana kadar bana destek veren, emeğini esirgemeyen rahmetli babam Bekir Ceviz'e ve annem Yurdagül Ceviz'e ve kardeşlerime özverileri, sevgileri ve beni her zaman cesaretlendirdikleri için sonsuz teşekkür ederim.

Çalışma sürecim boyunca ve her zaman yanımda olan olumlu düşünceleri ile beni teşvik eden ve bu çalışmayı yaparken her zaman bana destek veren arkadaşım Hatice Aktaş'a ve motivasyonumu sürekli yükselten, beni neşelendiren arkadaşım İremnur Duru'ya teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

ÇİZELGELERİN LİSTESİ ix

ŞEKİLLERİN LİSTESİ x

SİMGELER VE KISALTMALAR xii

1. GİRİŞ 1

2. LİTERATÜR ARAŞTIRMASI 7

2.1. Saldırı Analizi ve Güvenilir Protokol Önerileri 7

2.2. MANET Saldırı Tespiti 12

2.3. FANET Saldırı Tespiti 13

3. UÇAN TASARSIZ AĞLAR (FANET) 16

3.1. FANET Karakteristik Özellikleri 17

3.1.1. Düğüm hareketliliği 18

3.1.2. Düğüm yoğunluğu 18

3.1.3. Topoloji değişimi 19

3.1.4. Yayılma modeli 19

3.1.5. Enerji tüketimi 20

3.1.6. Lokalizasyon 20

3.1.7 Hareketlilik modeli 20

3.1.8. Platform kısıtlamaları 20

3.2. FANET İletişim Mimarisi 21

Sayfa

3.3. Hareketlilik Modeli 23
3.3.1. Rastgele yol noktası (RYN) hareketlilik modeli 24
3.3.2. Rastgele yön (RY) hareketlilik modeli 25
3.3.3. Gauss-Markov (GM) hareketlilik modeli 25
3.3.4. 3B Gauss Markov (GM) hareketlilik modeli 26
3.4. Yönlendirme Protokolleri 27
3.4.1. Proaktif yönlendirme protokolleri 28
3.4.2. Reaktif yönlendirme protokolleri 30
3.4.3. Hibrit yönlendirme protokolleri 34
3.4.4. Statik yönlendirme protokolleri 35
3.5. Fanet'te Güvenlik 35
4. MATERYAL ve YÖNTEM 38
4.1. FANET Saldırı Analizi 38
4.1.1. Ağ Katmanını Hedefleyen Saldırılar 38
4.1.2. Saldırı Analizi 42
4.2. FANET'ler İçin Yapay Sinir Ağları Temelli Bir Saldırı Tespit Sistemi 44
4.2.1. Yapay sinir ağları ile saldırı tespiti yapılması 45
4.2.2. Önerilen saldırı tespit sistemi 49
5. BULGULAR ve TARTIŞMA 52
5.1. FANET Saldırı Analiz Sonuçları 52
5.2. Saldırı Tespit Sonuçları 64
6. SONUÇ VE ÖNERİLER 73
KAYNAKLAR 75

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. Saldırı analizi literatür karşılaştırması 11

Çizelge 3.2. İHA iletişim türlerine ait özelliklerin karşılaştırılması 23

Çizelge 4.1. Ns-3'te kullanılan simülasyon parametreleri 43

Çizelge 4.2. YSA'ya ait detaylı parametre açıklamaları 47

Çizelge 4.3. Öznitelik listesi 49

Çizelge 5.1. Obruk saldırısı altındaki ağların ortalama performans metrikleri 53

Çizelge 5.2. Paket düşürme saldırısı altındaki ağların ortalama performans metrikleri 54

Çizelge 5.3. Kara delik saldırısı altındaki ağların ortalama performans metrikleri 55

Çizelge 5.4. Tasarsız ağ sel saldırısı altındaki ağların ortalama performans metrikleri 56

Çizelge 5.5. 25 düğüme sahip ağların saldırı altındaki performansları 61

Çizelge 5.6. FPR ve tespit oranı sonuçları (%5- %15 saldırgan oranı) 65

Çizelge 5.7. FPR ve tespit oranı sonuçları (%20- %25 saldırgan oranı) 65

Çizelge 5.8. YSA performans metrikleri 66

Çizelge 5.9. Saldırıdan etkilenen düğümlerle STS sonuçları (%5- %15) 69

Çizelge 5.10. Saldırıdan etkilenen düğümlerle STS sonuçları (%20- %25) 69

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 3.1. Uçan Tasarsız Ağlar (FANET) 17

Şekil 3.2. MANET, VANET ve FANET kümelenmesi 18

Şekil 3.3. FANET dinamik topoloji değişimi 19

Şekil 3.4. FANET iletişim mimarisi 22

Şekil 3.5. Rastgele yol noktası hareketlilik modelini kullanan bir düğümün modeli [59] ..24

Şekil 3.6. Rastgele yön hareketlilik modelini kullanan bir düğümün modeli [60] 25

Şekil 3.7. $\alpha = 1$ ve $\alpha = 0$ iken GM hareketlilik modeli [64] 26

Şekil 3.8. FANET yönlendirme protokolleri sınıflandırması 28

Şekil 3.9. ÇNR düğüm ile OLSR protokolü veri iletimi 30

Şekil 3.10. AODV akış şeması 32

Şekil 3.11. AODV yönlendirme protokolü rota bulma süreci 33

Şekil 4.1. AODV protokolünde obruk (sinkhole) saldırısı 39

Şekil 4.2. AODV protokolünde düşürme saldırısı 40

Şekil 4.3. AODV protokolüne yapılan kara delik saldırısı 41

Şekil 4.4. Yapay sinir ağı blok diyagramı 46

Şekil 4.5. Saldırı tespit sistemi uygulama adımları 50

Şekil 5.1. Obruk saldırısı altında ağın paket teslim oranları 53

Şekil 5.2. Paket düşürme saldırısı altında ağın paket teslim oranları 54

Şekil 5.3. Kara delik saldırısı altında ağın paket teslim oranları 55

Şekil 5.4. Tasarsız ağ sel saldırısı altında ağın paket teslim oranları 56

Şekil 5.5. Farklı saldırı türleri altındaki ağlarda PDR değerlerinin karşılaştırılması 58

Şekil 5.6. Farklı saldırı türleri altındaki ağlarda E2E değerlerinin karşılaştırılması 59

Şekil **Sayfa**

Şekil 5.7. Farklı saldırı türleri altındaki ağlarda ek yük değerlerinin karşılaştırılması.....60

Şekil 5.8. 25 ve 50 düğümlü ağların PDR oranlarının karşılaştırılması 62

Şekil 5.9. 25 ve 50 düğümlü ağların E2E oranlarının karşılaştırılması 63

Şekil 5.10. 25 ve 50 düğümlü ağların Ek Yük oranlarının karşılaştırılması.....64

Şekil 5.11. Saldırgan düğümden STS'ye ait farklı saldırı türlerine göre DR karşılaştırması6

Şekil 5.12. Saldırgan düğümden STS'ye ait farklı saldırı türlerine göre FPR karşılaştırmasıt

Şekil 5.13. Saldırıdan etkilenen düğümlerle STS'ye göre DR karşılaştırması 71

Şekil 5.14. Saldırıdan etkilenen düğümlerle STS'ye göre FPR oranı karşılaştırması 72

SİMGELER VE KISALTMALAR

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

Simgeler	**Açıklamalar**
α	alfa

Kısaltmalar	**Açıklamalar**
AODV	Tasarsız İsteğe Bağlı Uzaklık Vektörü (Ad Hoc On-Demand Vector)
ÇNR	Çok Noktalı Röle
DOS	Hizmet Reddi Saldırısı (Denial-of-service attack)
DSDV	Dinamik Sıralı Uzaklık Vektörü (Dynamic Sequence Distance Vector)
DSR	Dinamik Kaynak Yönlendirme (Dynamic Source Routing)
E2E	Uçtan Uca Gecikme (End-to-End Delay)
FANET	Uçan Tasarsız Ağlar (Flying Ad Hoc Network)
GM	Gauss Markov
İHA	İnsansız Hava Aracı
İGS	İzinsiz Giriş Tespit
MANET	Mobil Tasarsız Ağlar (Mobile Ad Hoc Network)
OLSR	İyileştirilmiş Bağ Durum Yönlendirme (Optimized Link State Routing)
PDR	Paket Teslim Oranı (Packet Deliver Ratio)
RERR	Rota Hata (Route Error)
RREP	Rota Yanıt (Route Reply)
RREQ	Rota İstek (Route Request)
RY	Rastgele Yön
RYN	Rastgele Yol Noktası

STS	Saldırı Tespit Sistemleri
YBİ	Yer Baz İstasyonu
YSA	Yapay Sinir Ağı
VANET	Araç Tasarsız Ağlar (Vanet Ad Hoc Network)

1. GİRİŞ

İnsansız hava aracı (İHA) sistemleri, teknolojinin hızla gelişmesiyle birlikte birçok alanda kullanılmaya başlanmıştır. Askeri, endüstriyel ve sivil uygulamalarda sıklıkla kullanılmaktadırlar. Özellikle İHA'ların insan müdahalesi olmadan grup halinde çalışması, bu alandaki araştırmaların daha fazla genişlemesine yol açmıştır. Ancak, İHA'ların yüksek hızları ve hareketliliği, ağ topolojisinin, hareketli tasarsız ağlar (MANET), araçsal tasarsız ağlar (VANET), vb. gibi diğer birçok tasarsız ağ türünden daha dinamik bir şekilde değişmesine neden olur. Bu nedenle, Uçan Tasarsız Ağlar (FANET) adı verilen yeni bir tür tasarsız ağ ortaya çıkmış ve son yıllarda popüler araştırma alanlarından birisi haline gelmiştir [2]. FANET'ler sınırlı bir alanda arama ve imha etme işlemlerinde [3], uluslararası sınır gözetleme [4], orman yangını izleme ve kontrol etme [5], tarımsal uzaktan algılama sistemleri [6] gibi birçok uygulamada kullanılmaktadır.

FANET'ler, MANET ve VANET'lerin bir alt kümesi olmasına rağmen karakteristik özellikleri ile bu geleneksel tasarsız ağlardan farklılaşmaktadırlar. En belirgin farklarından bir tanesi, yüksek hız nedeniyle değişen dinamik topolojisidir. FANET'ler üç boyutlu olarak hareket ettikleri için hareketlilik modelleri de diğer ağlara göre farklılık göstermektedir. Buna ek olarak uçuş alanlarının geniş olması nedeniyle FANET'lerin düğüm yoğunlukları diğer tasarsız ağlara göre daha düşüktür. Diğer bir fark ise platform kısıtlamalarıdır. Bu durum bataryaların minimal boyutlarda seçilmesini gerektirdiği için enerjinin hızlı bir şekilde tükenmesi problemi gündeme gelmektedir. FANET'lerin karakteristik özelliklerinin diğer ağlardan farklı olması yeni çalışma alanlarının da ortaya çıkmasına neden olmuştur. Bu çalışma alanları; FANET dinamik yapısına uyum sağlayacak yeni yönlendirme protokolleri ya da uyarlamalarının araştırılması, iletişim mimarilerinin geliştirilmesi, enerji tüketiminin düşürülmesini sağlayacak yeni çözümler üretilmesi ve yeni güvenlik çözümlerinin önerilmesidir.

İHA'lar, sivil ve askeri uygulamalarda kullanımının artması ile birlikte saldırıların hedefi haline gelmiştir. Bazı sivil uygulamalarda güvenlik sorunları, uygulamanın işleyişini yoğun bir şekilde etkilemediği için görmezden gelinebilir. Ancak, askeri alanlarda kullanılan İHA'ların verileri güvenli bir şekilde saklaması ve iletmesi büyük bir önem taşımaktadır. İHA'larda kablosuz bağlantıların kullanımı, ağı gizli dinleme ve aktif girişim saldırılarına karşı hassas hale getirir. Buna ek olarak, tasarsız ağlar için geliştirilen yönlendirme protokolleri düğümlerin iş birliğine dayanır, bu durum da içeriden saldırıların

bu tür ağlarda çok etkili olmasını sağlar. Tasarsız Ağ İsteğe Bağlı Mesafe Vektörü (Ad hoc On-Demand Distance Vector-AODV) protokolü, FANET'ler için popüler bir yönlendirme protokolü olmasına rağmen [7] saldırılara karşı savunmasızdır. Bu tür ağların yüksek hareketliliğe sahip olması da güvenliği farklı şekillerde etkileyebilir. Hareketlilik, saldırganların ağa zarar verirken bir yandan da güvenlik çözümlerinden kaçmasına olanak tanır. Öte yandan, saldırının etkisi çok hareketli hedefler üzerinde sınırlı olabilir. Ağdaki İHA'lar, hizmet reddi (DoS) saldırıları, kara delik saldırıları, obruk saldırıları gibi yönlendirme protokollerinin açıklarını kullanarak yapılan saldırıların hedefi olabilir ve bu nedenle ağın kullanılabilirliği tehlikeye girebilir. Bu tür saldırılar ağ kaynaklarını tüketebilir, oluşan bağlantı kopuklukları İHA'lar arsındaki iletişimin kesilmesine ve en önemlisi verilerin ele geçirilmesine neden olabilir. Bu durumların tamamı FANET'ler için yeni güvenlik çözümleri geliştirilmesinin gerekli olduğunu göstermektedir.

Literatürde Mobil Tasasız Ağlar (MANET) için pek çok güvenlik önerisi bulunmakla birlikte, üst düzey hareketliliklerinden dolayı FANET'lere doğrudan uygulanamazlar. FANET'ler için AODV protokolünün geliştirilmesi ile daha güvenli protokoller oluşturulmuştur [8][9]. Fakat, hala AODV yönlendirme protokolü, literatürde genel olarak kabul görmekte ve kullanılmaktadır. AODV yönlendirme protokolü reaktif bir protokol olması nedeniyle FANET'lerde ek yükü azaltmaktadır. Sürekli değişen topolojiye uyum sağlamakta ve isteklere hızlı bir şekilde yanıt verebilmektedir. Ancak AODV yönlendirme protokolünde saldırganlar için açıklar bulunmaktadır ve içeriden yapılacak saldırılara karşı savunmasızdır. İçeriden yapılan saldırılarda, saldırgan düğüm ağın içerisinde bulunan diğer düğümler gibi davranarak ağa doğrudan bir erişim sağlayabilir. Özellikle rota keşif süreçlerinde ağ, saldırgan düğümlerin hedefi olmaktadır. Ayrıca aktif rotalara yerleşen saldırgan düğümler de tehlike arz etmektedir.

İHA'lar, MANET'lerdeki ve Araç Tasarsız Ağlar'daki (VANET) düğümlerin aksine 3 boyutlu olarak hareket eder. Ayrıca, diğer tasarsız ağ türlerinden farklı hareketlilik modellerine sahip olabilirler. Örneğin, bazı görevleri tamamlamak için grup olarak bir yönde birlikte uçabilir ve periyodik olarak kontrolör yer sistemine doğru hareket edebilirler. Bu nedenle FANET'ler için yeni güvenlik çözümleri ve mimarileri geliştirilmeli veya tasarsız ağlar için önerilen mevcut çözümler FANET'lere uyarlanmalıdır. Bu durum mevcut çalışmanın da temel amacı olan FANET'lere yönelik saldırıların kapsamlı bir şekilde analiz edilmesini gerektirir.

Yeni güvenlik çözümlerinin üretilebilmesi için ilk olarak saldırıların analiz edilmesi gerekmektedir. Daha sonra ise saldırıların tespit edilmesini sağlayan sistemler kullanılarak

izinsiz girişler yakalanmalıdır. Saldırı tespit sistemleri (STS), kötü niyetli etkinliklerin fark edilmesi veya ağdaki anormal davranışların tespit edilmesini sağlayan bir mekanizmadır [10].Ağda izinsiz girişlerin olması veri iletimine engel olmakla birlikte verilerin ele geçirilmesi veya değiştirilmesi gibi durumlara neden olmaktadır. STS ile, ağ bütünlüğü tamamen bozulmadan ya da bütün düğümler saldırgan düğümler tarafından manipüle edilmeden önlemler alınabilmektedir. Bu nedenle STS'ler, güvenlik yaşam döngüsünün önemli bir bileşenidirler.

İmza tabanlı, anormallik tabanlı ve spesifikasyon tabanlı olmak üzere 3 çeşit saldırı tespit yöntemi kullanılmaktadır. İmza tabanlı yöntemlerde, mevcut trafikteki örüntüler, bilinen saldırı örüntüleri ile karşılaştırılır ve bir eşleşme mevcut ise saldırı olduğu anlaşılır. Bu tür sistemler, mevcutta kayıt altına alınmış saldırıları tespit etmekte çok başarılı iken, ilk defa ortaya çıkan saldırıyı imzalarını bilmedikleri için tespit edemeyebilirler. Bu sistemlerin sürekli olarak güncellenmeleri gerekir. Anormallik tabanlı yöntemlerde ise genellikle yapay zeka teknikleri ile bir model oluşturulur ve yeni aktiviteler oluşturulan bu model ile karşılaştırılır. Karşılaştırılan aktiviteler, modelden sapma gösteriyor ise durum şüpheli olarak bildirilir. Bu yöntem ile yeni saldırı türleri de tespit edilebilir. Spesifikasyona dayalı sistemler ise imza tabanlı ve anormallik tabanlı yöntemlerin avantajlarını bir arada kullanmayı amaçlamaktadır. Bu yöntem ile, kullanılan sistem ve protokollerin spesifikasyonları tanımlanır, bunlardan sapmalar saldırı olarak tespit edilir.

FANET'lerin kritik görevlerde yer alması nedeniyle, güvenliklerinin sağlanması son derece önem taşımaktadır. Ağ bütünlüğünün sağlanması veri iletişimin kesilmemesi verilerin ele geçirilip yok edilmemesi ya da değiştirilmemesi için önlemler alınmalıdır. Bunlara ek olarak, İHA'lar platform kısıtlamaları nedeniyle büyük bataryalara sahip değillerdir. Saldırı altındaki ağda yer alan bir İHA'nın bataryası da hızlı bir şekilde tükenebilir ve görevlerini tamamlayamayabilir. Bu nedenle FANET ağını güvenli tutmak için hem etkili hem de batarya tüketimi açısından verimli sistemler seçilmelidir [11].

Günümüzde, geleneksel saldırı tespit sistemlerinin yerini, yapay zeka tabanlı yaklaşımlar almıştır. Son yıllarda, özellikle makine öğrenmesi ve derin öğrenme tabanlı yaklaşımların bu probleme uygunluğu araştırılmaktadır. Bu yöntemler, büyük verilerin bilgiye çevrilerek öğrenilmesini hedeflemektedir [12]. Özellikle, saldırıların etiketlendiği veri kümelerinin varlığı ile olanaklı hale gelen denetimli öğrenme tabanlı sistemler, yüksek doğruluk üretmektedir.

İHA'ların kritik görevlerde kullanılması, etkin güvenlik çözümlerinin geliştirilmesini gerektirmektedir. Literatürde MANET ve VANET'lere yönelik birçok saldırı tespit sistemi

önerilmesine rağmen, FANET'lerle ilgili çok fazla çalışma bulunmamaktadır. Bu durumun en önemli sebeplerinden bir tanesi FANET'lerle ilgili detaylı saldırı analiz çalışmalarının yapılmamış olması ve hazır veri kümelerinin paylaşılmaması olabilir. Bu nedenle detaylı saldırı analizleri yapılarak tespit sistemlerinin de önü açılacaktır. Saldırıların tespit edilmesi için sistemler hızlı bir şekilde geliştirilebilecektir.

Bu çalışmada, FANET'lere yönelik çeşitli yönlendirme saldırılarının etkileri analiz edilmiştir. Tasarsız ağlar için en popüler yönlendirme protokollerinden biri olan AODV kullanılmaktadır. AODV ayrıca basitliği ve düşük ek yükü nedeniyle FANET'lerde popüler olarak kullanılan bir protokoldür [13]. Bu tez çalışmasında, paket düşürme, sel, kara delik ve obruk saldırıları, Ns-3 [14] kullanılarak simüle edilmiştir. Simülasyonlar için bütün parametreleri aynı olan 13 farklı topolojiye sahip ağlar kullanılmıştır. 13 kez saldırı olmadan, 13 kez ise %5- %25 aralığında saldırgan oranları için (5x13 kez) toplam 78 kez her bir saldırı türü için ayrı ayrı simülasyon çalıştırılmıştır. Uçan düğümleri simüle etmek için hareketlilik modeli olarak 3B Gauss Markov (GM) Hareketlilik Modeli kullanılmıştır. Literatürdeki çalışmalarda halen MANET uygulamaları için uygun olan Rastgele Yol Noktası Hareketlilik Modeli ve 20m/s gibi düşük düğüm hızları gibi 2B hareketlilik modelleri kullanılırken [15-16], burada FANET'ler için gerçekçi ağ senaryoları Ns-3 kullanılarak simüle edilmektedir.

Simülasyon sonuçları, kara delik saldırısının ağ performansını diğer saldırılardan daha fazla etkilediğini göstermektedir. Ağı en az etkileyen saldırı ise düşürme saldırısıdır. Çünkü saldırgan düğüm sadece aktif rotada bulunuyor ise paketleri düşürebilmektedir. Sel saldırısında ise saldırgan oranının artması ile birlikte ağda oluşan trafiğin de artması paketlerin düşmesine ve ağın performansının etkilenmesine neden olmaktadır. Saldırılar ek yükü arttırmaktadır. Uçtan uca gecikmeyi azalmaktadırlar. Bunun nedeni ise saldırılar sonucunda teslim edilecek paketlerde azalma olmasıdır. Yapılan deneyler, saldırgan düğümün konumunun saldırıların etkili olmasında önemli bir etken olduğunu göstermektedir. FANET'lerin karakteristik özelliği olan yüksek hız ve sürekli olarak değişen topoloji nedeniyle, saldırganlar bazı durumlarda yeteri kadar etkili olamayabilirler. Saldırgan olarak seçilen düğümlerin ağda etkili bir şekilde yerleşmesi, FANET güvenliğini önemli ölçüde etkileyebilmektedir ve ağ performansını düşürmektedir. Bu nedenle güçlü saldırı tespit sistemlerine ihtiyaç duyulmaktadır.

Bildiğimiz kadarıyla, bu tez çalışması, gerçekçi ağ senaryolarında FANET'e yönelik saldırıları titizlikle analiz eden ilk çalışmadır. Saldırıların simüle edilmiş ağlar üzerindeki etkileri, paket teslim oranı, ek yük ve uçtan uca gecikme kullanılarak değerlendirilir.

Yapılan detaylı analiz çalışmaları aynı zamanda yeni güvenlik çözümlerinin ortaya çıkabilmesi için bir alt yapı oluşturmayı hedeflemektedir. Bu hedef doğrultusunda ağ üzerinde saldırı olup olmadığını yapay zeka yöntemleri ile tespit etmek ve çözüm üretmek için veri kümesi oluşturulmuştur. Oluşturulan veri kümesi bir giriş, bir çıkış ve beş saklı katman olan yapay sinir ağları algoritmaları ile %80 eğitim, %20 test verisi olarak ayrılarak modelleme yapılmıştır. Önerilen yöntem, saldırgan düğümlerle saldırı tespiti ve saldırıdan etkilenen düğümlerle saldırı tespiti olarak iki farklı saldırı tespit mimarisi ile gerçekleştirilmektedir. Her iki yöntemde de bütün düğümlerden belirli aralıklarla hareketliliği ve kontrol paketlerini içeren öznitelikler toplanır. Bu öznitelikler kullanılarak saldırılar tespit edilir. Saldırgan düğümlerle STS'lerde, saldırgan düğümler yüksek başarım oranı ile tespit edilmektedir. Bu yöntemde STS'nin ele geçirilemeyeceğini varsaymaktayız. Saldırıdan etkilenen düğümlerle STS'de ise, saldırıların düğümler üzerindeki etkisinin tespit edilmesi hedeflenmektedir.

Yapılan tespit sonuçlarına göre en yüksek tespit oranı sel saldırısında gerçekleştirilmektedir. Sel saldırısında bütün düğümler saldırıdan etkilendiği için saldırının tespit oranı diğer saldırı oranlarına göre daha yüksek olmaktadır. En düşük sonuçlar ise düşürme saldırısından elde edilmektedir. FANET'lerde bağlantı kopukluklarının da sıklıkla olması nedeniyle bu saldırıda gerçekten saldırı mı var yoksa bağlantı kesintisi nedeniyle mi paketler düşüyor anlamak zordur. Saldırgan düğümlerle saldırı tespit sistemi, saldırıdan etkilenen düğümlerle saldırı tespit sistemine göre daha yüksek değerler vermektedir. Bunun nedeni saldırıdan etkilenen düğümlerle yaklaşımda saldırıdan bütün düğümlerin etkilenmemesidir.

Sonuç olarak literatürde, FANET'ler üzerinde gerçekleştirilen ilk detaylı saldırı analiz çalışması yapılmıştır. Buna ek olarak, AODV yönlendirme protokolü kullanılarak, gerçek sistemlere yakın veriler toplanabilmesi için gerçekçi senaryolar kullanılarak bir veri kümesi oluşturulmuştur. Oluşturulan veri kümesi yapay sinir ağları algoritmaları kullanılarak saldırı tespiti için başarılı bir şekilde kullanılmıştır.

Tezin katkıları, şu şekilde özetlenebilir:

Literatürde FANET'ler üzerine gerçekleştirilen ilk detaylı saldırı analiz çalışmasıdır. Dolayısıyla,

- FANET'lerin güvenliği üzerine çalışacak araştırmacılara yol göstermesi beklenmektedir.
- FANET'lerde, AODV'ye yönelik saldırıları kapsayan bir veri kümesi oluşturulmuştur. İsteyen araştırmacılar ile paylaşılması hedeflenmektedir.

- Bu veri kümesi kullanılarak, başarım oranı yüksek, yapay sinir ağları temelli STS'ler geliştirilmiş ve detaylı analiz edilmiştir.

2. LİTERATÜR ARAŞTIRMASI

Literatürde MANET güvenliği ile ilgili çok fazla çalışma olmasına rağmen, birçok uygulamada kullanılmaya başlanmış olsa da FANET güvenliği ile ilgili araştırmalar hala yeterli değildir. Literatürde mobil tasarsız ağlarda AODV'ye yönelik saldırıları analiz eden çok sayıda çalışma [17-24, 32] bulunmaktadır.

2.1. Saldırı Analizi ve Güvenilir Protokol Önerileri

Ning ve diğerleri [17], AODV yönlendirme protokolü kullanılarak MANET'lere içeriden gelen saldırılar analiz edilmiştir. Yönlendirme mesajlarını kötüye kullanan saldırganları içeren çalışmalar Ns-2 simülasyon aracı kullanılarak simüle edilmektedir. Elde edilen deneysel sonuçlarla saldırıların ağı kolay bir şekilde bozabileceği, rotaları ele geçirebileceği, saldırgan olmayan düğümleri ağdan izole edebileceği veya ağ kaynaklarının tüketilebileceği gösterilmiştir. Bu çalışmanın saldırıları sistematik olarak analiz etmesi ve bu analiz şemasının diğer protokollere uygulanabilir olması literatüre katkı sağlamaktadır.

Kara delik saldırı analizi yapan çalışmalar [18-22] aynı zamanda AODV yönlendirme protokolünü geliştirmektedir. Jain ve arkadaşları [18], AODV yönlendirme protokolü kullanarak kara delik saldırılarını analiz etmektedir. Elde ettikleri deneysel sonuçlar doğrultusunda AODV yönlendirme protokolünü geliştirmiş ve SAODV adı verilen yeni bir protokol önermişlerdir. Bu protokolde ilk gelen RREP mesajının saldırgan düğümden geldiği varsayımı kullanılmaktadır. Bu nedenle ilk gelen mesajı görmezden gelen bir yöntem geliştirilmiştir. Kara delik saldırısı altındaki AODV ve SAODV protokollerinin performansları karşılaştırılmıştır ve SAODV'nin saldırıya karşı daha güvenli olduğu gösterilmiştir.

Dokurer ve diğerleri [19], yalnızca kara delik saldırılarını analiz etmekle kalmıyor, aynı zamanda AODV'yi geliştirerek kara delik saldırılarına yönelik çözümler de sunuyor. Ns-2 simülasyon aracı kullanılarak 20 düğümlü 100 farklı senaryo oluşturulmuştur. Bu senaryolarda kara delik saldırısı altında ve saldırı yokken performans değerlendirmeleri yapılarak yeni bir yöntem önerilmektedir. Önerilen yöntemde kaynak düğüm ilk gelen RREP kontrol mesajının saldırgan düğüm tarafından gönderildiğini varsayarak ikinci bir RREP mesajı bekliyor ve mesaj gelirse yeni rotadan veri aktarımı sağlanıyor. Üçüncü olarak gönderilen RREP mesajları olursa bu rota da tercih edilmektedir. Fakat ikinci rota

ve üçüncü rota arasında performans açısından bir fark gözlenememiştir. Önerilen değiştirilmiş AODV protokolü yöntemi ile saldırı altındaki bir ağda paket kayıplarının %19 oranında azaldığı gösterilmektedir. Ağ saldırı altında değil iken bu yöntemin kullanılması paket kaybını %4 oranında arttırmaktadır. Sonuçlar doğrultusunda yeni geliştirilen yöntem ile saldırı altında ağ performansı daha iyi olmaktadır.

Lu ve diğerleri [20], AODV protokolü kullanılarak MANET'lere yönelik olarak yapılan kara delik saldırıları simüle edilmiştir. AODV protokolü geliştirilerek daha güvenli ve etkili bir protokol sunulmuştur. Bu protokolde kaynak düğüm bir RREP mesajı aldığında, RREP'nin tersi yönünde hedef düğüme bir doğrulama mesajı göndermektedir. Gönderilen bu doğrulama mesajının içeriğinde kaynak düğüm tarafından üretilen rastgele bir sayı bulunmaktadır. Kaynak düğüme ulaşan doğrulama mesajlarının aynı rastgele sayıyı içerip içermediği kontrol edilir ve aynı sayı içeriyorsa doğrulama gerçekleşir. Paket aynı sayıyı içermiyorsa aynı sayıyı içeren ikinci bir paket gelmesi beklenir. Daha sonra kaynak düğüme güvenli bir mesaj iletilir ve kaynak düğüm bu paket içerisindeki rastgele sayıları kontrol eder. Burada da iki paketin aynı sayıyı içermesi yöntemi kullanılmaktadır. Aynı sayıyı içeren iki veya daha fazla paket alındığında rotanın güvenilir olduğuna karar verilir ve veri iletimi gerçekleştirilir. Sunulan yeni protokol ile AODV güvenlik açıkları kapatılmaya çalışılmış ve kara delik saldırısına karşı daha güvenli hale getirilmiştir. Yapılan analizler sonucunda yeni geliştirilen protokolün AODV protokolünden daha güvenli olduğu gösterilmektedir.

Deshmukh ve arkadaşları [21], MANET'ler için AODV tabanlı güvenli bir yönlendirme sistemi önermektedir. Bu sistem rota keşfinin erken aşamalarında kara delik saldırısını ve etkilenen rotaları tespit etmek için oluşturulmuştur. Ns-2 ile simüle edilen yöntemde RREP mesajına bir geçerlilik değeri eklenir ve aktif rota üzerindeki bütün düğümlerin rota tablosunda saklanır. Saldırgan düğüm tabloya bakmada yanıt göndereceği için RREP geçerlilik değeri boş olacaktır. Bu durumda saldırgan bir düğümden gelen RREP mesajı düşürülecektir. RREP'de yer alacak bu geçerlilik değeri sadece tek bir bit olduğu için ek yükü arttırmayacaktır. Yeni geliştirilen protokol kullanıldığında saldırı altındaki bir ağ ile saldırısız ortamdaki AODV performansları neredeyse eşit çıkmaktadır. Bu durum da önerilen yöntemin güvenilir olduğunu göstermektedir.

Diğer bir çalışmada [22], karadelik saldırılarının etkisi, farklı yönlendirme protokolleri, AODV ve OLSR kullanan ağlar üzerinde değerlendirilir. Kara delik saldırısı altında ve saldırı olmadan ağ performansı paket teslim oranı (packet deliver ratio-PDR) ve ağ verimi (throughput) metriklerine göre değerlendirilmiştir. Sonuçlara göre saldırı olmadan AODV

protokolü OLSR protokolüne göre daha yüksek PDR değerlerine sahip olduğu için daha iyi bir ağ performansı göstermektedir. Ancak, ağda saldırı yoksa ve düğüm sayısı daha az ise verimin yüksek çıkması için OLSR yönlendirme protokolü önerilmektedir. Bu önermeye rağmen yazarlar AODV protokolünün bağlantı hatalarını bildirmesi ve işlemleri tekrarlama özelliği nedeniyle AODV protokolünün OLSR protokolüne göre daha iyi bir yaklaşıma sahip olduğunu belirtmişlerdir.

Kara delik saldırısında çok fazla çalışma olmasına rağmen acele (rushing) saldırısında daha az çalışma [23] vardır. [23]'de isteğe bağlı tasarsız ağlara yapılan acele (rushing) saldırısı anlatılmıştır. Bu saldırı rota keşfi esnasında kaynak düğümün, hedef düğüme giden 2 atlamadan daha uzun rotaları bulmasını engellemektedir. Çalışmada önerilen bütün güvenli isteğe bağlı tasarsız yönlendirme protokollerinin saldırıya açık olduğu açıklanmaktadır. Bu nedenle saldırıyı engellemeye yönelik yeni bir rota bulma RAP (Rushing Saldırı Koruma) protokolü önerilmiştir. Önerilen yöntem de rota keşfinde alınan RREQ mesajları arasından rastgele olarak seçilen bir RREQ mesajının iletilmesi sağlanır. Saldırgan tarafından birden fazla RREQ mesajı iletimini engellemek için her RREQ paketi içerisine geçtiği düğümlerin listesi yerleştirilir. Daha sonra her bağlantı için iki yönlü bir komşu doğrulaması gerçekleştirilir. Son olarak düğüm listesinin kimliğinin doğrulanması için her düğümden ilettiği RREQ mesajının doğrulanması istenir. Düğüm klasik rota bulma yöntemlerine göre daha fazla ek yük getirmesine rağmen diğer protokollerin bulamadığı yolları bularak, yönlendirme ve paket tesliminde başarılı olduğu gösterilmektedir.

MANET'lerde bir hizmet reddi saldırısı olan sel saldırısının etkisini gösteren çalışmalar [24-25]'de verilmektedir. Bandyopadhyay ve arkadaşları [24] çalışmada sel saldırısının MANET'lerde AODV yönlendirme protokolü üzerindeki etkisini araştırmışlardır. Sel saldırısı kötü niyetli bir düğüm tarafından ağda hizmet reddi başlatmayı hedefleyen bir saldırı türüdür. Ağda var olan ya da olmayan düğümlere çok sayıda RREQ paketi ya da gereksiz büyük boyutlu veri paketleri gönderilerek ağ performansının düşürülmesini hedefleyen bir saldırıdır. Ns-3 simülasyon aracı kullanılarak geçersiz hedef adreslere saniyede 8 adet RREQ paketi gönderilerek sel saldırılarının etkileri simüle edilmiştir. Çalışmada, saldırıların ağdaki paket kaybı yüzdesi, yönlendirme yükü ve bant genişliği gereksinimi değerlendirilmiştir. Değerlendirmeler sonucunda oluşturulan sahte RREQ mesajlarının yönlendirme ek yükünü arttırdığı saldırının bu değerleri arttırdığı ve veri paketlerinin düşmesine neden olduğu için paket kaybı yüzdesini arttırmaktadır. Bunlara ek olarak saldırgan düğüm sayısı arttırıldığında ortalamama bant genişliği kullanımı ve paket

kayıp yüzdesi de artmaktadır. Sel saldırısının MANET performansını azalttığı gözlemlenmiştir.

[25]'de ise Ns-2 simülasyon aracı kullanılarak sel saldırılarının MANET üzerindeki etkileri araştırılmaktadır. Farklı oranda taşma frekansı olarak adlandırılan saniyede 0 paketten saniyede 100 pakete çıkarılan bir simülasyon oluşturulmuştur. Paket değişimlerine en olarak saldırgan düğüm sayısı da 0'dan 5'e yükseltilerek paket teslim oranı ve paket gecikme süreleri ölçülmüştür. Paket gecikme süresinin önce arttığı sonra ise düştüğü gözlemlenmiştir. Bunun nedeni sel saldırısında ağ tıkanıklığı ile uzun yollardaki paketlerin düşürülmesi kısa yollardaki paketlerin kalması olarak sunulmuştur. Buna ek olarak taşma frekansı saniyede 100 pakete çıkarıldığında PDR %27'ye düşmektedir. Saldırgan oranı 5'e çıkarıldığında ise saniyede 20 paket gönderildiğinde PDR %17 olmaktadır. Saldırgan düğüm sayısındaki artış ve gönderilen paketlerin artması PDR hızını önemli ölçüde hızlandırır.

Literatürde MANET saldırı analizi ve protokol geliştirilmesi ile ilgili birçok çalışma olmasına rağmen FANET'lerde bu çalışmalar son zamanlarda araştırılmaya başlanılmıştır. İHA'lar, tasarsız ağlarda olduğu gibi bir grubun parçası olduğunda cihaza zarar vermek veya içerdiği verilere erişmek için saldırganların potansiyel hedefi olabilirler. İHA'ların gizliliğini, güvenliğini ve fiziksel bütünlüğünü hedef alan bu tür tehditlerin etkisi [26-27] hem İHA'nın görevini hem de içinde bulunduğu ağı ciddi şekilde etkileyebilir. Ayrıca, çoklu İHA iletişimi, güvenli iletişim mekanizmaları için ek tehditlere maruz kalmaktadır. FANET'ler daha yüksek düzeyde düğüm hareketliliğine sahiptir ve bu nedenle ağ topolojisinde geleneksel MANET'lerden daha sık değişiklik olur. Bu nedenle FANET'lerin benzersiz özelliklerini ve zorluklarını tartışan çalışmalar [28-29] yapılmıştır. Bekmezci ve diğerleri [30], FANET'lerin güvenlik gereksinimlerini ve bu yüksek düzeyde ağlara karşı olası tehditleri ele alır. Ayrıca, yazarlar iyi bilinen geçici ağ saldırılarını sunmakta ve FANET'lere yönelik bu tür saldırılar için güvenlik çözümlerini tartışmaktadır. Buna ek olarak FANET için başka bir çalışmada [8] FANET'ler için AODV tabanlı yeni bir yönlendirme ve güç kontrollü protokol sunulmuştur. MDRMA (Multi-data rate mobility-aware, MDRMA) protokolü, MDRMA-Yönlendirme ve MDRMA-Güç Kontrol olmak üzere iki algoritmadan oluşmaktadır. MDRMA-Yönlendirme verilerin hızlı ve verimli bir şekilde iletilmesini sağlamak için yönlendirme katmanı ve MAC alt katmanının bilgi alışverişi yapmasını sağlamaktadır. Buna ek olarak hızlı bir veri iletimi için iletim gücünün de kontrol edilmesi gerekmektedir. MDRMA-Güç Kontrol algoritması ise hedef ve kaynak düğüm arasında kurulan rota boyunca her bir bağlantıdaki veri akışları için iletim gücünü

kontrol etmektedir. Önerilen yönlendirme protokolünün performansı Ns-3 simülatöründe paket teslim oranı, ek yük ve uçtan uca gecikme metrikleri baz alınarak analiz edilmiştir. Çalışma sonucunda FANET için sunulan bu yeni protokolün hızlı veri iletimi ve kararlı yollar oluşturarak ağdaki bağlantı kopmalarını azalttığı gözlemlenmiştir.

Çizelge 2.1. Saldırı analizi literatür karşılaştırması

Referans	Ağ	Saldırı türü	Simülasyon aracı	Düğüm sayısı	Hareketlilik modeli	Hız
[18]	MANET	Kara delik	Ns-2	50	Rastgele yol noktası	5 m/s
[19]	MANET	Kara delik	Ns-2	20	Rastgele hareketlilik	rastgele hız
[21]	MANET	Kara delik	Ns-2	20,40,60,80,100	Rastgele hareketlilik	maksimum 25 m/s
[23]	MANET	Acele saldırı	Ns-2	100	Rastgele hareketlilik	0-20 m/s
[24]	MANET	Sel saldırısı	Ns-3	15	Rastgele yürüyüş	20 m/s
[25]	MANET	Sel saldırısı	Ns-2	50	Rastgele yol noktası	0-20 m/s
[34]	FANET	Sybil	Ns-2	35	Belirtilmemiş	30 m/s
[35]	FANET	Sybil	Ns-2	40,50,60	Rastgele hareketlilik	30 m/s

Literatürde saldırı analizi için yapılan çalışmalar, Çizelge 2.1.'de özetlenmiştir. Görüldüğü gibi, çalışmaların çoğu MANET'ler üzerinde yapılmıştır. FANET'ler için çalışmalar sınırlıdır. Çalışmaların çoğu Ns-2 simülasyon aracı kullanılarak yapılmıştır. Hareketlilik modeli olarak iki boyutlu hareketlilik modelleri kullanılmıştır. Bu hareketlilik modelleri FANET'lerin 3 boyutlu hareketlerini yansıtamamaktadır. Bu nedenle yapılan simülasyonların gerçek sistemlere uygulanması zor olmaktadır. Buna ek olarak hızlar maksimum 30 m/s olarak belirlenmiştir. Bu da saatte 108 km hıza denk gelmektedir (108 km/sa) ki, genellikle IHA'ların hızlarından çok düşüktür. [17]'de MANET'lere yönelik farklı saldırı türleri analiz edilmektedir. Ancak, çalışmaların geneli tek bir saldırı türüne odaklanmıştır. Yapılan çalışmaların çoğu kara delik ve sel saldırısını içermektedir. Bu çalışmada daha gerçekçi testlerin yapılması için Ns-3 simülasyon aracı kullanılmıştır ve 3 boyutlu Gauss-Markov hareketlilik modeli seçilmiştir. Gerçek İHA hızlarının yüksek olması nedeniyle hız saatte 720 km olarak belirlenmiştir (720km/sa). Bunlara ek olarak 4 farklı saldırı türünün, saldırgan oranları da %5- %25 aralığında değiştirilerek 13 farklı topoloji ile oluşturulan ağlar üzerindeki etkileri analiz edilmiştir.

2.2. MANET Saldırı Tespiti

İzinsiz giriş tespit çalışmaları MANET'ler için [31-33]'de yapılmıştır. [31]'de MANET korumasında geleneksel yöntemlerin yeterli olmaması nedeniyle bilgi görselleştirmeden yararlanan yapay sinir ağı ile saldırı tespit sistemi geliştirilmiştir. Ayrıca görselleştirme kullanılarak türetilen haritaların saldırgan tarafından değiştirilmesini önlemek için damgalama yöntemi kullanılmıştır. Bu yöntem orijinal bilgilerin içerisine benzersiz mesaj yerleştirmesi yapılarak oluşturulmaktadır. Önerilen yöntem farklı koşullarda (çeşitli trafik koşulları, hareketlilik modelleri ver görselleştirme ölçütleri) yüksek performans göstermiştir. Bu çalışmada MAC katmanına ait özniteliklerle veri kümesi oluşturulmuştur. Bu veri kümesi yapay sinir ağları ile eğitilerek saldırı tespit oranı ve yanlış alarm oranı metriklerine göre değerlendirme yapılmıştır. Ve tespit oranı ortalama %80, yanlış alarm oranı yaklaşık %20 oranlarındadır. Bizim yaptığımız çalışmadan farklı olarak görselleştirme üzerinden ve MAC katmanından toplanan verilere yapay sinir ağları uygulanmıştır. Bizim çalışmamızda YSA giriş katmanı için 30 farklı öznitelik kullanılmaktadır. Özniteliklerin fazla olması bu algoritmaların doğru sonuç vermesinde önemli bir rol oynamaktadır. Buna ek olarak çalışmamız kullanıcı ve ağ tabanlı iki farklı sınıflandırma yapmaktadır ve tespit oranı ortalama %94 ve yanlış pozitif oranı ortalama %9 çıkmaktadır.

Başka bir çalışmada [32] ise Matlab 2019b kullanılarak MANET'lerde solucan deliği saldırısı gerçekleştirilmiştir. MANET'te düğümlerin özellikleri ve hızları kullanılarak veriler toplanmıştır. Veriler işaretlenirken saldırgan düğümler belirtilmiştir ve toplamda 8 öznitelik kullanılmıştır. Bu veriler çeşitli makine öğrenme yöntemleri (en yakın komşu, destek vektör makinesi, karar ağacı, doğrusal ayrım analizi, naive bayes ve evrişimsel sinir ağları) ile sınıflandırılarak saldırı tespiti gerçekleştirilmiştir. Bu çalışmanın genel amacı normal düğümler arasındaki saldırgan düğümlerin tespit edilmesidir. Kullanılan yöntemler arasında en iyi sınıflandırmayı %92,6 duyarlılık (tespit oranı) ile karar ağacı yapmıştır.

Laqtib ve arkadaşları [33] MANET'lerin geleneksel şifreleme yöntemleri ile yeni tehditlerden korunamayacağını ve bu nedenle saldırı tespit sistemlerinde derin öğrenme yöntemlerinin uygulanması gerektiğini belirtmişlerdir. MANET'lerin değişken ortamlara uyarlanabilmesi ve izinsiz girişleri doğruluk oranı yüksek şekilde tespit edebilmesi için çalışmalar yapmışlardır. Çalışmalarında 1999 yılında yayınlanan NSL-KDD veri setine çeşitli derin öğrenme yöntemleri uygulamışlardır ve yüksek doğruluk oranları elde etmişlerdir.

2.3. FANET Saldırı Tespiti

Literatürde FANET'ler için önerilen birkaç güvenlik çözümü bulunmaktadır. Bazı çalışmalar [34-35] sybil saldırıları için çözümler önermektedir. Walia ve diğerleri [34], sybil saldırısını tespit etmek için karşılıklı bir kimlik doğrulama tekniği önerir. Bu yöntemde her düğüm komşu düğümlerini kontrol eder ve aynı kimliğe sahip farklı komşular varsa düğüm kötü niyetli olarak işaretlenir ve izlenir. Bu işaretli düğüm kimliğini değiştirirse, kötü niyetli olduğu varsayılır. Önerilen yöntem, diğer yöntemlere kıyasla maksimum verim, minimum ek yük ve minimum paket kaybına sahiptir. Bhatia ve diğerlerinin [35] önerdiği başka bir çözüm ise sybil saldırısını tetikleyen kötü amaçlı düğümleri belirlemek için izleme, algılama ve izolasyon adımlarından oluşur. İzleme adımında ağ içerisindeki etkinlikleri düğümlerin etkinlikleri merkezi bir kontrolörde gözlemlenmektedir. Bu merkezi sistem ağa katılan düğümlerin kimliklerini hafızada tutar ve düğüm kimliğini değiştirirse merkezi sistem bir doğrulama mekanizması çalıştırır. Kimlikler farklı olduğunda düğüm saldırgan olarak işaretlenir ve düğüm ağdan izole edilir.
Bütün bu çalışmalara ek olarak FANET'ler için yayınlanan bir veri kümesi olmadığı için yapay zeka ve makine öğrenmesi çalışmaları literatürde sınırlıdır. Geleneksel yöntemler kullanılarak yapılan bir çalışmada [36] ise, FANET izinsiz giriş tespiti için hibrit bir yöntem önerilmiştir. Önerilen yöntem iki adımdan oluşmaktadır. İlk olarak, spektral analiz, ağdaki izinsiz giriş türüyle ilgili temel düzeyde bilgi sunan belirli bir trafik imzası oluşturmak için kullanılır. İkinci olarak, ilk adımın çıktısı ile denetleyici/gözlemci tabanlı tahmin adımı ağda gözlemlenen saldırı düzeyini değerlendirir. Saldırıların hızlı ve doğru bir şekilde tespit edildiği sonuçlardan gözlemlenmiştir. Algılamadaki gecikme ihmal edilebilir düzeydedir ve izinsiz giriş trafiği ile normal trafik doğru bir şekilde ayrılabilmektedir.
Diğer çalışmalar [37], [11] makine öğrenimi ve yapay zeka algoritmaları kullanarak saldırı tespiti yapılmaktadır. Ouiazzane ve diğerleri [37] İHA filoları için yeni bir saldırı tespit modeli önermişlerdir. Bu çalışmada ağı sürekli olarak dinleyen ve anormallik tespit edildiğinde uyarı veren çok etmenli paradigmaya sahip bir sistem geliştirilmiştir. Normal referans profilinin öğretilmesi için makine öğrenim yöntemi kullanılmıştı ve modelden bir sapma bulunur ise saldırı olarak algılanmaktadır. İlk olarak İHA filosunu dolaşan bütün trafik ağ dinleme aracı ile yakalanmaktadır. Yakalanan trafik filtreleme aracına yollanarak bilinen bütün saldırı ve imzaları içeren veri tabanından eşleşme olup olmadığı kontrol edilir. Eşleşme var ise alarm verilir. Paket normal ise hiçbir işlem uygulanmaz. Ancak,

paket imza veri tabanı tarafından tanınmaz ise Hadoop Dağıtılmış Dosya Sisteminde depolanır. Daha sonra öznitelik seçimi yapılarak normal trafik modelinden sapmalar makine öğrenimi tekniği kullanılarak gerçekleştirilir. Saldırı tespit edilirse uyarı verilmektedir. Yeni model sonuç ne olursa olsun veri tabanına kaydedilir. Makine öğrenimi yöntemi olarak karar ağacı algoritması kullanılmıştır ve gerçek zamanlı olarak bilinen saldırıları tespit etmektedir. Sistemin doğruluk değeri %100 olarak gösterilmektedir. Bilinmeyen saldırıların tespit edilebilmesi için ise yarı denetimli makine öğrenme teknikleri kullanılmaktadır. Karar ağaç algoritmasının tespit edemediği bilinmeyen saldırılar var ise bu durum da ağ trafiği yarı denetimli makine öğrenim süreci için bir sonraki adıma gönderilmektedir. Bu adımlar çalışmada denenemediği için test sonuçları verilmemiştir.

[11]'da ise her bir İHA kendi içerisinde saldırıyı tespit etmeye çalışan tekrarlayan sinir ağı modülüne sahiptir. Aynı zamanda merkezi bir modül ile de saldırıyı onaylayıp diğer düğümlere haber veren bir baz istasyonu vardır. Tekrarlayan sinir ağı bir girdi aldığında sırasıyla dört katmandan geçmektedir. Son olarak önermeyi yapmak için son katmandan çıktı üretilmektedir. Algoritma trafikten çıkarılan parametreleri anormalliği tespit etmesi için tahmin fonksiyonuna yönlendirmektedir. Anormal bir davranış olduğunda sistem karar karar mekanizmasını çalıştırmak için kontrolörü bilgilendirir. Sistemin eğitim ve test aşamaları için KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, CICIDS2017 ve TON_IoT gibi veri kümeleri kullanılmıştır. Çalışmada da belirtildiği gibi literatürde FANET'lere ait işlenebilecek bir veri kümesi bulunmamaktadır. Bu nedenle MANET, VANET gibi ağlardan toplanan veri kümeleri kullanılmaktadır. Bu durum sonuçların gerçekçi olmasını engellemektedir. FANET'ler karakteristik özellikler bakımından diğer geleneksel ağlardan farklı bir yapıya sahiptir ve diğer ağlardan toplanan saldırı parametreleri FANET için geçersiz sayılabilmektedir. Bilindiği üzere bu tez çalışmasında FANET'lerde detaylı saldırı analizi yapılması sonucunda özel bir veri kümesi oluşturarak bu veri kümesi üzerine yapay zeka algoritmaları uygulandı. Sonuçların gerçekçi olabilmesi için FANET'lerin üç boyutlu hareketine uygun bir hareketlilik modeli seçilmiştir. Buna ek olarak, saldırgan düğümlerle ve saldırıdan etkilenen düğümlerle iki farklı saldırı tespiti gerçekleştirilmiştir ve sınıflandırma işlemi başarılı bir şekilde gerçekleştirilmiştir.

Özetle, AODV'ye yönelik yönlendirme saldırıları literatürde kapsamlı bir şekilde çalışılsa da, FANET'lerin daha yüksek hızlara ulaşan düğümlere sahip olma, 3 boyutlu hareket etme gibi farklı özellikleri, bu yüksek hareketliliğe sahip ağlara yönelik saldırıların yeni bir analizini gerektirmektedir. Böyle bir analizin olmaması, FANET'ler için güvenlik

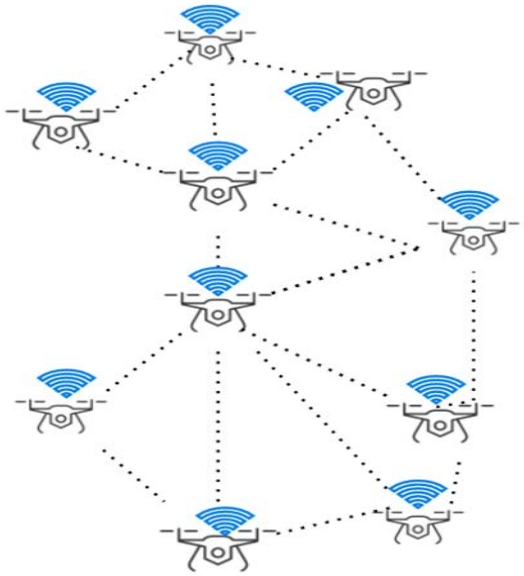
çözümlerinin geliştirilmesini de olumsuz etkiler. Ayrıca yapay zeka uygulamaları için FANET'e özel toplanan bir veri kümesi bulunmamaktadır. Yapılan çalışma ile FANET'ler üzerine detaylı saldırı analizi yapılmakla birlikte, saldırıların tespit edilmesi için üzerinde çalışılacak bir veri kümesi de oluşturulmuştur. Bu veri kümesi kullanılarak geleneksel saldırı tespit sistemlerinin yerine yapay sinir ağları ile saldırı tespiti gerçekleştirilmiştir.

3. UÇAN TASARSIZ AĞLAR (FANET)

Yıllardır kullanılan İHA'lar teknolojinin de gelişmesi ile birlikte daha küçük ve maliyeti en aza indirecek şekilde tasarlanmaya başlanmıştır. Fakat küçük bir İHA'nın yapabileceği işlemler sınırlıdır. Tekli İHA'lar, pillerinin hızlı bitmesi, görüş alanlarının kısıtlı olması, görevlerinin uzun süre devam etmesi, harici bir etki nedeniyle elektronik sistemlerinin düşmesi veya arızalanması gibi durumlarda görevlerini tamamlayamazlar. Grup halinde çalışabilen birden fazla İHA ile tek bir İHA'nın kapasitesinden daha fazlasına sahip olan bir sistem oluşturulabilir. Grup halinde çalışabilen İHA sistemlerinin sağladığı genel avantajlar;

- Gruplar halinde çalışabilen İHA'ların boyutları da küçük olmaktadır ve küçük İHA'ların maliyeti, büyük bir İHA'nın maliyetinden daha düşük olmaktadır.
- Çoklu İHA sistemleri ile yapılacak işlemlerin ölçeklenebilirliği arttırılır.
- Görevde olan tek bir İHA başarısız olduğunda görev devam ettirilemez. Fakat çoklu İHA kullanımında bir İHA başarısız olduğu zaman görev diğer İHA'lar tarafından sürdürülebilir.
- İHA sayısının fazla olması bir görevin daha hızlı tamamlanmasını sağlamaktadır.
- Çoklu İHA'lar küçük boyutlarda ve genellikle radar sinyallerini yansıtmayan maddelerden yapıldığı için küçük radar kesitleri üretir ve tespit edilmesi daha zordur.

Çoklu İHA sistemlerinin avantajlarının yanı sıra İHA'lar arasındaki iletişimin sağlanmasında zorluklar da vardır. Tek İHA sistemlerinde haberleşme için yer üssü veya uydu gibi altyapılar kullanılmaktadır ve İHA ile altyapı arasında tekli iletişim kurulur. Çoklu İHA sistemlerinde de uydu ve yer üssü sistemleri kullanılabilir. Fakat bu altyapılar, her bir İHA için pahalı ve karmaşık donanım gerektirmektedir. İHA sayısı arttıkça her bir İHA'nın tek tek yer üssü ile haberleşmesi iletişim problemlerine ve bant genişliğinin verimsiz kullanımına neden olacaktır. Bu nedenle daha verimli iletişim çözümleri bulunması gerekmektedir. Bu gibi durumlarda, birden fazla İHA'nın ortak bir ağa katılmasına ve karmaşık görevlerin organize bir şekilde yürütülmesine izin veren FANET önerilir [39]. Şekil 3.1'de FANET yapısı gösterilmektedir. FANET, MANET ve alt sınıflarından bazı özellikleri miras almasına rağmen, İHA'ların sahip olduğu yüksek hareketlilik, ön görülemeyen hareketler ve ağ üzerinde sık değişen topoloji gibi zor karakteristik özellikleri nedeniyle farklılar da içermektedir.

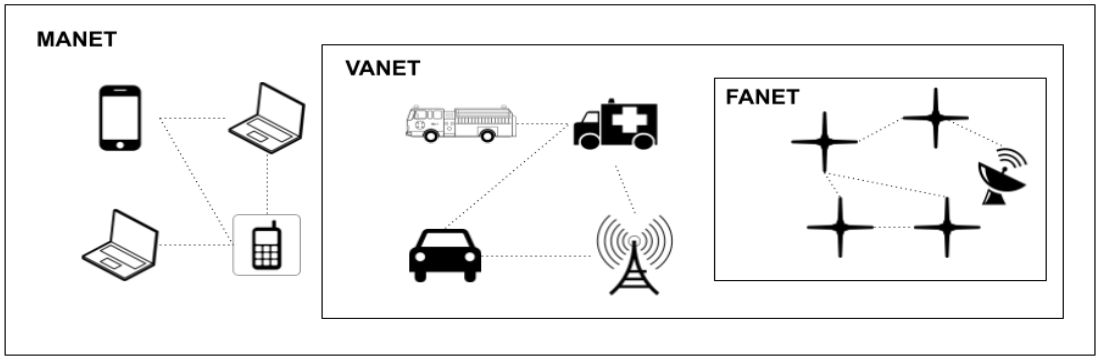


Şekil 3.1. Uçan Tasarsız Ağlar (FANET)

3.1. FANET Karakteristik Özellikleri

Son yıllarda popüler olan FANET, yeni bir tasarsız ağ ailesi olarak tanımlanmaktadır. FANET, MANET'ler ve VANET'lerin özelleştirilmesi ile oluşturulmuştur [28]. MANET mobil düğümlerin kendi kendini organize etmesi ile oluşan kablosuz bir ağ türüdür [40]. MANET'lerin uygulama alanlarının artması ile birlikte mobil düğümler, kablosuz bağlantılarla birbirine bağlanan hareketli araçlarda [41] da kullanılmaya başlanmıştır ve VANET kavramı ortaya çıkmıştır.

Kablosuz tasarsız ağlar görev amaçları, iletişim, dağıtım ve kullanım alanlarına göre sınıflandırılmaktadırlar. FANET, MANET ve VANET gibi geleneksel tasarsız ağlarla ortak özelliklere sahiptir. Ve Şekil 3.2'de gösterildiği gibi FANET'ler, MANET ve VANET'lerin alt kümesi olarak sınıflandırılabilir. Gelişmekte olan FANET'ler, bu ağlarla ortak özellikleri olmasına rağmen benzersiz tasarım problemlerine de sahiptir. FANET'lerin mevcut tasarsız ağlardan farkları şu başlıklar altında toplanmış ve aşağıda her başlık detaylı bir şekilde anlatılmaktadır: hareketlilik, yoğunluk, topoloji değişimi, yayılma modeli, enerji tüketimi, lokalizasyon, hareketlilik modeli, platform kısıtlamaları.



Şekil 3.2. MANET, VANET ve FANET kümelenmesi

3.1.1. Düğüm hareketliliği

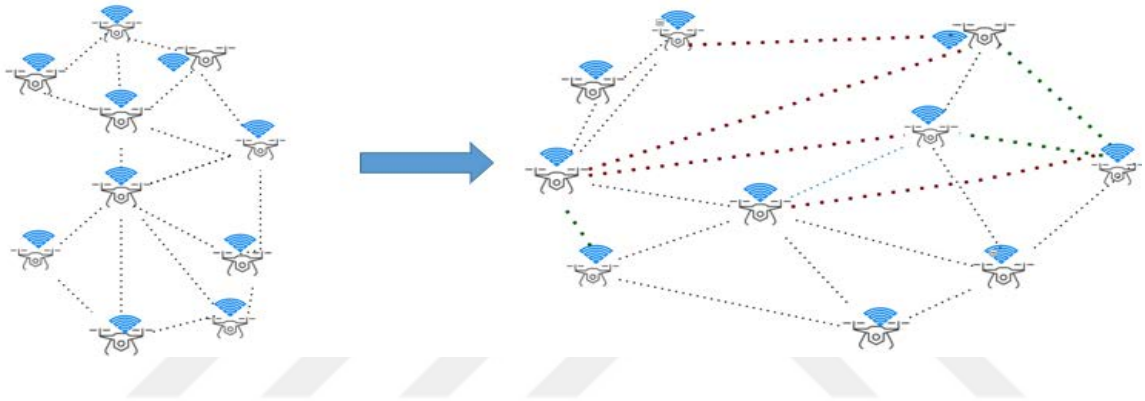
FANET'i diğer tasarsız ağlardan ayıran en belirgin özellik düğüm hareketliliğidir. FANET'ler 720 km/s hızın üzerine çıkabiliyorken, MANET'ler 72 km/s, VANET'ler ise 20 km/sa ile 100 km/s hıza sahiptir. MANET ve VANET düğüm hareketliliği ile karşılaştırıldığında FANET'in düğüm hareketliliği çok daha yüksektir. Bu ağlar düğümlerin yüksek hareketliliği nedeniyle çok dinamik bir yapıya sahiptir ve tam olarak güvenilir bir iletişim sağlayamaz [42]. İHA'ların zorlu görevleri tamamlayabilmesi için iletişimin iyileştirilmesi ve bağlantı kopukluklarının azaltılması gerekmektedir. Bu problemlerinin çözülmesi için İHA'ların konum ve hareketlerini optimize ederek bağlantıları iyileştiren farklı bağlantı türleri geliştiren çalışmalara yapılmıştır [43].

3.1.2. Düğüm yoğunluğu

Bir birim alandaki ortalama İHA sayısına düğüm yoğunluğu denir [44]. İHA'ların yoğunluğu kullanım alanları, gökyüzündeki dağılımları ve İHA çeşitlerine göre düşük yoğunluktan yüksek yoğunluğa kadar değişebilir. İHA'lar yüksek bir hıza ve geniş bir iletim menziline sahipse aralarındaki mesafe birkaç kilometre olabileceği için yoğunlukları düşük olabilir [45]. Bu nedenle FANET düğüm yoğunluğu MANET ve VANET'ten daha düşüktür.

3.1.3. Topoloji değişimi

FANET'ler Şekil 3.3'te gösterildiği gibi yüksek bir hareketliliğe sahip olduğu için düğümlerin konumları da sıklıkla değişmektedir. Bu duruma bağlı olarak FANET topolojisi de MANET ve VANET topolojisine göre daha fazla değişim göstermektedir. Hareketlilik nedeniyle değişen konuma ek olarak, İHA platform arızaları, İHA'ların başarısız olması, gruba yeni bir İHA'nın dahil olması ve bağlantı kalitesindeki hızlı değişimler de topolojiyi değiştirebilir [46].



Şekil 3.3. FANET dinamik topoloji değişimi

3.1.4. Yayılma modeli

İletişim sistemlerinin geliştirilmesinde radyo yayılım özelliği önemli bir yere sahiptir [39]. Çevresel şartlar nedeniyle FANET, VANET ve MANET'ten farklı radyo yayılım özelliklerine sahiptir. MANET'ler ve VANET'ler yere yakın oldukları için gönderici ve alıcı arasında görüş hattı yoktur ve coğrafi yapı radyo sinyallerini etkiler. Fakat FANET'teki düğümler yerden uzakta bulunduğu için çevresel faktörlerden çok fazla etkilenmezler. Buna ek olarak gökyüzündeki İHA'lar arasında engel olmayacağı için yüksek görüş hattı özelliğine sahiptir.

3.1.5. Enerji tüketimi

Enerji tüketimi FANET'ler için önemli tasarım konularından bir tanesidir. Enerji tüketimi İHA'ların boyutuna ve çeşitlerine bağlı olarak değişmektedir. Özellikle mini İHA'lar düşük kapasiteli piller ile çalıştırıldığı için [47] güç tüketim problemi hala çözülememiştir [46]. Ağ ömrünün arttırılması enerji verimi sağlayan bir iletişim protokolü tasarımı ile mümkün olmaktadır.

3.1.6. Lokalizasyon

Lokalizasyon her bir düğümün yerinin belirlenmesi demektir [44]. İHA sistemleri hızlarının yüksek olması ve çeşitli hareketlilik modellerine sahip olması nedeniyle kısa zaman aralıklarıyla doğru bir yerleştirme bilgisi gerektirir. Konum bilgisi için GPS kullanıldığında, bilgi bir saniyelik aralıklarla güncellenebilir ve bu durum İHA'ların farklı uygulamalarda (teslimat, arama kurtarma, yangın tespiti vb.) kullanımı için uygun değildir [48]. Fakat bir İHA, GPS ve bir atalet ölçüm birimi ile donatılırsa istenilen herhangi bir zamanda konum bilgisi sunabilmektedir [49]. Konum bilgisine daha kısa sürede ulaşılabilmesi için iki farklı yöntem de önerilmiştir. Birisi paket değişimini temel alan ağ tabanlı konumlandırma [50] diğeri ise irtifaya dayalı konumlandırmadır [51].

3.1.7 Hareketlilik modeli

FANET senaryolarına göre hareketlilik modelleri değişmektedir. İHA'lar önceden belirlenmiş bir yolda planlı olarak hareket edebilecekleri gibi rastgele hız ve yönler de kullanabilirler [44]. Hareketlilik modellerinin detaylı açıklaması Bölüm 3.3'te tartışılmaktadır.

3.1.8. Platform kısıtlamaları

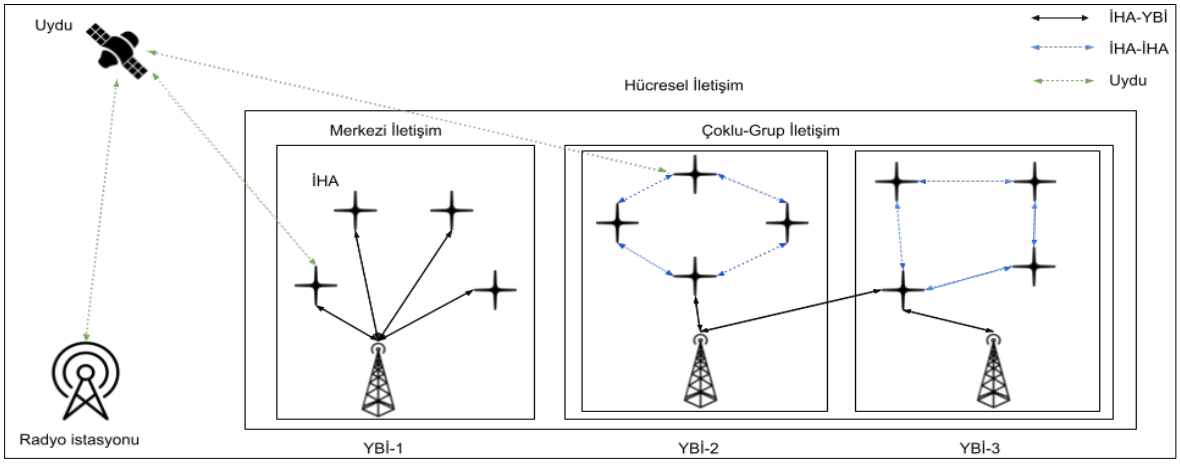
İHA platform kısıtlamaları nedeniyle yük kapasitesi sorunu oluşmaktadır. İHA'ların daha dayanıklı olması ve yüksek irtifa elde edebilmesi için hafif yüke sahip olmaları

gerekmektedir [52]. Bu nedenle boyut, ağırlık ve güç tüketimi gibi belirli kısıtlamalar FANET iletişim donanımının da hafif olmasını gerektirir. Donanımın hafif olması İHA'lara daha fazla ek sensör eklenebileceği anlamına gelir ve bu durum da İHA performansı için önemlidir. Mini İHA'ların da yaygın bir şekilde kullanılması ile birlikte ekipmanların daha hafif, küçük ve güç tüketimi düşük olacak şekilde tasarlanması önemlidir.

3.2. FANET İletişim Mimarisi

FANET iletişim mimarisi tasarlamak, yer baz istasyonu ve İHA'lar arasında bilgi iletiminin nasıl yapılacağını belirleyen bazı kural ve mekanizmalar ile tanımlanmaktadır. İletişim mimariler İHA'ların uygulama alanlarına göre çeşitlilik gösterir. Hangi mimarinin en iyi çalıştığına dair kesin sonuç veren bir araştırma bulunmamaktadır [39]. İletişim mimarileri Şekil 3.4'te gösterilmektedir.

Merkezi iletişim mimarisi, her bir İHA'nın bir veya birden fazla yer baz istasyonuna (YBİ) doğrudan bağlanması ile oluşturulur. Bu mimaride İHA'lar kendi aralarında iletişim kuramadıkları için veri trafiğinin tamamı YBİ'ler tarafından yönlendirilmelidir [53]. Bu mimari ile hatların azalması, hesaplama ve depolama yeteneklerinin geliştirilmesi bir avantaj olsa da dezavantajları çok daha fazladır. İlk olarak İHA sayısındaki artış ile birlikte İHA'lara ayrılmış bant genişliği de artacağı için maliyet yükselecektir. İkincisi, İHA'lar kendi aralarında iletişim kuramazlar ve verilerin YBİ ile aktarılmasından kaynaklanan yüksek bir gecikme vardır. Son dezavantaj ise ağda merkezi bir iletişim noktasının olması büyük bir güvenlik açığı oluşturmaktadır. YBİ kaynaklı bir arıza çıkması ya da bir saldırı olması durumda bütün ağ bu durumdan etkilenir ve İHA'ların iletişimi kesilir.



Şekil 3.4. FANET iletişim mimarisi

Hücresel iletişim mimarisi, İHA'ların bir veya birden fazla hücresel ışın oluşturan baz istasyonu alt yapısı kullanımı ile oluşmaktadır [54]. Bir araya gelen hücreler sinyal kapsama alanı artışı sağlamaktadır [55]. Ayrıca farklı frekans kullanımı ile olası müdahalelerin engellenmesi sağlanır. Hücresel mimari, merkezi mimarinin aksine İHA'ların kendi aralarında haberleşmesine olanak sağlamaktadır. Dezavantajı ise uygulaması pahalıdır ve bölgenin bilinmediği ya da baz istasyonu bulunmayan bölgelerde kullanımı mümkün değildir. Güvenlik açısından da çok fazla sabit nokta saldırılara karşı savunmasızdır ve bu saldırılar sonucunda İHA'larda kontrol kayıpları yaşanabilir.

Çoklu-Grup iletişim Mimarisi, merkezi iletişimin korunup aynı zamanda İHA'ların birbirleriyle sabit bir alt yapı olmadan tasarsız bir şekilde haberleşmesini sağlar. Grup içerisinde İHA'lar haberleşirken baz istasyonu iletişime dahil edilmez. Sadece seçilen İHA'lar baz istasyonuna bağlanır ve bu şekilde çoklu İHA grupları arasında iletişim sağlanmış olur [56]. Fakat yarı-merkezi durum nedeniyle trafiğin bir kısmı sabit yer istasyonlarından geçtiği için güvenilirlik problemi devam etmektedir.

FANET'lerde dikkate alınması gereken 3 iletişim türü vardır. Bunlar İHA'dan İHA'ya, İHA'dan YBİ'ye ve uydu iletişimidir. İHA'dan İHA'ya iletişim, doğrudan veya uzaklık nedeniyle iletişimin diğer İHA'lar üzerinden atlamalı olarak sağlanması ile gerçekleştirilir. Diğer İHA'lar üzerinden gerçekleştirilen iletişim sayesinde kapsama alanı genişleyebilmektedir.

İHA'ların kontrolünü daha iyi sağlamak için sabit bir YBİ, kontrol ve komut mesaj alışverişinde kullanılır. Bir İHA ve YBİ arasında iletişim sağlanırken yüksek kapasiteli bant genişliği istenmesi nedeniyle genel olarak grup arasından seçilen bir İHA, YBİ ile

iletişim sağlamaktadır. Bu şekilde maliyet azaltılmakta, ağ tıkanıklığı problemi ortadan kalkmakta ve verimli bir iletişim sağlanmaktadır. Ayrıca İHA ve YBİ arasındaki iletişim farklı İHA gruplarının da kendi aralarında haberleşmesine imkân tanımaktadır.

Çizelge 3.2. İHA iletişim türlerine ait özelliklerin karşılaştırılması

	İHA'dan İHA'ya	İHA'dan YBİ'ye	Uydu
Görüş Hattı	Yüksek	Orta	Yüksek
Maliyet	Ucuz	Pahalı	Çok Pahalı
Kapsama alanı	Orta	Geniş	Çok Geniş
Kötüye kullanım	Kısa süreli	Orta Süreli	Uzun Süreli

FANET bağlantı kopmalarının engellenmesi ve kalıcı bir bağlantı sağlanması için merkezi bir sisteme ihtiyaç duymaktadır. Bu ihtiyacın karşılanması için uydular kullanılmakta ve İHA'lara önemli bir görüş hattı oluşturmaktadır. Uydu iletişimi maliyeti arttırması nedeniyle YBİ'lerin kurulumunun zor olduğu coğrafik alanlarda daha çok tercih edilmektedir. Çizelge 3.2'de İHA'lara ait dikkat edilmesi gereken 3 iletişim türünün belirgin özelliklerinin karşılaştırılması verilmiştir. İHA'ların YBİ'ye doğrudan bağlantı sağlaması ile tek bir bağlantı noktası oluşmaktadır. Bu da saldırıların hedefi haline gelmesini sağlayacaktır. YBİ'ye ya da ona bağlı olan İHA'ya yapılan saldırı ile sistem kullanılmaz hale gelebilir. Ancak, İHA'lar kendi aralarında iletişim kurduklarında saldırgan düğüm diğer düğümlerin ağdaki durumunu da etkileyeceği için saldırının fark edilmesi ve önlenmesi daha kısa sürebilmektedir. Bu nedenle kötüye kullanımı ve ele geçirilme ihtimalleri diğer iletişim türlerine göre biraz daha azaltmaktadır.

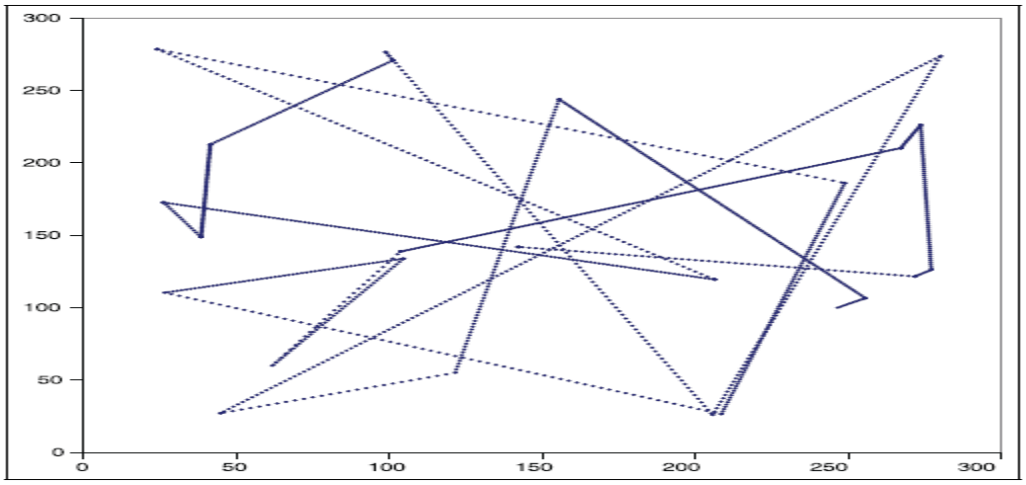
3.3. Hareketlilik Modeli

Tasarsız ağların performansı, gerçek deney ortamları veya genellikle simülasyon araçları kullanılarak simüle edilmektedir. [57]. Genellikle topoloji değişiminin yüksek olduğu büyük bir ağ yapısını oluşturmak karmaşık ve maliyeti fazla olduğu için simülasyon ortamları kullanılmaktadır. Bu nedenle, gerçekçi bir simülasyon ortamının oluşturulması ve olası sorunların görülebilmesi için hareketlilik modellerinin iyi tasarlanması gerekmektedir.

Ağda yer alan düğümlerin konumları ve belirli bir zamandaki hız değişimleri hareketlilik modelleri ile temsil edilmektedir [58]. Hareketlilik modeli ağ proformasını önemli oranda etkilemektedir. MANET'ler için tasarlanan Rastgele Yol Noktası ve Rastgele Yön Hareketlilik modelleri, FANET'ler simüle edilirken sıklıkla seçilen hareketlilik modellerindendir. Fakat düğüm hareketi ve yönü dışında İHA'ların aerodinamik ve mekanik kısıtlarını da yakalayan gerçekçi bir hareketlilik modeline ihtiyaç duyulmaktadır. Bu nedenle İHA'ların hareketlerini gerçekçi bir şekilde taklit edebilen ve üç boyutlu hareketin gözlenebileceği gerçekçi bir hareketlilik modeline ihtiyaç vardır. Bildiğimiz kadarıyla, üç boyutlu Gauss-Markov Hareketlilik Modeli bu ihtiyacı karşılamaktadır. Aşağıda her bir hareketlilik modelinin ayrıntısı verilmiştir.

3.3.1. Rastgele yol noktası (RYN) hareketlilik modeli

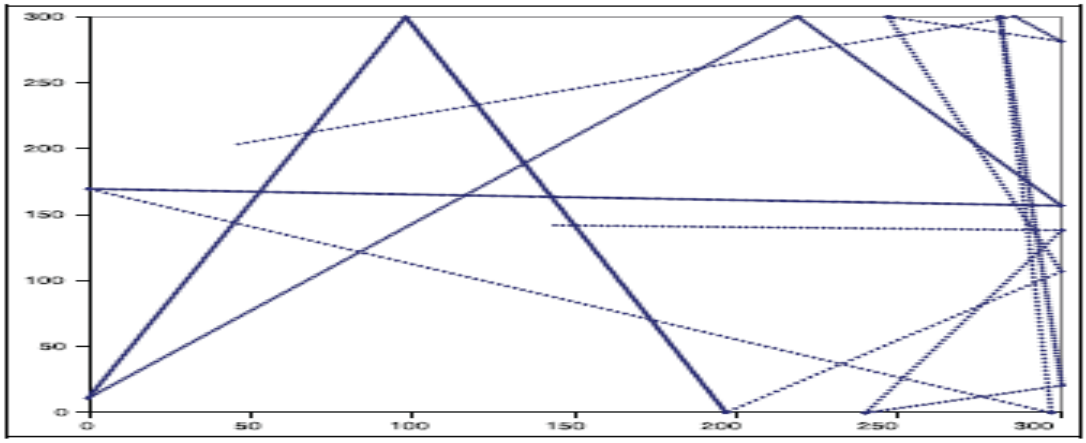
RYN hareketlilik modelinde [57] sabit bir duraklama süresi vardır. Düğümler bu sürede hareketsiz kaldıktan sonra kendilerine, hareket etmek için belirlenen simülasyon alanı içerisinde rastgele bir konum ve hız seçerek harekete geçerler. Seçilen konuma ulaştıktan sonra tekrar bir bekleme süresi olur ve rastgele konum ve hız seçim işlemi tekrarlanır. Simülasyonda belirlenen süre boyunca bu süreçler tekrarlanır. Şekil 3.5'te RYN hareketlilik modeli kullanılarak simüle edilmiş bir düğümün hareketi yer almaktadır. Gerçek bir İHA hareketine uygun olmayan durma süresi, ani yön ve hız değişikliklerine [59] sahip olması bu modelin büyük dezavantajlarındandır.



Şekil 3.5. Rastgele yol noktası hareketlilik modelini kullanan bir düğümün modeli [59]

3.3.2. Rastgele yön (RY) hareketlilik modeli

RY hareketlilik modeli RYN hareketlilik modelinden farklı olarak 0 ile 2π arasında rastgele bir hareket yönü seçer ve simülasyon alanının sınırına doğru harekete geçer. Sınıra ulaşıldığında bir süre bekler ve 0 ile π arasında yeni bir yön seçerek hareket eder. Yön seçiminin π ile sınırlı kalması düğümün sınır dışına çıkmasını engellemek içindir [60]. RY hareketlilik modeli RYN hareketlilik modelinde simülasyon alanının merkezinde oluşan düğüm yoğunluğu problemini aşmak için önerilmiştir. Bu problemi çözmüş olsa da keskin dönüşler, ani duruş ve kalkışlar nedeniyle gerçek bir İHA hareketini simüle etmekte yetersiz kalmaktadır. Şekil 3.6'da RY modelini kullanan bir düğüm hareketi gösterilmektedir.



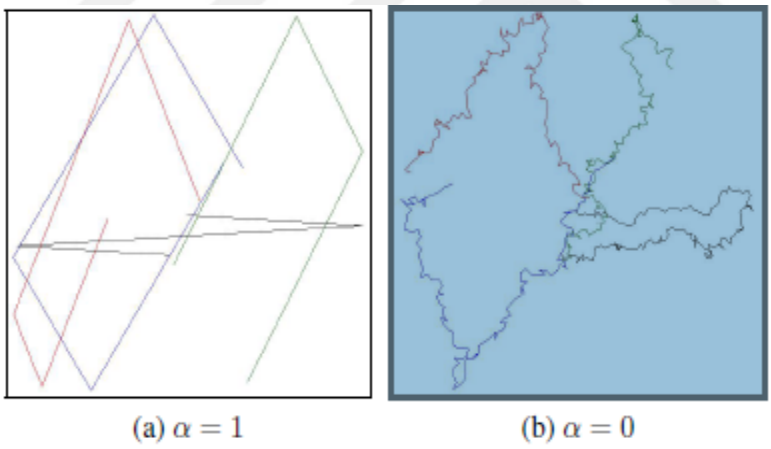
Şekil 3.6. Rastgele yön hareketlilik modelini kullanan bir düğümün modeli [60]

3.3.3. Gauss-Markov (GM) hareketlilik modeli

Liang ve Haas [61] tarafından önerilen GM Modeli çeşitli rastgelelik derecelerinin ayarlanabilmesi için tek bir parametreye sahip, bellek tabanlı bir modeldir [62]. İlk olarak her bir düğüm bir başlangıç hızı ve yönü ile harekete başlar. Sonrasında ise belirlenen zaman aralığında, düğümlerin hızı ve yönü tekrar hesaplanır ve güncellenir. Güncellenen yön, hız ve konuma göre sonraki gidilecek konum bilgisi elde edilir. GM modelinde ortalama yön kavramının tam olarak tanımlanmadığı ve gelişmiş bir sınırdan kaçma stratejine ihtiyaç duyulması nedeniyle gelişmiş GM Modeli tanıtılmıştır [63].

3.3.4. 3B Gauss Markov (GM) hareketlilik modeli

İHA'lar doğaları gereği üç boyutlu olarak hareket etmektedirler. Bu hareketliliğin gerçekçi bir şekilde simüle edilebilmesi için deneylerde üç boyutlu bir hareketlilik modeli kullanılmalıdır. Bildiğimiz kadarı ile literatürde önerilen 3B GM hareketlilik modeli bu özelliği sağlayan tek modeldir. Bu model, üç boyutlu hareketin yanı sıra ani hareket değişikliklerini önlemek ve çeşitli rastgelelik uyarlamalarını entegre etmek için tek bir ayar parametresi ile tasarlanmış, zamana dayalı bir hareketlilik modeli olarak kullanılmaktadır [57]. Bir düğümün ardışık konumları arasındaki hareketlerinin uyumlu olması gerektiğinden [64], model önceki hareketleri hafızasında tutar. Düğümlerin hareketlilik davranışı, 0 ile 1 arasında değerler alan α parametresi ile ayarlanır. Şekil 3.7'de gösterildiği gibi α = 0 iken, rastgele bir hareketlilik gerçekleşeceği için belleksiz bir modele karşılık gelir. α 1'e yaklaşırken, bellek kullanılır ve hareket daha öngörülebilir hale gelir.



Şekil 3.7. α = 1 ve α = 0 iken GM hareketlilik modeli [64]

GM hareketlilik modelini iki boyuttan üç boyuta genişletmek için ilk olarak üç boyutlu bir hız vektörü x, y ve z eksenlerine uygulanmaktadır.

$$x_n = \alpha x_{n-1} + (1-\alpha)\overline{x} + \sqrt{(1-\alpha^2)}x_{x_{n-1}}$$
$$y_n = \alpha y_{n-1} + (1-\alpha)\overline{y} + \sqrt{(1-\alpha^2)}y_{x_{n-1}} \quad (1)$$
$$z = \alpha z_{n-1} + (1-\alpha)\overline{z} + \sqrt{(1-\alpha^2)}z_{x_{n-1}}$$

Bu yöntemde x, y ve z yönlerindeki hızlara dayalı olarak uçuşu modellemek zordur. Hız ve yön değişkenleri ile başlayıp düğümün ufka doğru dikey hareketini takip etmek için üçüncü bir değişken eklenmelidir:

$$\begin{aligned} s_n &= \alpha s_{n-1} + (1-\alpha)\overline{s} + \sqrt{(1-\alpha^2)}s_{x_{n-1}} \\ d_n &= \alpha d_{n-1} + (1-\alpha)\overline{d} + \sqrt{(1-\alpha^2)}d_{x_{n-1}} \\ p_n &= \alpha p_{n-1} + (1-\alpha)\overline{p} + \sqrt{(1-\alpha^2)}p_{x_{n-1}} \end{aligned} \quad (2)$$

Algoritmada değişkenler hesaplandıktan sonra düğüm yeni bir hız belirlemeli ve hız vektörleri düğüm konumunun yeniden hesaplandığı bölüme aktarılmalıdır [64]. Hız vektörü aşağıdaki formül ile yeniden hesaplanmaktadır:

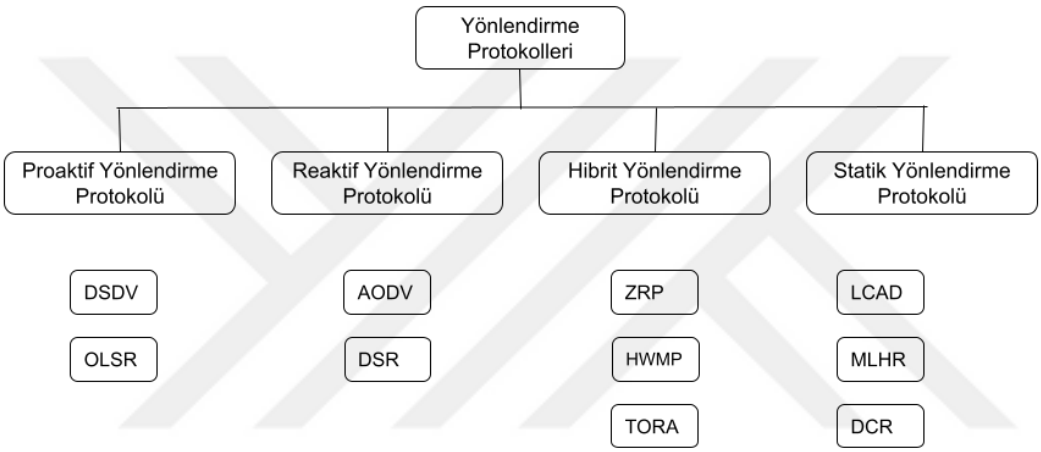
$$\begin{aligned} v_x &= s_n cos(d_n)\cos(p_n) \\ v_y &= s_n sin(d_n)\cos(p_n) \\ v_z &= s_n sin(p_n) \end{aligned} \quad (3)$$

3.4. Yönlendirme Protokolleri

Tasarsız ağlar, kablosuz erişim noktaları veya herhangi bir yönlendiriciye ihtiyaç duymadan cihazlar arasında geçici bir ağ bağlantısı kurulmasını sağlamaktadır. Sabit bir alt yapıya ihtiyaç duymadıkları için kısa sürede konfigürasyon yapılıp hızlı bir şekilde kullanıma hazır hale getirilebilirler. Herhangi bir alt yapı ihtiyaçlarının olmaması maliyetlerini de düşürmektedir. Buna ek olarak paket iletimlerinde ağ içerisinde bulunan bütün düğümler iş birliği yaptığı için iletimi gerçekleştirmesi için özel düğümlere ihtiyaç kalmamaktadır. Merkezi bir erişim noktası olmadan çoklu atlama (multi-hop) yöntemi kullanılarak düğümler doğrudan birbirleri üzerinden verileri göndermektedirler. Tasarsız ağlar sabit bir erişim noktası olmadığı için değişken bir topolojiye sahiptirler. Dinamik topolojiye uyum sağlanması için geleneksel yönlendirme protokollerinin yerini dinamik yapıya uyum sağlayabilecek uyarlanabilir yönlendirme protokolleri almaktadır.

FANET'lerin görevlerini gerçekleştirebilmeleri için düğümlerin hem kendi aralarında hem de yer baz istasyonu ile iletişim kurması gerekmektedir. Bu iletişim kurulurken gerçek

zamanlı olarak veri iletimini sağlayacak, işlemci ve enerji maliyetini azaltacak, kontrol mesajları ile ağ trafiğini etkilemeyecek ve sürekli olarak değişen topolojiye uyum sağlayacak [65] şekilde tasarlanan yönlendirme protokollerine ihtiyaç duyulmaktadır. Bütün FANET özellikleri göz önünde bulundurularak sıfırdan bir protokol tasarımı yapılmalı ya da MANET'ler için önerilen yönlendirme protokolleri FANET'lere uyarlanmalıdır. MANET'ler için önerilen yönlendirme protokolleri kopan bağlantının geri kazanımı [66], güvenlik [67] gibi konular için genişletilerek tekrar tasarlanmaktadır. FANET için yönlendirme protokolleri Şekil 3.8'de gösterildiği gibi 4 sınıfta incelenmiştir.



Şekil 3.8. FANET yönlendirme protokolleri sınıflandırması

3.4.1. Proaktif yönlendirme protokolleri

Proaktif yönlendirme protokolü tablo tabanlı bir protokoldür ve gönderilecek bir veri olup olmadığına bakılmadan her bir düğüm ağdaki diğer bütün düğümlerin son rota bilgilerini içerir [39]. Son rota bilgilerinin güncellenmesi için her bir düğüm belirli aralıklarla birbirlerine kontrol paketleri yollar. Proaktif yönlendirme protokolü ile kaynak ve hedef düğüm arasındaki en kısa yolun seçimi bütün düğümlerin son rota bilgisine sahip olması nedeniyle daha kolay gerçekleştirilir, bu nedenle paket teslim süresi azaltılabilir. Fakat FANET'ler gibi yüksek dinamik yapıya sahip ağlarda proaktif yönlendirme protokolleri kullanıldığında sürekli paket alışverişi gerçekleşir ve bant genişliği tüketilir. Bu durum ağda tıkanıklığa neden olduğu için bağlantı kesintileri oluşur. Ayrıca düğümler sürekli olarak ortamı dinleyeceği için enerji açısından da olumsuz bir durum oluşturur. Proaktif yönlendirme protokollerine, Dinamik sıralı uzaklık vektörü yönlendirme protokolü

(dynamic sequence distance vector- dsdv) ve İyileştirilmiş bağ durum (optimized link state) yönlendirme protokolü örnektir.

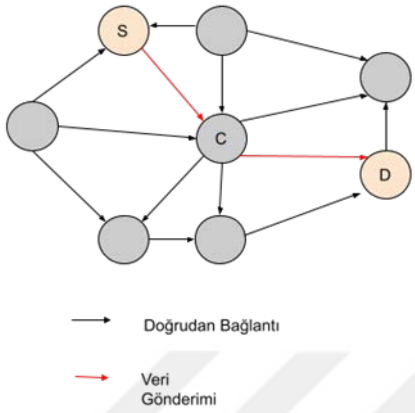
Dinamik Sıralı Uzaklık Vektörü Yönlendirme Protokolü (Dynamic Sequence Distance Vector-DSDV)

Tabloya dayalı bir yönlendirme protokolü olan DSDV [68]'nin temelleri, Bellman-Ford algoritmasına dayanmaktadır. Topoloji değişimleri sonrasında yönlendirme döngülerini ve ağda tıkanıklık oluşumunu engellemek için sıra numarası parametresi kullanılmaktadır. Yüksek sıra numarasına sahip olan rotalar güncel rotalar olarak belirlenmektedir. Buna ek olarak, kısa süreli topoloji değişimlerini bildirmeyi sağlayan bir sönüm parametresi de paketlere dahil edilmektedir. Bu parametre kısa süreli herhangi bir topoloji değişikliği için DSDV yönlendirme protokolü belirli zaman aralıklarında her düğümün, yönlendirme tablosunu komşu düğümlere iletmesi ve parametrelerin tekrar hesaplanması yöntemine dayanmaktadır [69].

İyileştirilmiş Bağ Durum Yönlendirme Protokolü (Optimized Link State Routing-OLSR)

OLSR, bağlantı durumu yönlendirme stratejisi yöntemi ile düğümler arasında var olan bütün bağlantıların küresel bir bilgisini oluşturur [39]. Bu protokol topoloji bilgisini güncellemek için ağda 2 mesaj yayınlamaktadır. İlki Hello mesajlarıdır ve komşu bağlantı durumlarını kontrol etmek için gönderilir. Diğeri ise topoloji kontrol (topology control) mesajıdır ve ağdaki değişim bilgilerini paylaşmak için yayınlanır [70]. Ağ üzerindeki ek yükü azaltmak için kaynak düğüm hedef düğümle iletişim kurmak istediğinde aracı olarak başka bir düğümü Çok Noktalı Röle (multipoint relays-ÇNR) olarak belirler. Her düğüm mesajları tekrar iletebilmek için 1 atlama uzağındaki komşuların listesini oluşturur. Bu liste topoloji kontrol ve hello mesajlarının periyodik değişimi aracılığı ile olmaktadır. Bir komşu listesi oluşturduktan sonra, her düğüm bir düğümü ÇNR olarak seçer. Yalnızca bu ÇNR düğümleri, bağlantı durumu bilgisi oluşturabilir ve veri paketlerini diğer ÇNR'lere iletebilir. Şekil 3.9'da gösterildiği gibi S kaynak ve D hedef düğümdür. C ise ÇNR olarak

belirlenen düğümdür. Veri paketi S düğümünden ÇNR düğümüne ve oradan da D düğümüne iletilmektedir. Bu mekanizma ek yükü azaltmak için geliştirilmiştir.



Şekil 3.9. ÇNR düğüm ile OLSR protokolü veri iletimi

3.4.2. Reaktif yönlendirme protokolleri

İsteğe bağlı yönlendirme protokolü olarak da adlandırılan reaktif yönlendirme protokolünde, hedef düğüme paket iletimi gerçekleştirilmek istenildiğinde rota oluşturulur. Ağ üzerinde yayınlanan rota istek paketleri ile rota arayışı başlatılır. Sonrasında ise hedef düğüm en kısa yolu kullanarak yol yanıt paketi gönderir. Bu durumda her düğüm bütün yolları kaydetmek yerine sadece kullanılan güncel yolu kaydeder ve ağdaki bütün tabloların yenilenmesine gerek kalmaz. Bu tekniği kullanmanın ana avantajı ise bant genişliği verimidir. Fakat rotalar periyodik olarak ağda bulunan bütün düğümlerle paylaşılmadığı için veri gönderimi yapılacağı zaman rota keşfi süreci vb. nedenlerle ağda gecikmeler olur. Bu nedenle reaktif yönlendirme protokolleri, proaktif yönlendirme protokollerine göre veri gönderimine daha geç başlamaktadır.

Dinamik kaynak yönlendirme protokolü (dynamic source routing protocol-DSR)

Reaktif bir yönlendirme protokolü olan DSR MANET'ler için tasarlanmıştır [71]. Ağın kendi kendini organize edebilmesine, bakım ve yapılandırmasına izin verir. Düğümler arasında iletişim kurulması için öncelikle rota keşif süreci başlar. Hedefe giden en kısa yol

belirlenir. Hedef düğümden kaynak düğüme yol yanıt paketi gönderilir ve veri gönderim süreci başlatılır. Bu protokolde her paket aktarılan düğümlerin bütün adreslerini içerdiği için büyük ve sürekli değişen bir topolojiye sahip ağlar için yetersizdir [39].

Tasarsız İsteğe Bağlı Uzaklık Vektörü Protokolü (Ad Hoc On Demand Distance Vector - AODV)

AODV, literatürde en fazla çalışılan reaktif protokollerden biridir. Bu protokolde rotalar sadece veri gönderilmek istenildiğinde kurulur. AODV protokolü üç mesaj türü kullanır. Bunlar;

- RREQ, rota istek mesajıdır. Rota keşfinde yayınlanmaktadır.
- RREP, rota yanıt mesajıdır. Rota keşfinde yayınlanan RREQ mesajına cevap olarak tek noktaya yayın yapar.
- RERR, hata mesajıdır. Aktif bir rotada bağlantı kopukluğu olduğunda kullanılır.

Veri transfer işlemi yapılması istenildiğinde, kaynak düğüm rota keşfini başlatmadan önce hedef düğüm için bir rotanın var olup olmadığını yönlendirme tablosundan kontrol eder [70]. Yönlendirme tablosu genel olarak hedef adres, sonraki atlama adresi, hedef sıra numarası ve atlama sayısı kayıtlarını tutmaktadır. Bu bilgiler kontrol edilerek rota oluşumuna bakılır. Eğer daha önce bir rota oluşturulmuş ise kaynak düğüm bu rota üzerinden veri paketlerini gönderir. Daha önceden bir rota oluşturulmamış ise kaynak düğüm rota istek (RREQ) paketleri yayınlar. Bu süreç Şekil 3.10'da bir akış şeması ile gösterilmektedir.

Hedefe yönelik geçerli bir rotaya sahip herhangi bir düğüm ya da hedef düğüm RREQ paketi aldığında, kaynak düğüme rota yanıt (RREP) paketi gönderir (tek noktaya yayınlanan RREP paketi gönderilir). RREP paketleri içerisinde kaynak düğümler tarafından tutulan tek düze artan sıra numarası ve minimum atlama sayısını içeren bilgiler yer almaktadır. Kaynak düğüm, minimum atlama sayısı ve maksimum sıra numarasına sahip olan en yeni ve en kısa rotayı seçer. Rota oluşturulduktan sonra hedef düğüm ve kaynak düğüm arasında veri transferi başlatılır. Düğümler arasında oluşan bağlantı kopukluklarını diğer düğümlere bildirmek için rota hata (RERR) paketleri gönderilir ve yerel bakım etkinleşmemiş ise veri paketleri düşürülür. Yerel bakım etkinleştiğinde ise

bağlantı hatasının gerçekleştiği düğüm hedef düğüme yeniden bir RREQ paketi göndererek yeni rota oluşturmaya çalışır.

Şekil 3.10. AODV akış şeması

AODV yönlendirme protokolü için rota keşfi ve veri gönderimi:

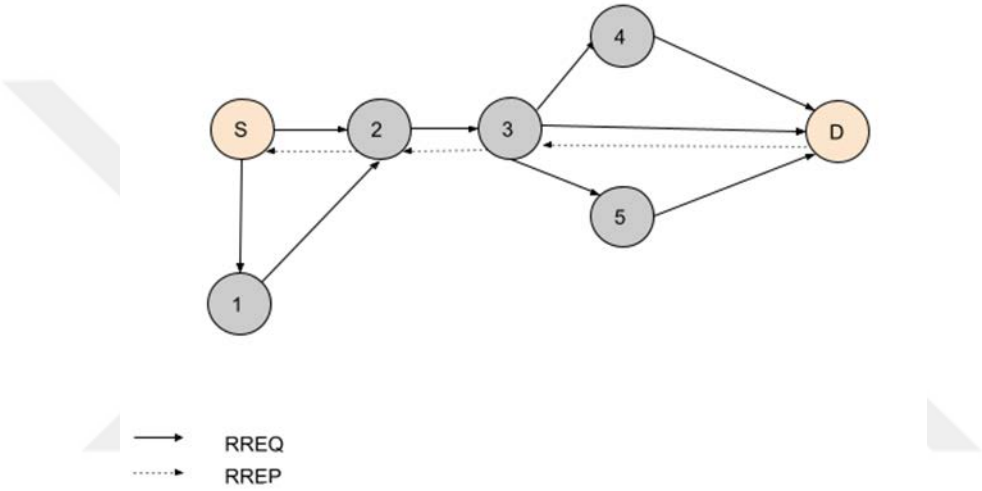
AODV protokolünde rota keşfi için RREQ mesajı yayınlandığında veya komşulara iletildiğinde, bir düğümün aynı mesajı birden fazla kez alma ihtimali yüksektir. Düğümlerin birbirlerine sürekli olarak ayı mesajları iletmesinin ve sonsuz döngü oluşumunun engellenmesi gerekmektedir. Bu nedenle düğüm bir RREQ aldığında yol keşif parametre süresi boyunca aynı kaynak IP adresi ve RREQ kimliği (RREQ ID) içeren herhangi bir RREQ alıp almadığına bakar. Daha önce böyle bir RREQ mesajı alınmış ise paket atılır, alınmamış ise başka bir düğüme transfer yapılır.

Gönderilen RREQ mesajlarına yanıt olarak RREP mesajı alınmaz ise belirlenen maksimum RREQ limitine kadar tekrar tekrar RREQ mesajı gönderilir. RREQ paketlerinin sonsuz döngüye girmesini engellemek için paket içerisinde yer alan maksimum atlama miktarı ya da yaşama süresi değerleri kontrol edilir. Belirtilen sınır değerlerden daha yüksek bir değere sahip paket, düğüm tarafından dikkate alınmaz.

Kaynak düğümden hedefe gönderilen RREQ mesajlarına tek noktaya yayın ile RREP mesaj yanıtları gönderilmektedir. Burada iki seçenek vardır. RREP hedef düğüm tarafından gönderilebilir ya da hedef düğüme giden aktif rotaya sahip olduğunu belirten ara düğüm tarafından gönderilir. Bir düğüm RREP ile yanıt verdikten sonra aldığı RREQ mesajını atar.

Hedef düğüm ya da hedefe giden aktif rotayı bildiren düğüm tarafından gönderilen RREP mesajı kaynak düğüme ulaştığında, pakette yer alan minimum atlama sayısı ve maksimum sıra numarasına sahip olan en yeni ve en kısa rota seçilerek veri gönderimi başlatılır.

Şekil 3.11'de gösterildiği gibi S kaynak düğüm, hedefe giden aktif rotaların bulunması için RREQ mesajı yayınlamaktadır. RREQ mesajı hedef düğüm D'ye ulaştığı zaman D tek noktaya yayın yaparak hedefin kendisi olduğunu belirten RREP mesajı göndermektedir. RREP mesajı alındıktan sonra veri transfer işlemi gerçekleştirilebilir.



Şekil 3.11. AODV yönlendirme protokolü rota bulma süreci

Tasarsız ağlarda düğümlerin hareketliliği ve kablosuz bağlantıların doğası gereği sıklıkla iletişim kesintileri olmaktadır. Bu kopuklukların önlenmesi için rotaların tekrar onarılmasını sağlayacak bir mekanizmaya ihtiyaç duyulmaktadır.

AODV yönlendirme protokolü için onarım süreci:

AODV'de yerel bağlantı, hello mesajları, geri bildirim mesajları, bağlantı katmanı seviyesinde kontroller, vb. gibi değişik yöntemler ile kontrol edilebilir. Bu tez çalışmasında, yerel bağlantı kontrolü için periyodik hello mesajları kullanılmaktadır. Ağda bulunan her düğüm aktif bir sonraki atlama noktasını ve hello mesajlarını ileten komşularına olan bağlantılarını sürekli olarak kontrol etmektedir. Bir düğüm, daha önce komşusu olan bir düğümden periyodik hello mesajları almıyorsa, bu komşuya olan bağlantının kesildiği varsayılmaktadır. Bağlantı kopukluğunun olduğu düğüm kaynak düğüme bir RERR mesajı göndererek kopukluğu bildirir. Bağlantıyı kullanan çok sayıda

düğüm varsa RERR mesajı yayınlanırken aksi bir durumda tek noktaya yayın yapılır. Herhangi bir düğüm RERR mesajı aldığında bu mesajı gönderen düğümün hedefe giden aktif rotada olup olmadığını kontrol eder. Eğer aktif rotada ise kendi rota tablosundan bu rotaları geçersiz olarak işaretler ve RERR mesajını kaynağa doğru gönderir. Bu süreç RERR kaynak tarafından alınana kadar devam etmektedir. Kaynak düğüm mesajı aldığında hala bu rotaya ihtiyaç duyuluyor ise rota keşfinin tekrar başlaması sağlanır.

AODV, düğümlerin yeni hedefler için hızlı bir şekilde rota oluşturmasını sağlar. Ağ topolojisindeki değişimlere ve bağlantı hatalarına gecikme olmadan cevap verebilir. Bu nedenle AODV diğer yönlendirme protokolleri ile karşılaştırıldığında FANET'lerde kullanıma daha uygundur. AODV'nin FANET'lere uyarlanması için [72-73] gibi çalışmalar yapılmıştır.

3.4.3. Hibrit yönlendirme protokolleri

Hibrit yönlendirme protokolleri, reaktif ve proaktif yönlendirme protokollerinin sınırlamalarını ortadan kaldırmak ve üstün özelliklerini birleştirmek için oluşturulmuştur. Reaktif yönlendirme protokolünün düşük ek yük özelliği ve proaktif yönlendirme protokolünün düşük gecikme özelliğinden yararlanmaktadır [74]. Bölge Yönlendirme Protokolü (Zone Routing Protocol), Grup Hareketliliği ile Sınır İşaret Yönlendirme Protokolü (Landmark Routing with Group Mobility) ve Keskin Hibrit Uyarlanabilir Yönlendirme Protokolü (Sharp Hybrid Adaptive Routing Protocol) hibrit protokol örneklerindendir.

Bölge Yönlendirme Protokolü'nde ağ bölge içi ve bölge dışı olmak üzere ikiye ayrılır. Bu bölgeler daha önceden belirlenmiş olan bir R yarı çapı kullanılarak düğümleri ayıran mesafeye göre ayrılmaktadır. Hedef ve kaynak düğüm aynı bölgede ise bölge içi kavramına dayalı proaktif yönlendirme protokolü özellikleri kullanılarak rota bulma işlemi ve veri gönderimi gerçekleştirilir. Hedef ve kaynak düğüm farklı bölgelerde ise bölge dışı kavramı devreye girmektedir. Bölge dışına veri iletimi yapılmak istenildiğinde optimum yolların bulunması ve ek yükün azaltılması için reaktif yönlendirme protokolü özellikleri kullanılır.

3.4.4. Statik yönlendirme protokolleri

Bağlantı kurmak için gerekli olan yönlendirme tabloları önceden hesaplanır ve düğümlerin içerisinde saklanır. Yönlendirme tabloları güncellenmediği için sabit topolojiye sahip ağlar için uygun bir yöntemdir [75]. Bağlantı hataları oluştuğunda hata toleransı yoktur. Sabit görevlerde kullanılan ve sadece belirli bir güzergahta hareket edecek olan İHA'larda kullanılabilir. Fakat genel olarak FANET'ler dinamik topoloji gerektiren görevlerde kullanıldığı için yetersiz bir protokol türüdür.

3.5. Fanet'te Güvenlik

FANET'lerde güvenliği sağlamak, bu ağlara özgü bazı özelliklerden dolayı zordur. Bu özellikleri şöyle listeleyebiliriz: kablosuz ağların kullanılması, düğümlerin iş birliği yapması, kontrolsüz ortam, FANET'lerin yüksek hız ve dinamik topolojiye sahip olmaları, tasarsız ağların sabit bir alt yapıya sahip olmamaları [76]. Bu bölümde FANET'leri saldırılara açık hale getiren bu özellikler ayrıntılı tartışılacaktır.

Kablosuz bağlantılar

FANET'ler kablosuz ağlar aracılığıyla radyo sinyallerini gönderir ve alır. Kablosuz bağlantıların kullanılması FANET'leri saldırıya açık bir hale getirir. Bu saldırılar genellikle, pasif dinlemeler, aktif saldırılar, bilgilerin gizli bir şekilde sızdırılması verilerin değiştirilmesi ya da düşürülmesi ve hizmet reddi saldırıları olarak çeşitlendirilebilir. Bu tip saldırılar ağ bütünlüğü ve kullanılabilirliğini engellemekle birlikte veri gizliliğinin de ihlal edilmesine yol açar.

Kontrolsüz ortam

FANET'lerde, kablolu ağlarda bulunan gelen ve giden paketleri işlemek için var olan merkezi bir yetki bulunmamaktadır. Anahtar yönetim sistemi bulunmadığı için saldırılar

ağın içerisinden olabildiği gibi ağın dışında da gerçekleşebilir. Yani saldırgan bir düğüm İHA'ların veri iletim menzili içerisinde yer aldığı süre boyunca, trafiğe müdahale edebilir.

Dinamik topoloji

FANET'ler yüksek hareketliliği nedeniyle dinamik bir topolojiye sahiptir. Ağın saldırı altında olmadığı durumlarda da bağlantı kopmaları oluşmaktadır. Bu nedenle ağdaki hatalı durumların saldırgan düğümden kaynaklı olup olmadığını tespit etmek önemli bir konudur. Düşen veri paketlerinin dinamik topolojinin neden olduğu bağlantı kopmasından mı yoksa ağ içerisinde yer alan saldırgan bir düğüm tarafından mı düşürüldüğü doğru bir şekilde tespit edilmelidir. Buna ek olarak, saldırgan bir düğüm de belirli zaman aralıklarında güven kazanmak için doğru çalışarak saldırının anlaşılmasını zorlaştırabilir.

İş Birliği

Yönlendirme algoritmaları bütün düğümlerin yönlendirme süreçlerinde bulunmasını gerektirmektedir [76]. Yani kaynak düğüm hedef düğüme giden güncel bir rota aramaya başladığında, ağdaki tüm düğümler bu rota keşif sürecinde yer alır. Daha önceden düğümler arasında güvenlik önlemi alınmadığı için bu durum ağı saldırıya açık hale getirir. Sonuç olarak, bir saldırgan düğüm, kolaylıkla yönlendirme sürecine katılabilir ve ağ trafiğini bozabilir.

Sınırlı kaynaklar

İHA'lar boyutları nedeniyle sınırlı yük kapasitesine sahiplerdir. Bu nedenle önerilen güvenlik çözümleri de genellikle İHA'ların gücüne ve depolama kapasitesine göre değişmektedir. Mesela İHA'lar için enerji tüketimi önemli bir konudur ve pil gücünü tüketmeye yönelik yapılan saldırıların [77] engellenmesi önemlidir. Buna ek olarak, ağ performansı ve güvenlik arasında bir denge olmalıdır. Veri trafiğinde oluşan gecikmeler ve güvenlik gereksinimleri birlikte tartışılmalıdır.

Saldırı Tespit Sistemlerinin Yetersizliği

FANET'lerde kablosuz ağların kullanılıyor oluşu, yönlendirme protokollerindeki açıklar ve net bir savunma hattının olmaması (saldırıların her yönden gelebilmesi) [78] güvenlik ihtiyaçlarını gündeme getirmektedir. FANET'lerde detaylı saldırı analizleri yapılmadığı için belirlenen ve doğruluğu kanıtlanmış STS'ler bulunmamaktadır. Kritik görevlerde yer alan ve neredeyse bütün alanlarda kullanılmaya başlanan İHA'lara yapılan saldırıların tespit edilmesi ve önlem alınması önemli bir konudur.

Yukarıdaki özellikler değerlendirildiğinde, FANET'ler diğer geleneksel tasarsız ağlardan daha zorlayıcı özelliklere sahiptir ve doğası gereği güvenlik tehditlerin açıktır. Bu nedenle, bu ağlar için önerilecek güvenlik çözümleri, bu özellikleri göz önünde bulundurmalıdır. Literatürde yapılan çalışmaların çoğu iletişim performansını geliştirmeye yöneliktir. Dolayısıyla, hala güvenlik konusunda yapılan çalışmalar Yetersizdir.

4. MATERYAL ve YÖNTEM

4.1. FANET Saldırı Analizi

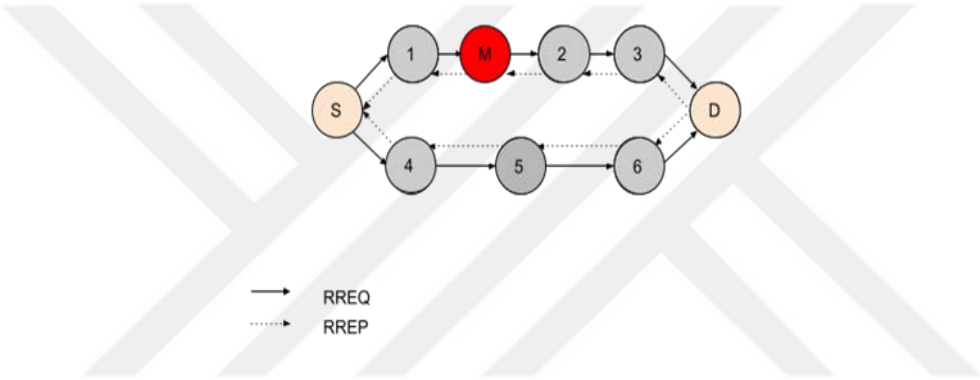
Bu çalışmada FANET'ler için ayrıntılı bir saldırı analizi yapılmıştır. Çalışmada 25 düğüm ve 50 düğüm içeren 13 farklı topolojiye sahip ağlarda %5- %25 aralığında saldırgan oranı kullanılarak simülasyonlar çalıştırılmaktadır. Simülasyonların gerçek hayata uygun senaryolarda olması için üç boyutlu uçuşu simüle etmeye yardımcı olan 3B GM hareketlilik modeli kullanılmıştır. Ağ katmanını etkileyen popüler saldırılar paket teslim oranı, uçtan uca gecikme ve ek yük karşılaştırmaları yapılarak tartışılmaktadır.

4.1.1. Ağ Katmanını Hedefleyen Saldırılar

FANET'ler farklı türde saldırılara maruz kalmaktadır. Ağ katmanını hedef alan saldırılar genellikle ağ trafiğini kontrol etmek, işlevini bozmak ve saldırgan düğümlerin ağa dahil olmasını sağlamaya yöneliktir. Ağa dahil olan saldırganlar paketlere erişebilir, onları istediği gibi yönlendirebilir ve hatta yönlendirme protokollerinin çalışmalarını bozabilir. Bu tip saldırılar pasif ve aktif saldırılar olmak üzere ikiye ayrılmaktadır. Pasif saldırılar sadece ağdaki trafiği dinlemeye yöneliktir. Aktif saldırılar ise düğümler arasında gönderilen veri paketlerinin çoğaltılması, değiştirilmesi ya da düşürülmesine yöneliktir. Bu çalışmada AODV yönlendirme protokolü kullanılarak çeşitli saldırıların analizi gerçekleştirilmiştir. AODV protokolü literatürde FANET'ler için önerilen bir protokoldür. Bunun en önemli sebebi AODV protokolünün yüksek hız nedeniyle sürekli olarak değişen topolojiye uyum sağlamasıdır. Aynı zamanda, reaktif bir protokol olduğu için yalnızca veri transferi yapılmak istenildiğinde rotalar oluşturmaktadır ve bu durum da ek yükü azaltmaktadır. FANET'ler yüksek hareketli bir yapıya sahip olduğu için bağlantı kopmaları da sıklıkla yaşanmaktadır. AODV protokolü bağlantı hatalarına hızlı bir şekilde cevap verebilir. Bu nedenle FANET'lerde kullanıma uygundur. Aşağıda her bir saldırı ayrıntılı bir şekilde tanıtılmıştır.

Obruk (sinkhole) Saldırısı

Bu saldırı senaryosunda Şekil 4.1'de gösterildiği gibi saldırgan düğüm, kaynak düğüme, hedefe giden daha iyi bir rotaya sahip olduğu tanıtımını (advertising) yaparak ağ trafiğini kendi üzerine çekmeyi amaçlar [79]. Uygulanacak yönteme göre saldırgan düğüm üzerine çektiği veri paketlerini değiştirebilir ya da sadece üzerine çekmekle sınırlı bir saldırı gerçekleştirir. Obruk saldırısı ağın ek yükünü artırdığı için bağlantı kopmalarına neden olabilir. Ayrıca enerji tüketimini arttırır ve ağın yaşam süresini kısaltır.



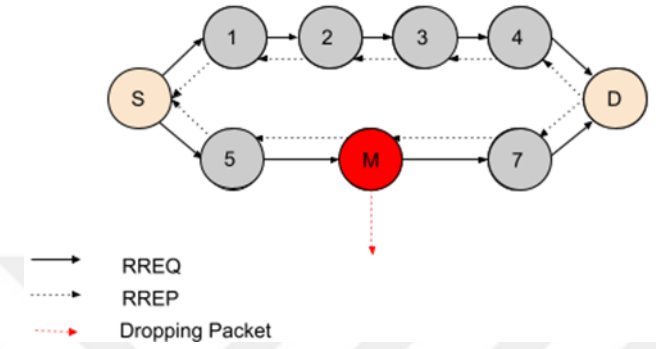
Şekil 4.1. AODV protokolünde obruk (sinkhole) saldırısı

Bu çalışmada uygulanan saldırı senaryosunda, saldırgan düğüm bir RREQ paketi aldığında, hedef düğümden bir atlama uzakta olduğunu bildiren sahte bir RREP paketi ile yanıt verir. Saldırgan düğüm bu davranışı ile hedef düğüme giden en kısa rotaya sahip olduğunu bildirir ve seçilme ihtimalini arttırır. Bunun yanı sıra, saldırgan düğüm hedef sıra numarasını artırarak hedefe giden en güncel rota olarak kendini tanıtır ve böylelikle hedefe giden rota olarak seçilmesini garanti eder. Bu rota seçildiğinde, saldırgan kaynak ve hedef düğümler arasındaki tüm iletişimi dinler, bu nedenle buna obruk saldırısı denir.

Paket Düşürme Saldırısı (Dropping Attack)

Genel olarak paket düşürme saldırısını başlatmak için saldırgan düğümün rota oluşumu sırasında devreye girmesi gerekir [80]. Bu basit saldırı senaryosunda, saldırgan aldığı paketleri düşürmeyi amaçlar. Belirli bir hedefe gönderilen paketleri seçerek düşürebilir.

Veya saldırının fark edilebilirliğini azaltmak için rastgele bazı paketleri düşürebilir, ancak bu durumda saldırının etkisinin daha sınırlı olması beklenir. Saldırgan veri paketlerinin yanı sıra yönlendirme kontrol paketlerini de bırakabilir. Bu durumda aktif rotalar oluşturulamayabilir veya aktif olmayan rotaların bildirilmesi zamanında gerçekleşmeyebilir.

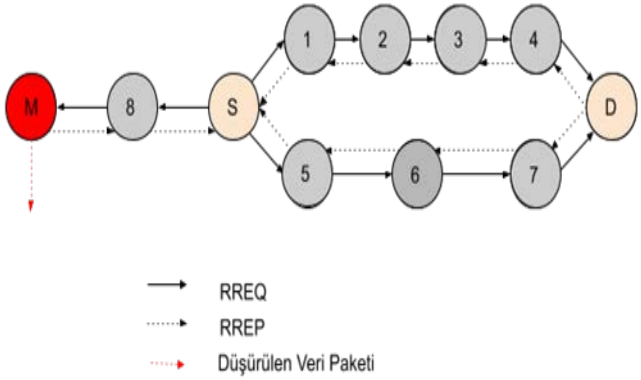


Şekil 4.2. AODV protokolünde düşürme saldırısı

Bu tür durumlarda, rota bulma mekanizması yeniden başlatılacağı için ağ kaynakları tüketilir, ağda tıkanıklığa ve gecikmelere neden olabilecek durumlar ortaya çıkabilir. Bu çalışmada saldırgan düğüm, kaynak düğüm ve hedef düğüm arasındaki rotada yer alıyor ise aldığı bütün veri paketlerini düşürür ve kaynak düğüm ile hedef düğüm arasındaki iletişimin kesintiye uğramasına neden olur. Şekil 4.2'de gösterildiği gibi kaynak düğüm ile hedef düğüm arasında oluşan rotada yer alan saldırgan düğüm üzerine gelen veri paketlerini düşürmektedir.

Kara Delik Saldırısı (Blackhole)

Kara delik saldırısı, ardışık olarak obruk ve paket düşürme saldırılarını gerçekleştiren birleşik bir saldırıdır. Hedefe giden en iyi rotaya sahip olduğu tanıtımını yaparak önce ağ trafiğini kendisine yönlendirir, ardından aldığı ağ trafiğine modifikasyon, paket düşürme saldırıları gibi diğer saldırıları gerçekleştirir. Buradaki simülasyonlarda, saldırının ilk aşamasında yukarıda anlatıldığı gibi obruk saldırısı gerçekleştirilir, daha sonra bu saldırının ikinci aşamasında sadece paket düşürme saldırısı yapılır. Yani saldırgan düğüm önce veri paketlerini üzerine çeker sonrasında ise bu paketleri düşürür.



Şekil 4.3. AODV protokolüne yapılan kara delik saldırısı

Şekil 4.3'te bir karadelik saldırısı gösterilmektedir. Kaynak düğüm (S), bir RREQ mesajı yayınlayarak hedef düğüme (D) giden bir rota keşfetmek ister. Kötü niyetli düğüm (M) bu RREQ mesajlarından birini aldığında, sahte bir RREP ile yanıt verir. Şekilde görüldüğü gibi M, hedefe giden yolda olmasa bile, hedefe giden en kısa yolda olduğunu iddia ettiği için S'den D'ye gönderilen veri paketlerini alır ve paketleri düşürür.

Tasarsız Ağ Sel Saldırısı

Bu saldırı senaryosunda, saldırgan düğüm rota bulma işlemi sırasında gönderilen kontrol paketlerinden yararlanır. Bu saldırının uygulama alanına göre birçok çeşidi bulunmaktadır. Çok sayıda RREP veya RREQ paketleri saldırı esnasında seçime göre gönderilebilir. Bu paketler ağda bulunan düğümlere gönderilebileceği gibi, ağda hiç bulunmayan düğüm adreslerine de gönderilebilir. Bu çalışmada, RREQ Sel Saldırısı senaryosu uygulanmıştır. Saldırgan düğümler seçilen düğümlere çok sayıda RREQ paketi gönderir. Bu saldırı, ağ trafiğinin artmasına, ağ ve düğüm kaynaklarının tüketilmesine, düğümler arasındaki bağlantının kesilmesine ve veri iletiminin kesilmesine neden olur. Simülasyonlarda rastgele bir hedef düğüm seçilir ve bu hedef düğüme giden yolları keşfetmek için 10 yeni RREQ mesajı gönderilir. Saldırı, rastgele seçilen başka bir hedef düğüm için her 12 saniyede bir simülasyon süresi boyunca tekrarlanır.

4.1.2. Saldırı Analizi

Bu çalışmanın temel amacı, FANET'lere yönelik yönlendirme saldırılarını analiz etmektir. 13 farklı topolojiye sahip olan ağ üzerinde önce saldırı olmadan, daha sonra ise yukarıda saldırılar bölümünde açıklanan saldırılarla simülasyon sonuçları elde edilir. Simüle edilen tüm ağların performansı analiz edilir. İlk olarak simülasyon ortamı tanıtılmakta, daha sonra saldırıların bu simüle edilmiş ağlar üzerindeki etkisi tartışılmaktadır.

Simülasyon Ayarları

Bu çalışmada, ağları ve FANET'lere yönelik saldırıları simüle etmek için Ns-3 simülasyon aracı kullanılmıştır. Ns-3.31 versiyonu TUBİTAK ULAKBİM tarafından sunulan Truba servisinde çalıştırılarak sonuçlar elde edilmiştir. AODV'nin çoklu atlama özelliklerini görmek için her ağda 50 düğüm oluşturulmuştur ve bir tanesi sunucu düğüm diğerleri istemci düğüm olarak belirlenmiştir. Her ağ saldırı olmadan çalıştırılır, ardından karadelik, obruk, paket düşürme ve tasarsız ağ sel saldırıları ile ayrı ayrı çalıştırılır. Bütün ağ topolojileri için ağdaki saldırgan sayısı %5 ile %25 arasında farklı oranlarda uygulanır. Bu nedenle her saldırı türü ve oranı için 13 farklı ağ topolojisi uygulanır ve sonuçlarda bu 13 ağdaki performans metriklerinin ortalaması verilmiştir. Toplamda saldırısız 13, saldırı altınsa ise 5x13 kez simülasyon çalıştırılmıştır (her bir saldırı türü için toplam 78 kez çalıştırılmıştır). Yukarıda belirtildiği gibi, düğümlerin hareketliliğini üç boyutlu olarak göstermek için 3B GM Hareketlilik Modeli kullanılmıştır. Rastgele hareketlilik ve öngörülebilir hareketlilik arasındaki dengeyi sağlamak için α değeri 0,495'ten başlatılır ve her seferinde farklı bir ağ topolojisi simüle etmek için 0,001 artırılır. Düğümlerin hızları gerçek hayatta olduğu gibi 720 km/s olarak ayarlanmıştır. 802.11b AC protokolü ve 11 Mbps bant genişliği kullanılmıştır. İHA'ların uçuş alanı için kapsama alanı 1700 m x 1700 m x 1500m olan dış sınır simülasyon alanıdır ve 220m x 220m x 220m olarak belirlenen bir iç sınırda İHA'lar uçmaktadır. İHA'lar yeni konumlarını belirlediğinde bir sonraki konum dış sınır ise İHA'ların merkezde tutulması için belirlenen iç sınıra itilmektedir. Bu şekilde İHA'lar kenar bölgelerden uzaklaştırılmaktadır. Ayrıca İHA'lar iç sınırda uçmakla birlikte dış sınırdan gelen herhangi bir durumdan etkilenmektedir. Gerçek dünyaya uygun olması için böyle bir senaryo belirlenmiştir. Çünkü gerçek hayatta yer alan İHA'larda

belirli bir bölgede uçuş sağlarken dış bölgedeki saldırılardan da etkilenebilmektedir. Verilen ağ alanı için düğümlerin iletim menzili (kapsama alanı) 250m olarak ayarlanmıştır. Her düğüm 1800 saniye simülasyon süresi boyunca, her 1 saniyede sunucu düğümüne 1024 baytlık 1 UDP paketi göndermektedir. Bütün simülasyon parametreleri Çizelge 4.1'de özetlenmiştir.

Çizelge 4.1. Ns-3'te kullanılan simülasyon parametreleri

Parametreler	Değerler
Yönlendirme Protokolü	AODV
MAC Protokolü	IEEE 802.11b
Simülasyon Süresi	1800 saniye
Alan	1700 m x 1700 m x1500 m
Düğüm Sayısı	25,50
Düğüm Hızı	720 km/h
İletim menzili	250 m
Trafik Türü	UDP
Paket Boyutu	1024 bayt
Paket oranı	1/saniye
Bant Genişliği	11 Mbps
Saldırgan düğüm oranı	0, %5, %10, %15, %20, %25
Hareketlilik Modeli	3B Gauss Markov Modeli
GM için sınırlar	X: [-110,110], Y: [-110,110], Z: [0,110]
GM α parametresi için değerler	[0.495, 0.507]

Saldırıların ağlar üzerindeki etkilerini görmek için aşağıdaki performans ölçütleri kullanılır:

Paket teslim oranı (PDR), ağdaki tüm düğümler tarafından alınan toplam paket sayısının, aynı düğümlere gönderilen toplam paket sayısına oranının ortalamasıdır.

Uçtan uca (E2E) gecikme, uç iletişim noktaları arasında veri iletimi sırasında ağda meydana gelen tüm gecikmelerin ortalamasının saniye cinsinden ölçümüdür.

Ek Yük (Overhead), yönlendirme protokolü tarafından üretilen ve düğümler tarafından alınan toplam kontrol paketlerinin, alınan veri paketlerine oranıdır.

4.2. FANET'ler İçin Yapay Sinir Ağları Temelli Bir Saldırı Tespit Sistemi

İHA'lar son on yılda yaygın kullanım ve uygulamaları ile son derece hızlı bir ilerleme kaydetmiştir. Elde ettikleri başarılar ve kullanım alanlarının yaygınlaşması ile birlikte güvenlik sorunları da ortaya çıkmaya başlamıştır. Gizli dinlemeler ve ağ üzerinden yapılan çeşitli saldırılar bu güvenlik sorunlarının temelini oluşturmaktadır. Bu nedenle, özellikle kritik görevlerde kullanılan İHA'lara yönelik saldırıların yüksek doğruluk ile tespit edilmesi büyük önem taşımaktadır.

Güvenlik sorunlarının üstesinden gelmek için iki temel yaklaşım vardır [81]. Bu yaklaşımlar saldırı önleme ve saldırı tespitidir. İlk yöntemde kimlik doğrulama işlemi ile ağda yer alan ve yönlendirme sürecine katılmak isteyen düğümlerin güvenilir olduğu kanıtlanır ve yetkisiz düğümlerin ağa katılması engellenir [78]. İkinci yöntem ise genellikle ağ içerisindeki izinsiz girişlerin tespit edilmesine yönelik çalışmalardır. STS, bir kaynağın gizliliğini, kullanılabilirliğini ve bütünlüğünü tehlikeye atacak [33] bütün izinsiz girişlerin tespit edilmesi için geliştirilen yöntemleri içermektedir.

Genellikle üç çeşit STS kullanılmaktadır [33]. İlk yöntem, imza tabanlı sistemlerdir ve saldırı altındaki sistemler ile mevcut sistemlerin karşılaştırılmasına dayalıdır. Genellikle doğruluk oranı yüksek ve yanlış tahmin oranı düşük [82] olduğu için tercih edilmektedir. Ancak, bu tür sistemler sadece veri tabanında bulunan saldırı imzaları ile karşılaştırmalar yapıldığı için yeni gelen saldırıları tespit etmek zordur. Sürekli olarak verilerin yeni saldırı imzalarına göre güncellenmesi gerekmektedir. İkinci yöntem de ise izinsiz girişler, genellikle gelenekselliğin dışına çıkılarak makine öğrenimi, derin öğrenme ve yapay zeka teknikleri ile tespit edilmektedir. Sistemler saldırı altındaki ağ davranışlarını öğrendikleri için farklı türdeki saldırıları ve yeni saldırıları fark etmeleri kolay olmaktadır. Ancak bu sistemde yanlış pozitiflerin oranını düşürmek önem taşımaktadır. Normal olarak belirlenen aktivitelerin, saldırı olarak anlaşılması sistemin güvenilirliğini düşürebilir. Son yöntem, literatürde spesifikasyona dayalı saldırı tespiti olarak geçmektedir. Bu yöntem de sistem üzerinde kısıtlamalar, eşik değerleri gibi özellikler belirlenir. Ve bu özelliklerin ihlalinde izinsiz giriş tespit edilir. Sistem hem anomaliye dayalı hem de imza tabanlı sistemleri birlikte kullandığı için yanlış pozitif oranlarının düşmesine ve yeni saldırıların da tespit edilmesine olanak tanımaktadır. Fakat sisteme, protokole ait bütün özelliklerin

tanımlanması iş gücü gerektirmekle birlikte çok uzun [82] sürmektedir. Aynı zamanda özelliklerin sürekli güncellenmesi ve yeni gelen özelliklerin de eklenmesi gerekmektedir.

Son yıllarda yapay zeka tabanlı sistemler, yüksek doğruluğa sahip olması ve insan müdahalesi gerektirmemesi nedeniyle daha fazla tercih edilmektedir. Diğer yöntemlerde belirli kısıtlamalara dayanan sistem karşılaştırmaları verilerin sürekli güncellenmesine ya da sürekli olarak öznitelik ekleme ihtiyacına neden olmaktadır. Farklı saldırı türlerinin ortaya çıkması veya protokollerin değişimi bu tür sistemleri etkilemektedir. Yapay zeka sistemlerinde ise modeller normal davranışları öğrendiği için yeni gelen saldırıları da başarılı bir şekilde tespit edebilmektedir. Buna ek olarak ağ trafiğinin yoğun olduğu karmaşık sistemlerde de büyük veriyi yüksek hesaplama yeteneği ile işleyebilmektedirler.

Yukarıda bahsedilen avantajlar nedeniyle bu çalışmada saldırı tespiti için yapay zeka teknikleri kullanılmaktadır. Farklı saldırgan oranları ve farklı ağ topolojileri kullanılarak 4 farklı saldırı türüne ait veriler ile bir veri seti oluşturulmuş ve yapay sinir ağları kullanılarak saldırı tespiti yapılmıştır. Saldırı tespiti için saldırgan düğümler ve saldırıdan etkilenen düğümler kullanılmıştır. Saldırgan düğümlerle saldırı tespit sistemleri, ağ içerisinde yer alan düğümlerin faaliyetlerini izleyerek saldırı tespiti yapmaktadır. Bu yöntemde, ağ içerisinde anormal etkinlikler gösteren düğümler saldırgan olarak işaretlenerek uyarı sistemi çalıştırılır ve burada saldırı tespit sisteminin ele geçirilemeyeceği varsayılmaktadır. Saldırıdan etkilenen düğümlerle saldırı tespitinde ise saldırıdan etkilenen düğümler izlenerek ağ üzerindeki anormal etkinlikler belirlenir. Saldırgan düğümler, ağda bulunan diğer düğümler üzerinde de bir etki oluştururlar. Bu nedenle saldırgan düğümler kendilerini normal düğüm gibi gösterseler de saldırı tespit sistemini yanıltılma oranı daha düşük olmaktadır.

4.2.1. Yapay sinir ağları ile saldırı tespiti yapılması

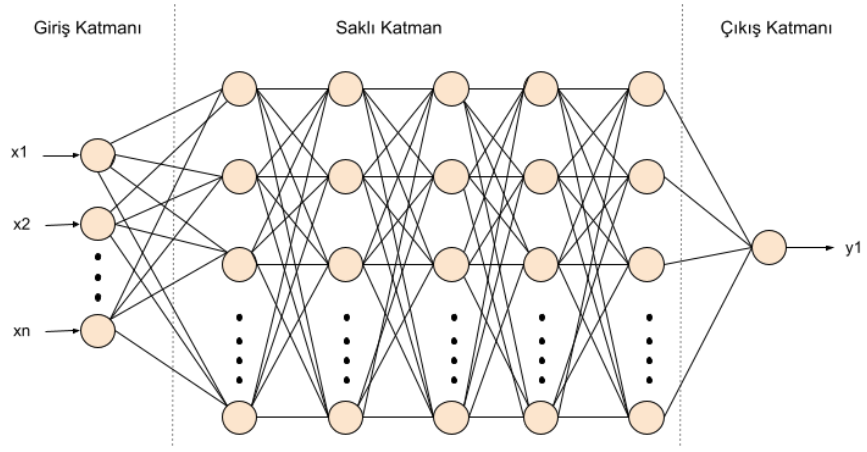
Biyolojik sinir sisteminden ilham alınarak sinir ağlarını yapı ve işlevsel yönlerden taklit etmek için yapay sinir ağı (YSA) kullanılmaktadır. YSA, tam olarak açıklanamayan karmaşık sinir sisteminin sadece bir soyutlamasıdır [83]. Doğrusal olmayan ve birbirine bağlı yapay nöron gruplarından oluşur. Yapay nöronların görevi bir aktivasyon fonksiyonu ile bazı girdi vektörlerini istenilen çıktı vektörlerine dönüştürmektir.

YSA'lar, dışarıdan veri girdileri almayı sağlayan giriş nöron katmanı ve sonuçları dışa aktarmayı sağlayan bir çıkış katmanına sahiptir. Buna ek olarak giriş ve çıkış katmanı arasında bulunan saklı katman olarak adlandırılan yapı da diğer nöronlardan ya da kendilerinden girdi verisi alırlar (geri bildirim).

YSA, ileri beslemeli ise yalnızca girdileri önceki katmandan alır ve çıktıları sonraki katmanda yer alan nöronlara iletir. Ancak, geri besleme var ise, ağ tekrarlayan bir yapıdadır. Yani çıktılar geçmişteki girdilere de bağlıdır ve statik değildir.

Tahmin, sınıflandırma veya kontrol ihtiyacı olan dinamik ortamlarda YSA kullanıma uygundur. Bunun nedeni ise bilgiyi paralel olarak işleyebiliyor olması (paralelizm), örnekle öğrenmeleri, doğrusal olmayan karmaşık işlemleri doğrusal olarak birleştirmeleri, çok yönlü ve esnek olmaları, gürültü ve eksik veriler ile de çalışabilmeleridir. YSA, mevcutta var olan öğrenilmiş bilgilerden genelleme yapabilir, bilinmeyen durumları işleyebilir. Bütün bunlara ek olarak, YSA biyolojik sinir hücrelerinin bir simülasyon şeklidir ve bu durum da onları sezgisel açıdan popüler hale getirir [83].

YSA'nın avantajları göz önünde bulundurulduğunda bu çalışmada da STS geliştirilirken YSA kullanılmıştır. Şekil 4.4'te bir giriş, 5 saklı katman ve 1 çıkış katmanından oluşan çalışmamızda kullandığımız YSA gösterilmektedir. Giriş katmanında Çizelge 5.2'de gösterin özniteliklerin tamamı alınmaktadır ve çıkış katmanında ikili sınıflandırma yapıldığı için saldırının var olması ya da saldırı olmaması durumlarına göre çıktı oluşturulmaktadır.



Şekil 4.4. Yapay sinir ağı blok diyagramı

Çalışmada kullanılan YSA'ya ait parametreler ise Çizelge 4.2'de ayrıntılı olarak gösterilmektedir. Çalışmada giriş verilerinin ölçeklendirilmesi için standardizasyon kullanılmıştır. Standardize edilirken değerler genel olarak standart sapması 1 olacak şekilde değiştirilmektedir. Verileri ölçeklendirmek, modelin daha hızlı bir yakınsama ve iyi bir performans göstermesini sağlamaktadır. Veriler %80 eğitim seti ve %20 test seti olarak ayrılmaktadır. Giriş katmanı özniteliklerin tamamını alacak şekilde oluşturulmuştur. Sonuçlar 5 saklı katmana sahip ve her katman 16 nörondan oluşan YSA ile elde edilmiştir.

Sinir ağlarında aktivasyon fonksiyonunun görevi düğümlerden alınan toplam ağırlıklı girdiyi çıktıya dönüştürmektir. Transfer fonksiyonu olarak da adlandırılmaktadır. Saklı katmanlarda relu aktivasyon fonksiyonu kullanılmaktadır. Saklı katmanlar da bu fonksiyonun kullanım nedeni ise hesaplama karmaşıklığının az olması ve hızlı çalışmasıdır.

$$f(x) = \max(0, x) \tag{4.1}$$

Çıkış katmanında ise sigmoid aktivasyon fonksiyonu kullanılmıştır.

$$S(x) = \frac{1}{1+e^{-x}} \tag{4.2}$$

Bu fonksiyon girdi olarak aldığı değerleri 0-1 aralığında çıktı olarak verdiği için seçilmiştir. Buna ek olarak model 100 iterasyon boyunca çalıştırılarak performans ölçümü yapılmaktadır. 100 iterasyon seçilme nedeni ise 25,50,75 değerlerinin arasında en iyi değere 100 ile ulaşılıyor olmasıdır.

Çizelge 4.2. YSA'ya ait detaylı parametre açıklamaları

Parametreler	Değerler
Ölçeklendirme	Standardizasyon
Eğitim ve test ayrım oranı	%80, %20
Çıkış ve giriş katman sayısı	1
Saklı katman sayısı	5
Saklı katman nöron sayısı	16
Saklı katman aktivasyon fonksiyonu	relu
Çıkış katmanı aktivasyon fonksiyonu	sigmoid
İterasyon sayısı	100

Veri Kümesi Oluşturulması

Veri kümesi, AODV yönlendirme protokolünü kullanan 49 istemci ve 1 sunucu düğümden Ns-3 aracı kullanılarak veri toplanması ile oluşturulmuştur. İstemci düğümler ve sunucu düğüm arasında UDP bağlantısı kullanılmıştır. Veriler saldırısız ve %5- %25 aralığında saldırgan oranına sahip 4 farklı saldırı altında 13 farklı ağ topolojisinden 1800 saniye boyunca toplanmıştır. Veri toplama işlemi 4. saniyede başlatılarak her düğümden 4 saniye de bir veri alınmıştır. Veri alım süreleri 1, 2 ve 3 saniye olarak denenmiş olup, deneylerin çalıştırıldığı sistemde veri yoğunluğundan dolayı sorunlara yol açmıştır. Bu nedenle, 4 saniyede bir ilgili öznitelikler çıkarılmıştır. Veri toplama sıklığı, sistemin başarımını pozitif etkilerken, kaynak harcamalarını da arttırmaktadır. İleriki çalışmalarımızda veri toplama sıklığının başarıma etkisinin araştırılması planlanmaktadır. Saldırgan düğümler ve saldırgan olmayan düğümlere etiketleme işlemi uygulanmıştır. Daha sonra ise saldırgan düğümler veri kümesinden çıkartılarak, sadece saldırılardan etkilenen düğümler işaretlenmiştir ve iki çeşit veri kümesi elde edilmiştir.

Düğümlerden toplanan öznitelikler Çizelge 4.3'te verilmiştir. Bu öznitelikler ve ilgili özniteliklerin çıkarımına ilişkin kodlar, [84] numaralı çalışmadan elde edilmiştir. Toplanan özniteliklerin bir kısmı hareketlilik, diğer kısmı ise ADOV kontrol mesajları ve veri paketleri ile ilgilidir [85]. Komşu sayısındaki değişimler gibi öznitelikler hareketlilik modeli hakkında bilgi vermektedir [84]. Rota sayısı ile ilgili bilgi veren öznitelikler ise yönlendirme tablosundaki değişiklikleri içermektedir. Bu durum da hareketliliğin bir sonucu olabilir [84]. RREQ, RREP ve RERR gibi yönlendirme protokolü kontrol paketleri ile ilgili öznitelikler ise bu paketlerin ne kadar sıklıkla iletildiği, gönderilip alındığı bilgisini vermektedir. Bu öznitelikler her düğümden belirli sıklıklarla toplanmaktadır. Bu tez çalışmasında, 4 saniyede bir toplanmaktadır.

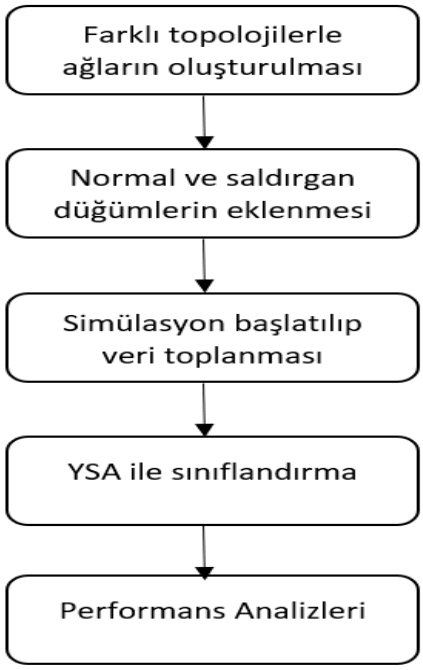
Çizelge 4.3. Öznitelik listesi

Özellikler	Açıklamalar
node_num	Düğüm numarası
num_of_totalneighs	Toplam komşu sayısı
num_of_addedneighs	Eklenen komşu sayısı
num_of_removedneighs	Silinen komşu sayısı
no_activeroutes	Aktif rota sayısı
no_invroutes	Geçersiz rota sayısı
no_addedroutes_discover	Keşifte eklenen rota sayısı
no_addedroutes_notice	Bildirimle eklenen rota sayısı
no_updatedroutes	Güncellenen rota sayısı
no_added_repairedroutes	Onarımla eklenen rota sayısı
no_invroutes_timeout	Süre nedeniyle geçersiz rota sayısı
no_invroutes_other	Diğer nedenlerle geçersiz rota sayısı
avg_hopcount	Aktif rotaların ortalama atlama sayısı
recv rreqPs	Düğüme yönlendirilen ve düğümün aldığı rota istek paket sayısı
recvF rreqPs	Düğüm tarafından iletilmek için alınan rota istek paketleri
send rreqPs	Düğümden yayınlanan rota istek paketlerinin sayısı
frw rreqPs	Düğümden iletilen yol istek paketlerinin sayısı
recv rrepPs	Düğüme yönlendirilen alınan rota yanıt paketlerinin sayısı
recvF rrepPs	Düğüm tarafından iletilmek için alınan yol yanıt paketlerinin sayısı
send rrepPs	Düğümden başlatılan rota yanıt paketlerinin sayısı
frw rrepPs	Düğümden iletilen yol yanıt paketlerinin sayısı
recvB rerrPs	Alınan yayın rotası hata paketlerinin sayısı (iletilecek veya iletilmeyecek)
send rerrPs	Düğümden yayınlanan rota hata paketlerinin sayısı
recv aodvPs	Alınan toplam yönlendirme protokolü paketlerinin sayısı
recvF aodvPs	İletilmek için alınan toplam yönlendirme protokolü paketlerinin sayısı
send aodvPs	Düğümden başlatılan toplam yönlendirme protokolü paketlerinin sayısı
frw aodvPs	Düğüm tarafından iletilen toplam yönlendirme protokolü paketlerinin sayısı
dropped dataPs	Düğüm tarafından iletilmeyen veri paketi sayısı

4.2.2. Önerilen saldırı tespit sistemi

Detaylı saldırı analizleri sonucunda, saldırgan düğümlerin ağa verdiği zararlar incelenmiştir. Bu gözlemler sonucunda saldırgan düğümlerin tespit edilmesi için bir sistem önerilmiştir. Şekil 4.5'te gösterildiği gibi uygulama adımları açıklanmaktadır. Öncelikle 13 farklı topolojiye sahip ağ ortamları oluşturulup parametreler ayarlanmaktadır. Daha sonra düğümler simüle edilir ve rastgele olarak seçilen saldırgan düğümler (%5 ile %25 arasında) ağa eklenir. Simülasyonların saldırısız ve saldırılı ortamlarda çalıştırılması ile

veriler her bir düğümden 4 saniye de bir olacak şekilde toplanmaktadır. Saldırı tespiti toplanan veri kümesinin YSA teknikleri ile işlenmesi sonucunda gerçekleştirilir. TÜBİTAK ULAKBİM tarafından sunulan Truba servisinde Python 3 kullanılarak model çalıştırılmıştır. Model 13 topoloji esas alınarak %5- %25 saldırgan oranı için 100 kez çalıştırıldıktan sonra 13 topolojinin ortalaması alınarak nihai değerler sunulmaktadır. Son olarak performans metrikleri ölçülerek sistemin performans analizi yapılmaktadır.



Şekil 4.5. Saldırı tespit sistemi uygulama adımları

Performans Metrikleri

Veri kümesindeki kayıtlar normal ve saldırı altında olarak sınıflandırılmaktadır. Bu nedenle önerilen saldırı tespit sisteminin performansını değerlendirmek için aşağıdaki parametreler kullanılarak formüller elde edilmiştir.

Doğru pozitif (True Positive-TP): Doğru sınıflandırılmış saldırı sayısı

Doğru Negatif (True Negative-TN): Doğru sınıflandırılmış saldırı olmayan kayıt sayısı

Yanlış Pozitif (False Positive-FP): Saldırı olarak tespit edilen fakat saldırı olmayan kayıt sayısı

Yanlış Negatif (False Negative-FN): Saldırı olmadığı tespit edilen fakat saldırı olan kayıt sayısı

Doğruluk (Accuracy): Doğru sınıflandırılan örnek sayısının toplam örnek sayısına oranıdır.

$$\mathrm{ACC} = \frac{\mathrm{TP+TN}}{\mathrm{TP+FP+FN+TN}} \tag{4.3}$$

Yanlış Pozitif Oranı (False Positive Rate-FPR): Saldırı olarak tespit edilen fakat saldırı olmayan kayıt sayısının oranıdır.

$$FPR = \frac{FP}{FP+TN} \tag{4.4}$$

Tespit Oranı (Sensitivity, Recall, DR): Saldırıları doğru olarak sınıflandırma başarısıdır. Tespit oranı olarak da adlandırılmaktadır (DetectionRate-DR).

$$DR = \frac{TP}{TP+FN} \tag{4.5}$$

Kesinlik (Precision): Saldırıolarak belirlenen kayıtların, gerçekten saldırı olup olmadığını göstermektedir.

$$P = \frac{TP}{TP+FP} \tag{4.6}$$

F1 Skor: Kesinlik ve duyarlılığın harmonik ortalaması olarak hesaplanır.

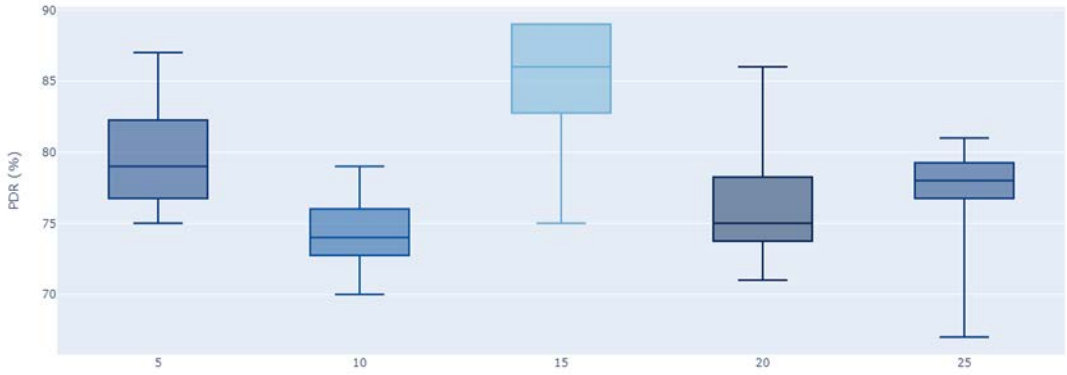
$$F1 = \frac{2TP}{2TP+FP+FN} \tag{4.7}$$

5. BULGULAR ve TARTIŞMA

5.1. FANET Saldırı Analiz Sonuçları

Deneylerde öncelikle farklı ağ topolojilerine sahip 13 ağ, saldırgan düğüm olmadan çalıştırılmıştır. Daha sonra aynı topolojilere farklı saldırgan düğüm oranları ile farklı saldırı türleri uygulanmıştır. Yani simülasyon 13 kez saldırı olmadan, 13 kez ise %5- %25 aralığındaki saldırgan oranları için (13x5) çalıştırılmıştır. Bu işlem hem 25 düğüm içeren ağlar hem de 50 düğüm içeren ağlar için tekrarlanmıştır. İlk olarak, 50 düğüm simülasyon sonuçları sonrasında ise 25 düğüm için sonuçlar gösterilmektedir.

50 düğümlü ağlar için, obruk (sinkhole) saldırısının etkileri Çizelge 5.1 ve Şekil 5.1'de verilmiştir. Çizelge 5.1, farklı saldırı oranlarına sahip ağlardaki performans ölçümlerinin ortalama değerlerini gösterir. Şekil 5.1, kutu grafiği gösterimini kullanarak 13 farklı ağ topolojisine ait PDR değerlerini vurgular. Yukarıda tanımlandığı gibi, saldırgan veri paketlerini üzerine çeker ve bu saldırı senaryosunda veri paketlerini kasıtlı olarak düşürmez. Ancak, saldırgan düğüm veri paketlerini üzerine çekerek onların aktif rotada yol alıp hedefe iletilmesini engeller ve bu nedenle veri paketleri düşürülmemesine rağmen hedefe ulaşamayabilir. Ayrıca saldırgan, kaynak ve hedef düğüm arasındaki bir rotada değil ise pasif rota oluşumuna sebep olduğu için paket teslim oranını düşürür. Ağdaki saldırgan oranı artmasına rağmen bazı ortalama PDR değerlerinin yükseldiği yapılan analizler sonucunda gözlemlenmiştir. Sonuçlara göre %5 oranında saldırgan düğüm, konumları nedeniyle daha yüksek bir saldırı başarısı sağlar. Buna göre %15 oranında saldırgan düğümün daha düşük paket teslim oranına sahip olması beklenirken, saldırının başarısının düşük olması nedeniyle ağda daha yüksek paket teslimi gerçekleşir. Bu durum ise FANET'lerin karakteristik özelliklerinin bir sonucu olarak açıklanmaktadır. Yani FANET'ler yüksek hareketlilik ve dinamik bir topolojiye sahip olduğu için seçilen saldırgan düğümlerin konumları saldırının başarısını etkilemektedir. Bunun dışında gecikme sürelerinin saldırı altında düştüğü gözlemlenmiştir. Saldırı altında hedefe ulaşan paket sayısında azalma olduğu için gecikme süresi de azalmaktadır. Bu durumlara ek olarak saldırı altında aktif rotaların geçersiz olması, paketlerin hedefe iletilmemesi gibi durumlar hata mesajları yayınlanmasına ya da tekrar rota keşfine neden olur. Bu nedenle ağdaki kontrol mesaj sayısı arttığı için ağdaki ek yük oranı artmaktadır.



Şekil 5.1. Obruk saldırısı altında ağın paket teslim oranları

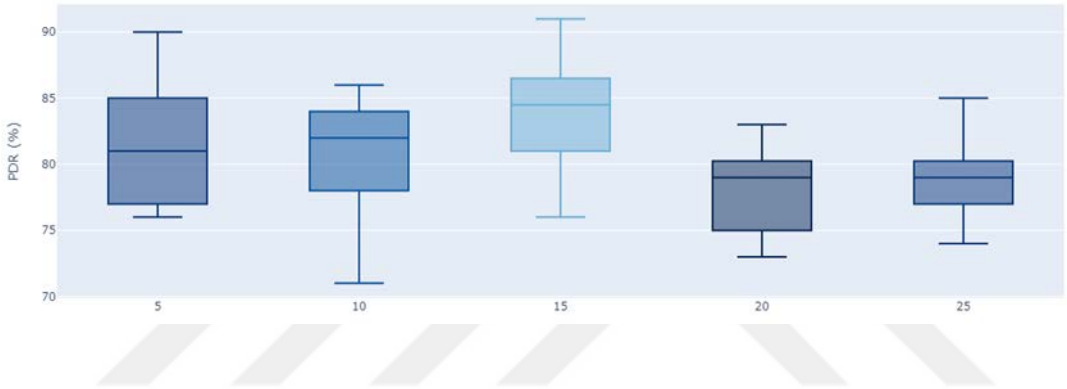
Çizelge 5.1. Obruk saldırısı altındaki ağların ortalama performans metrikleri

Saldırgan düğüm oranı (%)	PDR (%)	E2E (saniye)	Ek Yük
%0	87,77	0,077	0,853
%5	79,85	0,061	0,919
%10	74,15	0,051	0,989
%15	84,00	0,068	0,885
%20	76,54	0,059	0,975
%25	77,08	0,060	0,966

Paket düşürme saldırısının etkisi Çizelge 5.2 ve Şekil 5.2'de verilmiştir. Saldırgan pozisyonları rastgele seçilse de farklı saldırı senaryoları için her topolojide aynı saldırganlar kullanılır. Bu nedenle, her saldırı senaryosunda aynı veri paketleri saldırganlardan geçer. Paket düşürme saldırı senaryosunda veri paketinin saldırgan düğüm tarafından düşürülebilmesi için seçilen saldırgan düğümlerin aktif rota üzerinde bulunması gerekmektedir. Kaynak düğümden hedef düğüme doğru giden veri paketinin geçtiği rota üzerinde bir saldırgan düğüm var ise, saldırgan düğüm veri paketini aldıktan sonra hedefe doğru iletmek yerine paketi düşürmektedir. Saldırgan düğüm oranı artmasına rağmen düğümler aktif rotada yer almadığında, PDR değeri daha az saldırgan olan ağa göre daha yüksek çıkmaktadır. Bununla birlikte kaynak düğümden hedef düğüme paketlerin iletilmemesi önceki saldırıda olduğu gibi kontrol mesaj sayısını arttırarak ek yükü arttırmaktadır. Ağda bir saldırı varken, iletilen paketlerin daha az olması ise gecikme süresini azaltmaktadır.

Çizelge 5.2. Paket düşürme saldırısı altındaki ağların ortalama performans metrikleri

Saldırgan düğüm oranı (%)	PDR (%)	E2E (saniye)	Ek Yük
%0	87,77	0,077	0,853
%5	80,78	0,066	0,918
%10	81,00	0,069	0,914
%15	84,00	0,075	0,882
%20	78,08	0,069	0,942
%25	79,00	0,069	0,936

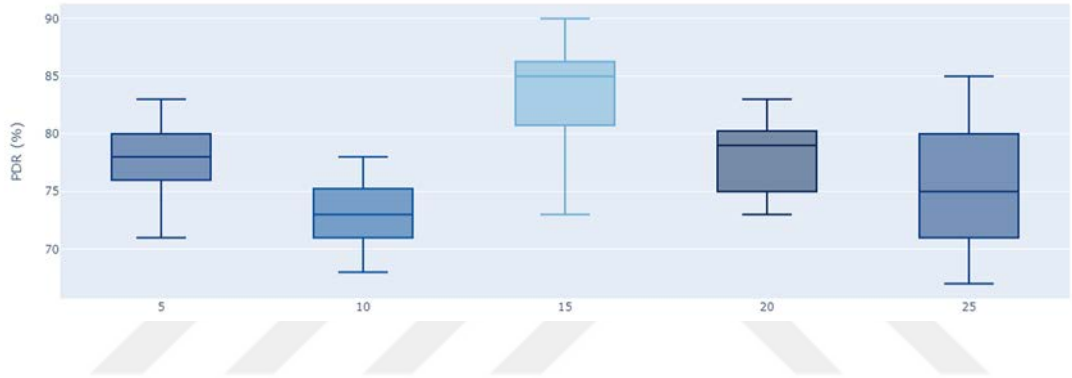


Şekil 5.2. Paket düşürme saldırısı altında ağın paket teslim oranları

Çizelge 5.3, karadelik saldırısı altında simüle edilmiş ağlardaki performans ölçümlerinin ortalamasını gösterir. PDR değerlerini daha yakından görmek için, Şekil 5.3 bu performans metriğinin kutu grafiğini göstermektedir. Sonuçlarda görüldüğü gibi saldırgan oranı %5'ten %10'a yükseltilerek saldırı simüle edildiğinde PDR yaklaşık olarak %73'e düşmektedir. Ayrıca saldırgan düğümler özellikle rastgele seçilmiştir ve düğüm konumlarının saldırının başarısına olan etkileri de gözlemlenmiştir. Saldırılar başlatılırken saldırgan düğümlerin konumlarının doğru bir şekilde belirlenmesi ağın paket teslim oranını önemli ölçüde düşürebilir. %10 ile %15 saldırgan oranlı değerler incelendiğinde de görüldüğü gibi saldırgan sayısı artmasına rağmen PDR değeri saldırgan düğümlerin konumu nedeniyle yükselmektedir. Şimdiye kadar incelenen bütün saldırılar veri paketlerinin düşmesine neden olduğundan ve dolayısıyla rota bulma mekanizması yeniden başlatıldığından, saldırgan sayısı arttıkça ağlar üzerindeki yönlendirme kontrol paketlerinin sayısı da artmaktadır.

Çizelge 5.3. Kara delik saldırısı altındaki ağların ortalama performans metrikleri

Saldırgan düğüm oranı (%)	PDR (%)	E2E (saniye)	Ek Yük
%0	87,77	0,077	0,853
%5	77,85	0,058	1,033
%10	73,23	0,054	0,964
%15	83,00	0,068	0,870
%20	75,46	0,058	0,975
%25	75,54	0,058	0,951

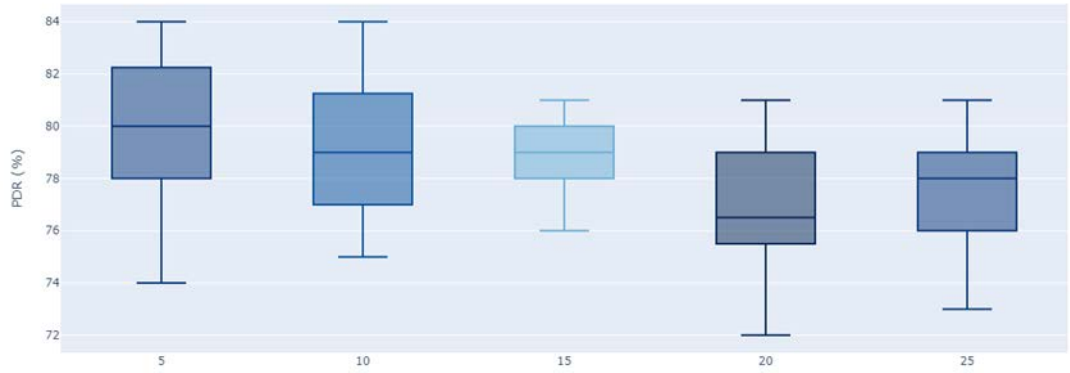


Şekil 5.3. Kara delik saldırısı altında ağın paket teslim oranları

Son olarak, bir DoS saldırı türü analiz edilmiştir. Sel saldırıları altındaki tasarsız ağların başarımları Tablo 5.4'te ve Şekil 5.4'te verilmiştir. Bu saldırı senaryosunda artan saldırgan oranı ağdaki paket teslim oranını azaltmaktadır. Belirli aralıklarla art arda yollanan RREQ kontrol paketleri hem ağ kaynaklarını tüketir hem de ağda tıkanıklığa sebep olur. Beklenildiği gibi ağdaki tıkanıklık bağlantı kesintileri oluşturur ve kaynak düğümden hedef düğüme giden veri paketleri düşer. Aynı zamanda sürekli olarak gönderilen RREQ mesajları ek yükü arttırarak ağda bir tıkanıklık oluşturabilir ve RREP mesajlarında gecikme olabilir. Bu nedenle saldırı altındaki ağlarda paket teslim sürelerinde uzama olmaktadır.

Çizelge 5.4. Tasarsız ağ sel saldırısı altındaki ağların ortalama performans metrikleri

Saldırgan düğüm oranı (%)	PDR (%)	E2E (saniye)	Ek Yük
%0	87,77	0,077	0,853
%5	80,08	0,070	0,924793
%10	79,15	0,078	0,945659
%15	79,00	0,088	0,917349
%20	78,00	0,087	0,963114
%25	77,62	0,096	0,952917



Şekil 5.4. Tasarsız ağ sel saldırısı altında ağın paket teslim oranları

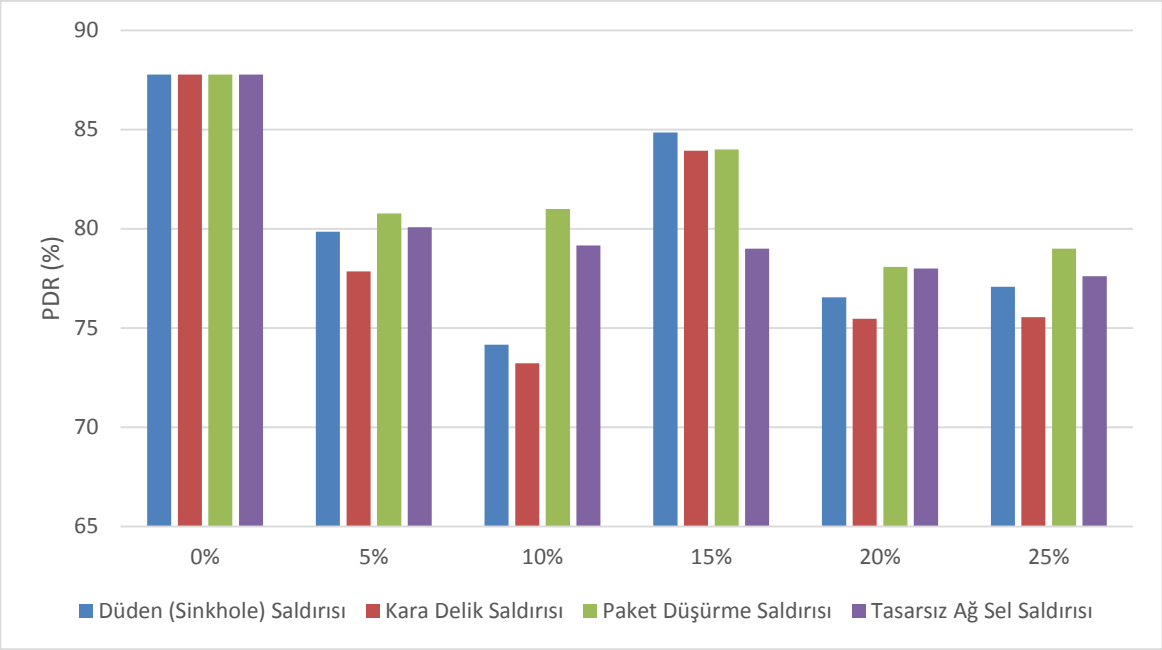
Saldırıların etkileri sırasıyla Şekil 5.5, 5.6, 5.7'de PDR, paket teslim gecikmesi ve ek yük kullanılarak birbirleriyle karşılaştırılmıştır. Karadelik saldırısı paket düşürme ve obruk saldırısının kombinasyonu olduğu için diğer saldırı türlerine göre daha güçlü bir saldırıdır. Şekil 5.5'de de gösterildiği gibi ağdaki ortalama PDR değerini en fazla düşüren saldırı karadelik saldırısıdır. Bu saldırı senaryosunda, saldırgan düğümlerin pozisyonlarının doğru seçilmesi ağdaki PDR oranını ciddi oranda azaltıp, kritik görevlerin engellenmesine neden olabilir.

Kara delik saldırısı, ağdaki ortalama PDR değerini obruk saldırısından daha fazla azaltır. Fakat kara delik ve obruk saldırısı PDR değerleri arasındaki fark beklenildiği kadar fazla değildir. Obruk saldırısında, saldırgan düğüm veri paketlerini kasıtlı olarak düşürmemesine rağmen, pasif yollar oluşturmakta ve veri paketinin hedefe ulaşmasını engellemektedir. Buna ek olarak obruk saldırısında kara delik saldırısından farklı olarak veri paketlerinin hedefe ulaştırılması beklenmektedir. Ancak, hedef düğüm saldırgan düğümün tek atlamalı

komşusu olduğunda veri paketleri düşürülmeden hedefe iletilebilir. Diğer durumlarda, saldırgan düğüm gerçekten kaynak ile hedef düğüm arasında yer almıyor ise veri paketleri hedef düğüme ulaşmayabilir. Bu durum da obruk ve kara delik saldırıları altındaki ağların ortalama PDR değerleri arasındaki küçük farkları açıklar.

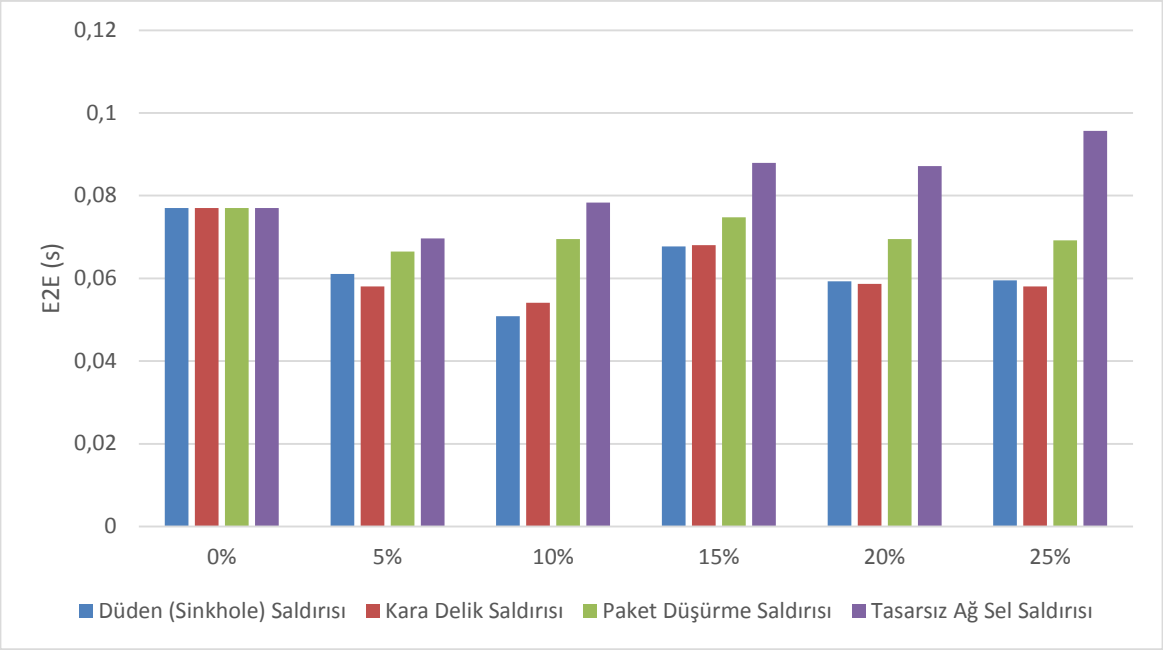
Paket düşürme saldırısı ise ağı en az etkileyen saldırılardandır. Bunun nedeni ise saldırgan düğümün sadece aktif rotada olduğu zamanlarda veri paketini düşürebiliyor olmasıdır. Bununla birlikte, sel saldırıları senaryosunda saldırgan oranlarının artması ile birlikte ağda tıkanıklık ve kaynak tüketimi fazla olur. Sel saldırısında parametreleri değiştirerek 3saniyede bir 20 RREQ mesajı gönderildiğinde saldırı, ağın performansını diğer saldırılara göre daha çok etkilemektedir. Ancak bu saldırının bu parametreler ile çalıştırılmasında veri yoğunluğundan dolayı sorunlar yaşanmış ve bazı simülasyonlar tamamlanamadan kesintiye uğramıştır. Bu nedenle, bütün sel saldırıları, 12 saniyede bir 10 RREQ mesajı gönderilerek gerçekleştirilmiştir. Bu durum da sel saldırısının etkisinin azalmasına neden olmuştur. Eğer iki uç düğüm arasındaki yol uzunsa (çok sayıda atlama içeriyorsa), veri paketlerini yolda kaybolma olasılığı artar.

Sonuçların tamamı analiz edildiğinde %15 saldırgan oranı ve sonrası için PDR değerlerinde bir artış oluştuğu gözlemlenmektedir. Bunun sebebi ise FANET karakteristiği ile açıklanmaktadır. Yani yüksek hareketlilik ve dinamik topoloji nedeniyle seçilen saldırgan düğümlerin konumları, saldırının başarısı açısından önem taşımasıdır. Ağda %15 oranında saldırgan düğüm bulunduğunda PDR'nin %10 oranından yüksek olması bu şekilde açıklanabilir.



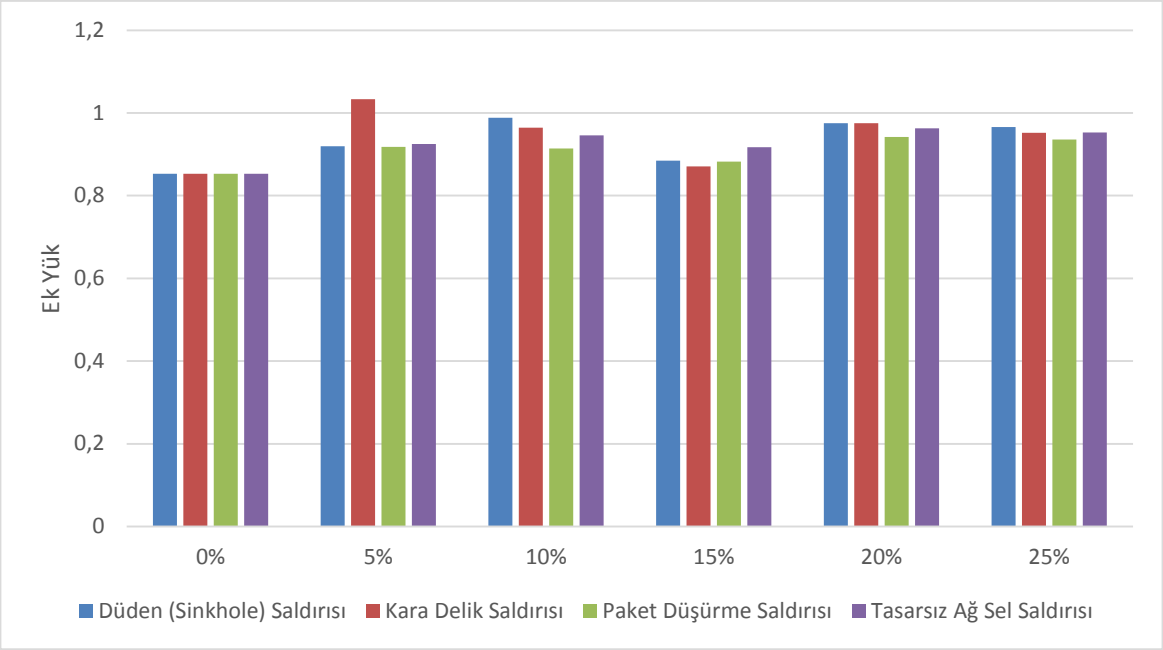
Şekil 5.5. Farklı saldırı türleri altındaki ağlarda PDR değerlerinin karşılaştırılması

Şekil 5.6'da gösterildiği gibi, E2E gecikmesi, ağdaki PDR değeri ile ters orantılı olarak değişmektedir. Ağ saldıra altında olmadığında E2E gecikme süresi daha fazladır. Yani hedefe ulaşan paket sayısı arttığında E2E gecikmesi de artmaktadır. Bu nedenle saldırı altındaki bir ağda gecikme de daha kısa süreli olacaktır. Ancak tasarsız ağ sel saldırısında durum farklıdır. Ağdaki saldırgan oranlarının artması ile birlikte kontrol paketleri de artmakta ve paket iletim sürelerinde gecikme olmaktadır.



Şekil 5.6. Farklı saldırı türleri altındaki ağlarda E2E değerlerinin karşılaştırılması

Ağdaki saldırganların sayısı artmaya devam ettikçe, Şekil 5.7'de gösterildiği gibi rota bulma mekanizmasının yeniden başlatılması nedeniyle ek yük de önemli ölçüde artar. Bu artış, beklendiği gibi bütün saldırılar için çok çarpıcıdır. Özellikle sel saldırısında ağda çok daha fazla RREQ paketi olduğu için ek yük sürekli olarak artış göstermektedir.



Şekil 5.7. Farklı saldırı türleri altındaki ağlarda ek yük değerlerinin karşılaştırılması

Çizelge 5.5'te 25 düğüme sahip 13 ağa yapılan obruk saldırısının performans metrikleri gösterilmiştir. Saldırı altında olmadan %95 PDR değeri elde edilmektedir. Obruk saldırısı başlatıldığında %20 saldırgan oranına kadar PDR değeri beklenildiği gibi azalmaktadır. Fakat yukarıda 50 düğüm için bahsedilen saldırgan düğümlerin konumlarının önemi burada da geçerli olmaktadır. %25 saldırgan oranında PDR azalması gerekirken düğümler üzerine paketleri başarılı bir şekilde çekememektedir. Buna ek olarak iletilmesi gereken paketin azalması E2E değerinin de azalmasına neden olmaktadır. Daha az paket daha kısa sürede ulaşmaktadır. Ek yük ise saldırıların etkisiyle, ağda kontrol paketlerinin artması sonucunda artış göstermektedir.

Düşürme saldırı senaryosunda da %20 saldırgan oranına kadar PDR değeri azalmaktadır. E2E gecikme süresi veri paketlerindeki azalma nedeniyle azalmaktadır ve ek yük artmaktadır.

Düşürme saldırı senaryosunda da %20 saldırgan oranına kadar PDR değeri azalmaktadır. E2E gecikme süresi veri paketlerindeki azalma nedeniyle azalmaktadır ve ek yük artmaktadır.

Kara delik saldırısı diğer saldırılara oranla ağı daha çok etkilemiştir. %20 saldırgan oranına sahip ağlarda ortalama PDR %83'e düşmektedir. Fakat %10 saldırgan oranında elde edilen sonuçlar üç atağın (obruk, düşürme ve kara delik saldırıları) etkisinin de neredeyse aynı olduğunu göstermektedir. Kara delik saldırısının, sadece aktif rota üzerinde yer alarak

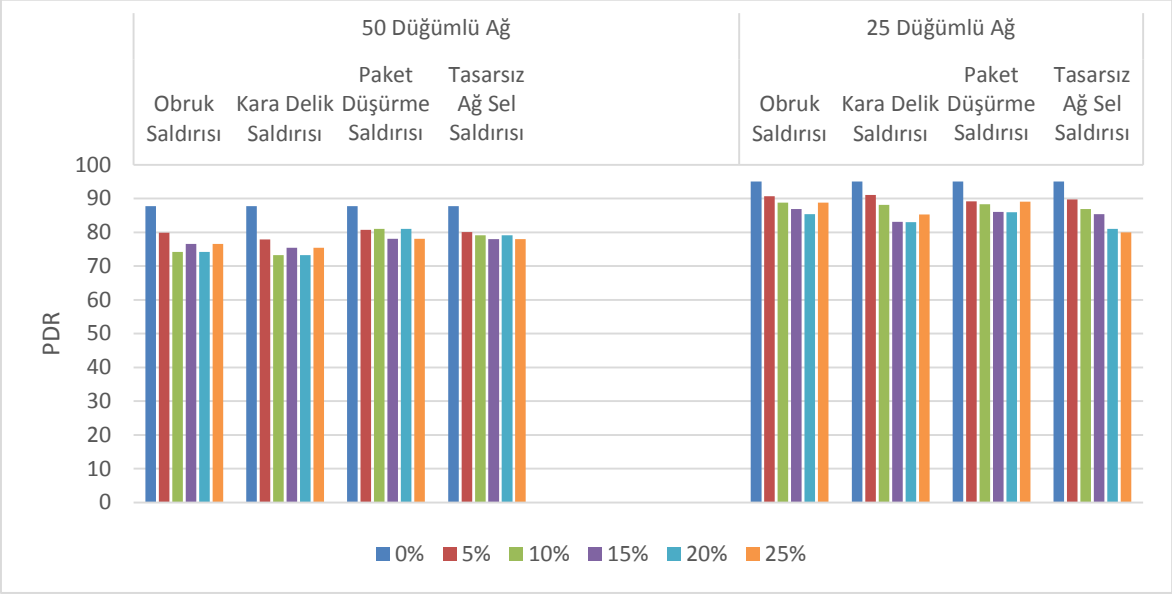
paketleri düşüren saldırıdan daha başarılı olması beklenmektedir. Fakat Ağın 25 düğüm içermesi ve alanın geniş olması düğümlerin seyrek uçmasına neden olmaktadır bu nedenle de %10 saldırgan oranı için seçilen saldırgan düğümler kara delik ve obruk saldırısında paketleri üzerine çekememiştir. Genel sonuçlara bakıldığında kara delik saldırısının güçlü bir saldırı olduğunu doğruluyoruz. Buna ek olarak karadelik saldırısında da E2E teslim edilen paket sayısı azaldıkça azalmakta ve Ek yük artmaktadır.

Sel saldırısında saldırgan düğüm sayısı arttıkça PDR değeri azalmaktadır. Ağda trafik yoğunluğu nedeniyle iletişim düzgün bir şekilde sağlanamaz. Ağda bağlantı kopuklukları olur ve veri paketleri düşer. Kontrol paketlerinin ek yükü arttırması ve RREP mesajlarının gecikmesi nedeni ile diğer saldırılara göre sel saldırısında gecikme biraz daha fazla olmaktadır.

Çizelge 5.5. 25 düğüme sahip ağların saldırı altındaki performansları

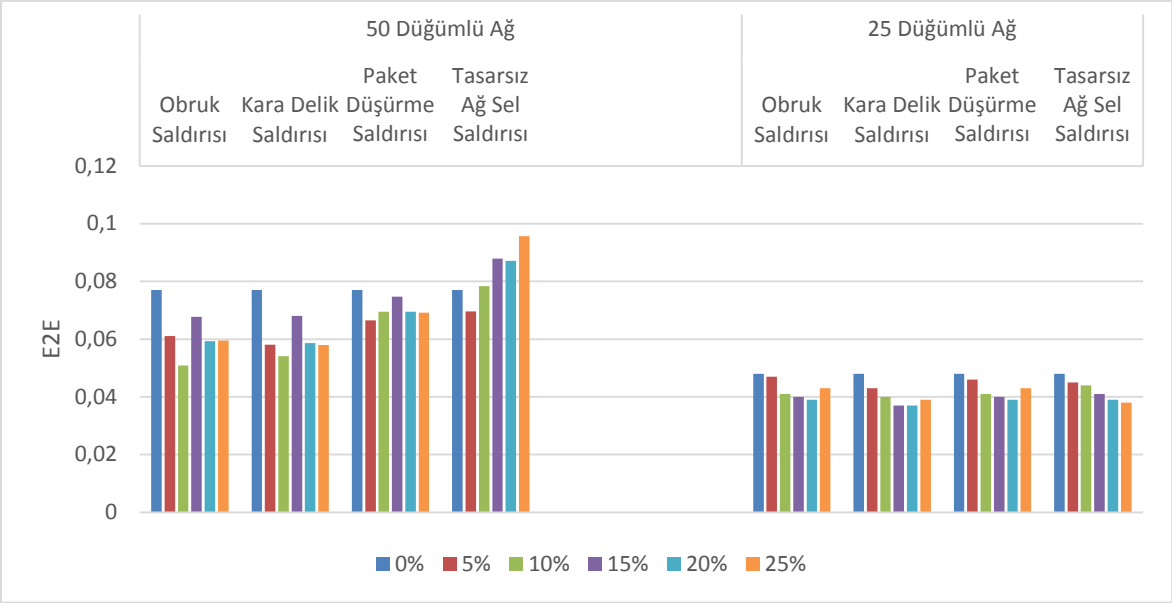
Saldırı Türü	Saldırgan düğüm oranı (%)	PDR (%)	E2E (saniye)	Ek Yük
Saldırı yok	%0	95,00	0,048	1,13
Obruk saldırısı	%5	90,69	0,047	1,20
	%10	88,76	0,041	1,11
	%15	86,85	0,040	1,19
	%20	85,37	0,039	1,14
	%25	88,80	0,043	1,18
Paket düşürme saldırısı	%5	91,01	0,046	1,24
	%10	88,33	0,041	1,11
	%15	86,00	0,040	1,22
	%20	85,97	0,039	1,15
	%25	89,02	0,043	1,21
Kara delik saldırısı	%5	89,19	0,043	1,23
	%10	88,15	0,040	1,12
	%15	83,05	0,037	1,24
	%20	83,00	0,037	1,17
	%25	85,23	0,039	1,23
Sel saldırısı	%5	89,77	0,045	1,454086
	%10	86,86	0,044	1,74383
	%15	85,35	0,041	1,794945
	%20	81,03	0,039	1,863565
	%25	80,00	0,038	1,790466

Şekil 5.8, 5.9, 5.10'da 25 ve 50 düğümlü ağlara ait PDR, E2E ve ek yük değerleri karşılaştırılmaktadır. 25 düğüm ve 50 düğüm sonuçları karşılaştırıldığında düğüm yoğunluğunun artmasıyla birlikte veri trafiğinde de yoğun bir artış olmaktadır. Bant genişliği de yetersiz kaldığı için veri paketleri düşmektedir ve PDR değeri azalmaktadır. Bu nedenle daha az yoğun bir ağda trafik azaldığı ve bant genişliği yeterli olduğu için daha iyi bir performans sağlanmaktadır. Buna ek olarak, ağda daha fazla düğümün yer alması kontrol paketlerinde artışa neden olduğu için trafik yoğunluğu ve ağ tıkanıklıkları bağlantıları etkilemektedir.



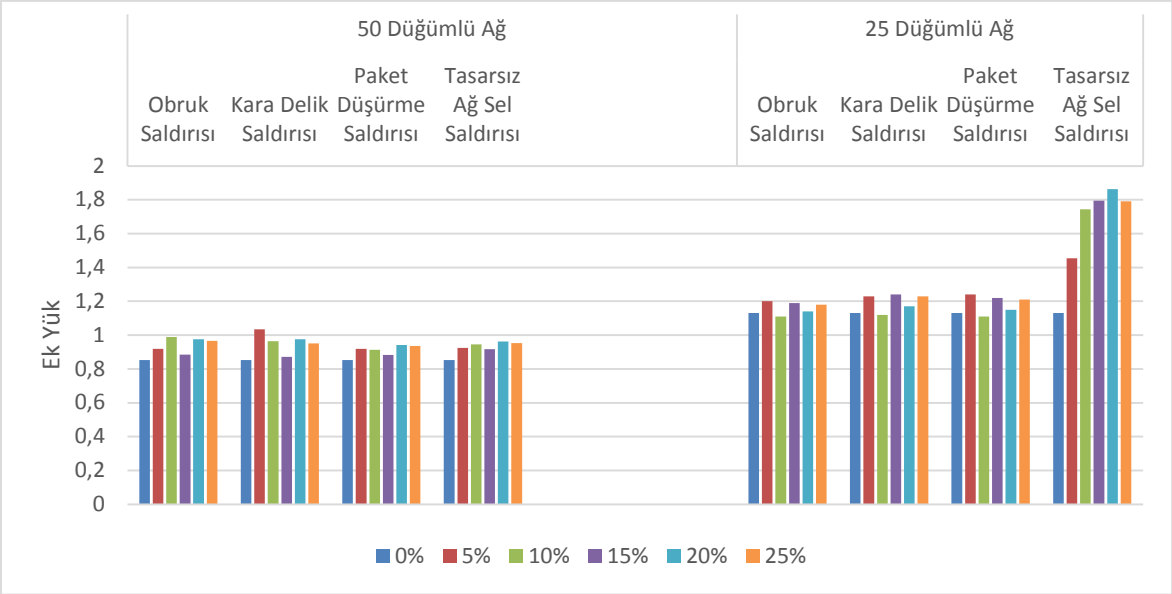
Şekil 5.8. 25 ve 50 düğümlü ağların PDR oranlarının karşılaştırılması

Saldırılar açısından bakıldığında daha yoğun bir ağda iş birliği yapan düğüm sayısı artacağı için kara delik ve obruk saldırı senaryosunda, saldırgan düğümlerin araya girip verileri üzerine çekmeleri daha kolay olacaktır. Bu saldırı türleri yönlendirme protokolünün rota keşfinden faydalanır ve daha fazla düğüm daha fazla rota keşfine neden olur. Yoğun ağlar bu saldırıların etkisini gösterebilmesi için daha uygundur. Buna ek olarak yoğun bir ağda daha fazla aktif rota seçeneği olduğu için paket düşürme saldırısı da bu tür ağlarda daha etkilidir.



Şekil 5.9. 25 ve 50 düğümlü ağların E2E oranlarının karşılaştırılması

Sel saldırısı düğüm yoğunluğu azaldıkça daha çok etkisini göstermektedir. Buna ek olarak yoğunluğu fazla olan ağlarda sel saldırısı, saldırgan oranı arttıkça paket teslim süresinin de artmasına neden olmaktadır. Şekil 6.9'da gösterildiği gibi E2E oranları 25 düğümlü ağda paket oranı azaldığı için düşmektedir. Yoğunluk fazla olan ağ saldırı altındayken ağ kaynakları tüketilmekte ve ağ tıkanıklıkları söz konusu olmaktadır. Bu nedenle oluşan tıkanıklık nedeniyle paket teslim süreci gecikmektedir. Daha az yoğun olan bir ağda ise ağ kaynaklarında aşırı bir tükenme olmadığı için paket teslim süresi diğer saldırılarda olduğu gibi teslim edilecek paket azaldığı için giderek düşmektedir. Ek yük ise 25 düğümlü ağlarda daha yüksek iken 50 düğümlü ağlarda daha düşüktür. 50 düğümlü ağlarda kapsama alanına giren düğüm sayısı artmaktadır ve ağdaki trafik yoğunluğunda bir artış olmaktadır. Bant genişliğinin yetersiz kalması ve yönlendirme protokolünün gönderdiği paketlerdeki artış nedeniyle ağda tıkanıklık oluşmaktadır. Ağda oluşan tıkanıklık nedeniyle düğümler tarafından alınacak olan kontrol paketleri bağlantı kesintisi nedeniyle düğümlere ulaşmadan düşmektedir. Ek yük hesaplanırken alınan kontrol paket sayısının alınan veri paketi sayısına oranı kullanılmaktadır. Düğüm yoğunluğunun artması ile ek yükün artması beklenirken, ek yük belirtilen nedenlerden azalmaktadır. Bu nedenle 50 düğümlü ağlar, 25 düğümlü ağlara göre daha az ek yüke neden olmuştur.



Şekil 5.10. 25 ve 50 düğümlü ağların Ek Yük oranlarının karşılaştırılması

5.2. Saldırı Tespit Sonuçları

Saldırılı ve saldırısız ağ verileri birlikte kullanılarak kesinlik değerinin arttırılması ve FPR oranının azaltılması hedeflenmiştir. Önerilen saldırı tespit sisteminin performansını arttırmak ve eğitim süresini azaltmak için her saldırı türü ve her saldırgan oranı (%5'ten %25'e kadar) ayrı ayrı eğitilir. Verilerin %80'i eğitim, %20'si test verisi olarak ayrılmaktadır. 13 farklı ağ topolojisi için belirlenen saldırgan oranlarıyla 1 giriş ve 5 saklı katmana sahip yapay sinir ağı ile 100 iterasyonda sonuçlar elde edilir. Her ağ topolojisine ait değerlerin ortalaması alınarak nihai değerlere ulaşılır.

Çizelge 9.8 ve Çizelge 9.9'da %5- %25 aralığında saldırgan oranlı veri kümelerine YSA uygulaması sonucunda alınan değerler gösterilmektedir. Veri kümesinde saldırısız bir ağdan alınan veriler ve saldırılı ağdan alınan veriler birlikte etiketlenmektedir. Saldırı altındaki ağdan alınan veriler işaretlenirken saldırı yapan düğümler 1, diğer düğümler 0 olarak işaretlenmektedir. Bu işaretleme sisteminin kullanılmasındaki temel neden ağda yer alan saldırgan düğümlerin takip edilmesi ve hangi düğümün saldırgan olduğunun tespit edilmesinin sağlanmasıdır. Buna ek olarak, çalışma bütün ağı dinleyen merkezi bir sistemin bulunduğu ortamlarda anormal değerlere sahip düğümleri tespit edip (Çizelge 4.3'te belirlenen özelliklerden yola çıkarak), bu düğümleri saldırgan olarak işaretleyen sistemler oluşturmak için bir alt yapı sağlamaktadır. Bu sayede, hem ağda bir saldırının

olduğu anlaşılmakta hem de hangi düğümün saldırgan olduğu bilinmektedir. Burada saldırgan düğümlerle saldırı tespit sistemi gerçekleştirilmiştir. Saldırı olup olmadığını doğrulama başarısı yüksektir. Ancak bu sistemlerin ele geçirilmesi ya da devre dışı bırakılması da söz konusu olmaktadır

Çizelge 5.6. FPR ve tespit oranı sonuçları (%5- %15 saldırgan oranı)

	%5 Saldırgan Oranı		%10 Saldırgan Oranı		%15 Saldırgan Oranı	
Saldırı Türü	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)
Obruk Saldırısı (SH)	98,9	9,1	96,9	5,8	95,9	5,8
Düşürme Saldırısı	98,8	12,6	95,7	11,0	94,5	8,7
Kara Delik Saldırısı	99,0	6,9	96,9	6,7	95,7	4,8
Sel Saldırısı	99,6	8,4	98,0	12,9	97,2	11,1

Çizelge 5.7. FPR ve tespit oranı sonuçları (%20- %25 saldırgan oranı)

	%20 Saldırgan Oranı		%25 Saldırgan Oranı	
Saldırı Türü	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)
Obruk Saldırısı (SH)	93,4	05,8	92,1	7,8
Düşürme Saldırısı	92,8	9,4	89,0	14,1
Kara Delik Saldırısı	92,9	5,8	91,8	7,1
Sel Saldırısı	94,2	10,8	94,6	18,9

Çizelge 5.6 ve 5.7'ye göre, sel saldırısı %5 saldırgan olan bir ağda %99,6 tespit oranı ile en yüksek değere sahiptir. %25 saldırgan oranına sahip bir ağda ise bu değer %94,6'dır. Saldırgan oranı arttıkça tespit oranında bir düşme olmaktadır. Bu düşüşe rağmen tespit oranı ortalama %95,4'tür. Sel saldırısı için FPR oranı ise %5 saldırgan oranlı bir ağda diğer oranlara göre daha düşüktür. En düşük tespit oranı ise düşürme saldırısına aittir. 25 saldırgan oranlı bir ağda, tespit oranı %89'a kadar düşmektedir. Bunun nedeni ise düşürme saldırısında sadece aktif rota üzerindeki verilerin düşürülüyor olmasıdır ve düşen paketlerin saldırgan tarafından düşürüldüğünün ayırt edilmesi diğer saldırı türlerine göre daha zor olmaktadır. FPR oranının yüksek olması da bu durumun bir kanıtıdır. Saldırgan olmayan düğümler de saldırgan olarak sınıflandırılmaktadır. Ancak yine genel duruma

baktığımızda ortalama %94 oranında başarı elde edilmektedir. Kara delik ve obruk saldırılarının tespit edilme oranı neredeyse aynıdır ve ortalama %95 oranındadır. FPR oranı ise ortalama %6 oranındadır ve sınıflandırma başarılı bir şekilde gerçekleştirilmektedir. Bu iki saldırı da paketleri üzerine çektiği için bu çalışmada kullanılan öznitelikleri etkilemektedir. Bu nedenle saldırgan düğüm ve saldırgan olmayan düğümü ayırt etmek kolaydır ve FPR oranı diğer senaryolara göre düşük çıkmaktadır.

Çizelge 5.8'de doğruluk, kesinlik ve F1 skor değerleri gösterilmektedir. En yüksek doğruluk değeri sel saldırısına ve en düşük doğruluk değeri paket düşürme saldırısına aittir. Kesinlik değerleri de ortalama %99 oranındadır ve F1 skor değeri de ortalama %97'dir. F1 skor kesinlik ve tespit oranının eşit derece de önem taşıdığı sistemlerde kullanılmaktadır. Saldırı tespit sistemleri için saldırganları sınıflandırma başarısı önemli olduğu kadar saldırgan olarak belirlenen kayıtların gerçekten saldırgan olup olmadığını anlamamız da önemlidir. Çünkü saldırı tespit sisteminin, saldırgan olmayan düğümleri devre dışı bırakması istenilmeyen bir durumdur.

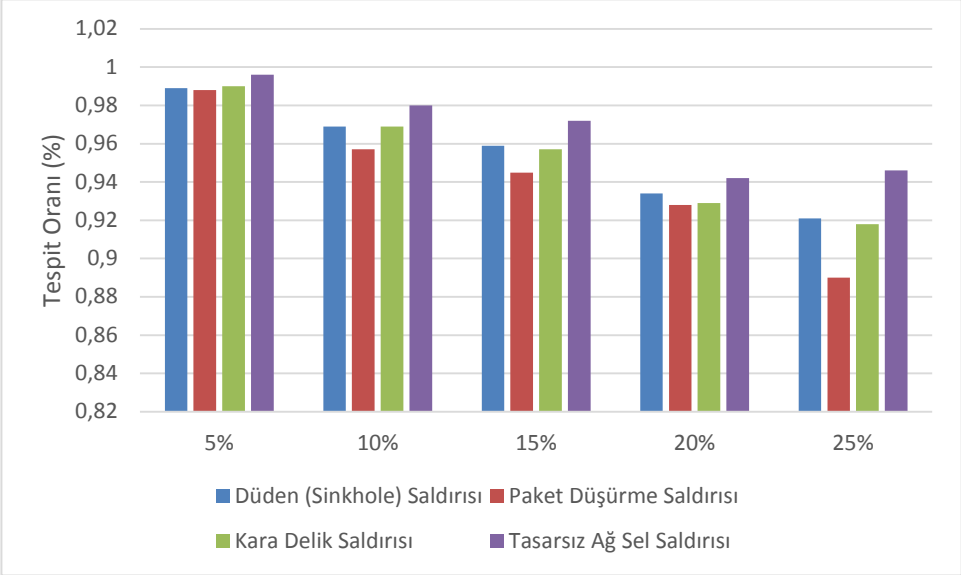
Çizelge 5.8. YSA performans metrikleri

Saldırgan Oranı	Saldırı Türleri	Doğruluk	Kesinlik	F1 Skor
%5 Saldırgan Oranı	Obruk Saldırısı	0,988	0,998	0,994
	Düşürme Saldırısı	0,986	0,997	0,993
	Kara Delik Saldırısı	0,989	0,999	0,994
	Sel Saldırısı	0,995	0,998	0,997
%10 Saldırgan oranı	Obruk Saldırısı	0,968	0,997	0,983
	Düşürme Saldırısı	0,954	0,994	0,975
	Kara Delik Saldırısı	0,955	0,985	0,976
	Sel Saldırısı	0,975	0,994	0,987
%15 Saldırgan oranı	Obruk Saldırısı	0,958	0,996	0,977
	Düşürme Saldırısı	0,943	0,994	0,969
	Kara Delik Saldırısı	0,957	0,996	0,976
	Sel Saldırısı	0,967	0,992	0,982
%20 Saldırgan Oranı	Obruk Saldırısı	0,935	0,994	0,963
	Düşürme Saldırısı	0,926	0,990	0,958
	Kara Delik Saldırısı	0,930	0,994	0,960
	Sel Saldırısı	0,942	0,988	0,964

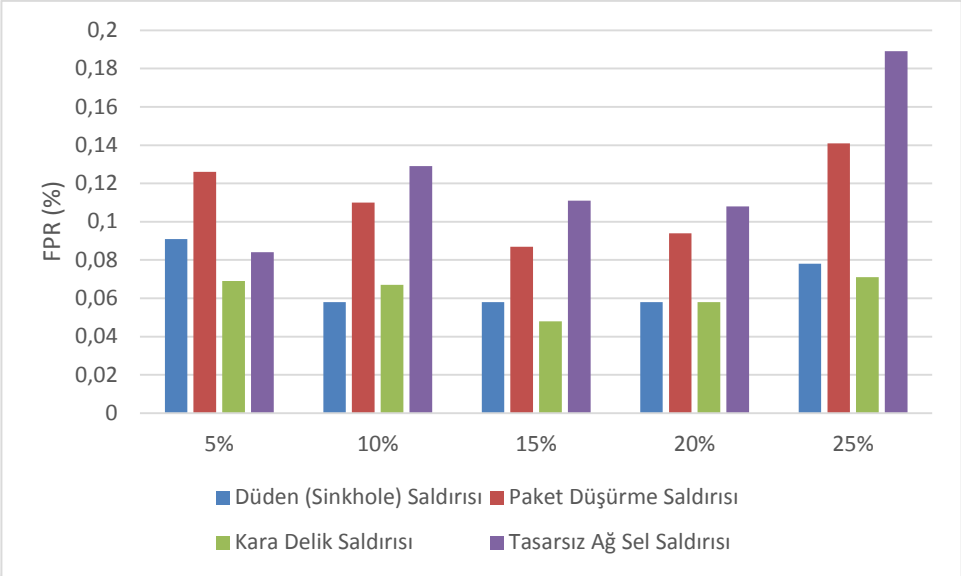
%25 Saldırgan Oranı	Obruk Saldırısı	0,921	0,989	0,954
	Düşürme Saldırısı	0,887	0,980	0,933
	Kara Delik Saldırısı	0,919	0,990	0,953
	Sel Saldırısı	0,912	0,958	0,949

Şekil 5.11 ve Şekil 5.12'da FPR ve tespit değerlerinin bütün saldırı çeşitleri ve oranları için karşılaştırılması verilmiştir. Şekil 5.11'de gösterilen değerlere göre neredeyse bütün saldırgan oranlarında başarı ortalama %95'in üzerindedir. En iyi saldırı tespit oranı sel saldırısına aittir. Saldırgan düğüm belirli aralıklarla RREQ paketi gönderir ve RREQ sayısındaki artış YSA algoritması tarafından kolaylıkla fark edilir.

Paket düşürme saldırısında ise saldırısının diğer saldırı türlerine göre tespit edilmesi daha zor olabilir. Saldırgan aktif bir rotada yer alıyorsa paketleri düşürür. Bu nedenle sistemler bağlantı kopukluğu nedeniyle düşen paket ile saldırgan tarafında düşürülen paketleri ayırt etmekte zorlanırlar. Sonuçlara baktığımız zaman diğer saldırgan tespitlerine oranla biraz düşük olsa da modelimiz yaklaşık %94 gibi bir tespit oranı ile başarılı bir şekilde saldırganları tespit etmektedir. Buna ek olarak saldırgan oranlarındaki artış az da olsa tespit oranının düşmesine neden olmaktadır. Çalışma geneline bakıldığında yüksek oranlarda tespit değerleri elde edilerek sistemin güçlü ve güvenilir olduğunu söyleyebiliriz.



Şekil 5.11. Saldırgan düğümden STS'ye ait farklı saldırı türlerine göre DR karşılaştırması



Şekil 5.12. Saldırgan düğümden STS'ye ait farklı saldırı türlerine göre FPR karşılaştırması

Şekil 5.12'ye göre ortalama FPR oranı %9 oranındadır. %25 saldırgan oranlı ağlarda FPR oranı diğerlerinden daha yüksek çıkmaktadır. Çünkü yüksek oranda saldırgan olduğunda model saldırgan olmayan düğümleri de saldırgan olarak işaretleyerek, yanlış alarm verilebilir. Genel olarak kara delik ve obruk saldırısının FPR oranı diğer saldırılardan daha düşüktür. Paketleri üzerine çekip düşmelerine neden olduğu için sınıflandırması daha kolay olmaktadır. Paket düşürme saldırısında ise düşürülen paketin bağlantı kopukluğundan olup olmadığı kolay anlaşılamayacağı için FPR diğer saldırılara oranla daha yüksek çıkmaktadır.

Sonuçlar analiz edildiğinde tespit oranının yüksek olması sınıflandırma işleminin başarılı bir şekilde gerçekleştiğini göstermektedir. Normal düğümlerin saldırgan olarak işaretlenmesi sistemin güvenilirliğini sorgulatacağı için saldırgan tespit sistemlerinde bu oranın düşük olması önerilir [85]. Buna ek olarak, saldırgan olmayan düğümler saldırgan olarak işaretlendiği zaman, bir kontrol mekanizması çalışıyor ise bu düğümü ağdan izole edecektir. Bu da güvenilir bir düğümün yanlış alarm nedeniyle görevini yapamamasına neden olur. Buna ek olarak tespit değerlerinin de yüksek çıkması yöntemin güvenilirliği kanıtlanmaktadır.

Saldırgan düğümlerden etkilenen STS için topladığımız veri kümesini farklı bir şekilde etiketlendirdik. Bu etiketleme sisteminde saldırıdan etkilenen düğümleri 1 olarak işaretleyerek saldırgan düğümler listeden çıkarılmıştır. Saldırısız ortamda alınan veriler ise

0 olarak işaretli kalmaktadır. Veri kümesi yukarıda bahsedildiği gibi saldırısız ve %5- %25 saldırgan oranlı ağlarda 13 farklı topoloji ile elde edilen verilerdir. Bu analizi yapma nedenimiz ağ saldırı altında olduğunda saldırıdan etkilenen düğümlerin de durumlarının kontrol edilmesi ve saldırı tespiti yapılmasıdır. Bu tespit sisteminde saldırı yapan düğümlerin ağa yanlış bilgilendirme yaparak kendilerini güvenilir düğüm olarak göstermeleri engellenmiş olacaktır. Saldırgan düğümlerden etkilenen STS'ler ağda yer alan diğer düğümler üzerinden saldırı tespiti yaptığı için saldırgan düğümlü STS'lere göre daha kapsamlıdır. Ancak bütün düğümler saldırılardan aynı oranda etkilenmediği için etkilenen düğümleri bulmak ve saldırı tespit oranını yükseltmek daha zordur.

Çizelge 5.9. Saldırıdan etkilenen düğümlerle STS sonuçları (%5- %15)

	%5 Saldırgan Oranı		%10 Saldırgan Oranı		%15 Saldırgan Oranı	
Saldırı Türü	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)
Obruk Saldırısı (SH)	59,4	4,7	70,9	3,7	60,3	4,8
Düşürme Saldırısı	54,5	4,6	51,2	4,7	54,3	5,0
Kara Delik Saldırısı	61,2	3,8	59,0	4,0	58,7	5,1
Sel Saldırısı	80,9	5,6	82,6	5,1	83,7	4,9

Çizelge 5.10. Saldırıdan etkilenen düğümlerle STS sonuçları (%20- %25)

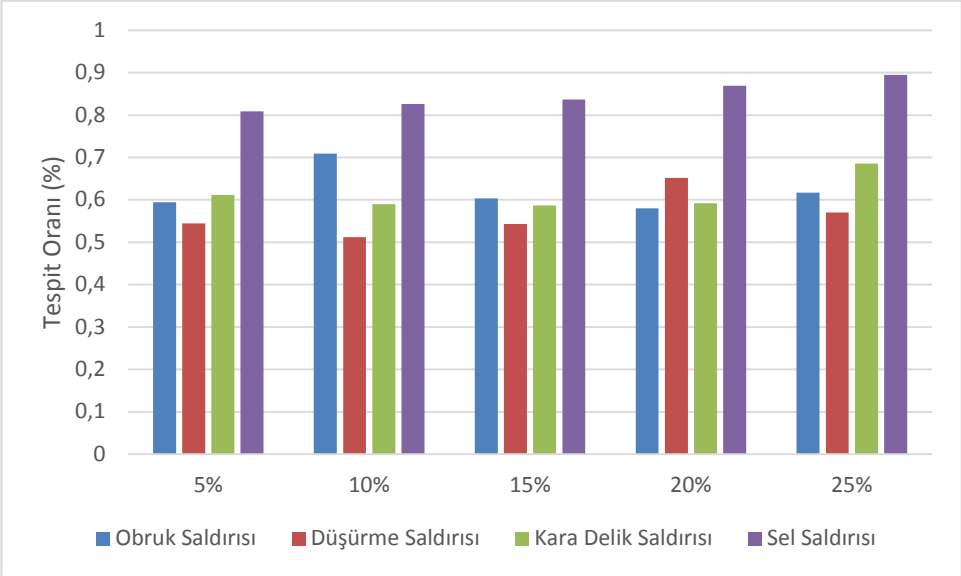
	%20 Saldırgan Oranı		%25 Saldırgan Oranı	
Saldırı Türü	DR (%) (*Sensitivity*)	FPR (%)	DR (%) (*Sensitivity*)	FPR (%)
Obruk Saldırısı (SH)	58,0	5,5	61,7	6,1
Düşürme Saldırısı	65,1	6,4	57,0	7,8
Kara Delik Saldırısı	59,2	6,5	68,5	6,9
Sel Saldırısı	86,9	4,7	89,5	12,8

Çizelge 5.9 ve 5.10'da ağ tabanlı STS yöntemi kullanılarak alınan sonuçlar gösterilmektedir. Kullanıcı tabanlı yönteme göre tespit oranı düşük çıkmaktadır. Bu durumun nedeni ağdaki bütün düğümlerin saldırıdan aynı şekilde etkilenmemiş olmasıdır. Sonuçlar sadece sel saldırısında yüksek çıkmaktadır. Bunun nedeni ise sel saldırısının bütün düğümleri aynı oranda etkiliyor oluşudur. İlerleyen çalışmalarda sadece saldırgan

düğüme yakın olan ve saldırıdan tamamen etkilenen düğümlerin etiketlenmesi ile deneyler yapılabilir ve tespit oranı arttırılabilir. Gösterilen değerlere göre Obruk saldırısı %10 saldırgan oranında %70 oranı ile diğer oranlardan daha yüksek değere sahiptir. FPR oranı ise doğru tespit oranının yüksek olması nedeniyle diğer oranlardan daha düşük çıkmaktadır. Kara delik saldırısı ise %25 saldırgan oranlı bir ağda saldırıdan daha fazla düğüm etkilendiği için %68,5 değeri ile daha yüksek sonuç vermektedir. Genel olarak FPR değerleri de düşük çıkmaktadır. Buna ek olarak düşürme saldırısından etkilenen düğümlerin ayırt edilme zorluğu nedeniyle diğer saldırılara göre tespit edilme oranı daha düşük çıkmaktadır. Bunun nedeni bağlantı kopmalarının da ağda fazla olmasıdır. Sel saldırısı ise %25 saldırgan oranlı bir ağda %89 tespit oranına sahiptir. Diğer oranlara göre burada tespit oranının daha yüksek çıkmasının nedeni ise daha fazla saldırgan oranında, düğümlerin saldırıdan daha çok etkilenmesidir. Bu nedenle sınıflandırma yapmak daha kolay olmaktadır.

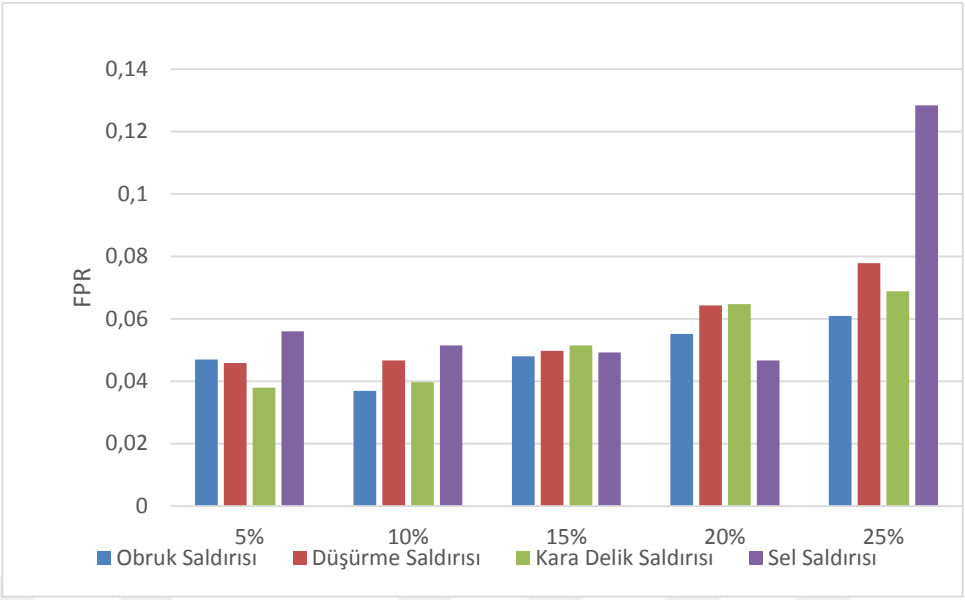
Şekil 5.13 ve 5.14'te bütün saldırıların ve saldırgan oranlarının FPR ve TO karşılaştırılması verilmektedir. Şekil 5.13'deki sonuçlara göre ortalama %84 tespit oranı ile sel saldırıları en yüksek değere sahiptir. Sel saldırısı bütün düğümleri etkilediği için etkilenen düğüm sayısı oranı fazladır ve tespit oranı daha yüksek olmaktadır. Buna ek olarak daha az düğümü etkilediği için düşürme saldırılarına ait tespit oranı da en düşük değerdedir. Düğümlerin saldırıdan etkilendiği için mi yoksa bağlantı kesintisi nedeniyle mi veri düşürdüğünü anlamak zor olmaktadır. Kara delik ve obruk saldırısı ise bazı düğümleri etkileyerek verileri üzerine seçtikleri için tespit oranları yaklaşık olarak aynı olmaktadır. Bu saldırılarda da hangi düğümün saldırıdan etkilendiğini tespit etmek düşürme saldırısına göre daha kolay olsa da sınıflandırma işlemi yine de zordur.

Şekil 5.14'te FPR sonuçlarına göre en düşük orana %4,9 değeri ile obruk saldırısı sahiptir. Burada saldırıdan etkilenmeyen düğümlerin etkilenmiş gibi işaretlenmesi daha düşük bir ihtimale sahiptir. Ortalama %6 FPR oranı ile en yüksek değer ise sel saldırısına ait olmaktadır. Tespit oranı yüksek olduğu için bu değer göz ardı edilebilmektedir. Kara delik ve obruk saldırısı ise neredeyse aynı FPR oranlarına sahiptir.



Şekil 5.13. Saldırıdan etkilenen düğümlerle STS'ye göre DR karşılaştırması

Bu çalışmada aynı model kullanılarak iki farklı etiketleme sistemi ile alınan sonuçlar sunulmuştur. Kullanıcı tabanlı STS'de saldırgan düğümler işaretlenerek eğitim ve test süreçleri gerçekleştirilmiştir. Buradaki amacımız ağda hangi düğümün saldırgan olduğunu tespit etmektir. Ağ tabanlı STS kullanılarak yapılan çalışmada ise saldırıdan etkilenen düğümler işaretlenerek bu düğümler aracılığı ile saldırı olup olmadığı tespit edilmeye çalışılmıştır. Çünkü ilk sistemde saldırgan ele geçirdiği düğümü normal bir düğüm gibi göstererek diğer düğümlerin güvenini sağlayabilir. Fakat ikinci sistemde etkilenen düğümlerden yola çıkarak tespit sistemi gerçekleştiğinde daha gerçekçi bir saldırı tespit senaryosu oluşturulabilir. Fakat ikinci yöntemde tespit oranı ilk yönteme göre daha düşük çıkmaktadır. Bunun nedeni bütün düğümlerin saldırılardan aynı oranda etkilenmemesi ve sistemin tespit yapmakta zorlanmasıdır. YSA uygulama katmanları ya da parametreler değiştirilerek sonuçlar yükseltilebilir. Burada karşılaştırma yapmak amacı ile iki durum için aynı model kullanılmaktadır.



Şekil 5.14. Saldırıdan etkilenen düğümlerle STS'ye göre FPR oranı karşılaştırması

6. SONUÇ VE ÖNERİLER

Bu çalışmada, FANET'lere yönelik çeşitli saldırıların ağ performansını nasıl etkilediğini analiz etmektedir. Özellikle AODV'yi hedef alan yönlendirme saldırıları yani obruk, düşürme, kara delik ve tasarsız ağ sel saldırıları dikkate alınmaktadır. Ns-3 simülasyon aracı kullanılarak 13 farklı ağ topolojisinde 25 ve 50 düğüm için önce saldırı olmadan, daha sonra ise %5- %25 aralığında değişen saldırgan düğüm oranları ile her bir saldırı türü için toplam 78 kez simülasyon çalıştırılmıştır. Bu test sonuçları PDR, E2E ve ek yük metrikleri kullanılarak ağ performansları analiz edilmiştir. Deney sonuçlarında 13 farklı topolojiden elde edilen değerlerin ortalaması kullanılmaktadır. Buna ek olarak saldırı tespit sistemlerinde kullanılmak üzere bir veri kümesi oluşturulmuştur. Veri kümesi, düğümlerin ağdaki hareketliliği ve ağda gönderilen AODV kontrol mesajları ve veri paketleri hakkında bilgi veren özniteliklerden oluşmaktadır. Oluşturulan veri kümesi YSA kullanılarak, saldırgan düğümler üzerinden ve saldırıdan etkilenen düğümler üzerinden olarak iki farklı saldırı tespiti gerçekleştirilmiştir.

Analiz deney sonuçları, 50 düğüm için saldırganların oranı %10'a, 25 düğüm için ise %20'ye ulaştığında tüm saldırıların ağın performansını düşürdüğünü göstermektedir. Saldırgan oranının yükselmesi ile performansın düşmesi beklenirken sonuçlarda bazı saldırgan oranlarında performansın düşmediği gözlemlenmiştir. Bu gibi durumlarda, saldırıların etkileri FANET karakteristik özellikleri (dinamik topoloji ve yüksek hız) nedeniyle sınırlı olabilir. Böylece saldırganlar ağa doğru bir şekilde yerleştirilirlerse en basit saldırı da dahi PDR'yi düşürebilir, böylece küçük ağlarda saldırganın trafiği kendi üzerinden çekmesine bile gerek kalmaz. Yalnızca sel saldırısı, doğası gereği belirli periyotlarla paket yolladığı için saldırgan oranının artması ile ağda tıkanıklığa neden olmakta ve performansı sürekli olarak düşürmektedir. Çalışma ile toplanan veri kümesi saldırı tespiti için kullanılmıştır. YSA algoritması veri kümesine uygulanarak başarılı bir saldırı tespiti gerçekleştirilmiştir. Saldırı tespit sistemlerinin başarılı bir sınıflandırma yapması için saldırganları yüksek oranda tespit etmesi ve saldırgan olmayan düğümleri ayırt edebilmesi gerekmektedir. Bu tez çalışmasında önerilen saldırı tespit sistemi, bu iki metrikte de iyi bir başarım göstermiştir.

Bildiğimiz kadarıyla, bu gerçekçi simülasyon parametreleriyle FANET'ler üzerinde yapılan ilk detaylı saldırı analizidir. Literatürdeki çalışmalarda halen 2B hareketlilik modelleri kullanılmaktadır. Dolayısıyla bu çalışmanın FANET'lerin güvenliği ile ilgili çalışmaları

hızlandırabileceği düşünülmektedir. Araştırmacılar, FANET'leri gerçekten etkileyebilecek saldırıları simüle etmek için buradaki ağ parametrelerini kullanabilir, böylece bu tür saldırıları azaltmak/tespit etmek için çözümler önerebilirler. Bunlara ek olarak, çalışma ile toplanan veri kümesi kullanılarak saldırı tespit sürecine katkı sağlanmaktadır. Bildiğimiz kadarı ile FANET'ler için toplanan bir veri kümesi literatürde mevcut değildir. Bu nedenle çalışmalarda diğer geleneksel tasarsız ağlara ait veriler kullanılmaktadır. Bu durum gerçekçi senaryoların oluşmasına engel olmaktadır. Çalışmamız FANET saldırı tespit sistemlerinin geliştirilmesi için bir temel oluşturmaktadır. İleride, bu veri kümesinin isteyen araştırmacılar ile paylaşılabileceği planlanmaktadır. Gelecekte, daha büyük ağlarda daha karmaşık saldırı senaryolarının analiz edilmesi planlanmaktadır. Buna ek olarak veri kümesi toplanırken saldırgan düğüme yakın ve saldırıdan daha çok etkilenen düğümler etiketlenerek ağ tabanlı saldırı tespit sistemlerine katkı sağlanması hedeflenmektedir. Son olarak veri kümesi genişletilerek farklı makine öğrenimi, derin öğrenme ve yapay zeka algoritmaları kullanılarak saldırı tespit sistemlerinin başarı oranları karşılaştırılabilir.

KAYNAKLAR

1. Maxa, J., Mahmoud, M. Ben, Larrieu, N., Maxa, J., Mahmoud, M. Ben, Larrieu, N. verification, E., Maxa, J., Slim, M., Mahmoud, B. ve Larrieu, N. (2016). *Extended Verification of Secure UAANET Routing Protocol To cite this version : HAL Id : hal-01365933 Extended Verification of Secure UAANET Routing Protocol*.

2. Mahmud, I. ve Cho, Y. Z. (2019). Adaptive Hello Interval in FANET Routing Protocols for Green UAVs. *IEEE Access*, *7*, 63004–63015.

3. George, J., Sujit, P. B. ve Sousa, J. B. (2011). Search strategies for multiple UAV search and destroy missions. *Journal of Intelligent and Robotic Systems: Theory and Applications*.

4. Al Fayez, F., Hammoudeh, M., Adebisi, B. ve Abdul Sattar, K. N. (2019). Assessing the effectiveness of flying ad hoc networks for international border surveillance. *International Journal of Distributed Sensor Networks*.

5. Barrado, C., Meseguer, R., López, J., Pastor, E., Santamaria, E. ve Royo, P. (2010). Wildfire monitoring using a mixed air-ground mobile network. *IEEE Pervasive Computing*, *9*(4), 24–32.

6. Xiang, H. ve Tian, L. (2011). Development of a low-cost agricultural remote sensing system based on an autonomous unmanned aerial vehicle (UAV). *Biosystems Engineering*.

7. El-Semary, A. M. ve Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. *IEEE Access*, *7*, 95197–95211.

8. Darabkh, K. A., Alfawares, M. G. ve Althunibat, S. (2019). MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks. *Vehicular Communications*, *18*, 100163.

9. Rezwan, S. ve Choi, W. (2021). A survey on applications of reinforcement learning in flying Ad-hoc networks. *Electronics (Switzerland)*, *10*(4), 1–19.

10. Zalte, S. S. ve Ghorpade, V. R. (2018). Intrusion Detection System for MANET. *2018 3rd International Conference for Convergence in Technology, I2CT 2018*, 7–10.

11. Ramadan, R. A., Emara, A. H., Al-Sarem, M. ve Elhamahmy, M. (2021). Internet of drones intrusion detection using deep learning. *Electronics (Switzerland)*, *10*(21).

12. Carneiro, G., Fortuna, P. ve Ricardo, M. (2012). *FlowMonitor - a network monitoring framework for the Network Simulator 3 (NS-3)*. *3*.

13. Tan, X., Zuo, Z., Su, S., Guo, X. ve Sun, X. (2020). Research of Security Routing Protocol for UAV Communication Network Based on AODV. *Electronics 9(8):1185*

14. The ns-3 network simulator. (2021), http://www.nsnam.org/

15. Ochola, E. O., Mejaele, L. F., Eloff, M. M. ve Van Der Poll, J. A. (2017). Manet reactive routing protocols node mobility variation effect in analysing the impact of black hole attack. *SAIEE Africa Research Journal*, *108*(2), 80–91.

16. Sen, J., Koilakonda, S. ve Ukil, A. (2011). A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. *Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011*, 338–343.

17. Ning, P. ve Sun, K. (2005). How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. *Ad Hoc Networks*, *3*(6), 795–819.

18. Jain, A. K. ve Attack, A. B. H. (2015). Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks. *2015 International Conference on Pervasive Computing (ICPC)*

19. Dokurer, S., Erten, Y. M. ve Acar, C. E. (2007). Performance analysis of ad-hoc networks under black hole attacks. *Conference Proceedings - IEEE SOUTHEASTCON*, 148–153.

20. Lu, S., Li, L., Lam, K. Y. ve Jia, L. (2009). SAODV: A MANET routing protocol that can withstand black hole attack. *CIS 2009 - 2009 International Conference on Computational Intelligence and Security*, 2, 421–425.

21. Deshmukh, S. R., Chatur, P. N. ve Bhople, N. B. (2017). AODV-Based secure routing against blackhole attack in MANET. *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016 - Proceedings*, 1960–1964.

22. Praveen, K. S., Gururaj, H. L. ve Ramesh, B. (2016). Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. *Procedia Computer Science*, *85*(Cms), 325–330.

23. Hu, Y.-C., Perrig, A. ve Johnson, D. B. (2003). Rushing attacks and defense in wireless ad hoc network routing protocols. *Proceedings of the 2nd ACM workshop on Wireless security.*

24. Bandyopadhyay, A., Vuppala, S. ve Choudhury, P. (2011). A simulation analysis of flooding attack in MANET using NS-3. *2011 2nd International Conference on Wireless Communicationvehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*, 0–4.

25. Yi, P., Wu, Y. ve Ma, J. (2009). Experimental evaluation of flooding attacks in mobile ad hoc networks. *Proceedings - 2009 IEEE International Conference on Communications Workshops, ICC 2009*, *60803117*, 9–12.

26. Altawy, R. ve Youssef, A. M. (2017). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2).

27. Akram, R. N., Markantonakis, K., Mayes, K., Habachi, O., Sauveron, D., Steyven, A. ve Chaumette, S. (2017). Security, privacy and safety evaluation of dynamic and static fleets of drones. *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, *2017-Eylül*.

28. Bekmezci, I., Sahingoz, O. K. ve Temel, Ş. (2013). Flying Ad-Hoc Networks (FANETs): A survey. *Ad Hoc Networks*, *11*(3), 1254–1270.

29. Sahingoz, O. K. (2014). Networking models in flying Ad-hoc networks (FANETs): Concepts and challenges. *Journal of Intelligent and Robotic Systems: Theory and Applications*, *74*(1–2), 513–527.

30. Bekmezcİ, İ. ve Şentürk, E. (2016). Securıty Issues In Flyıng Ad-Hoc Networks (FANETs). *Journal of Aeronautics and Space Technologies*, 9(2), 13-21.

31. Mitrokotsa, A., Komninos, N. ve Douligeris, C. (2007). Intrusion detection with neural networks and watermarking techniques for MANET. *2007 IEEE International Conference on Pervasive Services, ICPS*, *118–127*.

32. Abdan, M. (2021). Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET). *Wireless Communications and Mobile Computing*.

33. Laqtib, S., El Yassini, K. ve Hasnaoui, M. L. (2019). A deep learning methods for intrusion detection systems based machine learning in MANET. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*.

34. Walia, E., Bhatia, V. ve Kaur, G. (2018). Detection Of Malicious Nodes in Flying Ad-HOC Networks (FANET). *International Journal of Electronics and Communication Engineering*, 5(9), 6–12.

35. Bhatia, V., Walia, E. ve Singla, P. (2019). VANET and FANET under the impact of the security attack. *International Journal of Innovative Technology and Exploring Engineering*, *8*(9 Special Issue), 390–397.

36. Condomines, J. P., Zhang, R. ve Larrieu, N. (2019). Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*, *90*, 101759.

37. Ouiazzane, S., Barramou, F. ve Addou, M. (2020). Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones. *International Journal of Advanced Computer Science and Applications*, *11*(10), 351–362.

38. Mowla, N. I., Tran, N. H., Doh, I. ve Chae, K. (2020). Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network. *IEEE Access*, *8*, 4338–4350.

39. Oubbati, O. S., Atiquzzaman, M., Lorenz, P., Tareque, M. H. ve Hossain, M. S. (2019). Routing in flying Ad Hoc networks: Survey, constraints, and future challenge perspectives. *IEEE Access*.

40. Lin, J., Cai, W., Zhang, S., Fan, X., Guo, S. ve Dai, J. (2018). A survey of flying ad-hoc networks: Characteristics and challenges. *Proceedings - 8th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2018*, 766–771.

41. Jarupan, B. ve Ekici, E. (2011). A survey of cross-layer design for VANETs. *Ad Hoc Networks*, *9*(5), 966–983.

42. Rosati, S., Kruzelecki, K., Traynard, L. ve Rimoldi, B. (2013). Speed-aware routing for UAV ad-hoc networks. *2013 IEEE Globecom Workshops, GC Wkshps 2013, December 2014*, 1367–1373.

43. Han, Z., Swindlehurst, A. L. ve Liu, K. J. R. (2009). Optimization of MANET connectivity via smart deployment/movement of unmanned air vehicles. *IEEE Transactions on Vehicular Technology*, *58*(7), 3533–3546.

44. Bani, M. ve Alhuda", "Nour. (2016). Flying Ad-Hoc Networks: Routing Protocols, Mobility Models, Issues. *International Journal of Advanced Computer Science and Applications*, *7*(6), 162–168.

45. Van Der Bergh, B., Chiumento, A. ve Pollin, S. (2016). LTE in the sky: Trading off propagation benefits with interference costs for aerial nodes. *IEEE Communications Magazine*.

46. Purohit, A., Mokaya, F. ve Zhang, P. (2012). Collaborative indoor sensing with the SensorFly aerial sensor network. *IPSN'12 - Proceedings of the 11th International Conference on Information Processing in Sensor Networks*.

47. Ullah, H., Abu-Tair, M., McClean, S., Nixon, P., Parr, G. ve Luo, C. (2017). An unmanned aerial vehicle based wireless network for bridging communication. *Proceedings - 14th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2017, 11th International Conference on Frontier of Computer Science and Technology, FCST 2017 and 3rd International Symposium of Creative Computing, ISCC 2017*.

48. Arafat, M. Y. ve Moh, S. (2018). Location-Aided Delay Tolerant Routing Protocol in UAV Networks for Post-Disaster Operation. *IEEE Access*.

49. Jung, D. ve Tsiotras, P. (2007). Inertial attitude and position reference system development for a small UAV. *Collection of Technical Papers - 2007 AIAA InfoTech at Aerospace Conference*.

50. Fadlullah, Z. M., Takaishi, D., Nishiyama, H., Kato, N. ve Miura, R. (2016). A dynamic trajectory control algorithm for improving the communication throughput and delay in UAV-aided networks. *IEEE Network*.

51. Al-Hourani, A., Kandeepan, S. ve Lardner, S. (2014). Optimal LAP altitude for maximum coverage. *IEEE Wireless Communications Letters*.

52. US Department of Defense. (2007). Unmanned systems roadmap 2007-2032. *Defence Technical Information Centre*.

53. Bacco, M., Cassarà, P., Colucci, M., Gotta, A., Marchese, M. ve Patrone, F. (2018). A Survey on Network Architectures and Applications for Nanosat and UAV Swarms. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *231*, 75–85.

54. Frew, E. W. ve Brown, T. X. (2009). Networking issues for small unmanned aircraft systems. *Journal of Intelligent and Robotic Systems: Theory and Applications*, *54*(1-3 SPEC. ISS.), 21–37.

55. Chakraborty, A., Chai, E., Sundaresan, K., Khojastepour, A. ve Rangarajan, S. (2018). SkyRAN: A self-organizing LTE RAN in the sky. *CoNEXT 2018 - Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies*, 280–292.

56. Vanitha, N. ve Padmavathi, G. (2018). A Comparative Study on Communication Architecture of Unmanned Aerial Vehicles and Security Analysis of False Data Dissemination Attacks. *Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018*, 1–8.

57. Shumeye Lakew, D., Sa'Ad, U., Dao, N. N., Na, W. ve Cho, S. (2020). Routing in Flying Ad Hoc Networks: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, *22*(2), 1071–1120.

58. Camp, T., Boleng, J. ve Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, *2*(5), 483–502.

59. Bujari, A., Calafate, C. T., Cano, J. C., Manzoni, P., Palazzi, C. E. ve Ronzani, D. (2017). Flying ad-hoc network application scenarios and mobility models. *International Journal of Distributed Sensor Networks*, *13*(10), 1–17.

60. Atsan, E. ve Özkasap, Ö. (2006). A classification and performance comparison of mobility models for ad hoc networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4104 LNCS*(August), 444–457.

61. Liang, B. ve Haas, Z. J. (2003). Predictive distance-based mobility management for multidimensional PCS networks. *IEEE/ACM Transactions on Networking*, *11*(5), 718–732.

62. Tolety, V. ve Camp, T. (1999). Load reduction in ad hoc networks using mobile servers. *Mathematical and Computer Sciences*, *Master*.

63. Biomo, J. D. M. M., Kunz, T. ve St-Hilaire, M. (2014). An enhanced Gauss-Markov mobility model for simulations of unmanned aerial ad hoc networks. *2014 7th IFIP Wireless and Mobile Networking Conference, WMNC 2014*.

64. Broyles, D., Jabbar, A. ve Sterbenz, J. P. G. (2010). Design and analysis of a 3-D gauss-markov mobility model for highly dynamic airborne networks. *Proceedings of the International Telemetering Conference*, 46(June 2014).

65. Şentürk, E. (2016). Uçan Tasarsız Ağlarda Güvenlik Sorunları, Yüksek Lisans Tezi, *Hava Harp Okulu Havacılık Ve Uzay Teknolojileri Enstitüsü*, 113108

66. Li, C., Zheng, L., Xie, W. ve Yang, P. (2018). Ad Hoc Network Routing Protocol Based on Location and Neighbor Sensing. *2018 IEEE International Conference on Computer and Communication Engineering Technology, CCET 2018*, 1–5.

67. Cerri, D. ve Ghioni, A. (2008). Securing AODV: The A-SAODV Secure Routing Prototype. *IEEE Communications Magazine*, *46*(2), 120–125.

68. Perkins, C. E., Bhagwat, P., E. Perkins, C., Bhagwat, P., Perkins, C. E. ve Bhagwat, P. (1994). Highly Dynamic (DSDV) for Mobile Computers Routing. *Proceedings of the ACM SIGCOMM94, London, UK*, *24*(4), 234–244.

69. Nayyar, A. (2018). Flying Adhoc Network (FANETs): Simulation Based Performance Comparison of Routing Protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, IcABCD 2018*, *October*, 1–9.

70. Me Biomo, J. D. M., Kunz, T., St-Hilaire, M. ve Zhou, Y. (2015). Unmanned aerial ad hoc networks: Simulation-based evaluation of entity mobility models' impact on routing performance. *Aerospace*, *2*(3), 392–422.

71. Johnson, D., Hu, Y. ve Maltz, D. (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. *document RFC 47283*

72. Leonov, A. V., Litvinov, G. A. ve Shcherba, E. V. (2018). Simulation and comparative analysis of packet delivery in flying ad hoc network (FANET) Using AODV. *International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices, EDM*, *2018-July*, 71–78.

73. Garcia-Santiago, A., Castaneda-Camacho, J., Guerrero-Castellanos, J. F. ve Mino-Aguilar, G. (2018). Evaluation of AODV and DSDV routing protocols for a FANET: Further results towards robotic vehicle networks. *9th IEEE Latin American Symposium on Circuits and Systems, LASCAS 2018 - Proceedings*, 1–4.

74. Liu, J., Wang, Q., He, C. T., Jaffrès-Runser, K., Xu, Y., Li, Z. ve Xu, Y. J. (2020). QMR:Q-learning based Multi-objective optimization Routing protocol for Flying Ad Hoc Networks. *Computer Communications*, *150* (Kasım 2019), 304–316.

75. Franchi, A., Secchi, C., Ryll, M., Bülthoff, H. ve Giordano, P. R. (2012). Shared control: Balancing autonomy and human assistance with a group of quadrotor UAVs. *IEEE Robotics and Automation Magazine*, *19*(3), 57–68.

76. Maxa, J., Mahmoud, M. Ben, Larrieu, N., Maxa, J., Mahmoud, M. Ben, Larrieu, N., Routing, U., Maxa, J., Slim, M., Mahmoud, B. ve Larrieu, N. (2017). Survey on UAANET Routing Protocols and Network Security Challenges To cite this version : HAL Id : hal-01465993 Survey on UAANET Routing Protocols and Network Security Challenges. *Ad Hoc ve Sensor Wireless Networks*.

77. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M. ve Brooks, R. (2006). The sleep deprivation attack in sensor networks: Analysis and methods of defense. *International Journal of Distributed Sensor Networks*, *2*(3), 267–287.

78. Sen, S., Clark, J. A. ve Tapiador, J. E. (2015). Security Threats in Mobile Ad Hoc Network. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology*, *1*(2), 1–22.

79. Daniel, A. (2014). A Survey on Detection of Sinkhole Attack in Wireless Sensor Networks. *International Journal of Computer Science and Information Security, 13(5):1-9*.

80. Edemacu, K., Euku, M. ve Ssekibuule, R. (2014). Packet Drop Attack Detection Techniques in Wireless Ad Hoc Networks: A Review. *International Journal of Network Security ve Its Applications*, *6*(5), 75–86.

81. Sedjelmaci, H., Senouci, S. M. ve Messous, M. A. (2016). How to detect cyber-attacks in unmanned aerial vehicles network? *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*.

82. Sen, S. ve Clark, J. A. (2009). *Intrusion Detection in Mobile Ad Hoc Networks*. 427–454.

83. Bitter, C., Elizondo, D. A. ve Watson, T. (2010). Application of artificial neural networks and related techniques to intrusion detection. *Proceedings of the International Joint Conference on Neural Networks*.

84. Sen, S. ve Clark, J. A. (2011). Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. *Computer Networks*, *55*(15), 3441–3457.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyad, Ad	:CEVİZ, Özlem
Uyruğu	: T.C.
Doğum tarihi ve yeri	:
Medeni hali	:
Telefon	:
Faks	:
e-mail	:

Eğitim

Yüksek lisans	SBTÜ/ Savunma Teknolojileri	2022
Lisans	Erciyes Üniversitesi / Bilgisayar Mühendisliği	2017
Lise	Hasanoğlan Atatürk AÖL	2012

İş Deneyimi

Yıl	Yer	Görev
2019-Halen	Sivas Bilim ve Teknoloji Üniversitesi	Araştırma Görevlisi
2017-2019	Boytaş A.Ş.	Yazılım Mühendisi

Yabancı Dil

İngilizce

Yayınlar

1) Ceviz, Ö., Sadioğlu, P., Şen S. (2021). Analysis of Routing Attacks in FANETs, *EAI ADHOCNETS*

Hobiler

Teknoloji, Yüzme, Müzik

KÖKLERDEN GÖKLERE…