
**T.C.**
**DÜZCE ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# AOMDV PROTOKOLÜNDE BLACK HOLE ATAKLARA KARŞI GELİŞTİRİLMİŞ GÜVENLİK UYGULAMASI

**AZİZ AYDIN**

**YÜKSEK LİSANS TEZİ**
**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**DANIŞMAN**
**YRD. DOÇ. DR. SİNAN TOKLU**

**Ekim-2016**

**T.C.**
**DÜZCE ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# AOMDV PROTOKOLÜNDE BLACK HOLE ATAKLARA KARŞI GELİŞTİRİLMİŞ GÜVENLİK UYGULAMASI

Aziz AYDIN tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

**Tez Danışmanı**

Yrd. Doç. Dr. Sinan TOKLU

Düzce Üniversitesi

**Jüri Üyeleri**

Yrd. Doç. Dr. Sinan TOKLU
Düzce Üniversitesi _____

Doç. Dr. Resul KARA
Düzce Üniversitesi _____

Yrd. Doç. Dr. İbrahim Alper DOĞRU
Gazi Üniversitesi _____

Tez Savunma Tarihi: 03/10/2016

# BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

03 Ekim 2016 (Tarih)

(İmza)

Aziz AYDIN

*Sevgili Aileme*

# TEŞEKKÜR

Yüksek lisans öğrenimim ve bu tezin hazırlanmasında süresince gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Yrd. Doç. Dr. Sinan TOKLU'ya en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili aileme ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

**03 Ekim 2016** **Aziz AYDIN**

**İÇİNDEKİLER** **Sayfa**

# ŞEKİL LİSTESİ

# ÇİZELGE LİSTESİ

# SİMGELER VE KISALTMALAR

| | |
|---|---|
| AOMDV | Ad hoc On-demand Multipath Distance Vector |
| AODV | Ad hoc On-demand Distance Vector |
| Black hole | Networking, a packet drop attack |
| CBR | Constant Bit Rate |
| DSDV | Destination Sequenced Distance Vector |
| DSR | Dynamic Source Routing |
| IP | Internet Protocol |
| MAC | Medium Access Control |
| MANET | Mobile Ad hoc Networks |
| NS 2 | Network Simulator 2 |
| OTcl | Object Tcl |
| RREP | Route Reply |
| RREQ | Route Request |
| QoS | Quality of Service |
| TCP | Transmission Control Protocol |

# ÖZET

## AOMDV PROTOKOLÜNDE BLACK HOLE ATAKLARA KARŞI GELİŞTİRİLMİŞ GÜVENLİK UYGULAMASI

Aziz AYDIN
Düzce Üniversitesi
Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Yrd. Doç. Dr. Sinan TOKLU
Ekim 2016, 44 sayfa

İletişimin büyük kısmını oluşturan kablosuz ağların kullanımı hızlı bir şekilde artmaktadır. Kablosuz ağların bir kolu olan tasarsız ağlar da akademik çevrede ilgi çeken bir çalışma alanıdır. Tasarsız ağlar sıklıkla hareketli düğümlerden oluşan alt yapısız kablosuz ağlardır. Tasarsız ağlarda düğümler hem diğer düğümlerle iletişim kurabilirler hem de paketleri ileterek yönlendirici görevi üstlenirler. Bu ağlar arama kurtarma, ofis, kampüs, konferans salonu, üniversite ve şehir ağlarında kullanılmaktadır. Tasarsız ağlarda düğümlerin hareketli olması, bir altyapının mevcut olmaması, bant genişliğinin ve güç kapasitesinin sınırlı olması bu ağların en önemli sorunlarındandır. Düğümlerin hareketliliği topolojinin hızlı bir şekilde değişmesine ve kurulan yolların bozulmasına neden olmaktadır. Topolojinin sık sık değişimi etkili bir yönlendirme protokolünün kullanımını gerektirmektedir. Bu ağların değişken, çok adımlı topolojiye sahip olması, düğümlerin hareketli olması ve kablosuz ağdan kaynaklanan sorunlar çok sayıda probleme neden olmaktadır.

Bu çalışmada, ağın güvenliğini bozacak black hole ataklar tasarlayıp, ağın güvenirliğini artıracak güvenlik uygulaması geliştirilmiştir. Çalışmada tasarsız ağlarda kullanılan en güncel protokollerden birisi olan AOMDV protokolü kullanılmıştır. Bu amaçla, güvenlik uygulamasında senaryolar üretilmiş olup, daha sonra da bu senaryolardan yararlanılarak AOMDV protokolünde güvenlik uygulamasının yapısı oluşturulmuştur. Çalışmada simülasyon aracı olarak Network Simulator (NS 2) programının 2.35 sürümü ve diğer ağ simülasyon yazılımları için yardımcı programlar olan tracegraph202, APP-Tool-master grafik yazılımları kullanılmıştır.

**Anahtar sözcükler:** AOMDV, Manet, Black hole, AODV

# ABSTRACT

## IN PROTOCOL AOMDV IMPROVED SECURITY APPLICATION AGAINST THE BLACK HOLE ATTACKS

Aziz AYDIN
Duzce University
Graduate School of Natural and Applied Sciences, Department of Computer Engineering
Master of Science Thesis
Supervisor: Assist. Prof. Dr. Sinan TOKLU
October 2016, 44 pages

The use of wireless network forming the major part of the communication is increasing rapidly. Which is a branch of wireless ad hoc networks is also a work area that attracts attention in academic circles. Ad-hoc networks are typically composed of mobile nodes lower unstructured wireless networks. In ad-hoc network nodes can communicate with other nodes as they undertake the task of the router transmits both packages. These networks are search and rescue, office, campus, conference hall, university and city are used in the network. Be mobile nodes in ad-hoc networking, the absence of infrastructure, limited bandwidth and power capacity of the most important problem of this network. The topology of the nodes mobility leads to deterioration of rapid change and established ways. frequent changes of the topology requires the use of an effective routing protocol. variables of this network possess multistep topology is movable nodes and the problems arising from the wireless network causes many problems.

In this study, the design of black hole attacks to disrupt network security, is a security application that will increase the reliability of the network developed. Most of the current protocols used in networks tasarsiz study, which is one of AOMDV protocol was used. For this purpose, scenarios are being produced in a security application, and then utilizing the aomdv Protocol security in these scenarios the structure of the application has been established. In the study as a simulation tool the network Simulator (ns-2) Version 2.35 of the program, and other network utilities for the simulation software tracegraph202 app-tool-master software was used for graphics.

**Keywords:** AOMDV, Manet, Black hole, AODV

# 1. GİRİŞ

Tasarsız ağlardaki geleceğe dönük uygulamalar araştırmalarda büyük önem kazanmıştır. Tasarsız ağlar bir grup hareketli ya da hareketsiz düğümün bir araya gelerek oluşturduğu çok adımlı, önceden kurulmuş bir altyapıya sahip olmayan kablosuz ağlardır. Bu ağlardaki düğümler genelde hareketli olmakla beraber sabit düğümler de içerebilirler. Altyapılı ağlardaki gibi bir merkezi bir yönetim bulunmamaktadır. Düğümler hem yönlendirici görevini üstlenirler hem de diğer düğümlerle iletişim kurarlar. Ağ altyapısız olduğundan düğümler istedikleri gibi hareket edebilirler, bu durum ağın hizmet dışı kalmasına sebep olmaz. Tüm düğümler birbirlerinin kapsama alanında bulunamayacaklarından iletişim çok adımlıdır.

Tasarsız ağlar topoloji değişimlerine kolay uyum sağlayabilirler. Herhangi bir düğüm kurulan yoldan çıktığında durum fark edilir ve yeni bir yol kurma süreciyle iletişime kalınan yerden devam edilir. Bu durum gecikmeye sebep olsa da ağ hala iletişime imkan tanımaktadır. Tasarsız ağlardaki düğümlerin güç kaynakları, işlemci kabiliyetleri, saklama kapasiteleri ve bant genişlikleri kısıtlıdır. Güç kaynağının kısıtlı olması düğümlerin kapsama alanlarını sınırlandırmaktadır. Düğümlerin hareketli olması ağırlıklarına sınırlamalar getirmektedir. Bant genişliğinin sınırlı olması da tasarsız ağlarda gönderilecek kontrol mesajlarının sıklığına ve miktarına kısıtlamalar getirmektedir. Tasarsız ağlarda başarılı bir iletişim oluşabilmesi için bu kıt kaynakların etkin olarak kullanılabilmesi gerekmektedir.

Tasarsız ağların birçok kullanım alanı vardır. Bu alanlar askeri, arama kurtarma, polis, konferans, duyarga ağ uygulamaları, kişisel alan ağları (PAN), üniversite, kampüs ve şehir ağları olabilir. Ağ altyapısının kurulmasının fiyat ve ortamın uygunluğu açısından tercih edilmediği durumlarda da tasarsız ağlar kullanılabilir. Özellikle arama kurtarma ve askeri çalışmalarda altyapısız bir sisteme ihtiyaç duyulmaktadır. Bir havaalanında ya da bir konferans salonunda haberleşmek isteyen gruplar da kablosuz ağ arayüz kartlarını kullanarak tasarsız ağ oluşturabilirler. Kişisel alan ağları uygulamalarında ise hareketli ve hareketsiz cihazlar tasarsız olarak örneğin bir ev ağı oluşturabilirler. Tüm uygulama alanlarının yönlendirme protokollerinden kendilerine has istekleri ve ihtiyaçları vardır. Duyarga ağ uygulamaları minimum enerji tüketimi isterken konferans uygulamaları gerçek zamanlı uygulamalar servis kalitesine önem

vermektedirler. Tasarsız ağlarda kullanılan iletişim ortamının da -radyo haberleşmesi- kendine has özellikleri vardır. Örneğin, düğümler arasındaki bağlantılar tek yönlü olabilir. Bunun sebebi iki düğümün ileticilerinin güçlerinin farklılığı yüzünden sadece birinin diğerini duyabilmesi ya da ortamdaki gürültü olabilir. Çok adımlı iletişim yapılması hem güçte hem de iletim kapasitesinde yüksek kazançlara yol açmaktadır. Böylece düğümler paketleri çok daha az çıkış gücüyle çok adımda gönderebilmektedirler.Tasarsız ağların daha karmaşık uygulamalarda kullanılmasıyla, servis kalitesine (QoS) olan ihtiyaç artmaktadır. Bu ağların kullanılması ise güvenlik gereksinimlerini ortaya çıkarmıştır. MANET'te gömülü bir güvenlik tasarımı yer almadığından ataklara karşı savunmasız yapıdadır. Dolayısıyla kablosuz kanal hem ağdaki kullanıcılara hem de ağda yeralan kötü niyetli kullanıcılara erişilebilir durumdadır. Güvenlik Ad hoc ağlarda ki en önemli konulardan biridir. Ad hoc ağlardaki en yaygın ataklar ağdan gönderilen paketlerin kötü niyetli düğümler tarafından yok edilmesi ve gelen paketlerde kötü niyetli düğümlerin değişiklik yaparak ağda karışıklığa yol açması ve ağın performansının düşürülmesinin hedeflenmesidir. MANET paylaşılan kablosuz ağ ortamı vasıtasıyla hareketli düğümlerin birbiriyle iletişim isteğinde bulunduğu bir yapıya sahiptir.

Bu tezin temel amacı tasarsız ağların önemli bir sorunu olan güvenlik konusunda tasarsız ağlardaki güncel protokollerden biri olan AOMDV protokolü kullanılarak, ağda black hole saldırısı yaratmak ve düğümlerin ağa katılımıda ki hız parametreleri dikkate alınarak senaryolar üretip kötü niyetli düğümlere karşı ağda daha iyi performansın elde edilmesi için güvenlik uygulaması geliştirilmektedir. Güvenlik uygulaması senaryolarında kötü niyetli düğüm karşısında ağda düşen paketlerin azalması ve ağın performansının arttığı ortaya çıkmıştır. Yapılan simülasyonlar sonucunda önerilen güvenlik uygulamasının düğümlerin ağa katılım hızlarının değişkenlik gösterdiği durumlarda performanslarının daha yüksek olduğu belirlenmiştir.

İkinci bölümde konunun daha iyi kavranması için altyapısız, altyapılı ve karma kablosuz ağların genel yapısı ve uygulama alanları anlatılmaktadır. Tasarsız ağlarda yönlendirme protokollerinin sınıflandırılma bilgileri, AODV protokolü ve önerilen güvenlik uygulamasının uygulandığı AOMDV protokolü de bu bölümde ayrıntılı olarak açıklanmaktadır.

Üçüncü bölümde tasarsız ağlarda güvenlik konusunun incelendiği ve güvenlik önlemleri ağ katmanlarına göre açıklanmıştır. Tasarsız ağlarda güvenliği bozacak dos atakları araştırılmıştır. Güvenlik uygulamasında güvenliği bozacak black hole saldırısı detaylı şekilde anlatılmıştır.

Dördüncü bölüm AOMDV protokolünde blackhole saldırısı gerçekleştirmenin aşamaları açıklanmıştır. Sonrasında kötü niyetli düğümün paket kaybını azaltacak güvenlik uygulamasının akış diagramı çıkarılarak diagram üzerinden tasarım yapısı detaylandırılmaktadır.

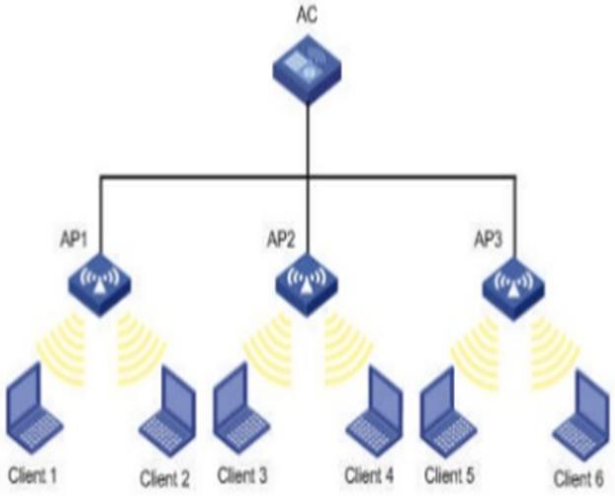
Beşinci bölüm önerilen güvenlik uygulamasının senaryolarını, performans kriterlerini ve simülasyonların sonuçlarını içermektedir. Bölümün son kısımda tezde yapılan iş özetlenmekte ve sonucu belirlenmektedir.

# 2. GEZGİN TASARSIZ AĞLAR

## 2.1. ALTYAPILI KABLOSUZ AĞLAR

Altyapılı ağ topolojisinde sıklıkla kablolu bir şekilde oluşturulan altyapı ve mobil cihazlar üzerinden iletişim yapılmaktadır. Altyapılı kablosuz ağ topolojisi geniş kapsama alanlarında ve çok sayıda baz istasyonuyla beraber kullanılmaktadır. Altyapılı ağlarda ağı kontrol etmek için bir erişim noktası yer alır. Baz istasyonu (base station) veya erişim noktası (access point) sayısı kapsama alanının genişliğine çok sayıda olabilir. Erişim noktaları cihazların birbiriyle iletişimlerinde denetlenebilmelerini sağlar. Kurulan ağ topolojilerinde en sık kullanılan ağ yapısı altyapılı ağlardır [3].

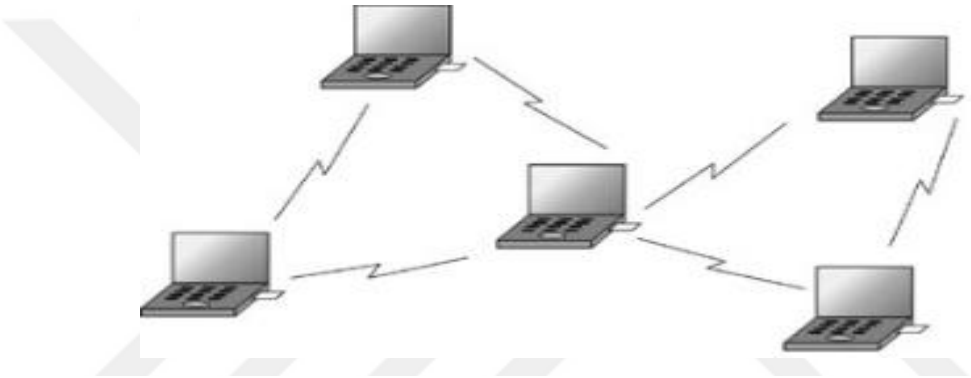
Ağlarda kapsama alanını genişletmek için başvurulan ağ yapısı altyapılı ağlardır. Günümüzde kullanılan mobil cihazlar baz istasyonları ile etkileşim içerisinde bulunmaktadır. Baz istasyonu, iki yönlü bir mobil ağ sisteminde yayın yapmaktadır. Cep telefonu teknolojileri altyapılı ağlar ile çalışır. İletişimin sağlanabilmesi ve hareket durumunda konuşmanın yapılabilmesi için çok daha fazla sayıda baz istasyonu gerekmektedir. Nüfusun yoğun olduğu bölgelerde baz istasyonların sayısı daha fazladır. Bu bölgelerde yüksek yapılar ve engeller radyo dalgalarının yayılmasını engel olur.




Şekil 2.1. Altyapılı kablosuz ağ örneği.

## 2.2. ALTYAPISIZ KABLOSUZ AĞLAR

Gezgin tasarsız ağlar (Mobil Ad-hoc Networks - MANET) kendi kendine organize olabilen, otonom bir yapıya sahip ağlardır. Ağ oluşturmak için erişim noktasına ihtiyaç duymayan düğümlerin ağda konumlanabildiği bir yapıya sahiptir. Ağdaki düğümler diğer düğümlerle iletişim içerisindedir. Bu tür ağlarda merkezi yapı olmadığı için her dğüm yönlendirici görevi görmektedir. Düğümlerde hareketlilik çok fazla olduğundan ağ topolojisinde beklenmeyen değişimler olmaktadır.



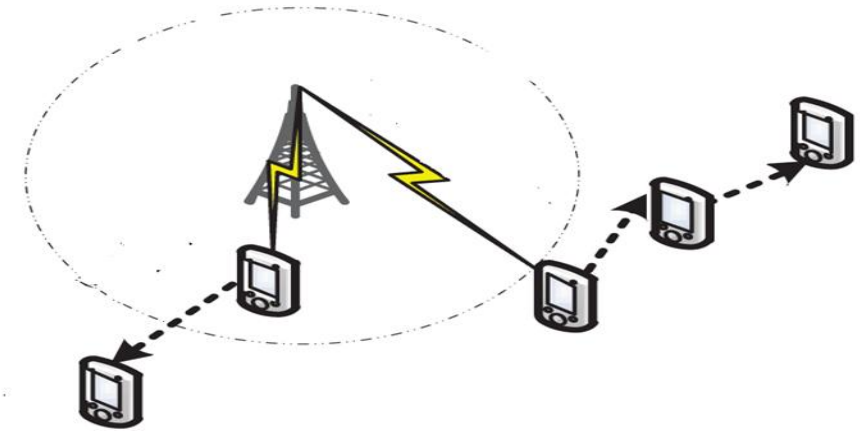
Şekil 2.2. Altyapısız kablosuz ağ örneği.

Birden fazla düğümün eşler arası bağlantı ile birbirine bağlanması sonucu en küçük kablosuz ağ yapısı oluşturulmaktadır. Bu ağlarda erişim noktası yer almadığından geçici olarak ağ kurulur. Bundan dolayı bu ağlara geçici ağlarda denir.

Geçici ağların erişim noktası olmadığından ağ yapılandırma ayarlarına gerek kalmamaktadır. Fakat bant genişliğinin ve düğümlerin enerjilerinin kısıtlı olması geçici ağların dezavantajlarıdır. Ayrıca geçici ağlarda iletişimi kontrol edecek bir cihaz olmadığı için bağlantı kalitesi azalmaktadır [3].

## 2.3. KARMA KABLOSUZ AĞLAR

Altyapılı ve altyapısız kablosuz ağların ortak yapıda kullanılmasıyla oluşmaktadır. Baz istasyonlarının erişemediği noktalarda karma kablosuz ağlar kullanılır. İnternet gibi ağlara erişilebilmesini baz istasyonları sağlayabilmektedir.



Şekil 2.3. Karma kablosuz ağ örneği.

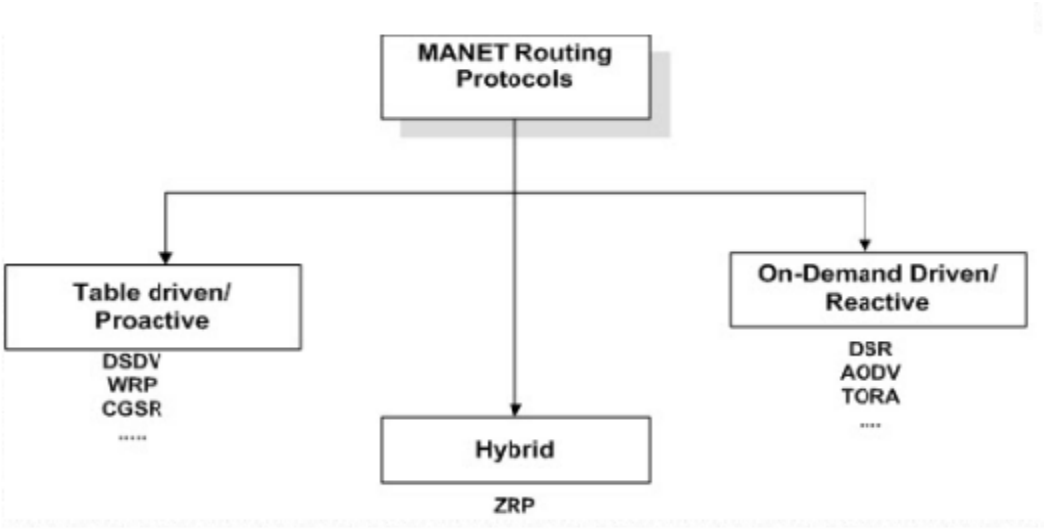
## 2.4. MANET'DE YÖNLENDİRME PROTOKOLLERİNİN SINIFLANDIRILMASI

Tasarsız ağlardaki protokoller ağın stratejisine ve ağ yapısına göre üçe ayrılmaktadır.

- Proaktif Protokoller
- Reaktif Protokoller
- Hybrid Protokoller

Yönlendirme protokolleri, düğümlerin iletişimleri sırasında yönlendirme tablolarının hazırlanmasına göre sınıflandırılmaktadır. Tasarsız ağlardaki protokollerin çoğu iki kategori altında yer almaktadır.

- Mesafe Vektörü Yönlendirme (Distance Vector Routing)
- Bağlantı Durumu Yönlendirme (Link State Routing)




Şekil 2.4. Yönlendirme protokollerinin sınıflandırılması.

### 2.4.1. Proaktif Yönlendirme Protokolleri

Proaktif protokoller yönlendirme bilgisinin gerekmediği durumlarda da düğümler tarafından kayıt altına alınmaktadır. Her düğüm tüm düğümlerin yol bilgilerini tutmaktadır. Düğümlerin yol bilgisi yönlendirme tablolarında tutulmaktadır. Topoloji değiştikçe yönlendirme tabloları güncellenecektir. Bu protokolün özelliği yönlendirme bilgisi öncesinde hazırlanmıştır. Yönlendirme bilgisinin tablolarda güncel tutulmasının getireceği yük geniş ağlarda bu protokolünün kullanılması zorlaştırmaktadır. Tablolardaki yüklerden dolayı ağda bant genişliğinin kullanımı fazla olacaktır [2], [4].

### 2.4.2. Reaktif Yönlendirme Protokolleri

Reaktif yönlendirme protokollerde yönlendirme bilgisinin tablolarda tutulmasının zorunluluğu yoktur. Yönlendirme olduğunda hedef düğüme doğru bir yöneliş olmaktadır. Hedef düğüme paket ulaşana kadar yön bilgisine ihtiyaç devam edecektir. Bu yönlendirme protokolü düğümler tarafından yol ihtiyacı olduğunda yol bilgisi tablolarda saklanmaktadır. Düğümler hedef düğüme gitmek istediklerinde yol bilgisi düğümler üzerinden yayılır. Bu keşif işlemi ihtiyaç duyulduğunda başlatılır. Yol bilgisi tespit edildikten sonra keşif işlemi sona erer. Yol bilgisi bozulmadığı sürece paketlerin iletilmesi bu yol üzerinden gerçekleşir. Düğümler arasında iletişim bulunmadığı sürece yol bilgisi kurulmasına gerek duyulmamaktadır. Geniş ağlarda proaktif protokollere göre daha çok tercih edilmektedir. Ağın yoğun olması durumunda performas düşebilmektedir. Düğümler ağda yol bulabilmek için düğümler ağa hızlı şekilde yayılım

gösterecektir. Dolayısıyla ağda tıkanıklık olacaktır. Diğer bir dezavantajı ise ağda yol bulabilmek için gecikmelere neden olmaktadır [1], [2].

### 2.4.3. Hybrid Yönlendirme Protokolleri

Proaktif ve reaktif protokollerin iyi özelliklerinin kombinasyonundan oluşmaktadır.

### 2.4.4. Mesafe Vektörü Yönlendirme

Mesafe vektörü yönlendirme basit dağıtılmış yönlendirme protokolüdür. Mesafe vektörü yönlendirmede yönlendiriciler ağa otomatik olarak dağılırlar. Hedefe en kısa yoldan ulaşabilmek için ağda rota keşfi başlatılmaktadır. En kısa yol her bağlantı için ilişkili metrikler veya maliyetlere dayalı hesaplanır. Mesafe vektör yönlendirmesinde mesafeye göre belirli bir hedefe giden en iyi yolu bulmak için yolun metrik gecikmesi, kayıp paketler veya benzer bir şeyle ölçülebilmektedir. Fakat mesafe genellikle atlama ile ölçülür. Belirli bir ağda atlama sayısı az olan güzergahlarda atlama sayısının az olması hedefe giden en iyi yol olduğu sonucuna varılmıştır. Mesafe vektörü yönlendirme kullanan bir yönlendirici düzenli olarak tüm arayüzler üzerinden uzaklığı vektör olarak gönderir. Mesafe vektörü bilinen her hedefe doğru mesafeyi gösterir. Yönlendiricilerde genellikle ulaşılabilir hedefler hakkında bilgi içeren veri yapısının korunması gerekmektedir. Veri yapısı yönlendirme tablosudur. Yönlendirme tablosu giden arabirimi, atlama ve ek özellikleri bir dizi hedef ile ilişkilendiren veri yapısıdır. Farklı yönlendirme protokolleri her hedef için farklı özellikleri ilişkilendirebilirsiniz. Mesafe vektör yönlendirme protokolleri kısa yoldan hedefe ulaşmak için maliyet saklayacaktır. Ağ topolojilerinde en çok tercih edilen RIP, EGP, BGP ve IGRP protokolleridir [4].

### 2.4.5. Bağlantı Durumu Yönlendirme

Bağlantı durumu protokolleri de en kısa yol protokol yapısına sahiptir. Bağlantı durumu yönlendirme protokollerinde ağ topolojisinde eksiksiz bir tablo vardır. Her bağlantı durumu yönlendirmesi etkin yönlendirici üzerinde oluşturulur. Bu tablo doğrudan bağlı olduğu komşuları hakkında ayrıntıları ve ağ topolojisini tutmak için kullanılır. Her etkin yönlendirici periyodik olarak bağlantıların her birini bir “hello” mesajı gönderir. Komşu yönlendiriciler kendilerini tanıtacak bu “hello” iletilerini yanıtlarlar. Yapılan testler komşularının her maliyetini ölçmek için tüm yönlendiriciler üzerinde gerçekleştirilir. Maliyet uçtan uca gecikme protokolde bir verim ölçüsüdür [4].

## 2.5. PROAKTİF VE REAKTİF YÖNLENDİRME PROTOKELLERİNİN KARŞILAŞTIRILMASI

Yönlendirme protokollerinin kullanımı ağ topolojisine göre değişkenlik göstermektedir.

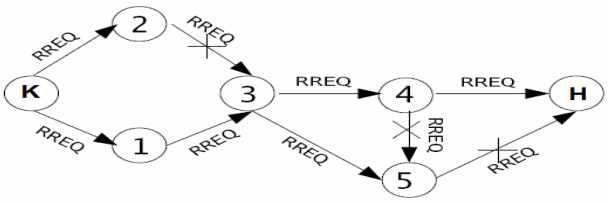
Çizelge 2.1. Yönlendirme protokollerinin karşılaştırılması.

| Tipi | Karakteristikleri | Örnekler |
|---|---|---|
| Proactive (Table-driven) | Yönlendirme istekleri öncesinden hesaplanır. Yönlendirme bilgisi periyodik olarak güncellenir. | DSDV, OLSR, WRP, CGSR, FSR |
| Reactive (On-demand) | Yönlendirme talep edilmesi durumunda tespit edilir. Yönlendirme bilgisinin yayılmasına gerek duyulmamaktadır. | AODV, AOMDV, DSR, ACOR, ABR |
| Hybrid | Proactive ve reaktif protokollerin iyi özelliklerinin kombinasyonundan oluşmaktadır. | TORA, ZRP, ARPAM, OORP, HSR, CGSR, LANMAR |

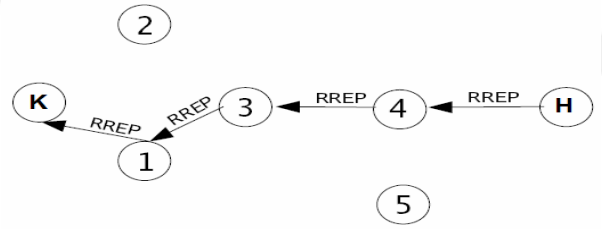
## 2.6. AODV (AD HOC ON-DEMAND DİSTANCE VECTOR ) PROTOKOLÜ

Mobil ad hoc ağlar, mobil cihazlar için dinamik olarak değişen ağ topolojisine sahiptir. AODV protokolünde yön bilgisi düğümlerin yönlendirme tablolarında bulunmamaktadır. Düğümün hedefe düğüme giden yola ulaşabilmesi için kaynak düğüm tarafından topolojide rota keşfini başlatması gerekecektir. Düğümler rota keşfini başlatabilmek özel olarak oluşturduğu istek paketini tüm ağa gönderecektir. Topolojide döngülerin oluşmasını engellemek için RREQ paketlerine benzersiz sıra numarası

verilmektedir. Düğümler göndermiş olduğu RREQ paketlerinden sonra sıra numaralarını arttırmaktadır. Aynı sıra numarasına sahip paketler olabilmektedir. Bundan dolayı gelen paketin tekrar paketi olup olmadığına tespit etmek için paketi gönderen düğümün adreside kontrol edilmektedir. Hedef düğüme gelen RREQ paketleri aynıysa en eski sıra numarasına sahip paket atılır. Şekil 2.5'de tekrar paketlerinin atılması gösterilmektedir. Paketi alan hedef düğüm kaynak düğüme RREP cevap paketini gönderecektir. Komşu düğümlerde daha güncel yol bilgisi bulunuyorsa kaynak düğüme güncel paket gönderilecektir. Paketin güncelliğinin kontrolü sıra numarasına bakılarak tespit edilir. Şekil 2.6' da hedef düğümden kaynak düğüme gönderilen RREP paketleri gösterilmiştir [8].




Şekil 2.5. Yol Bulma Süreci.




Şekil 2.6. Hedeften Kaynağa Yol Oluşumu.

Protokolün reaktif olması sadece yol ihtiyacı olduğunda yol isteğinde bulunması ve iletişimde bulunmadığı düğümlere olan yolları tutmaması anlamına gelir. AODV, Dinamik Kaynak Yönlendirmesi (DSR) protokolünün yol keşif ve yol bakım, Varış Sıralı Uzaklık Vektörü (DSDV) protokolünün sıra numarası ve düğümden düğüme yönlendirme mekanizmalarını kullanır. DSR'deki gibi kaynak yönlendirme yapmak yerine ara düğümlerde dinamik olarak tutulan yönlendirme tabloları kullanır. Böylece büyük ağlarda veri paketlerinde tüm kaynak yolunu tutmaktan kaynaklanan sıkıntı aşılmış olur. AODV bu iki protokolün başarılı özelliklerini birleştirerek bantgenişliğini daha etkin kullanan, topolojik değişikliklere duyarlı ve döngülerden arındırılmış bir protokoldür.

AODV protokolünde her düğüm iletişimde bulunduğu diğer düğümlere olan yol bilgilerini bir yönlendirme tablosunda tutar. Bu tablonun her satırında aşağıdaki bilgiler tutulur:

- Varış adresi: iletişimde bulunulan düğümün adresi
- Varış sıra numarası: ilgili yolun varış sıra numarası
- Bir sonraki adım: Paketleri varışa iletmek için kullanılan bir sonraki düğüm
- Adım sayısı: Kaynaktan varışa olan yol üzerindeki düğüm sayısı
- Ömür: Yolun geçerli olacağı süre (milisaniye)
- Yayın no: Yol keşif sürecine özgü bir sayı
- Yönlendirme bayrakları: Yolun durumunu belli eder: kullanılıyor, kullanılmıyor, bozuk, vs.

Bir kaynak düğümü başka bir düğümle haberleşmek istediğinde yol istek paketini (RREQ) yayınlayarak yol bulma sürecini başlatır. RREQ paketi aşağıdaki gibidir.

RREQ [source_addr, source_sequence #, broadcast_id, dest_addr, dest_sequence #,hop_cnt ]

RREQ paketleri kaynak adresi (source_addr) ve yayın numarası (broadcast_id) ile ayırt edilir. Kaynak her yeni RREQ gönderdiğinde yayın numarası artırılır. Kaynak sıra numarası (source_sequence #) kaynağa olan geri yolun tazeliğini gösterir. Varış sıra numarası (dest_sequence #) varışa olan yolun kaynak tarafından Kabul edilmesi için ne kadar taze olması gerektiğini gösterir. RREQ paketini alan bir düğümün yönlendirme tablosunda varış için bir yol yoksa RREQ paketi yayınlanır ve kaynağa geri yol kurulur. Geri yol kurulurken kaynak için yönlendirme tablosuna bir kayıt eklenir.

RREQ paketini varışa yolu olan bir düğüm aldığında yönlendirme tablosuna bakılıp gelen paketteki ve tablodaki varış sıra numaraları karşılaştırılarak yolun taze olup olmadığına karar verilir. Eğer paketin sıra numarası RREQ paketindekinden daha büyükse ya da sıra numaraları eşitse ve adım sayısı daha küçükse bu RREQ daha önce değerlendirilmediyse pakete cevap verilir. Yol cevap paketi (RREP) aşağıdaki gibidir.

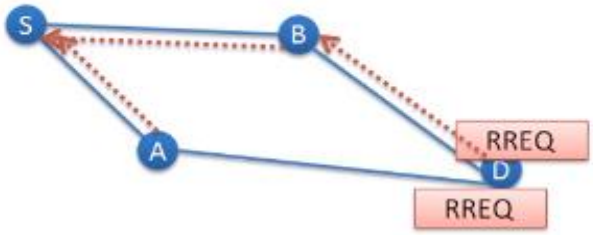
RREP [source_addr, dest_addr, dest_sequence #, hop_cnt, lifetime ]

Pakete cevap verilirken önceden kurulmuş olan geri yol izlenir. RREP paketini alan her düğüm RREP paketini aldığı komşunun adresini ve en son varış sıra numarasını kaydederek ileri yönde yol kurar. Yönlendirme tablosunun varış ve kaynakla ilgili kayıtlarının sona erme sürelerini de günceller. Eğer düğüm yeni RREP paketleri alırsa, ancak yeni RREP daha taze ya da aynı tazelikte ve daha az adım sayılı ise tablosunu günceller. Kaynak düğüm ilk RREP paketini alır almaz varışa veri paketlerini iletmeye başlar, zaman içinde daha iyi bir yol öğrenirse bu yolu bırakıp diğer yolu kullanmaya başlar.

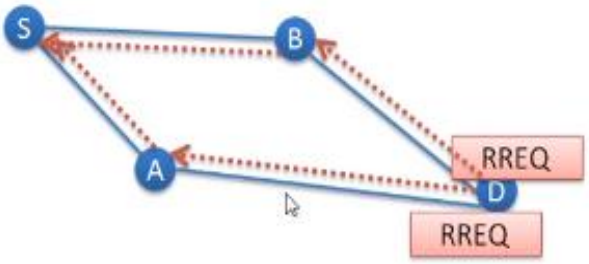
## 2.7. AOMDV (AD HOC ON-DEMAND MULTIPATH DISTANCE VECTOR ) PROTOKOLÜ

AOMDV protokolü Ad hoc ağlarda kullanılan en güncel protokollerden birisidir. Bu protokol DSDV protokolünden temel alınmıştır. AOMDV protokolünde on binlerce dinamik düğümden atlamalar yapılarak bir network sistemi yaratılabilmektedir. AOMDV protokolünde temel konsept yön bulma süreçlerinde birçok yolun üretilmesi ve hesaplanmasıdır. Bağlantının kopması ve genellikle yanlış yönlendirmelerin gerçekleşmesi dinamik bir yapıya sahip olan AOMDV protokolünde avantaj sağlamaktadır. Yönlendirmede tek yol kullanan AODV protokolü yönlendirmede herhangi bir yol kullanılmadığında yeni yol arayışına girmektedir. Bu durum her yol bulmada gecikmeye ve ağa yük getirisine neden olmaktadır. AOMDV protokolünde belirtilen verimsizliğin önüne geçmek için çoklu yol kullanılmaktadır.

AOMDV protokolünde kaynak düğüm ağa RREQ istek paketi yayar. Paketi alan ara düğüm yönlendirme tablosunu kontrol eder. Yönlendirme tablosunda hedef düğüme ulaşacak yol bilgisi mevcut ise kaynak düğüme geriye dönük RREP paketi gönderir. Hedef düğüme gidecek yol bilgisi yönlendirme tablosunda bulunmuyorsa komşu düğümlere RREQ paketi yaymaya devam edecektir. AODV Protokolünde paketi alan ara düğümde kopya RREQ paketleri oluştuğunda kopya RREQ paketlerden en geç gelen istek paketi göz ardı edilir. D hedef düğüme gelen geç gelen RREQ paketi atılır.AOMDV protokolünde kopya RREQ paketleri atılmaz. Her kopya işlenir. AODV ve AOMDV protokollerinde Şekil 2.7 ve Şekil 2.8'de kopya RREQ paketlerinin iletimi gösterilmiştir [5], [6].




Şekil 2.7. AODV protokolünde RREQ paketlerinin iletimi.



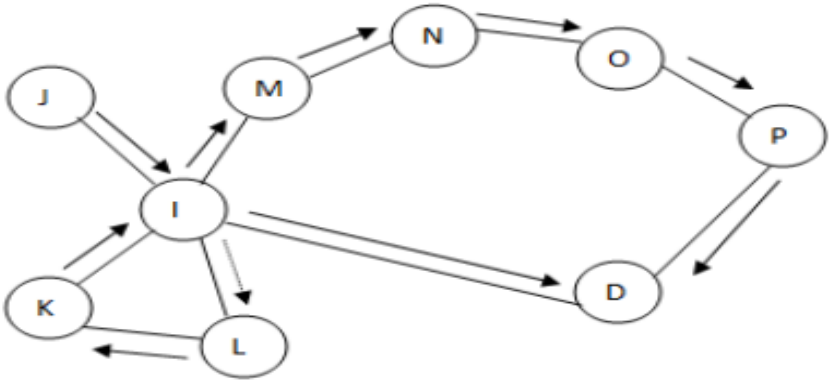

Şekil 2.8. AOMDV protokolünde RREQ paketlerinin iletimi.

### 2.7.1. Aomdv Protokolünün Loop Freedom Özelliği

AOMDV protokolünde hedef düğüme gelen paketler işlenmektedir. Gelen paketlerin çoklu olması, hedef düğümden gönderilen yayının diğer düğümlere birden çok yol sunması ve hangi yolların düğümlere ilan edilmesi ve düğümlerin hangi yolları kabul etmesi gerektiği sorusunu AOMDV protokolünün loop freedom özelliği belirlemektedir [5].

Döngüyü sağlayan koşullar aşağıda listelenmiştir:

1. Farklı sıra numarası: Hedef düğüme gelen farklı sıra numarasına sahip paketlerden AODV protokolünde olduğu gibi en eski sıra numarasına sahip paket döngüden kaçınmak için atılır.
2. Aynı sıra numarası: Atlama sayısı daha kısa olan yol seçilir. Daha kısa yol bulunmazsa seçilen kısa yoldan başka seçenek bulunmamaktadır.



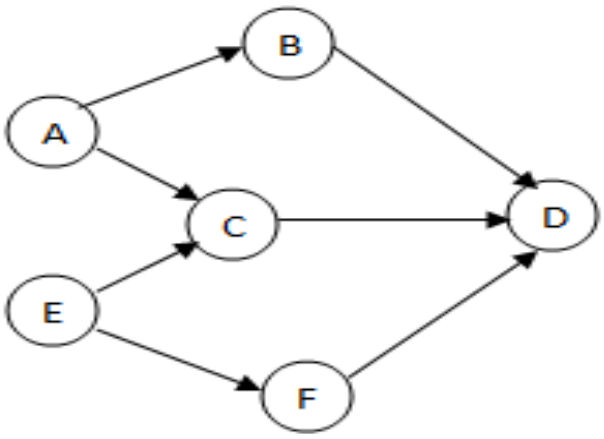

Şekil 2.9. loopfreedom yapısı örneği.

### 2.7.2. Aomdv Protokolünün Path Disjointness Özelliği

Hedef düğüme gidecek birden fazla ortak bağlantı bulunması ağda trafik oluşmasına ve tıkanıklığa neden olacaktır.Bundan dolayı ayrık düğüm ve linkler gereklidir.

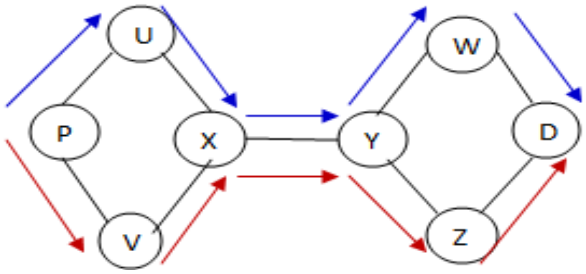
Şekil 2.9'da P den D ye giden yollar ayrıktır. Ağdaki tüm düğümler hedef düğüme ayrık yolllardan ulaşmaktadır. Bu durum ağda trafik veya tıkanıklığın önüne geçmektedir.

Şekil 2.10'da D hedef düğümdür. A ve E düğümlerinden D hedef düğüme 2 ayrık bağlantı görülmektedir. A-B-D, A-C-D, E-C-D ve E-F-D yolları kullanılarak hedef düğüme gidilmektedir. Fakat A-C-D ve E-C-D yolları ortak C-D bağlantısını kullandıklarından ayrık bağlantı değildir [5].



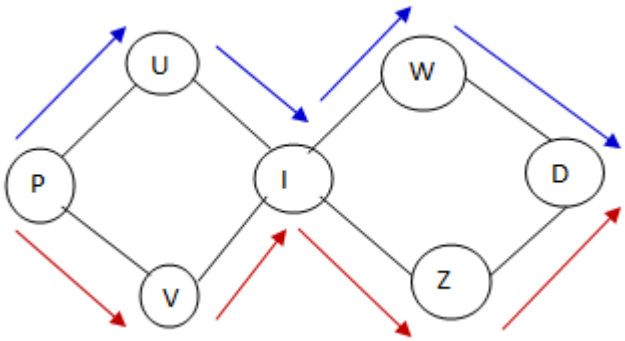

Şekil 2.10. Ağdaki tüm yollar ayrık olmayabilir.

Ayrık bağlantı sağlama koşulunun gerçekleşmesi sonraki atlama ve son atlamanın birbirinden farklı olmasına bağlıdır. Şekil 2.11'de P den D ye giden yolda X düğümü belirtilen koşulu sağlamamaktadır. Bu durumda P-U-X-Y-W-D veya P-V-X-Y-Z-D yollarından biri kullanılacaktır [5], [11].




Şekil 2.11. Ayrık bağlantı fikri.

Şekil 2.12' de hedef düğüme giden tüm yolların sonraki atlama ve son atlaması farklı olduğundan iki ayrık bağlantı görülmektedir [5].




Şekil 2.12. İki ayrık Bağlantı (P-U-I-W-D ve P-V-I-Z-D).

AOMDV protokolünde çoklu yol sayesinde RREP paketleri tüm düğümlere gönderilmektedir. Ad-hoc ağlarda bağlantı hataları hareketlilik, tıkanıklık, paket çakışmaları, düğüm ya da hop hataları vb. görülebilmektedir. Gönderilen paket yol boyunca bozuk bağlantıya rastladığında hedef düğümden kaynak düğüme doğru RRER paketi yayılır. Yeni bir yol düğümlerin yönlendirme tablolarından tespit edilerek paket akışına devam edilir. Tüm bağlantı yolları bozulduğunda yeni bir yol kurmak gerekecektir. AODV protokolünde bozuk bağlantıya rastlanıldığın da ağın kaynaklarını tüketerek yeni bir yol kurma arayışına gidilmektedir. AOMDV çoklu yol sayesinde bulunduğu ağın kaynaklarını daha verimli kullanabilmektedir.

# 3. TASARSIZ AĞLARDA GÜVENLİK

Tasarsız ağlarda güvenlik önemli ilgi alanlarından biridir. Altyapısal kablosuz ağlara göre MANET ataklara karşı daha savunmasız durumdadır. MANET ağlarda etkili güvenlik protokol tasarımının gerçekleştirilmesi zor bir görevdir. Bu durum MANET'in benzersiz özelliklerinden kaynaklanmaktadır. Radyo kanalı üzerinden paylaşılan yayın, güvensiz çalışma ortamı, belli bir merkezi düğümün olmaması, kullanıcılar arasındaki işbirliği eksikliği, kaynakların hazır bulunabilme durumu ve fiziksel eksiklikler protokol tasarımında karşılaşılan güçlüklerdir.

Ağ topolojisinin hareketli bir yapıya sahip olması tasarsız ağlarda bazı problemleri ortaya çıkarmaktadır. Tasarsız ağlarda merkezi bir erişim noktası yer almadığından güvenlik uygulamalarının geliştirilmesinde zorluk olarak karşımıza çıkmaktadır. Düğümler ağda rastgele konumlandıklarından dinamik olarak değişen ağ topolojisinde düğümlerin kaynakları yeterli omadığından ve herhangi bir güvenlik politikası bulunmadığından güvenlik açığı tasarsız ağlardaki önemli konulardan biridir [20].

Tasarsız ağlarda ağın varlığını koruyabilmesi ve ağda kesintilerin oluşmaması hedeflenmektedir. Ağda yaratılan Dos saldırılarının önüne geçmek ve ağın sürekliliğini sağlamak için güvenlik uygulamalarının geliştirilmesi gerekmektedir. Saldırılar her katmanda gerçekleşebilir. Bazı kötü niyetli düğümler ağın alt katmanlarında etkili olup, üst katmanlarda ağdaki hizmetleri aksatmaktadır [10].

Ağda iletilen paketlerin bütünlüğünün korunması gerekmektedir. Bundan dolayı kötü niyetli düğümlerin ağa sızmaları güvenirlik açısından istenmeyen durumdur. Kötü niyetli düğümlere karşı ağın katmanlarında alınan önlemler aşağıda belirtilmiştir.

Erişim noktası olmayan tasarsız ağlarda topolojide saldırıların tespit edilmesi düğümlerin giriş ve çıkış parametreleriyle sınırlıdır. Saldırı tespitinde kullanıların diğer yöntem topolojide kullanılan algoritmalardır. Düğümler ağı gözlemleyebildiği sürece etkilidir. Ağda kullanılan algoritmaların benzer olması durumunda saldırıdan şüphelenebilir. Bundan dolayı topolojiden çıkan saldırılar sadece dışarıdan olmayabilir. İçerden saldırılara karşı önlem alınması gerekmektedir [20].

Tasarsız ağlar dinamik bir yapıya sahip olduklarında diğer ağlara göre saldırılara karşı

daha savunmasız yapıdadır. Saldırılar daha çok ağın iletişimini kesmek yerine kötü niyetli düğümler tarafından ağda koas ve düzensizlik oluşturmak üzerine kuruludur. Bu saldırı şekli daha çok tasarsız ağların yapısını bozmak için kullanılan saldırı tipleridir.

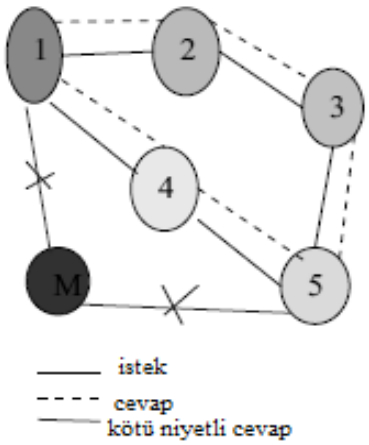
Ad-hoc ağlardaki geleceğe dönük uygulamalar araştırmalarda büyük önem kazanmıştır. MANET'te gömülü bir güvenlik tasarımı yer almadığından ataklara karşı savunmasız yapıdadır. Dolayısıyla kablosuz kanal hem ağdaki kullanıcılara hem de ağda yeralan kötü niyetli kullanıcılara erişilebilir durumdadır. Güvenlik Ad-hoc ağlarda ki en önemli konulardan biridir. Ad-hoc ağlardaki en yaygın ataklar ağdan gönderilen paketlerin kötü niyetli düğümler tarafından yok edilmesi ve gelen paketlerde kötü niyetli düğümlerin değişiklik yaparak ağda karışıklığa yol açmasından ağın performansının düşürülmesinin hedeflenmesidir. MANET paylaşılan kablosuz ağ ortamı vasıtasıyla hareketli düğümlerin birbiriyle iletişim isteğinde bulunduğu bir yapıya sahiptir. Bu yapı değişen ağ gereksinimlerine bağlı olduğundan yüksek derecede uyarlanabilmektedir. Herhangi bir düğümde iletişim sınırlandığında başka bir düğüm paketleri iletmek için yönlendirici olarak davranmaktadır. Düğümlerden biri kendi kaynağını paylaşmak istemediğinden diğer düğümler üzerinde fayda sağlamak için girişimde bulunabilir. Bu düğümler bencil düğümler olarak adlandırılır. MANET'te hareketli düğümlerin enerjisinin tükenmesinin başlıca nedenlerinden biri kablosuz iletimdir. Bencil düğümler enerjisini korumak için diğer düğümlere paket göndermeyi reddeder. MANET deki bencil düğümlerin etkisini azaltmak için çeşitli teknikler ileri sürülmüştür. Kaynak düğümden hedef düğüme paketleri göndermek için MANET'te optimum bir yol kurulmalıdır.

## 3.1.TASARSIZ AĞLARDA SALDIRI TİPLERİ

### 3.1.1.Black Hole Atak

Black hole atak Dos saldırı ataklarının türlerinden biridir. Uydurma yönlendirme bilgisi dağıtır ve üretir. Black hole saldırısında kötü niyetli bir düğüm uydurma yönlendirme bilgilerini gönderir. Kötü niyetli düğüm yönlendirme bilgisinin optimum olduğunu diğer düğümlere yayar. Saldırgan düğüm kaynak düğüme uydurma RREP paketi göndererek hedef düğüme giden daha iyi bir yol olduğunu iddia eder. Hedef düğüme gönderilen RREP paketindeki hedef sıra numarası RREQ paketindeki sıra numarasından daha büyük veya eşit uydurma numarasıdır. Saldırgan kaynak düğümün kendisi üzerinden

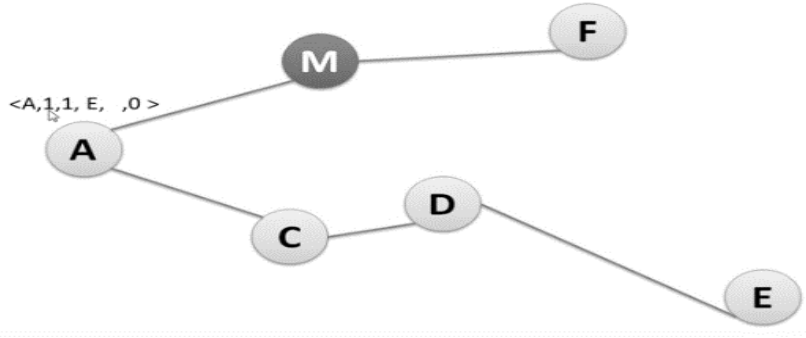
geçmesi gerektiği bilgisini yayarak ağdaki tüm trafiği yönetmektedir. Black hole örnek saldırısı Şekil 3.1' de gösterilmektedir [11].




Şekil 3.1. Black hole saldırısı.

Black hole atağı aşamalarla örneklendirilmiştir. A kaynak düğümü E hedef düğümüne veri göndermek istemektedir. Kötü niyetli düğümün (M) ağa etkisini tespit edilmiştir. Kaynak düğümde hedef düğüme gidecek yol bilgisi bulunmadığından, tüm komşu düğümlere istek paketi (RREQ) yayacaktır. Gönderilecek RREQ paketinin yapısı aşağıdaki bilgilerden oluşmaktadır. Kaynak düğümün adresi, kaynak düğümün adresi, broadcast numarası, hedef düğümün adresi, hedef sıra numarası ve atlama sayısından oluşmaktadır.

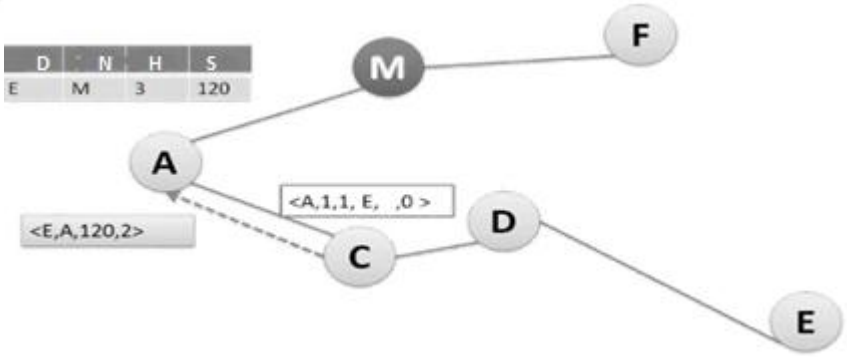
Kaynak düğüm RREQ paketini gönderdiğinde oluşacak RREQ paket içeriği <A,1,1,E, ,0> yapısında olacaktır. Komşu düğümlere gönderilen RREQ paket yapısı aşağıdaki şekilde gösterilmektedir.




Şekil 3.2. Komşu düğümlere gönderilen RREQ paket yapısı.

Paketi alan komşu düğümler (C,M) yönlendirme tablolarını kontrol edeceklerdir. C düğümü yönlendirme tablosunu kontrol ederek, E ye giden bir yol olduğunu belirlerse geriye dönük A düğümüne RREP paketi gönderecektir. Hedef düğüme giden yol bilgisi yönlendirme tablosunda mevcut değilse kaynak düğümden gelen bilgiyi yönlendirme tablosuna kaydedecektir. Komşu düğümlere istek paketi yaymaya devam edecektir.

Kötü niyetli düğüm paketi aldığında hedef düğüm bilgisinin kendisinde bulunduğu uydurma bilgisini kaynak düğüme RREP paketini göndererek belirtir. Kötü niyetli düğüm hedef düğüme kendisi üzerinden gidildiğinde daha az atlama sayısıyla ulaşabileceğini, RREP paketini kaynak düğüme göndererek, kaynak düğümden iletilen verinin kendisi üzerinden geçmesini istemektedir. Kaynak düğüme gönderilecek RREP paket yapısı hedef düğümün adresi, gelecek düğümün adresi, atlama sayısı ve hedef düğümün sıra numarasından oluşmaktadır. RREP paket içeriği <E,M,120,2> belirtildiği gibi olacaktır. RREP paketini alan kaynak düğüm şekil 3.3'de gösterilmektedir [10], [11].

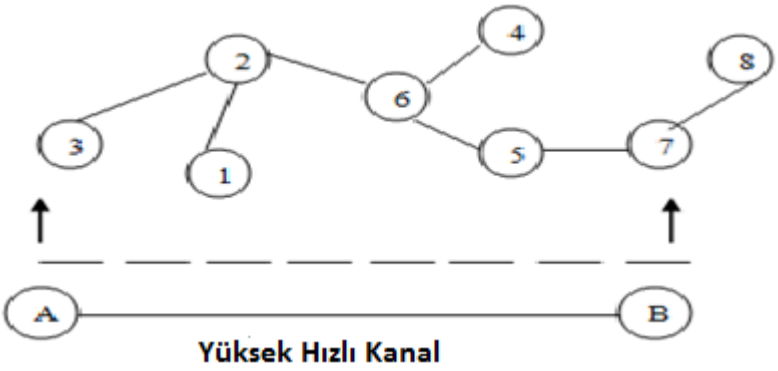



Şekil 3.3**.** RREP paketini alan kaynak düğüm örneği.

Kaynak düğüm RREP bilgisini aldıktan sonra veriyi M düğümüne gönderecektir. M düğümüne gelen paketler kaybolacaktır. Kötü niyetli düğüm amacına ulaşacaktır.

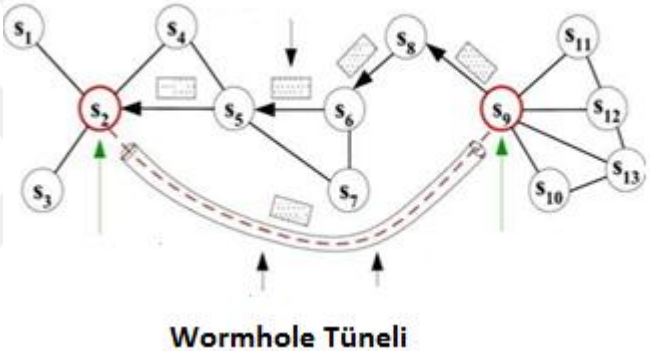
### 3.1.2. Worm Hole Atak

Wormhole atak MANET'teki en karmaşık ataklardan biridir. Bu atakta kötü niyetli düğümler bir çift tuzakla bir konumdaki paketleri kayıt altına alabilmektedir. Ataklar, yüksek hızlı özel bir ağ kullanarak farklı konumlarda yeniden tekrarlanabilmektedir. Wormhole ataklarının şiddetli bir atak olmasından yetkilerin ele geçirilmesi ve gizlilik konusunda ağdaki tüm iletişime karşı başlatılabilmektedir. Şekil 3.4'te reaktif yönlendirme protokollerine karşı Wormhole atak örneği gösterilmiştir [17].




Şekil 3.4. Wormhole atak örneği.

Wormhole atakla belirnenen konumlar arasında ethernet kabloları ve uzun mesafeli kablosuz yayınlar ile bağlantı kurulabilmektedir. Gönderilen paketler kurulan tünel aracılığıyla kayıt altına alınabilmektedir [5].



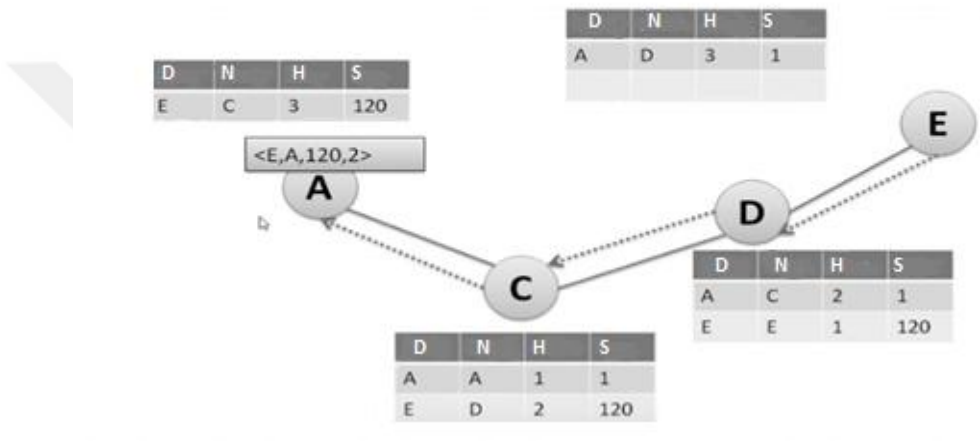

Şekil 3.5. Worm hole tüneli.

### 3.1.3. Gray Hole Atak

Gray hole atak Black hole atağın bir uzantısıdır. Grayhole atağın 3 atak tipi bulunmaktadır. Bunlardan ilk atak tipi düğümler tarafından gönderilen paketlerin kötü niyetli düğüm tarafından yok edilmesidir. İkinci tip atak olarak bir düğüm belirli bir süre için kötü niyetli davranabilir, ama daha sonra sadece diğer sıradan düğümler gibi davranmaktadır. Üçüncü atak bu iki atağın ortak görülebildiği atak tipidir. Belli bir zaman atağı yapacak olan düğüm normal bir düğüm gibi davranmaktadır. Ağda belli bir zaman sonra kötü niyetli düğüm gibi davranarak gelen paketleri yok etmektedir [12].

Grayhole atağı aşamalarla örneklendirilmiştir. A kaynak düğümü E hedef düğümüne veri göndermek istemektedir. Kötü niyetli düğümün (D) ağı etkilediğini ve atağı yapacak olan düğümün belirli bir süre sonra davranışını değiştirdiği tespit edilmektedir.

Kaynak düğümde hedef düğüme gidecek yol bilgisi bulunmadığından, tüm komşu düğümlere istek paketi (RREQ) yayacaktır. Komşu düğümün yönlendirme tablolarında hedef düğüme giden yol belli ise komşu düğüm geriye (RREP) paketi göndererek kaynak düğüm tarafından yol bilgisi alınarak veri akışı başlatılacaktır. Komşu düğümün yönlendirme tablolarında yol bilgisi mevcut değil ise komşu düğüm ağa yeniden RREQ paketi göndererek yayın yapmaya devam edecektir. Kötü niyetli düğüm bir süre ağdaki normal düğümler gibi davranarak ağda veri akışı başlayacaktır. Kötü niyetli düğüm kendisine gelen paketleri belli bir zaman geçtikten sonra yok edecektir [12], [11].




Şekil 3.6. Worm hole atak.

# 4. AOMDV PROTOKOLÜNDE BLACK HOLE ATAKLARINA KARŞI GÜVENLİK UYGULAMASI

Kötü niyetli düğümlerin ağdaki saldırısının tüm ağa etkileyecek düzeyde azaltılmasını önleyen, dinamik yapıdaki düğümlerin belirli hızlarla ağa katılımını sağlayan, ağ kaynaklarının verimsiz kullanımını azaltan güvenlik tasarımı önerilmektedir. AOMDV protokolünün çalışma yapısı incelenerek kötü niyetli ataklara karşı ağın güvenirliğini artıracak yöntemler araştırılmıştır. Çalışmada ağdaki data akışını bozabilecek düğümlerin ağ topolojisindeki karmaşıklık düzeyi incelenerek atakların etkisini azaltmaya dönük güvenlik uygulaması önerilmektedir.

## 4.1. AOMDV PROTOKOLÜNDE BLACK HOLE SALDIRISI YARATMAK

AOMDV protokolünde black hole atağını gerçekleştirebilmek için ağa kötü niyetli düğüm eklenmiştir. Kötü niyetli düğümün ağa etkisi incelenmiştir. Kötü niyetli düğüm üzerinden yol kurulmuş, bu yol üzerinden geçen paketler atılmıştır. Kötü niyetli düğüm bunu yapmak için hedefe gidecek yolun kendisi üzerinden daha az atlama sayısıyla ve daha büyük sıra numarasıyla komşu düğümlere yanlış cevap olarak göndermektedir. Komşu düğümlerden gelen paketler kötü niyetli düğüm tarafından atılmaktadır. AOMDV protokolüde diğer kablosuz yönlendirme protokolleri olan DSDV, AODV, DSR, HWMP vb. black hole saldırısına açıktır [5], [15].

1-) aomdv.h dosyasında kötü niyetli düğümü tanımlamak için malicious_black isminde değişken belirlenmiştir.

```
double          PerHopTime(aomdv_rt_entry *rt);

nsaddr_t malicious_black;
```

2-) aomdv.cc dosyasında başlangıçta değişkenin değeri 999 olarak belirlenmiştir. aomdv.cc dosyasında kötü niyetli düğümlere rastlanıldığında değişkenin değerini 1000 olarak set edilmiştir. Strncasecmp fonksiyonu içinde blackhole geçen düğümleri belirlemektedir. Belirlenen kötü niyetli düğüm bir sonraki adımda yanlış rota bilgisi göndermeye başlayacaktır.

```
Int

AOMDV::command(int argc, const char*const* argv) {
```

```
if(argc == 2) {
Tcl& tcl = Tcl::instance();
if(strncasecmp(argv[1], "blackhole", 9) == 0) {
 malicious_black=1000;
  return TCL_OK;
    }
AOMDV::AOMDV(nsaddr_t id) : Agent(PT_AOMDV),
btimer(this), htimer(this), ntimer(this),
rtimer(this), lrtimer(this), rqueue() {
aomdv_max_paths_ = 3;
bind("aomdv_max_paths_", &aomdv_max_paths_);
aomdv_prim_alt_path_len_diff_ = 1;
bind("aomdv_prim_alt_path_len_diff_", &aomdv_prim_alt_path_len_diff_);
index = id;
seqno = 2;
bid = 1;
LIST_INIT(&nbhead);
LIST_INIT(&bihead);
logtarget = 0;
AOMDVifqueue = 0;
 malicious_black=999;
}
```

3-) Kötü niyetli düğümün paketleri atabilmesi için ağa yanlış yön bilgisi cevabının verildiği kısım düzenlenmiştir.

```
else if(malicious_black==1000){

if (seqno < rq->rq_dst_seqno) {

seqno = rq->rq_dst_seqno + 1;

if (seqno%2)

seqno++;

sendReply(rq->rq_src,
                  0,
                   index,
                  seqno,
                  MY_ROUTE_TIMEOUT,
                   rq->rq_timestamp,
                   ih->saddr(),
                  rq->rq_bcast_id,
                   ih->saddr());

                  Packet::free(p);

 }
```

4-) .tcl uzantılı dosyamızda hangi düğümlerin kötü niyetli düğüm olduğunu belirliyoruz.

```
 $ns at 0.0 [$n(5) set ragent_] blackhole1
```

## 4.2. AOMDV PROTOKOLÜNDE KÖTÜ NİYETLİ DÜĞÜMÜN PAKET KAYBINI AZALTACAK GÜVENLİK UYGULAMASI

AOMDV protokolünde kötü niyetli düğümün davranışının ağın performasını düşürmesi ve ağdaki veri akışını bozması dolayısıyla paket kaybının artmasını engellemek için güvenlik uygulaması geliştirilmiştir. Düğümlerin ağa katılımında hareket özelliklerini kullanarak konumlanması ağın performansını artıracaktır. Düğümlerin ağa belirli hızlarla katılımında kaynak düğümün komşu düğümlere istek paketi göndermeleri, paketleri alan komşu düğümlerin yönlendirme tablolarını güncellemesi ve hedef düğüme gidecek yol bilgisi cevabı yer alan düğümlerin kaynak düğüme cevap paketini göndermesiyle veri akışı başlamaktadır. Kötü niyetli düğümün ağdaki davranışı incelendiğinde düğümlerin ağa katılımında belirli hızlarla yer almaları ve hedef düğüme gidecek sahte yönlendirme bilgisini kaynak düğüme kolayca gönderebilmektedir. Ağda düşük hızla konumlanan düğümler kötü niyetli düğümün

paketleri kaybetmesine neden olmaktadır. Düğümlerin hız parametrelerinin artırılması ağda kurulacak yapının belirsizliği dolayısıyla kötü niyetli düğümlerin sahte yol bilgisi göndermelerini zorlaştırmaktadır.

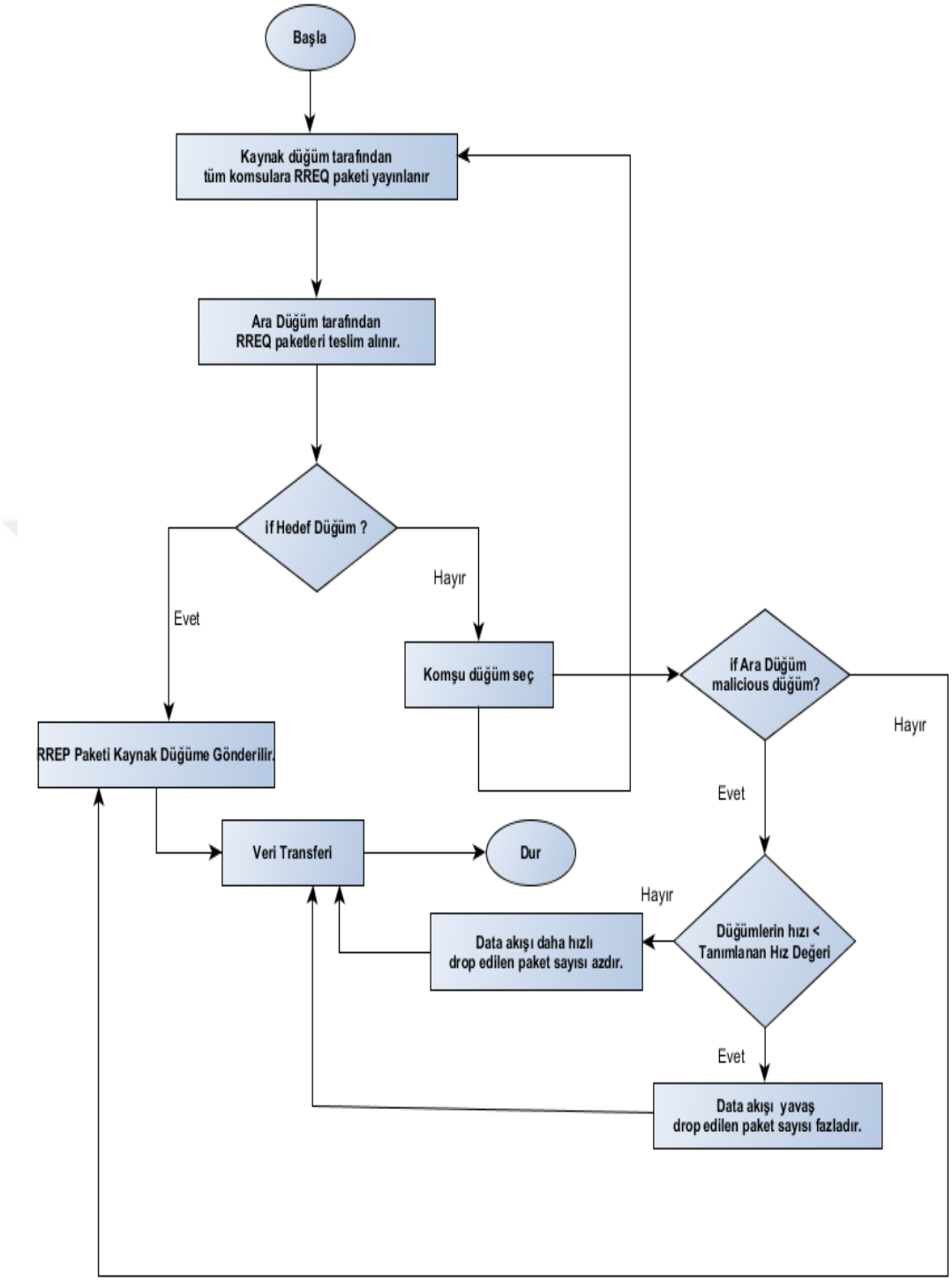
AOMDV protokolünde çoklu yol kullanıldığından hedef düğüme giden yollardan birisi bozulduğunda hedef düğüme ulaşan diğer yollar üzerinden data akışı devam etmektedir. AOMDV protokolünün bu yapısı ağda yeni bir yol kurma arayısı için zaman harcamaması düğümlerin ağda konumlanmasının, kötü niyetli düğümün davranışının hız parametresi üzerinde değerlendirebilmekteyiz.

Düğümlerin ağa katılım hız değerleri kontrol edilerek zaman aşımı maksimum hız değerini düğümlerin eşik değeri olarak tanımlayacağız. Eşik değere yaklaşan düğümlerin ağa katılma hızlarının eşik değere yaklaşması kötü niyetli düğümün ağdaki paket kaybına etkisini azaltmaktadır. Eşik atlama hız değeri aşağıda tanımlanmaktadır.

lb = En düşük atlama (0.2 m/s NS2 [6].)

ub = En yüksek atlama ($10^5$ m/s NS2 [6].)

AOMDV protokolü güvenlik tasarım yapısında tanımlanan hız değeri üzerinden ortaya çıkan akış diyagramı şekil 4.1 de gösterilmiştir. Akış diagramında tanımlanan hız değeri en yüksek atlama hız değeri olarak belirlenmiştir.




Şekil 4.1. Güvenlik uygulaması akış diagramı.

# 5. SİMÜLASYONLAR VE SONUÇLARI

## 5.1 KULLANILAN SİMÜLASYON ARACI

Tez çalışması için simülasyon aracı olarak Network Simulator (NS 2) programının 2.35 sürümü kullanılmıştır. NS kullanılmasının sebebi kullanıcılara çok sayıda fonksiyon sunması, kablosuz ağları desteklemesi ve açık kaynak kodlu olduğundan protokol eklemeye, mevcut protokolleri değiştirmeye imkan vermesidir.

NS 2 kablolu ve kablosuz ağ araştırmalarında kullanılan nesneye dayalı bir ayrık olay simülatörüdür. NS, TCP ve UDP protokollerini, FTP, Telnet, CBR, VBR gibi farklı trafik kaynaklarının davranışlarını ve yönlendirme protokollerinin kablolu ve kablosuz (yerel ve uydu) ağlarda simülasyonunu gerçekleştirebilir. Ayrıca çoklu yönlendirme protokollerini ve bazı MAC katmanı protokollerini de destekler. NS, C++ ve OTcl (TCL betik dilinin nesneye dayalı mimariye uyarlanmış hali) programlama dilleri ile yazılmıştır. NS, komut ve konfigürasyon arayüzü olarak OTcl yorumlayıcısını kullanır. Protokoller C++ ile gerçeklenmiştir, bu nedenle daha hızlı çalışırlar. Simülasyonlar ise OTcl ile yazılır ve daha yavaş çalışırlar. Simülatörü kullanmak için OTcl bilmek yeterli iken simülatörü geliştirmek için her iki dilde de programlamaya hakim olmak gerekmektedir.

## 5.2 GERÇEKLEŞTİRİLEN SİMÜLASYONLAR

Önerilen güvenlik tasarım yapısının performanslarını karşılaştırmak için birçok simülasyon gerçekleştirilmiştir. Simülasyonlar Dell Intel core i 7 Linux Ubuntu 14.04 LTS işletim sistemine, 2.1 GHz işlemci, 2 GB RAM'li bir bilgisayarda gerçekleştirilmiştir.

### 5.2.1. Simülasyon Senaryoları

Protokollerin performanslarının karşılaştırılması için 2 farklı senaryo, 6 farklı hareket modeline göre simüle edilmiştir.

Tüm senaryolarda hareketli düğümler aynı atlama hızlarıyla alana rastgele dağıtılmıştır. Düğümlerin X,Y,Z koordinatları ve ağa katılım hızları aşağıdaki tablo yapısında belirtilmiştir.

**Çizelge 5.1.** düğümlerin koordinatları (tüm senaryolar için).

| | Senaryo 1 | | | | Senaryo 2 | | | |
|---|---|---|---|---|---|---|---|---|
| | **X** | **Y** | **Z** | **U1** | **X** | **Y** | **Z** | **U2** |
| düğüm 1 | 100.0 | 300.0 | 0 | 100 | 100.0 | 300.0 | 0 | 10000 |
| düğüm 2 | 200.0 | 400.0 | 0 | 100 | 200.0 | 400.0 | 0 | 10000 |
| düğüm 3 | 200.0 | 300.0 | 0 | 100 | 200.0 | 300.0 | 0 | 10000 |
| düğüm 4 | 200.0 | 225.0 | 0 | 100 | 200.0 | 225.0 | 0 | 10000 |
| düğüm 5 | 300.0 | 450.0 | 0 | 100 | 300.0 | 450.0 | 0 | 10000 |
| düğüm 6 | 300.0 | 350.0 | 0 | 100 | 300.0 | 350.0 | 0 | 10000 |
| düğüm 7 | 300.0 | 250.0 | 0 | 100 | 300.0 | 250.0 | 0 | 10000 |
| düğüm 8 | 400.0 | 450.0 | 0 | 100 | 400.0 | 450.0 | 0 | 10000 |
| düğüm 9 | 400.0 | 280.0 | 0 | 100 | 400.0 | 280.0 | 0 | 10000 |
| düğüm 10 | 500.0 | 400.0 | 0 | 100 | 500.0 | 400.0 | 0 | 10000 |
| düğüm 11 | 600.0 | 350.0 | 0 | 100 | 600.0 | 350.0 | 0 | 10000 |
| düğüm 12 | 700.0 | 400.0 | 0 | 100 | 700.0 | 400.0 | 0 | 10000 |
| düğüm 13 | 500.0 | 500.0 | 0 | 100 | 500.0 | 500.0 | 0 | 10000 |
| düğüm 14 | 450.0 | 600.0 | 0 | 100 | 450.0 | 600.0 | 0 | 10000 |
| düğüm 15 | 600.0 | 600.0 | 0 | 100 | 600.0 | 600.0 | 0 | 10000 |
| düğüm 16 | 700.0 | 500.0 | 0 | 100 | 700.0 | 500.0 | 0 | 10000 |
| düğüm 17 | 720.0 | 450.0 | 0 | 100 | 720.0 | 450.0 | 0 | 10000 |
| düğüm 18 | 650.0 | 200.0 | 0 | 100 | 650.0 | 200.0 | 0 | 10000 |
| düğüm 19 | 800.0 | 500.0 | 0 | 100 | 800.0 | 500.0 | 0 | 10000 |
| düğüm 20 | 800.0 | 400.0 | 0 | 100 | 800.0 | 400.0 | 0 | 10000 |

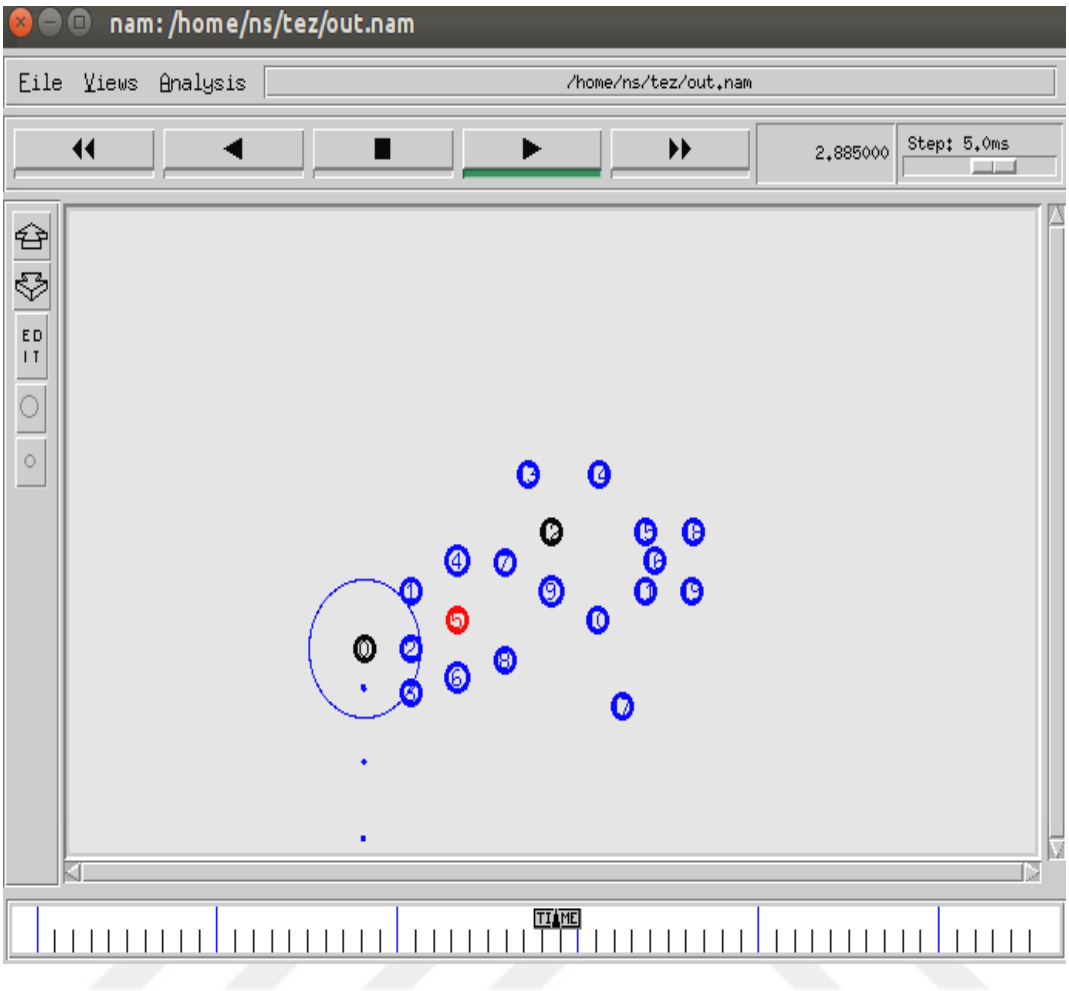
.tcl dosyalarımızı düğümlerin ağa katılımındaki hız değerlerini dikkate alarak oluşturuyoruz. Dosyalarımızda kötü niyetli düğümlerin ağa katılım hızını diğer düğümlerin hızlarıyla eş değer olarak belirliyoruz. Düğümlerin ağa değişken hız tanımlarıyla katıldıklarında ağın performansını hangi ölçüde etkilediği simülasyon araçlarıyla tespit edilmiştir. Senaryolarımızda atlama hızları artan bir şekilde devam edecektir. Senaryolarda tanımlanan hız değerlerini maksimum hız değeri ve minumum hız değeri aralığında belirliyoruz. Senaryo1 de tanımlanan atlama hızı değerini u1,senaryo 2 de tanımlanan hız değerini u2 belirtilmiştir.

Güvenlik uygulaması senaryomuzda ağda yer alan beş numaralı düğümü kötü niyetli düğüm olarak belirliyoruz. Kötü niyetli düğümün ağda görünmesi için düğüm farklı bir renkte tanımlanmıştır. .tcl uzantılı dosyalarımızda kötü niyetli düğümün tespiti ve renk ataması aşağıda belirtilmiştir.

```
$ns at 0.0 [$n(5) set ragent_] blackhole1

$ns at 0.0 "$n(5) color red"

$n(5) color "red"

$n(5) shape "circle"
```

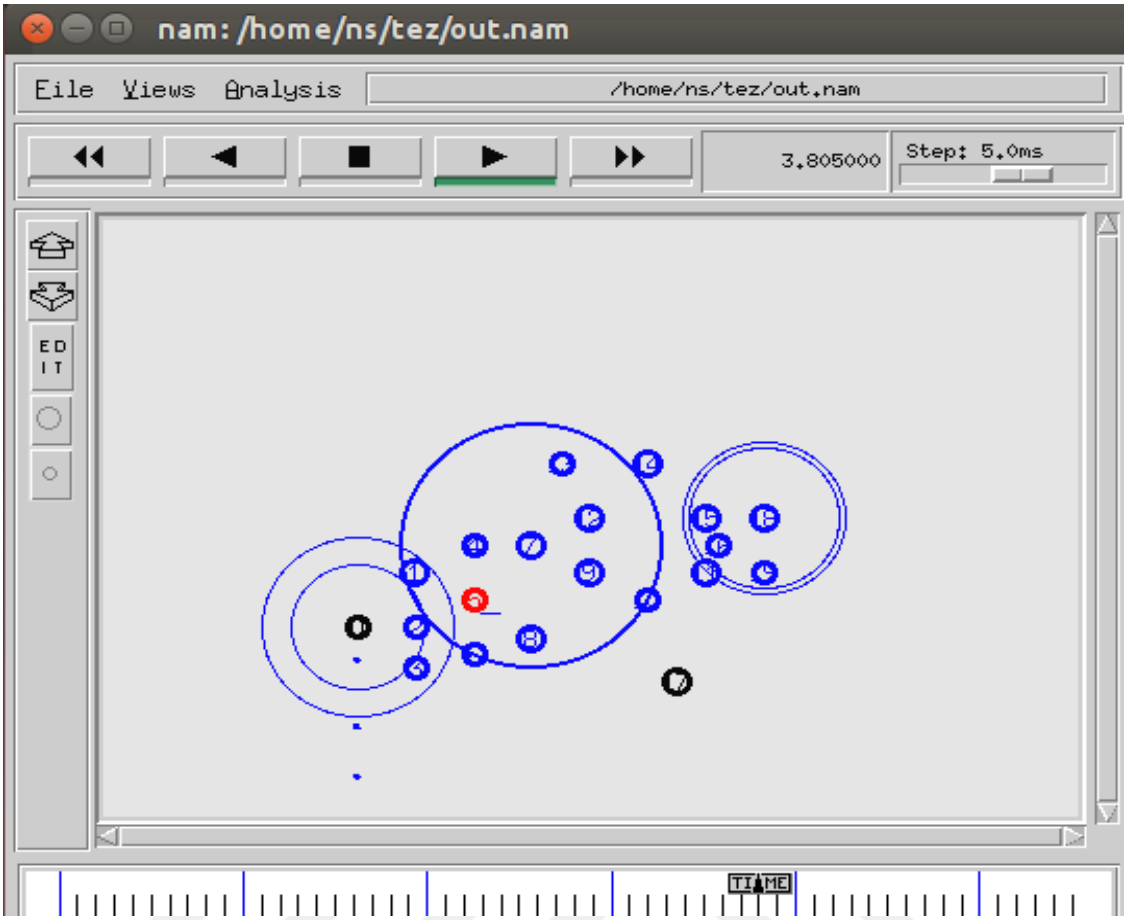
Düğümlerin ağdaki davranışları üç hareket senaryosu üzerinden incelenmiştir. Hareket modellerinde kaynak düğümden hedef düğüme giden yollar değişecektir. İki farklı hareket senaryosunda hedef düğümler değişkenlik gösterecektir. Ağa değişken atlama hızlarıyla katılan düğümlerin atlama hızlarında artış gerçekleştiğinde kötü niyetli düğümün ağdaki performansının etkisi simulatör araçlarıyla tespit edilmektedir.

İlk hareket modeli 20 hareketli düğümden oluşmaktadır. Topoloji 700*700 m'lik bir alana kurulmuştur. Simülasyon süresi 60sn dir. Hedef düğüm 12. Düğüm olarak belirlenmiştir. Kaynak ve hedef düğüm aynı renklerde ve kötü niyetli düğüm farklı renkte tanımlanmıştır.



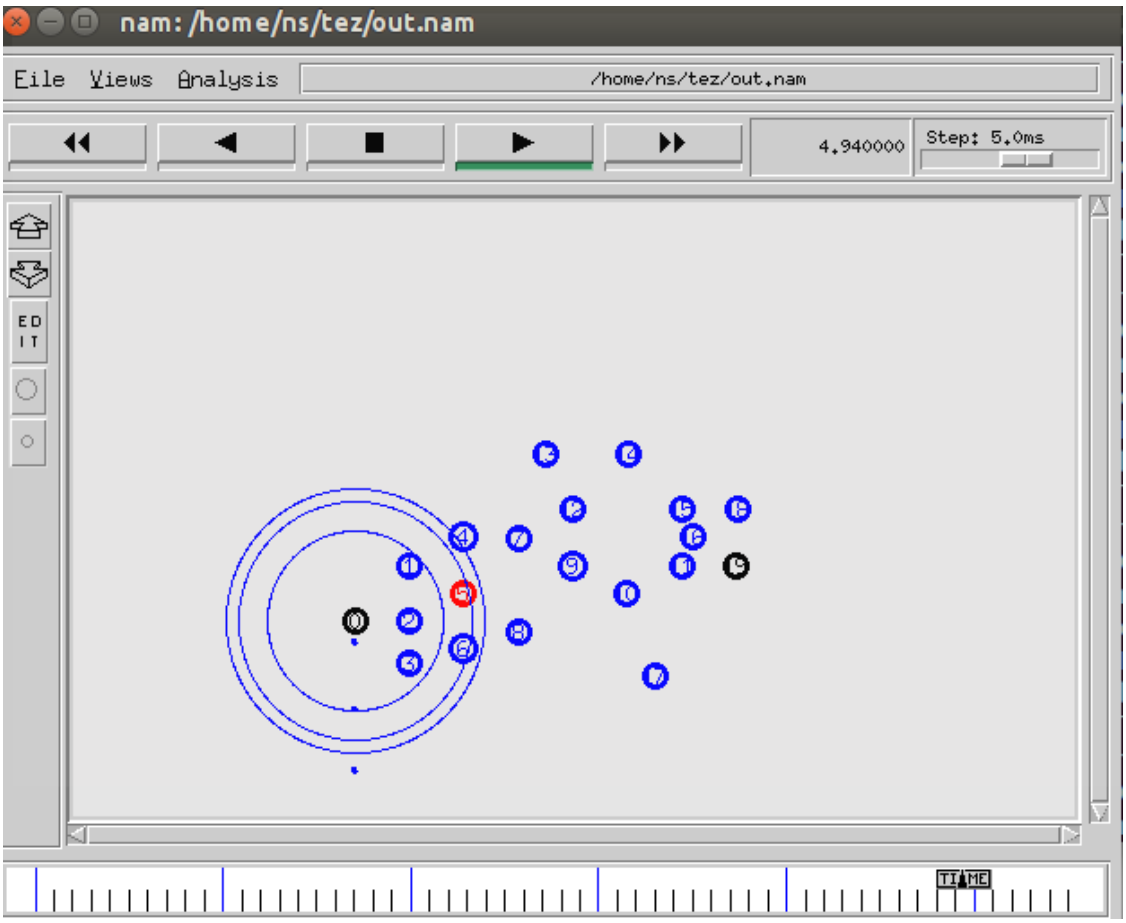

Şekil 5.1. Birinci hareket topolojisi.

İkinci hareket modeli 20 hareketli düğümden oluşmaktadır. Topoloji 800*800 m'lik bir alana kurulmuştur. Simülasyon süresi 60sn dir. Hedef düğüm 17. Düğüm olarak belirlenmiştir. Kaynak ve hedef düğüm aynı renklerde ve kötü niyetli düğüm farklı renkte tanımlanmıştır.




Şekil 5.2. İkinci hareket topolojisi.

Üçüncü hareket modeli 20 hareketli düğümden oluşmaktadır. Topoloji 1000*1000 m'lik bir alana kurulmuştur. Simülasyon süresi 60sn dir. Hedef düğüm 17. Düğüm olarak belirlenmiştir. Kaynak ve hedef düğüm aynı renklerde ve kötü niyetli düğüm farklı renkte tanımlanmıştır.




Şekil 5.3. Üçüncü hareket topolojisi.

Hareketli düğümler "random waypoint" modeline göre hareket etmektedirler. NS2 aracının düğüm hareket üreteci "setdest" kullanılarak düğümlerin hareketlerini belirten hareket dosyaları oluşturulur. Setdest aracının kullanımı aşağıdaki komutla gerçekleştirilir [6].

./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] [-x maxx] [-y maxy] > [outdir/movement-file]

Hareket dosyası üretilirken ilgili senaryonun hareketli düğüm sayısı, maksimum hızı, simülasyon süresi (60s), duraklama süresi ve topolojinin koordinatları verilir. Simülasyonda kullanılacak rastlantısal trafik bağlantıları NS aracının trafik senaryo üreteci "cbrgen" ile üretilir. Üretecin kullanımı aşağıdaki komutla olur.

ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections][-rate rate]

Trafik tipi olarak CBR (constant bit rate) trafiği seçilmiştir. –mc kurulacak maksimum bağlantı sayısı, -rate paket üretme hızı, -nn düğüm sayısı ve –seed rastlantısallık için

kullanılan parametrelerdir. Her iki senaryo için kullanılan trafik parametreleri ve senaryolarda kullanılan genel paramereler çizelge 5.3'de verilmiştir.

Çizelge 5.2. Simülasyon parametreleri

| | **Senaryo 1** | **Senaryo 2** |
|---|---|---|
| Düğüm sayısı | 20 | 20 |
| Trafik tipi | CBR | CBR |
| Seed | 1 | 1 |
| Paket boyutu | 512 Byte | 512 Byte |
| Simülasyon süresi | 60 s | 60 s |

### 5.2.2. Performans Kriterleri

Ağa katılım hızları değişken olan düğümlerin katılım hızları ve varış noktalarına göre oluşturulan senaryoların kötü niyetli düğümün ağdaki performansı AOMDV protokolünde karşılaştırmak için aşağıdaki kriterler kullanılmıştır.

- Düşürülen paket miktarı: kaynaklar tarafından üretilen veri paketi sayısının kötü niyetli düğüm tarafından düşürülmesi olarak ifade edilmesidir. İletiminin verimi, düşürülen paket miktarı ve sonuç itibariyle kullanılan yönlendirme protokolünün güvenilirliği hakkında bilgi sağlar.

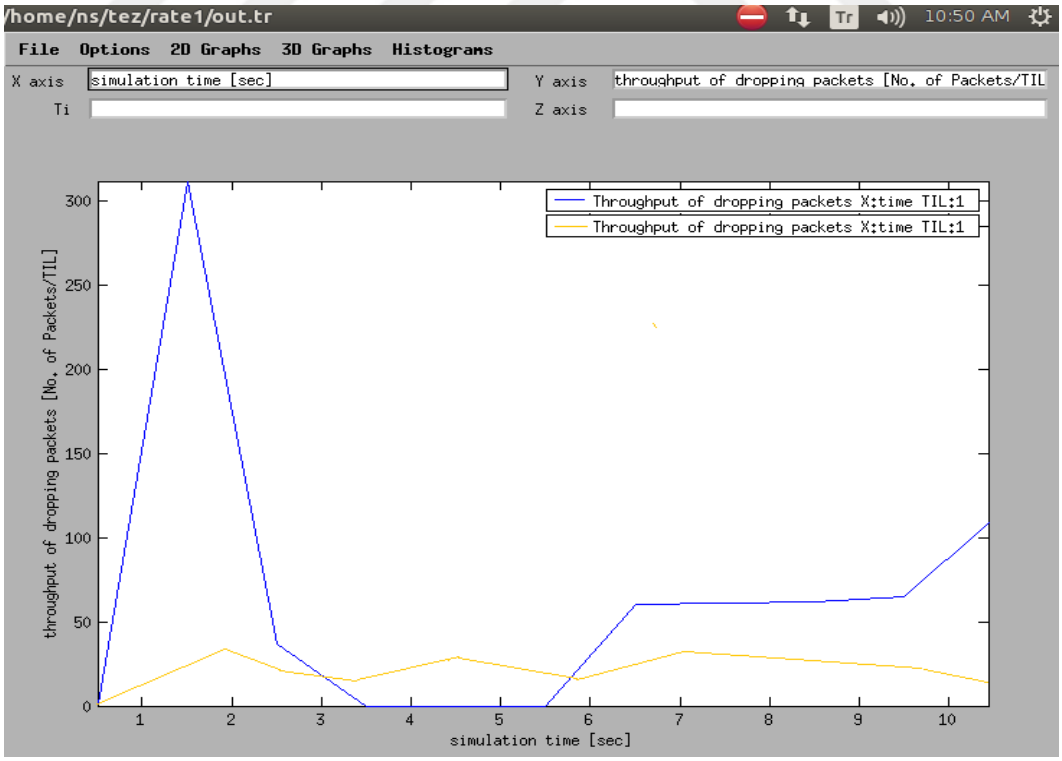
- Ortalama gecikme: Gecikme bir veri paketinin varış tarafından alındığı zamandan paketin kaynak tarafından üretildiği zamanın çıkarılmasıyla elde edilir. Gecikme, kuyrukta beklemeden, MAC seviyesindeki gecikmeden, iletim ve yayılım gecikmelerinden oluşur. Gecikme servis kalitesi için önemli bir parameter olduğundan kullanılan yönlendirme protokolünün güvenilirliği hakkında bilgi sağlar.

## 5.3. SİMÜLASYON SONUÇLARI

Bu bölümde önerilen 2 senaryonun ağa farklı katılım hızlarıyla yer almalarının kötü niyetli düğüm karşısındaki performansları simülasyon sonuçlarına göre karşılaştırılmaktadır. Her senaryo için 2 farklı ağa katılım hızlarıyla oluşturulan ve kaynak düğümden hedef düğüme giden farklı yollar kullamılarak 6 farklı hareket modeline göre simülasyon yapılmıştır. Simülasyon sonuçlarımızı değerlendirmek için NS2 ve diğer ağ simülasyon yazılımları için yardımcı bir program olan tracegraph202 ve APP-Tool-master grafik yazılımı kullanılmıştır.

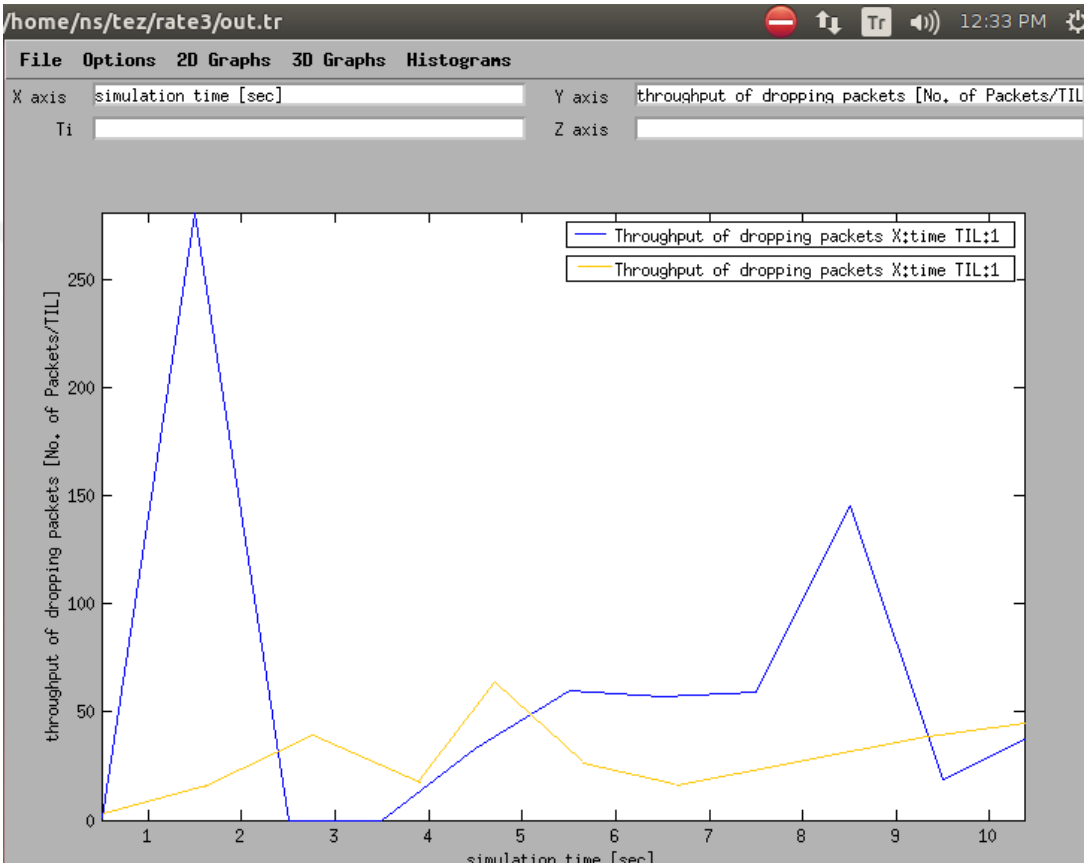
Düşürülen paket miktarı:

Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında düşürülen paket miktarı gösterilmektedir. Senaryo 1-1 hareket modelinde 707 paket düşürülmüştür. Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında düşürülen paket miktarı gösterilmektedir. Senaryo 2-1 hareket modelinde 204 paket düşürülmüştür. Kaynak düğüm 0.ıncı düğüm hedef düğüm 12.düğüm olarak belirlenmiştir.



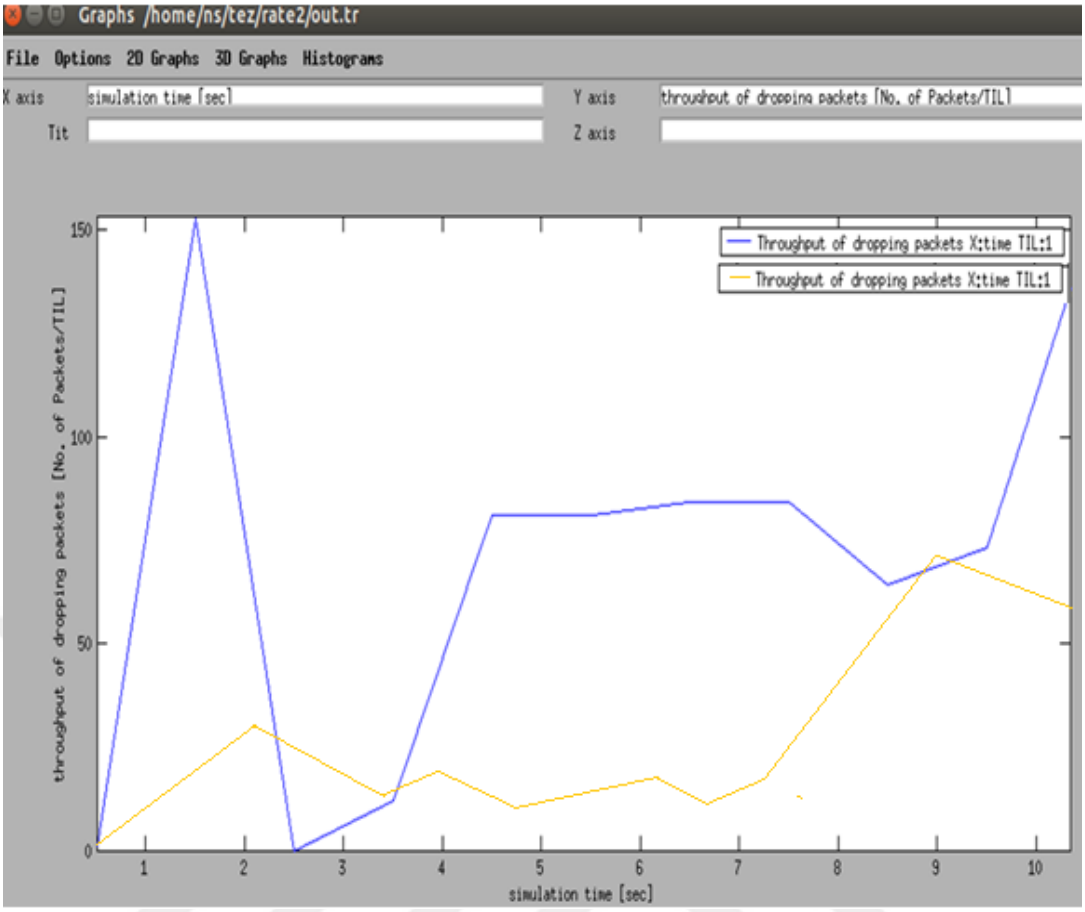

Şekil 5.4. Senaryo 1-1 ve Senaryo 2-1 hareket modeli.

Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında düşürülen paket miktarı gösterilmektedir. Senaryo 1-2 hareket modelinde 692 paket düşürülmüştür. Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında düşürülen paket miktarı gösterilmektedir. Senaryo 2-1 hareket modelinde 204 paket düşürülmüştür. Kaynak düğüm 0.ıncı düğüm hedef düğüm 17.düğüm olarak belirlenmiştir




Şekil 5.5. Senaryo 1-2 ve Senaryo 2-2 hareket modeli.

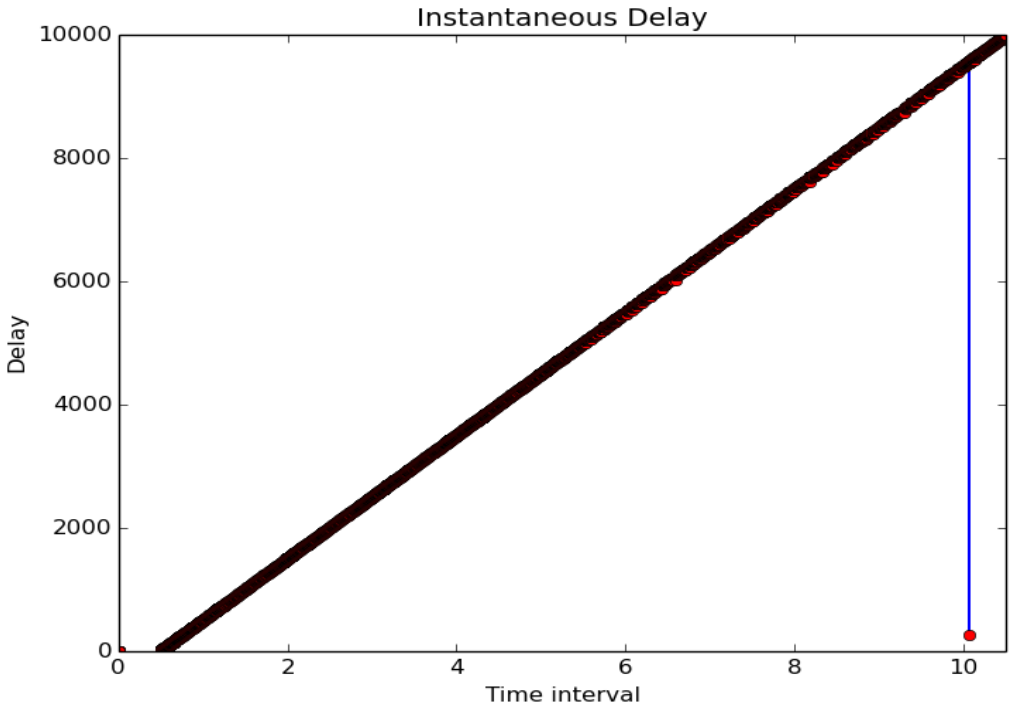
Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında düşürülen paket miktarını gösterilmektedir. Senaryo 1-3 hareket modelinde 769 paket düşürülmüştür. Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında düşürülen paket miktarını gösterilmektedir. Senaryo 2-3 hareket modelinde 355 paket düşürülmüştür. Kaynak düğüm 0.ıncı düğüm hedef düğüm 19.düğüm olarak belirlenmiştir.




Şekil 5.6. Senaryo 1-3 ve Senaryo 2-3 hareket modeli.

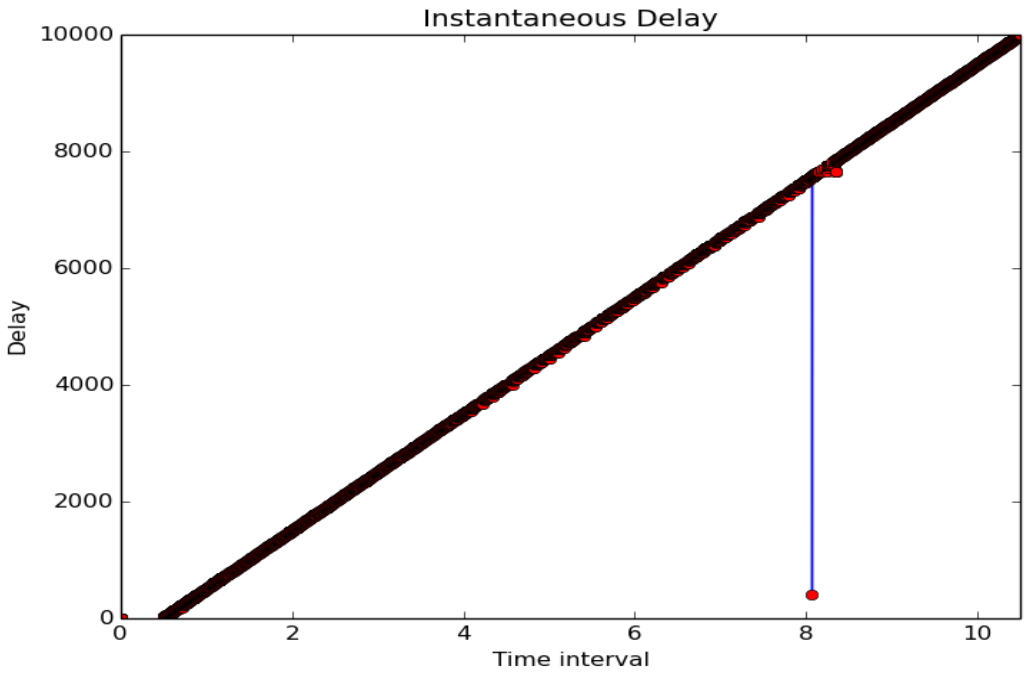
Ortalama gecikme :

Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 12.düğüm olarak belirlenmiştir. Senaryo 1-1 hareket modelinde ortalama gecikme 9873.62 ms dir.



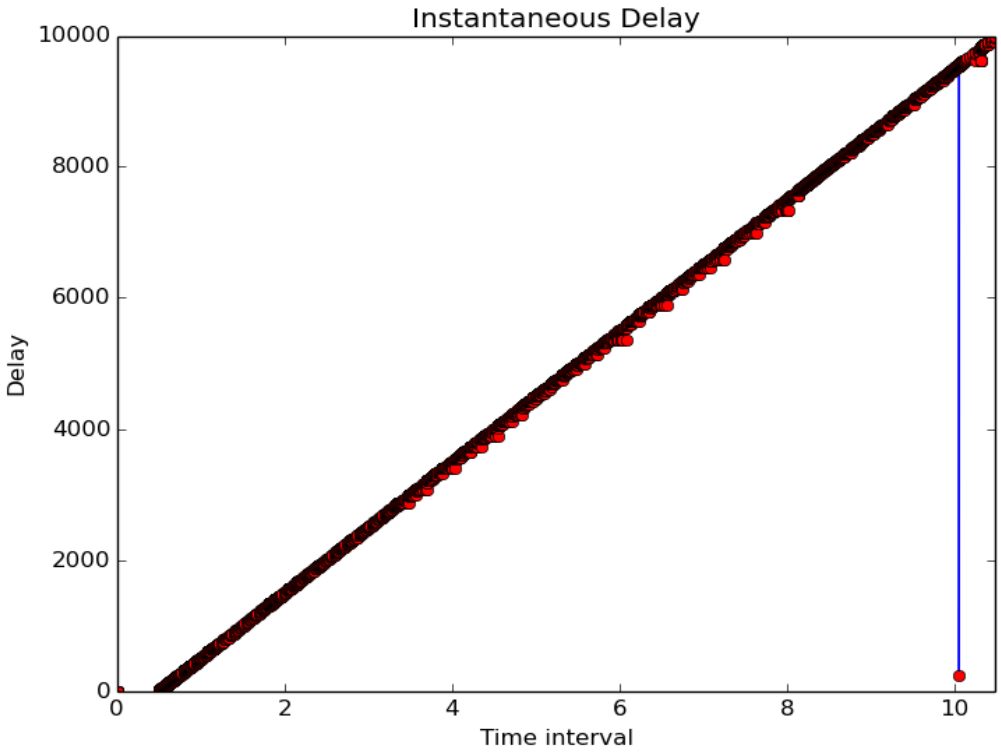

Şekil 5.7. Senaryo 1-1 hareket modeli ortalama gecikme.

Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 17.düğüm olarak belirlenmiştir. Senaryo 1-2 hareket modelinde ortalama gecikme 9275.3 ms dir.



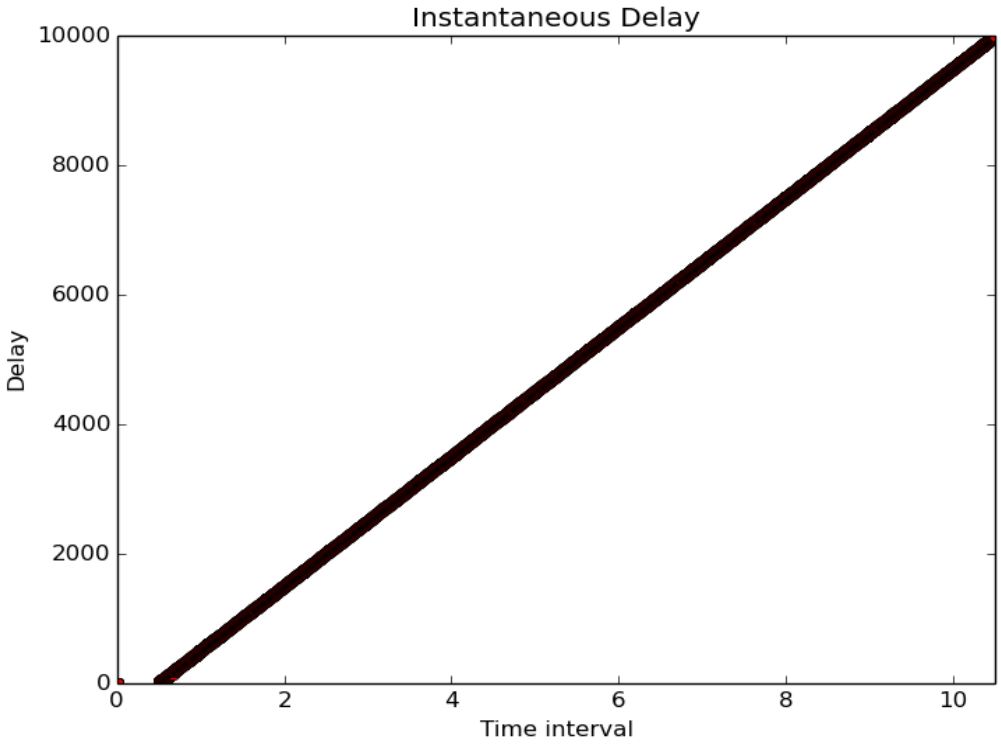

Şekil 5.8. Senaryo 1-2 hareket modeli ortalama gecikme.

Senaryo 1'de düğümlerin ağa u1 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 19.düğüm olarak belirlenmiştir. Senaryo 1-3 hareket modelinde ortalama gecikme 9943.79 ms dir.



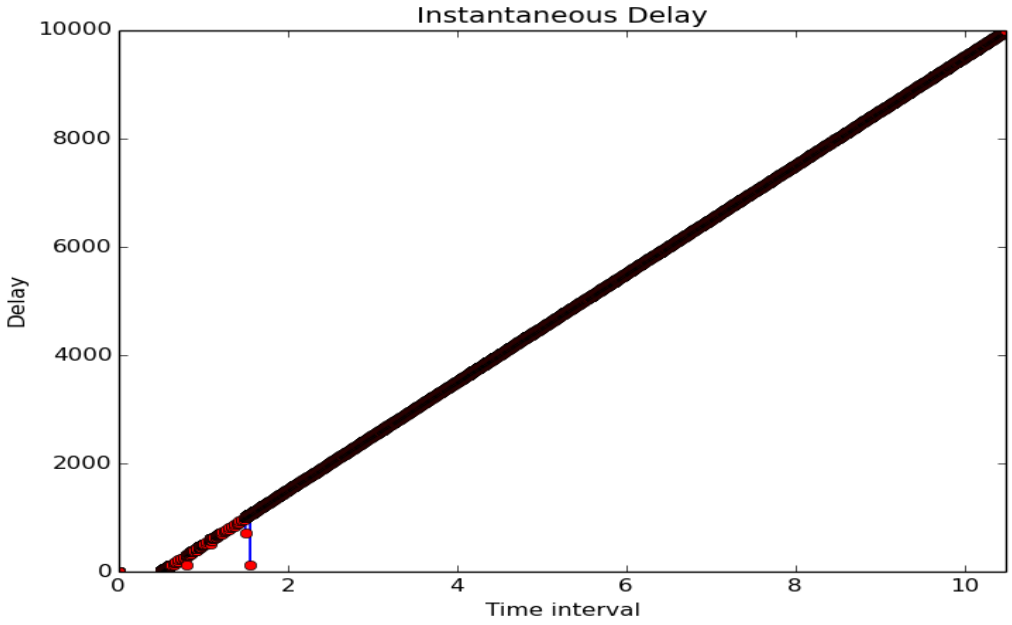

Şekil 5.9. Senaryo 1-3 hareket modeli ortalama gecikme.

Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 12.düğüm olarak belirlenmiştir. Senaryo 2-1 hareket modelinde ortalama gecikme 6726.43 ms dir.



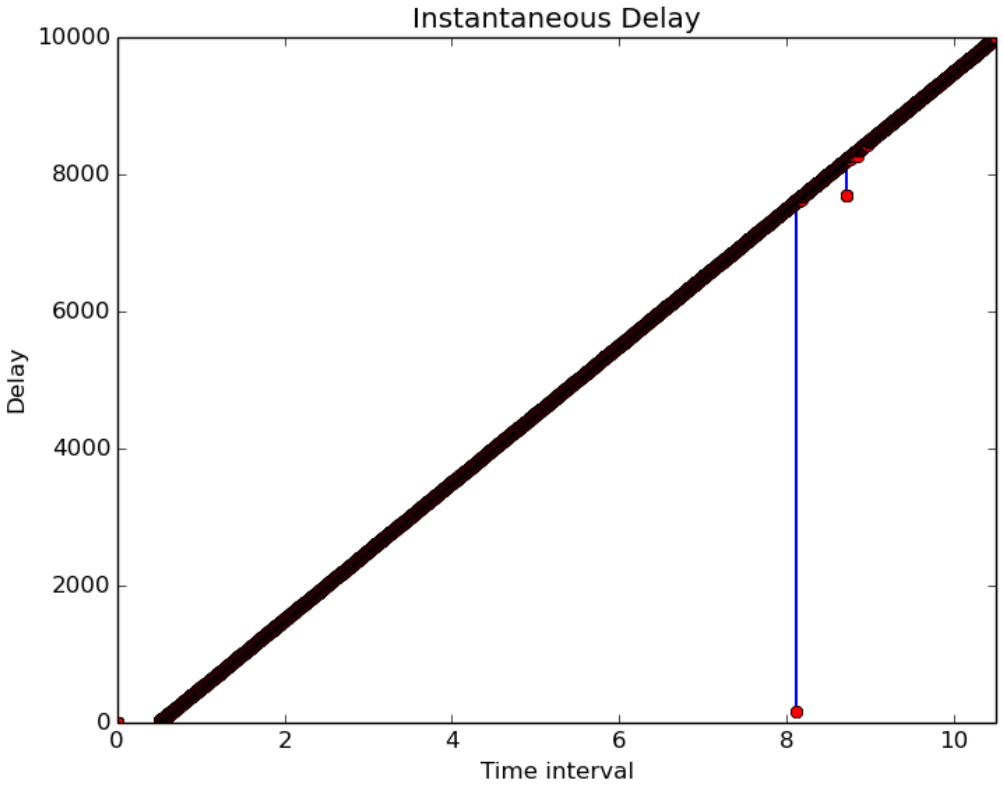

Şekil 5.10. Senaryo 2-1 hareket modeli ortalama gecikme.

Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 17.düğüm olarak belirlenmiştir. Senaryo 2-2 hareket modelinde ortalama gecikme 7034.08 ms dir.




Şekil 5.11. Senaryo 2-2 hareket modeli ortalama gecikme.

Senaryo 2 de düğümlerin ağa u2 katılım hızıyla katıldıklarında ortalama gecikme gösterilmektedir. Kaynak düğüm 0.ıncı düğüm hedef düğüm 19.düğüm olarak belirlenmiştir. Senaryo 2-3 hareket modelinde ortalama gecikme 7050.09 ms dir.




Şekil 5.12. Senaryo 2-3 hareket modeli ortalama gecikme.

# 6. SONUÇLAR VE ÖNERİLER

Tasarsız ağlarda gömülü bir güvenlik tasarımı yer almadığından ataklara karşı savunmasız yapıdadır. Tasarsız ağların değişken topolojiye sahip olması, düğümlerin hareketli olması ve kablosuz ağ ortamından kaynaklanan olumsuzluklar birçok soruna neden olmuştur. Dolayısıyla kablosuz kanal hem ağdaki kullanıcılara hem de ağda yer alan kötü niyetli kullanıcılara erişilebilir durumdadır. Tasarsız ağlarda düğümlerin hareketliliği ve topolojinin değişken olması yönlendirme işlemini bu ağların önemli problemlerinden biri kılmaktadır. Tez çalışmasında güncel protokollerden AOMDV protokolü kullanılarak, Dos atak türlerinden Black hole saldırısı ağdaki güvenliği bozacak şekilde oluşturulmuştur. Düğümlerin ağa katılım hızları değerlendirilerek çalışmamızda maksimum hız değerini eşik değer olarak belirlenmektedir. Gerçekleştirdiğimiz simülasyon senaryolarında düğümlerin ağa katılım hızlarında artış gerçekleştiğinde kötü niyetli düğümün daha az paket düşürdüğü ve ağdaki ortalama gecikmenin azaldığı simülasyon araçlarıyla tespit edilmiştir.

Kötü niyetli düğümün davranışının ağın performasını düşürmesi ve ağdaki veri akışını bozması dolayısıyla paket kaybının artmasını engellemek için düğümlerin ağa katılım hızları artırılarak, farklı topolojilerdeki ağ ortamları simüle edilerek ağın performansının arttığı görülmüştür.

Bu tez çalışması tasarsız ağların önemli sorunlarından biri olan güvenlik konusunda Black hole ataklarına karşı güvenlik uygulaması geliştirilmiştir.

# 7. KAYNAKLAR


[1] B. Nevatia, Y., "Ad-Hoc Routing for USARSim", *Networks and Distributed Systems Seminar*, 2007.

[2] M. Cordeiro, C. Agrawal, "Mobile ad hoc networking Center for Distributed and Mobile Computing", *OBR Research Center for Distributed and Mobile Computing*, University of Cincinnati, 2002.

[3] T.C. Milli Eğitim Bakanlığı, "Bilişim Teknolojileri: Kablosuz Ağlar", 2011.

[4] Gorantala, K., "Routing Protocols in Mobile Ad-hoc Networks", *Master Thesis*, UMEA University, 2006.

[5] P. Gupta, S. Pandey, "Performance Analysis of AOMDV and AODV Routing Protocol in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, 2015.

[6] (2016). [Online]. Available: http://www.isi.edu/nsnam/ns/tutorial/.

[7] P. CE, Belding-Royer E, Das SR., "Ad hoc on-demand distance vector (AODV) routing", July 2003.

[8] Chen H.-L., Lee C.-H., "Two Hops Backup Routing Protocol in Mobile Ad Hoc Networks",*11th International Conference on Parallel and Distributed Systems Workshops (ICPADS'05)*, pp. 600-604, 2005.

[9] M. Chadha, R. Joon, Sandeep, "Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", *International Journal of Soft Computing and Engineering (IJSCE)*, 2002.

[10] S. Agrawal, S. Jain and S. Sharma , "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", *Journal of Computing*, 2011.

[11] K. Gupta, P.Bansal , "Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol", *International Journal of Innovations in Engineering and Technology (IJIET)*, 2014.

[12] B.Revathi et.all, "A Survey of Cooperative Black and Gray hole Attack in MANET", *International Journal of C.S. And Management Research* ,Vol 1 , September 2012.

[13] K. Wang, Jia Chen, H. Zhou and Y. Qin, "Content-Centric Networking: Efect of Content Cachingon Mitigating DoS Attack", *International Journal of Computer Science Issue*, vol.9, pp.43-52, November 2012.

[14] H. Gupta , S. Shrivastav ,S. Sharma , "Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing", *International Conference on Computational Intelligence and Communication Networks*, 2013.

[15] N. Bhardwaj, R. Singh , "Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2014.

[16] Y.Adhyaru, Y. Patel , "Multipath Routing in Fast Moving Mobile Adhoc Network", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 2013.

[17] S. Upadhyay, Brije, "Avoiding Wormhole Attack Approach CCSIT 2012, Partesh Kumar Chaurasia", *Detecting in MANET Using Statistical Analysis*, LNICST 84, pp. 402–408, 2012.

[18] T. YİĞİT , S. DEMİR, "Tasarsız Ağlar için bir Güvenlik Simülatörü", *2. Ağ ve Bilgi Güvenliği Sempozyumu* ,16-18 Mayıs 2005, Girne, KKTC

[19] A. Cárdenas, S.Radosavac and John S. Baras, "Ad hoc networks: Detection and prevention of MAC layer misbehavior in ad hoc Networks", *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor Networks*, October 2004, pp.17-22.

[20] F.Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Adhoc Wireless Networks, Security Protocols", *7th International Workshop Proceedings, Lecture Notes in Computer Science*, pp.1-11, 1999.

# ÖZGEÇMİŞ

## KİŞİSEL BİLGİLER

Adı Soyadı : Aziz AYDIN

Doğum Tarihi ve Yeri : 26.11.1986 BİSMİL

Yabancı Dili : İngilizce

E-posta :aziz45024@duzce.edu.tr

## ÖĞRENİM DURUMU

| Derece | Alan | Okul/Üniversite | Mezuniyet Yılı |
|---|---|---|---|
| Y. Lisans | Bilgisayar Müh. | Düzce Üniversitesi | - |
| Lisans | Bilgisayar Müh. | Kocaeli Üniversitesi | 2014 |
| Lise | Fen Bilimleri | Bismil Lisesi | 2005 |