KABLOSUZ GENİŞBANT MOBİL AĞLARDA GÜVENLİK BİLİNÇLİ ZEKİ YÖNLENDİRME PROTOKOLÜ

Muhammet ÜNAL

DOKTORA TEZİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKİM 2010
ANKARA

Muhammet ÜNAL tarafından hazırlanan "KABLOSUZ GENİŞBANT MOBİL AĞLARDA GÜVENLİK BİLİNÇLİ ZEKİ YÖNLENDİRME PROTOKOLÜ" adlı bu tezin Doktora tezi olarak uygun olduğunu onaylarım.

Doç. Dr. M. Ali AKCAYOL …….
Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Elektrik Elektronik Mühendisliği Anabilim Dalında Doktora tezi olarak kabul edilmiştir.

Prof. Dr. Sezai DİNÇER …….
Elektrik Elektronik Mühendisliği Anabilim Dalı, G. Ü.

Doç. Dr. M. Ali AKCAYOL …….
Bilgisayar Mühendisliği Anabilim Dalı, G. Ü.

Prof. Dr. Erdem YAZGAN …….
Elektrik Elektronik Mühendisliği Anabilim Dalı, H. Ü.

Prof. Dr. Şeref SAĞIROĞLU …….
Bilgisayar Mühendisliği Anabilim Dalı, G. Ü.

Yrd. Doç. Dr. Hasan Şakir BİLGE …….
Bilgisayar Mühendisliği Anabilim Dalı, G. Ü.

Tarih: 01/10/2010

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Doktora derecesini onamıştır.

Prof. Dr. Bilal TOKLU …….
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Muhammet ÜNAL

KABLOSUZ GENİŞBANT MOBİL AĞLARDA GÜVENLİK BİLİNÇLİ ZEKİ YÖNLENDİRME PROTOKOLÜ

(Doktora Tezi)

Muhammet ÜNAL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ekim 2010

ÖZET

Bu çalışmada kablosuz genişbant mobil ağlar için güvenlik bilinçli zeki bir yönlendirme protokolü geliştirilmiştir. Geliştirilen protokol proaktif ve deterministik olmayan yönlendirme algoritmasına sahiptir. Genetik algoritma en kısa yolu bulmak ve bulanık mantık yolların güvenlik seviyelerini dilsel olarak ifade etmek amacıyla kullanılmaktadır. Kullanıcı tarafından belirlenen bir güvenlik seviyesine göre kaynak ve hedef düğümler arasında en uygun yol bulanık mantık ve genetik algoritmayla hesaplanmaktadır.

Benzetim sonuçları, bulanık mantık ile dilsel olarak güvenlik seviyesi belirlenmiş yollar üzerinde genetik algoritmayla en kısa yol bulmanın başarılı olduğunu göstermiştir. Geliştirilen protokolün benzetimi ve en uygun parametrelerinin belirlenebilmesi için Matlab programı kullanılmıştır.

Bilim Kodu : **902.1.063**
Anahtar Kelimeler : **Kablosuz ağlar, yönlendirme protokolü, güvenlik, bulanık mantık, genetik algoritma, ağ benzetimi**
Sayfa Adedi : **137**
Tez Yöneticisi : **Doç. Dr. M. Ali AKCAYOL**

SECURITY AWARE ROUTING PROTOCOL FOR WIRELESS BROADBAND MOBILE NETWORKS

(Ph.D. Thesis)

Muhammet ÜNAL

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

October 2010

ABSTRACT

In this thesis, a security-aware routing protocol is developed for wireless broadband mobile networks. The developed protocol is proactive and has nondeterministic routing algorithm. Genetic algorithm is used to find shortest path and fuzzy logic is used to define the level of security of paths as linguistic labels. Based on the user defined security level, the best path between the source and the destination is determined using fuzzy logic and genetic algorithm.

Experimental results illustrated that obtaining the shortest path by genetic algorithm using the paths with linguistic security levels determined by fuzzy logic is successful. Matlab is used for network simulation and determination of suitable parameters of the developed protocol.

Science Code : 902.1.063
Key Words : Wireless networks, routing protocol, security, fuzzy logic, genetic algorithm, network simulation
Page Number : 137
Adviser : Assoc. Prof. Dr. M. Ali AKCAYOL

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Doç. Dr. M. Ali AKCAYOL'a, tez çalışmalarım sırasında yardımlarını esirgemeyen çok değerli arkadaşlarım Dr. Tolga PIRASACI, Yrd. Doç. Dr. Diyar AKAY, Yrd. Doç. Dr. Tuncay KARAÇAY, Yrd. Doç. Dr. Nureddin DİNLER'e çok teşekkür ederim. Fikir ve eleştirileri ile tezime katkı ve yönlendirmede bulunan Tez İzleme Komitesi üyeleri Sayın Prof. Dr. Erdem YAZGAN ve Sayın Prof. Dr. Şeref SAĞIROĞLU'na çok teşekkür ederim. Kütüphane çalışanlarımız Yrd. Doç. Dr. Mehmet TOPLU ve Nurhayat Özdemir İDİL'e kitap ve makalelere erişmemde verdikleri destekten dolayı çok teşekkür ederim. Çalışmama maddi destek sağlayan Gazi Üniversitesi Bilimsel Araştırma Projeleri Birimi'ne teşekkür ederim. Doktora çalışmalarım sırasında bana desteklerini hiç esirgemeyen aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklama
MAC	Medya Erişim Kontrol (Media Access Control)
DoS	Servis Reddetme Saldırısı (Denial of Service)
SSID	Abone İstasyonu Tanımlaması (Subscriber Station Identification)
STS	Saldırı Tespit Sistemleri (Intrusion Dedection System)
IEEE	Amerikan Elektrik Elektronik Mühendisleri Enstitüsü
WLAN	Kablosuz Yerel Ağlar (Wireless Local Area Networks)
AP	Erişim Noktası (Access Point)
STA	İstasyon
DSL	Dijital Abone Hattı (Digital Subscribers Line)
SEAD	Güvenli Verimli Ad Hoc Mesafe Vektörü (Secure Efficient Ad-Hoc Distance Vector)
DSDV	Varış Noktası Amaçlı Ardışıl Mesafe Vektörü (Destination Sequenced Distance Vector)
ARIADNE	Verimli İsteğe Dayalı Güvenli Bir Yönlendirme Protokolü (An Efficient On-Demand Secure Routing Protocol)
DSR	Dinamik Kaynak Yönlendirme (Dynamic Source Routing),
TESLA	Zaman Verimli Akışa Sahip Kayıp Toleranslı Doğrulama (Timed Efficient Stream Loss-Tolerant Authentication)
TIK	Geçici Yular (Temporal Leashes)

Kısaltmalar	Açıklama
SAR	Güvenlik Bilinçli Yönlendirme (Security Aware Routing)
AODV	İsteğe Dayalı Mesafe Vektör Yönlendirme (Ad-Hoc On-Demand Distance Vector Routing)
QoP	Güvenlik Kalitesi (Quality of Protection)
SRP	Güvenli Yönlendirme Protokolü (Secure Routing Protocol)
Gİ	Güvenlik İlişkisi
YKP	Yol Keşif Paketi
REP	Cevap Paketi
ARAN	Ad-Hoc Ağlar için Güvenli Yönlendirme Protokolü (A Secure Routing Protocol for Ad Hoc Networks)
OSPF	Açık En Kısa Öncelikli (Open Shortest Path First)
TTL	Maksimum Atlama Sayısı (Time to Live)
İÖÇO	İşleme Özel Çaprazlama Operatörü
İÖMO	İşleme Özel Mutasyon Operatörü
NYY	Normalize Yönlendirme Ek Yükü
PDO	Paket Dağıtım Oranı

1. GİRİŞ

Haberleşme eski çağlardan itibaren insan hayatında çok önemli bir yer tutmaktadır. Bir zamanlar ulak ve duman gibi yöntemler ile uzun zaman alan ve kısa mesafelerde yapılan haberleşme, elektriğin bulunuşu ile yeni bir boyut kazanmıştır. 1820 yılında telgrafın icadı [1] ile bakır teller üzerinden başlayan kablolu iletişim insanların mobil haberleşme ihtiyaçları sonucunda telsiz cihazlar ile kablosuz boyuta taşınmıştır. Bilgisayarların kullanılmaya başlaması ile bilgisayarlar arası haberleşme ihtiyacı ortaya çıkmıştır. Ethernet gibi kablolu teknolojiler kullanılarak gerçekleştirilen bilgisayarlar arası haberleşme, bu teknolojilerin kurulumunun zor ve maliyetli olması ayrıca fiyatların birbirine yaklaşması sebebiyle günümüzde yerini kablosuz teknolojilere bırakmaktadır [1].

Kablosuz teknolojiler iletim ortamı olarak açık havayı kullanmaktadır. Böylece herhangi bir fiziki bağlantıya ihtiyaç duymamaktadırlar. Bu nedenle kablosuz teknolojilerin getirdiği mekandan bağımsızlık büyük bir rahatlık sağlamaktadır.

Kablosuz teknolojiler, sürekli gelişen daha zeki ve daha çok amaca hizmet eden elektronik cihazların çevrelerinden ve birbirlerinden haberdar olmaları ve haberleşebilmeleri için çok önemlidir. Bu yüzden elektronik sistemler arasında çeşitli ağ sistemleri oluşturulmuştur. Bu sistemlerde çok sayıda cihazın karşılıklı olarak birbirleri ile haberleşmesi istenir. Haberleşme sistemlerinde değişik üreticilerin ürettiği cihazların birbirleri ile olabildiğince uyumlu haberleşebilmeleri için belirli bazı protokoller ve kurallara ihtiyaç vardır.

Haberleşmenin sürekliliğini sağlamak için, trafiği düzenleyen trafik kuralları gibi bir takım kurallar ve protokoller yapısı oluşturulmuştur. Her protokol ve düzenleme belirli bir haberleşme hızı ve ortamı için optimumdur. Bu sebeple yeni ortamlar ortaya çıktığında ve bu hızlar için yeni ihtiyaçlar oluştuğunda yeni düzenlemeler ve ayarlamalar gerekmektedir. Bu tür düzenlemeler eski protokollerin yeniden düzenlenmesi ile elde edilebileceği gibi, tamamen yeniden hazırlanabilmektedir.

Protokollerde genel amaç birbirinden bağımsız çeşitli şirketlerin yapmış olduğu farklı cihazların, çok hızlı bir şekilde kurulup birbiri ile kolaylıkla ve istenen niteliklerde güvenli bir şekilde haberleşmesini sağlama amacını gütmektedir. Ayrıca ağlarda, özellikle kablosuz ağlarda kişiselleşmenin ve esnekliğin ayrıca bağımsızlığın bir sonucu olarak güvenliğinin sağlanmasındaki yeni zorluklar ortaya çıkmaktadır [1]. Çünkü bu yapıda sinyaller, sistemleri birbirine bağlayan kablolarla sınırlı kalmayıp, istenen ağ alanının sınırlarını geçerek yakındaki yabancı cihazlara da ulaşabilir veya bu yabancı cihazlar bizim cihazımıza ulaşabilir. Uygun bir alıcı ile kablosuz ağ üzerinden iletilen veriye belirli bir menzil içinde erişebilmek mümkündür. Bu istenmeyen durumların engellenmesi gerekir. Fakat yapılan her hamle, karşısında yeni karşı hamleleri getirmektedir. Bu yüzden kötü niyetli kişilere karşı kullanıcı rahatlığından ödün vermeden, bilgi güvenliğinin sağlanabilmesi için yeni yöntemler ve politikalar belirlenmesi gerekmektedir [2, 3].

Kablosuz ağlar çeşitli tarzda birçok saldırı yöntemine maruz kalırlar. Bu saldırıların birçoğu fiziksel ve MAC (Medya erişim kontrol) katmanını hedeflemesine rağmen, verilere erişmek veya onları engellemek veya uygulama katmanında bazı aktiviteler gerçekleştirmek, asıl amaçtır.

Aşağıda kablosuz ağlar için kısaca bazı genel saldırı türleri ve açıklar anlatılmıştır [1];

- Servis reddetme saldırısı (DoS- Denial of Service): Saldırgan ağ cihazını fazla trafik yoluyla yavaşlatır. Bu ise cihaza erişimi engeller veya ciddi anlamda yavaşlatır. Hedef çeşitli katmanlarda olabilir. Örneğin, web sunucusu sayfa istekleriyle veya bir erişim noktası bağlanma ve yetkilendirme istekleriyle yavaşlatılabilir.

- Karıştırma (Jamming): Bir çeşit DoS saldırısıdır. Saldırgan radyo frekans bandını bir parazit dalga ile doldurur. Böylece haberleşmeyi engeller. Bu 2.4 GHz.

bandında Bluetooth cihazları, bazı telsiz telefonlar veya mikrodalga fırın yardımıyla yapılabilir.

- Ekleme Saldırıları (Insertion Attack): Saldırgan, yetkilendirme erişimi yapılmayan veya yetkilendirme varsa bile kendisini yetkili kullanıcı gibi maskeleyerek yetkisiz bir terminali erişim noktasına bağlayabilir.

- Tekrar Saldırıları (Replay Attack): Saldırgan ağ trafiğini dinleyerek elde etiği kayıtları inceleyip işleyerek, bunu daha sonra ağa yetkisiz erişebilmek için kullanır.

- Ağ Trafiğini İzlemek (Broadcast Monitoring): Zayıf tasarlanmış ağlarda eğer erişim noktası anahtar yerine hub'a bağlanmış ise, hub kablosuz terminaller için olan trafiği de yayınlayacaktır. Bu bilgiler bir saldırgan tarafından kullanılabilir.

- ARP Yanıltma (ARP Spoofing): Saldırgan ağı aldatıp hassas yönlendirme bilgilerini kendi kablosuz terminaline yönlendirir. MAC ve IP ikililerinin bulunduğu ARP önbelleğine erişir ve değiştirerek ağ yönetimini eline geçirir.

- Oturum Korsanlığı (Session Hijacking, Man-in-the-middle Attack): Saldırganın kurban terminalin, erişim noktası ile olan bağlantısını kesmesini sağlayan bir çeşit ARP yanıltma saldırısıdır. Burada saldırgan kendini terminal gibi gösterip bağlantısını erişim noktası ile keser. Ardından kurbana kendisini erişim noktası gibi tanıtıp ilişkilendirir.

- Hileci Erişim Noktası (Rogue Access Point): Saldırgan yetkilendirilmemiş bir erişim noktasını, yetkilendirilmiş ikizi gibi yani aynı SSID ile beraber kurar. Eğer yetkisiz erişim noktasının sinyalleri bir amplifikatör veya yüksek kazançlı bir anten vasıtası ile güçlendirilir ise terminaller sahte erişim noktasını tercih edeceklerdir. Böylece değerli bilgiler toplanabilir.

- Kriptoanalitik Saldırılar (Cryptoanalytic Attacks): Saldırgan kriptografik sistemin zayıflıklarını kullanarak saldırıda bulunur. Örneğin RC4 şifrelemesinde bulunan bir zayıflık buna dayalı olan WEP protokolünü savunmasız bırakmıştır.

- Kenar Kanal Saldırıları (Side Channel Attacks): Saldırgan güç tüketimi, zamanlama bilgisi, akustik veya elektromanyetik emisyonları kullanarak kriptografik sistem hakkında bilgi edinmeye çalışır. Bu bilgilerin analizi saldırgan şifreleme anahtarını elde edebilir.

- Wormhole Saldırısı: Saldırgan ağın bir bölümündeki iletilen yönlendirme paketlerini kaydedip ağın başka bir bölümünde tekrar kullanırsa ağın çalışmasını engelleyebilir.

Görüldüğü gibi tehditler geniş bir çeşitlilik göstermekte ve tek bir bakış açısından yapılan çözüm yöntemleri yetersiz kalmaktadır. Ayrıca kablosuz ağların kapsama alanları arttıkça bu tür ağlara saldırı yapılma riskleri daha da artmaktadır.

Bu tez çalışmasında, yüksek menzile sahip genişbant kablosuz ağlarda paketlerin kaynaktan hedefe verimli ve istenilen güvenlik seviyesinde iletimi amaçlanmıştır. Üzerinde çalışılan sistemin genişbant olması, menzili arttırdığından hareketliliğin bağıl anlamda daha az olmasına neden olmaktadır. Böylece yüksek hareketli kablosuz ağlar için verimli olmayacak yeni yöntemler görece olarak daha az hareketli genişbant kablosuz ağlar için verimli ve kullanışlı olabilmektedir. Aynı şekilde bunun tersi de doğrudur. Hızlı değişen ağlar için hazırlanmış protokoller, yavaş değişen ağlar için gereksiz işlemler içererek yavaşlamaya neden olmaktadırlar. Hazırlanan protokolde komşuluk matrisi tablosuna dayalı yeni bir yönlendirme algoritması önerilmiştir. Ayrıca protokol algoritmasında iletilen paketler istenen belirli bir güvenlik seviyesi ile damgalanmakta ve o güvenlik seviyesindeki düğümler üzerinden hedef düğüme ulaşmaktadırlar.

Düğümler arasındaki bağların güvenlik seviyelerinin tespiti, hazırlanan protokol için çok önemli bir sorundur. Düğümler, komşu düğümlerine ve onlardan gelen saldırı türlerine göre belirli bir bakseç tablosu üzerinden aralarındaki bağı puanlamaktadırlar. Sürekli değişen bu puanlar iletim yolunun hesaplanmasında kullanılmaktadır.

Düğümler üzerinde iletilen paketlerin izleyecekleri yolların hesaplanması önemli bir sorundur. Ayrıca izlenecek yol üzerindeki düğümlerin saldırılar ve hareketlilik nedeniyle oluşacak dinamik durumu yolların seçimini büyük ölçüde etkilemektedir. Çünkü paketler ilk yola çıktıklarında doğru olan bir yol, zamana bağlı olarak yanlış bir yola dönüşebilir. Ayrıca bazı yollar uygun hale gelerek kullanıma açılmış olabilir. Bu nedenle zaman bağımlı bir yönlendirme yapılması daha uygun görülmüştür.

İletim yollarının dinamik olarak hesaplanması düğüm sayısı arttıkça zaman alan bir görev halini almaktadır. Bu süreyi kısaltmak için bulanık-genetik bir yol bulma algoritması geliştirilmiştir. Geliştirilen bu algoritmanın çalışabilirliğinin ispatı ve performans parametrelerinin elde edilebilmesi için Matlab programlama dili ile bir benzetim programı yazılmış ve hazırlanan protokol, benzetim programına gömülerek gerekli parametreler üzerinde benzetim çalışmaları yapılmıştır. Hazırlanan benzetim programı nesne yönelik ve fonksiyonel yapıda olduğu için diğer protokollerin uygulanması için de ideal bir altyapı sağlamaktadır.

Tezin ikinci bölümünde daha önce konu üzerine yapılan çalışmalara değinilmiştir. Üçüncü bölümde, önerilen protokolde uyarlanan yapay zeka yöntemleri ve saldırı tespit sistemleri genel olarak anlatılmıştır. Dördüncü bölümde önerilen model olan "Genişbant Ağlar için Güvenlik Bilinçli Zeki Yönlendirme Protokolü" hakkında detaylı bilgi verilmiştir. Protokolde düğümler arasındaki bağların puanlanmasını sağlayan Saldırı Tespit Sistemlerinden (STS) alınan geribeslemenin bulanık mantık ile sınıflandırılması detaylı olarak anlatılmıştır. Yönlendirmenin temelini oluşturan bulanık-genetik algoritma giriş-çıkış kısıtları ve çalışma algoritması detaylı açıklanmıştır. Beşinci bölümde ağ benzetim programı hakkında bilgi verilmiştir.

İşleyişi ve bölümleri işlenmiştir. Ardından protokolün benzetim sonuçları ve öneriler ele alınmıştır.

2. KABLOSUZ AĞLAR VE GÜVENLİĞİ

Kablosuz haberleşme 1895 yılında Guglielmo Marconi'nin Wight adasından 18 mil uzaktaki bir römorköre yaptığı yayın ile başlamıştır. İlk kablosuz haberleşme teknikleri analogdur. Bugün radyo haberleşme sistemlerinin birçoğu iletimlerini dijital bitler kullanarak yaparlar. Bu haberleşme sürekli bit iletimi veya "paket radyo" adı verilen paketler halindeki bit grupları ile oluşmaktadır. Kablosuz ağlarda paket tabanlı ilk network ALOHANET adında 1971 yılında Hawaii Üniversitesinde geliştirilmiştir [4]. 4 adaya dağılmış 7 kampüsteki bilgisayar merkezleri Oahu'da bulunan merkez bilgisayarı ile haberleşmekteydi. Sistem hub olarak merkez bilgisayarını kullanan Star topolojisinde bir ağ mimarisine sahipti. Haberleşmek isteyen iki bilgisayar merkezi hub üzerinden haberleşmek zorundaydı. ALOHANET kanal erişimi ve yönlendirme protokollerinin ilk şekillerini içermektedir [4]. Bu protokolleri oluşturan temel fikirler bugün hala kullanımdadır.

Kablolu ağların bant genişliği ve fiyat baskısı altında kalan kablosuz ağların belirli bir standarda kavuşması zaman almıştır. 1991 yılında Amerikan Elektrik Elektronik Mühendisleri Enstitüsü (IEEE - Institute of Electrical and Electronics Engineers) öncülüğünde IEEE 802.11 grubu kurulmuştur. Bu grup 1999 yılında IEEE 802.11 standardını çıkarmıştır [5]. Bu standart açık alanda 100 metre gibi kısa mesafeler için 11 Mbps bağlantı hızı ile haberleşmeyi sağlayabilmektedir. Haberleşme mesafesi açısından bu standart kablosuz yerel ağlar (Wireless Local Area Networks-WLAN) sınıfına dahildir [6]. Bu standartta merkezde bir erişim noktası(AP-Access Point) ve ona bağlı istasyonlar (STA-Stations) bulunmaktadır. STA'lar genelde AP kullanarak haberleşse bile kendi aralarında Ad-Hoc tarzında bir ağ kurabilirler. Bugün gelişen ihtiyaçlar ışığında, WLAN standardı olan IEEE 802.11 standardının IEEE 802.11a, 802.11b, 802.11g, 802.11n 802.11i gibi yeni versiyonları geliştirilmiş ve bu standart daha yaygın kullanılır hale getirilmiştir [7-10].

Daha geniş alanlarda kablosuz veri iletişimi için çalışmalar, 1996 yılında bazı telefon şirketlerinin DSL ve kablolu televizyon veri sistemlerinin yetersiz menzilleri

dolayısıyla alternatif genişbant kablosuz haberleşme sistemleri üretmesi ile başlamaktadır [6]. 1997 yılında genişbant internet erişimi için Clary çok kanallı çok noktalı dağıtım sistemlerini (Multichannel Multipoint Distribution System-MMDS) anlatmış, 30 Mbps uygulamalı ve 27 Mbps kullanılabilir paylaşımlı hızlarla haberleşebilen 50 km yarıçaplı sistem önermiştir [11]. 2000 yılında Agne Nordbotten yerel çok noktalı dağıtım sistemlerini (Local Multipoint Distribution System-LMDS) anlatmış, 38 Mbps uygulamalı, 25.6 Mbps kullanılabilir paylaşımlı hız ve 5 km yarıçapa sahip sistemleri incelemiştir. Bu sistemlerin kablolu sistemlerle karşılaştırmalarını yapmıştır. Küçük köy ve kasabalar için bu sistemin daha uygun olabileceğini göstermiştir. IEEE bünyesinde kurulan Çalışma Grubu 16, 2002 yılında IEEE 802.16 standardını oluşturmuştur [12]. 802.16 standardı tek noktadan çok noktaya (Point to Multipoint-PMP) topolojisinde sadece sabit ve birbirini gören antenler arasında 10-66 GHz bant aralığında haberleşmeyi düzenlemektedir. Kullanılan kanal bant genişliği ve modülasyon tipine göre 36-135 Mbps uygulamalı bant genişliğine sahiptir [13, 14].

2003 yılında birbirini görmeyen antenler için 2-11 GHz bant aralığını kullanan IEEE 802.16a standardı yayınlanmıştır. Bu standart aynı zamanda meş teknolojisini de desteklemektedir. Çeşitli hata düzeltmeleri ve düzenlemeler ile bu iki standart birleştirilerek 2004 yılında IEEE 802.16-2004 adı altında yayınlanmıştır [13]. 2005 yılında mobil kullanıcılar için IEEE 802.16e, 2006 yılında IEEE 802.16f, ve 2007 yılında IEEE 802.16g, IEEE 802.16k standartları düzenlenmiş ve bu standart diğer standartlarla beraber IEEE 802.16-2007 adı ile yayınlanmıştır. Böylece IEEE 802.16-2007 standardı 2-11 GHz ile birbirini görmeyen antenlerin haberleşmesini, 10-66 GHz ile birbirini gören antenlerin haberleşmesini, 2-6 GHz ile mobil kullanıcıların haberleşmesini sağlayan toplu bir standart halini almıştır. IEEE 802.16 standardında mobil kullanıcıların maksimum hareket hızları 30 km/s ve 30 Mbps uygulamalı veri iletişim hızları bulunmaktadır [15-18]. Hızlı tren gibi daha yüksek hareketlilik gerektiren hızlar için IEEE 802.20 mobil genişbant kablosuz erişim (Mobile Broadband Wireless Access-MBWA) standardı için çalışmalar devam etmektedir. Şu

anda taslak halinde olan çalışmalarda 250 km/s hareket hızlarında ve 1-10 Mbps paylaşımsız hızların desteklemesi planlanmaktadır [19, 20].

Kablosuz ağların iletişim hızlarını ve erişim menzillerini arttırmak için yapılan çalışmaların yanı sıra bu ağların güvenliği konusunda da çalışmalar yapılmaktadır. Kablosuz ağlarda veriler kablolu ağlarda olduğu gibi paketler halinde iletilmektedirler [21]. Gönderilen paketlerin içindeki bilgilerin, ağa karşı bozucu saldırılar yapılsa bile, hızlı bir şekilde ve değişmeden varış adresine iletimi çok önemlidir. Veri paketlerinin ağ üzerinde takip edecekleri güvenli yolun hesaplanmasından yönlendirme protokolleri sorumludurlar. Kablolu ağlarda, paketlerin yönlendirilmesi amacıyla iç alan (intra-domain) ve dış alan (inter-domain) olmak üzere iki alan mevcuttur. İç alanda, çoğunlukla mesafe vektörü (distance vector) yönlendirme protokolü veya bağ durumu (link state) yönlendirme protokolleri kullanılmaktadır. Dış alanda ise sınır kapısı (border gateway) yönlendirme protokolü kullanılmaktadır. Bu protokoller daha çok hatların kopması veya düğümlerin bozulması gibi basit hata durumları ile başa çıkabilecek şekilde tasarlanmışlardır [22]. Çünkü kablolu ağlarda saldırı gerçekleştirebilmek için o ağa fiziksel olarak bağlı olmak gerekir. Bu nedenle kablolu ağlarda güvenlik ikinci planda kalmıştır. Fakat kablosuz ağlarda ağa bağlanmak için fiziksel bir bağlantı gerekmemektedir. Kablosuz bir ağa, gerekli donanımı bulunan herhangi bir saldırgan rahatlıkla erişebilmektedir. Ayrıca kablolu ağlarda yönlendirme görevi yönlendiricilerde olduğu halde kablosuz ağlarda bu görev çoğunlukla hem kablosuz yönlendiricilerin hem de o ağı kullanan mobil kullanıcıların yükümlülüğündedir [23]. Kablosuz ağlarda bu nedenlerle güvenlik daha ön plandadır. Böylece kablosuz ağlarda yönlendirme protokolleri üzerinde güvenliğin arttırılmasına yönelik birçok çalışma yapılmıştır.

Hu ve arkadaşları tarafından önerilen "güvenli verimli ad hoc mesafe vektörü" (SEAD-Secure Efficient Ad-Hoc Distance Vector) [24] proaktif bir yönlendirme protokolüdür. "Varış noktası amaçlı ardışıl mesafe vektörü" (DSDV-Destination Sequenced Distance Vector) [25] baz alınarak dizayn edilmiştir. DSDV ile ortak olan

hedef, metrik, bir sonraki atlama (next hop) ve sıra numarası gibi alanların yanı sıra SEAD yönlendirme tablosu her giriş için bir sağlama değeri sağlamaktadır. Makalede saldırganın metrik ve sıra numaralarına saldırı düzenlenmesini engellemek için yönlendirme güncellemelerini koruma konusu üzerinde durulmuştur. Önerilen güvenlik protokolünde tek yönlü sağlama zincir fonksiyonu olarak adlandırılan H fonksiyonu, anahtar özelliktir. Her düğüm h_1, h_2, h_3, …, h_n değerleri listesini hesaplamaktadır. h_0'ın rassal başlangıç değerine göre $0 < i \leq n$ alınarak $h_i = H(h_{i-1})$ hesaplanmaktadır. Makale h_n'in gönderilmek istenen tüm alıcılara dağıtım mekanizmasının var olduğunu kabul etmektedir. Bir düğüm H fonksiyonunu ve h_n değerini biliyorsa herhangi bir h_i değerini hesaplayıp h_n ile karşılaştırıp giriş doğrulama işlemini gerçekleştirebilmektedir. Yönlendirme güncellemesinin doğrulanması için her yönlendirme tablosu girişine bir sağlama değeri düğümler tarafından eklenmektedir. j metriği ve i sıra numarası için h_{n-mi+j} değeri yönlendirme güncellemesi için doğrulamada kullanılmaktadır. Burada maksimum ağ çapı $(m-1)$ olarak alınmıştır. Saldırgan kendisine bildirilen sağlama değerinden daha küçük indeks değerlerine sahip bir sağlama değeri hesaplayamayacağı için, aynı hedefe daha büyük sıra numarası veya daha iyi bir metrik ile yönlendirme bildiremeyecektir. SEAD diğer düğümlerdeki sıra numarasını ve yönlendirme metriğini değiştirerek, yanlış yönlendirme durumları ortaya çıkarmaya çalışan saldırganlara karşı güçlü bir protokoldür. Fakat SEAD saldırganın bir sonraki atlama düğümü yanıltmasını veya yönlendirme güncellemesindeki hedef alanını değiştirmesini engelleyememektedir. Ayrıca saldırganın bir önceki güncellemeden öğrendiği sıra numarası ve metriği kullanarak başka bir hedefe yeni bir yönlendirme güncellemesi göndermesini engelleyememektedir [24].

Hu ve arkadaşları "verimli isteğe dayalı güvenli bir yönlendirme protokolü" (ARIADNE – an efficient on-demand secure routing protocol) [26] önermişlerdir. Bu protokol simetrik kriptografiye dayanmaktadır. Düğümlerde bulunan yönlendirmelerinin saldırıya uğramasını engellenmesini amaçlamaktadır. ARIADNE MAC adresi seviyesinde, iki düğüm arasında, paylaşılmış bir anahtar vasıtasıyla, yönlendirilmiş mesajların doğrulamasını sağlamaktadır. Fakat yönlendirilmiş

mesajların güvenli olarak doğrulanması için “Zaman verimli akışa sahip kayıp toleranslı doğrulama” (TESLA-Timed Efficient Stream Loss-tolerant Authentication) yayın doğrulama protokolünü kullanmaktadır [27]. ARIADNE “Dinamik Kaynak Yönlendirme ”(DSR-Dynamic Source Routing) temelli bir yapıdadır [23]. DSR gibi iki temel fonksiyon içermektedir; yönlendirmenin keşfi ve bakımından sorumludur. ARIADNE paylaşılmış anahtarların ve tek yönlü sağlama fonksiyonunun verimli bir bileşimini kullanmaktadır. Mesajın doğrulanması amacıyla alıcı ve verici için gizli bir anahtarın paylaşıldığı kabul edilmektedir. Şifreleme doğrulamayı sağlamaktayken, sağlama mekanizmasıysa düğümler arası atlamanın doğruluğunu sağlamaktadır. Ölü bir bağın olması durumunda, yönlendirme hata mesajı gönderilene iletilmektedir ve ara düğümler seçilen yoldaki ölü bağları kullanan yönlendirmeleri kaldırmaktadırlar. ARIADNE yönlendirme bilgisinin değiştirilmesine ve tekrar üretilmesi saldırılarına karşı önemli bir koruma sağlamaktadır. TESLA’nın gelişmiş bir versiyonu olan “geçici yular” (TIK-Temporal Leashes) ile beraber kullanıldığında wormhole saldırılarına karşı bağışıklık sağlamaktadır. Fakat bencil düğüm saldırılarına karşı açık bir yapısı bulunmaktadır. Gerçek hayatta kullanılması, anahtar değişimlerinin yapılması karmaşık olduğu için zordur [26].

Cravetz ve arkadaşları “güvenlik bilinçli yönlendirme” (SAR – Security Aware Routing) “isteğe dayalı mesafe vektör yönlendirme” [28] (AODV- Ad-hoc On-Demand Distance Vector Routing) [29] tabanlı, isteğe dayalı(on demand) bir yönlendirme protokolü önermişlerdir. SAR bir düğümün güven seviyesini ve yönlendirmenin güvenlik özelliklerini bir araya getirip kullanarak, istenen yönlendirme için kullanılmak üzere entegre güvenlik metriği oluşturmaktadır. Yönlendirme metriği olarak "güvenlik kalitesi" (QoP-Quality of Protection) oluşturulmuş böylece yol keşfiyle kalitatif güvenli yollar elde edilmiştir. QoP vektörü güvenlik seviyesi ile uygun kriptografik tekniklerin bir kombinasyonudur. SAR, güven hiyerarşi tabanlı bir notasyon oluşturarak Ad-hoc kablosuz ağların değişik güven seviyelerine bölmesini sağlamaktadır. Böylece kaynak ile varış noktası arasındaki haberleşmede görev alacak düğümler için gerekli olan minimum güven

seviyesini sağlamaktadır. Kablosuz olarak birbirine bağlı bir ağ olsa bile gerekli güven seviyesini sağlayacak yol olmayabilmektedir. SAR, AODV'den daha az yol üretmesine rağmen oluşturulan bu yollar istenen belirli bir güvenlik seviyesini sağlamaktadır [28].

Papadimitratos ve Haas "Güvenli Yönlendirme Protokolü" (SRP-Secure Routing Protocol) [30] önermişlerdir. SRP yönlendirme keşfinin engelleyen saldırılara karşı koruma sağlamaktadır. Böylece sistemin topolojik bilgisinin doğru elde edilmesi garanti edilmektedir. SRP'de başlangıç ve varış düğümleri arasındaki ara düğümler haberleşirken, verilerin kriptografik onaylanmasına ihtiyaç duymadan yapılabilmesi için düğümler arası güvenlik ilişkisi kurmak temel fikirdir. Bu güvenlik ilişkisinin kaynak ve hedef arasında paylaşılacak ortak $K_{Gİ}$ anahtarı ile elde edilebileceğini kabul edilmektedir. Ayrıca bu güvenlik ilişkisinin yönlendirme başlangıç fazından daha önce var olması gerekmektedir [30].

Sanzgiri ve arkadaşları "Ad-Hoc Ağlar için Güvenli Yönlendirme Protokolü" (ARAN-A Secure Routing Protocol for Ad Hoc Networks) [31] önermişlerdir. ARAN isteğe dayalı (on demand) bir yönlendirme protokoldür. Bu protokol yönetilebilir açık ortamlarda güvenli haberleşmeyi sağlamak üzere dizayn edilmiştir. Yönetilebilir açık ortamlardaki düğümler haberleşmenin başlangıcından önce birbirleriyle başlangıç parametrelerini paylaşırlar. Oturum anahtarları karşılıklı değiştirilir veya sertifika sunucusu gibi üçüncü şahıs üzerinden dağıtılır. ARAN'da her düğümün bir sertifikası vardır. Düğümler güvenilir sertifika sunucusu T'ye kimliklerini güvenli bir şekilde doğrulattıktan sonra sunucudan bir sertifika alırlar. Düğümler bu sertifikaları kullanarak birbirlerinin doğrulamasını yaparlar ve yönlendirme mesajlarının iletimini gerçekleştirirler. Sertifika Düğümün IP adresini açık anahtarı ve sertifikanın başlangıç ve bitiş tarihini içermektedir. Bu alanlar T sunucusu tarafından işaretlenir ve sabitlenir. A düğümü şu şekilde bir sertifika alır; $T \rightarrow A$: $cert_A=[IP_A, K_{A+}, t, e] K_{T-}$. Doğrulama sırasında, varış noktasına güvenli bir yol aranmaktadır. Ağdaki ara düğümlerin her biri yönlendirme çiftini saklamaktadır. Bu çift bir önceki düğüm ile varış düğümüdür. Yönlendirme mesajındaki tüm bilgiler

I başlangıç düğümünün özel anahtarı tarafından işaretlenmiştir ve sabittir. Zaman damgası (t) ve özel bir sayı (N_I) dan olan bir bileşim verinin yeni ve zamanlı olup olmadığını kontrol etmektedir. I düğümü her yönlendirme yolu için keşif isteğinde bulunduğunda N_I özel sayısı tek tek artmaktadır. İmza yolu değiştirecek ve döngü oluşturabilecek spoofing saldırılarını engeller. Kaynak düğümü I, varış düğümü D'ye erişmek için bir yol keşif paketi (YKP) yayınlar [31].

İlk defa YKP'yi alan her düğüm diğer ara düğümlerin imzalarını çıkarır, daha sonra kendi anahtarı ile YKP'yi imzalar ve tüm komşu düğümlerine yayımlar. Bu olay D düğümüne YKP paketi ulaşana kadar devam etmektedir. D düğümü YKP paketini aldıktan sonra Cevap (REP) paketini ters yoldan I kaynak düğümüne geri gönderir. I düğümü REP paketini aldığında D'nin imzasını ve N_I özel sayısını kontrol eder. Düğümlerde yer alan yönlendirme tablolarında bulunan yönlendirme girdileri zaman aşımına uğrar ve belli bir süre kullanılmadıkları zaman otomatik olarak kaldırılırlar. Ayrıca hareketlilikten kaynaklanan yol kırılmalarında düğümler hata mesajı göndererek göndericiyi uyarırlar.

ARAN önceden belirlenmiş kriptografik sertifikalar kullanarak, doğrulama ve inkâr edememeyi sağlamaktadır. Yapılan benzetimler yol keşfinde ve bu yolların yönetiminde başarılı olduğunu fakat paketlerin çok büyümeleri nedeniyle toplam yönlendirme yükünün ağır olduğunu göstermiştir. Ağır simetrik kriptografik hesaplamalar gerektirdiğinden enerji yönünden de başarılı değildir. Ayrıca wormhole saldırılarını engellemez. Eğer düğümler arasında zaman senkronizasyonu yoksa tekrar saldırılarına karşı da açıktır.

Nie ve arkadaşları "Bulanık mantık tabanlı güvenlik seviyeli yönlendirme protokolü" (FLSL-Fuzzy Logic Based Security-Level Routing Protocol) [32] önermişlerdir. Bu protokolde en yüksek seviyede iletişim sağlanabilmesi için bulanık mantık kullanılmaktadır. Protokolde anahtar uzunluğu (*l*) anahtar değiştirme frekansı (*f*) ve düğüm sayısı (*n*) alınmış ve çıktı olarak güvenlik seviyesi (*s*) belirlenmiştir. Bu

değişkenler arasında $s \propto l \bullet f \bullet n^{-1}$ bağıntısı olduğu önerilmiştir. Bu değerler bulanıklaştırılarak istenen güvenlik seviyesine ulaşılmaya çalışılmıştır.

Literatürde yayınlanmış başlıca güvenlik protokolleri ve bu protokollerin özellikleri Çizelge 2.1'de özet halinde sunulmuştur.

Çizelge 2.1. Literatürde bulunan kablosuz güvenli haberleşme protokolleri ve bu protokollerin özellikleri

Protokol	**Güvenlik Mekanizması**	**Engellenen Saldırılar**	**Açıklamalar**
SEAD [24]	Tek yönlü sağlama zincirleri	Saldırganın yönlendirme güncelleme paketlerine daha iyi metrik veya sekans numarası yerleştirerek saldırı düzenlemesini engellemektedir.	• DSDV ile beraber kullanılmaktadır. • Yönlendirme güncelleme paketlerini korumak için dizayn edilmiştir. • Saldırganın diğer alanları değiştirmesini engelleyememektedir. • Saldırganın öğrendiği sekans numarası ve metriği kullanarak yeni yol güncellemeleri göndermesini engelleyememektedir.
ARIADNE [26]	Tek yönlü sağlama zincirleri	Saldırganın aralarında belirli bir anahtar anlaşması olmayan düğümlerin haberleşme yollarının değişmesini engellemektedir.	• DSR ile kullanılmaktadır. • Yönlendirme bilgisinin değiştirilmesi saldırılarını engellemektedir. • Bencil düğüm saldırılarına açıktır.
SAR [28]	Korunma kalitesi metriği	Yol güncelleme paketlerinde tekrar saldırılarını engellemek için sekans numaraları ve zaman damgaları kullanmaktadır.	• AODV ile beraber kullanılmaktadır. • Üretilen yol ara-düğüm sayısı anlamında en kısa yol olmayabilir, fakat daha güvenlidir. • Değiştirme ve üretim(fabrication) saldırılarına karşı koruma sağlamaktadır.
SRP [30]	Güvenli sertifika sunucusu	Yönlendirme keşfini engelleyen saldırılara karşı koruma sağlamaktadır. Böylece sistemin topolojik bilgisinin doğru elde edilmesi sağlanmaktadır.	• DSR ve ZRP ile beraber kullanılmaktadır. • Yönlendirme yönetim mesajları için doğrulama mekanizması bulunmamaktadır. • Wormhole ve görünmez düğüm saldırılarına açıktır.
ARAN [31]	Güvenli sertifika sunucusu	Doğrulama ve inkar edilememe servisleri sağlamaktadır.	• AODV ve DSR ile beraber kullanılmaktadır. • Ağır asimetrik şifreleme hesapları gerektirmektedir. • Dakik zaman senkronizasyonu yoksa wormhole saldırılarına açıktır.
CONFIDANT [33]	• Monitör • İtibar sistemi • Dizin yöneticisi • Güven yöneticisi	Paket iletimi ve yönlendirme saldırılarını engellemektedir.	• DSR ile beraber kullanılmaktadır. • İtibar sistemi temelinde oluşturulmuş tespit sisteminin limitleri bulunmaktadır. • Spoofing ve Sybil saldırılarına açıktır.

Çizelge 2.1. Literatürde bulunan kablosuz güvenli haberleşme protokolleri ve bu protokollerin özellikleri (devam)

Rushing Saldırıları ve Korunma [34, 35]	• Güvenli komşu tespiti • Güvenli yol delagasyonu • Rastgeleleştirilmiş yönlendirme isteği ile yönlendirme	Bir düğüm tarafından gönderilen toplam istekleri limitlemek ve rastgele iletmek rushing saldırılarını belirli bir seviyeye kadar engellemektedir.	• DSR ve ARIADNE ile beraber kullanılmaktadır. • Saldırgan çok fazla düğüm ele geçirebilirse, rushing saldırılarına açıktır. • Diğer protokollerden daha fazla maliyeti vardır.
Wormhole Saldırıları ve Korunma [36]	Paket tasması Merkle sağlama ağacı Tek yönlü sağlama zincirleri	Paket tasması ile beraber TIK uygulanırsa wormhole ve DoS saldırılarını engellemektedir.	• Uygulanan ağır kriptografik yöntemlerden ötürü kaynak sıkıntısı olan ağlar için uygun değildir. • Dakik zaman senkronizasyonu elde etmek kolay değildir.
Sybil Saldırıları ve Korunma [37]	Radyo kaynağı testi Önceden rastgele anahtar dağıtımı Tek yollu pseudo-random sağlama fonksiyonu		
TESLA [27]	Tek yönlü sağlama fonksiyonu	Güvenli iletişim sağlamak için birbirine bağlı ve geciktirilmiş zaman senkronizasyonu kullanmaktadır.	DoS saldırılarına açıktır. (Zararlı düğümler buffer overflow durumu oluşturabilmektedir.)
FLSL [32]	Bulanıklaştırılmış güvenlik paramatreleri	Network büyüklüğüne ve diğer parametrelere göre sistem güvenliğinin en üst seviyede tutulması amaçlanmaktadır.	Sybil ve wormhole saldırılarına açıktır.

İncelenen güvenlik protokollerinden kablosuz ağlar için Cravetz tarafından önerilen Security Aware Routing (SAR) protokolünde yer alan entegre güvenlik metriği kavramı ağ kurulurken oluşturulan ve sabit bir yapıdır. Ayrıca güvenlik ilişkisinin zamana bağlı olarak değişmediği kabul edilmiştir. Fakat bu ilişki gerçek hayatta zamana bağlı olarak değişebilir.

Bu yapı sabit olduğu için SAR protokolünün zaman içinde değişen ağlarda verimi azalır. Çünkü ağdaki güvenlik ilişkisi zamanla değiştiği halde düğümler üzerine kayıtlı sabit güvenlik ilişkisi zamanla geçerliliğini yitirebilir.

SAR protokolünde bulunan sabit güvenlik ilişkisi yapısının dinamik hale getirilmesi amaçlanan bu yönlendirme protokolünde, mevcut literatürde bulunan SAR yapısının bu iş için uygun olmadığı gözlemlenmiştir.

Zamana bağlı dinamik bir yönlendirme yapısının oluşması nedeniyle mevcut SAR protokolünün kullandığı AODV tabanlı yönlendirme yerine link state routing (LS) tabanlı bir yönlendirme algoritması tasarlanmıştır.

Hazırlanan bu algoritmada belirlenen bir güvenlik seviyesini karşılayan yol çözümü karşıladığı için, çözüme daha hızlı ulaşabilmek amacıyla genetik algoritma kullanılmıştır. Ayrıca genetik algoritmaya giriş olacak dinamik güvenlik seviyeleri için bulanık mantık kümelerinde kullanılan dilsel ifadeler tercih edilmiştir. Böylece saldırılara karşı uyum sağlayarak adapte olabilen bir protokol elde edilmiştir.

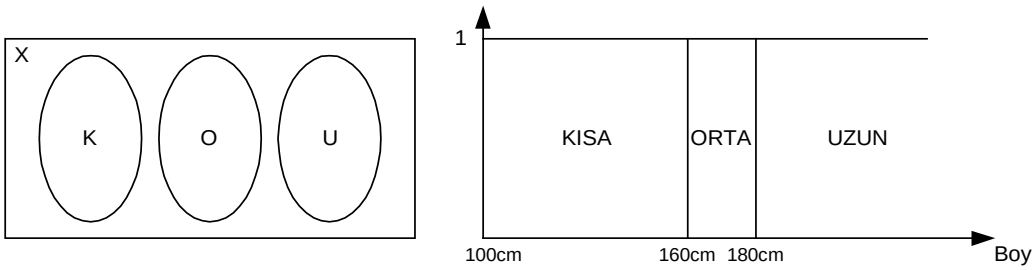
Üçüncü bölümde anlatılan gerekler dahilinde hazırlanan güvenlik bilinçli zeki yönlendirme protokolünün dayandığı temel prensipler irdelenmiştir. Dördüncü bölümde protokolün yapısı ve işleyişi kapsamlı olarak anlatılmıştır.

3. PROTOKOLDE KULLANILAN METODLAR

Geliştirilen protokolde yönlendirmenin ve güvenliğin sağlanabilmesi için çeşitli metotlar kullanılmıştır. Protokole bilinç kazandıran bu metotlar bu bölümde açıklanmıştır.

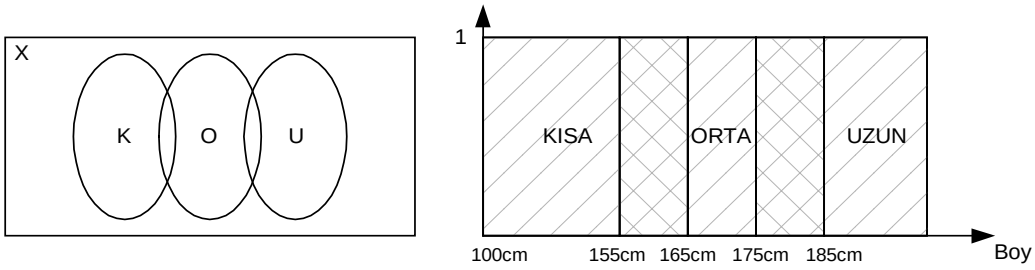
3.1. Bulanık Kümeler

Geleneksel kümeler olarak bilinen ve kesin sınırlara sahip olan kümeler, ait oldukları evrensel kümenin her bir elemanına 0 veya 1 değerini atayarak, o elemanın kendisine ait olup olmadığını belirler. Bir nesne 1 değerini alıyorsa kümenin elemanıdır. 0 değerini alıyorsa elemanı değildir. Örneğin bir evrensel küme X, cm olarak insanların boy uzunluklarının kümesi olsun. Burada tanımlanacak K kısa boyluların, O orta boyluların ve U uzun boyluların kümesi Şekil 3.1' deki gibi gösterilebilir.



Şekil 3.1. Boy uzunluklarına ait klasik kümeler

Yukarıdaki şekilde görüldüğü gibi 160 cm' nin altı kısa boylu, 160 cm ile 180 cm arası orta boylu ve 180 cm' nin üzeri uzun boylu olarak kabul edilmiştir. Burada 159 cm boyunda olan bir kişi kısa, 161 cm boyunda olan bir kişi orta boylu, aynı şekilde 179 cm uzunluğundaki bir kişi orta boylu iken, 181 cm uzunluğunda olan birisi uzun boylu olarak ifade edilmektedir. Oysa gerçek hayatta 159 cm uzunluğunda olan birisi ile 161 cm olan veya 179 cm uzunluğunda olan birisi ile 181 cm olan birisi arasında çok fazla fark yoktur. 159 cm orta boylu sayılabileceği gibi 161 cm' de kısa boylu sayılabilir. Eğer bu değerler her iki kümeye ait olarak düşünülürse o zamanda Şekil 3.2' deki durum ortaya çıkmaktadır.

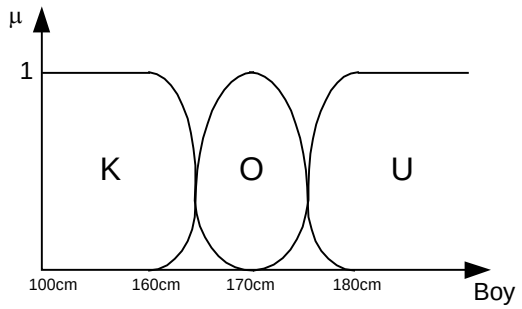


Şekil 3.2. Boy uzunlukları klasik kümelerinde kesişim

Burada da görüldüğü gibi 155 cm ile 165 cm arası hem kısa boylu hem de orta boylu, 175 cm ile 185 cm arası hem orta boylu hem de uzun boylu olarak kabul edilmiştir. Bir önceki durumda ortaya çıkan keskin geçişler daha değişik şekildedir ve ortaya yeni bir problem çıkmıştır. 164 cm olan birisi ile 156 cm olan birisinin hem K kümesine hem de O kümesine aitlik derecesi 1 değerinde olmuştur. Gerçekte 164 cm olan birisi 156 cm olan birisine göre daha çok O kümesine aittir, aynı durumlar ısı ve hız ile ilgili ifadelerde de meydana gelmektedir.

Bu tür problemlere, bulanık küme teorisi çok güzel bir çözüm getirmiştir. Nesnelere keskin kümelerin (0,1) değerlerini vererek eleman olup olmadığına karar veren fonksiyonuna karşılık, [0,1] aralığında değişebilen değerler veren bir fonksiyon ortaya konulmuştur. Bulanık küme tarafından tanımlanan ve ilgili kümeye aitlik derecesi büyük olan elemanlara 1'e doğru büyüyen, aitlik derecesi küçük olan elemanlara ise 0'a doğru küçülen üyelik değeri verebilen bu fonksiyona üyelik fonksiyonu denilmektedir [39]. Boy uzunlukları ile ilgili kümeler bulanık kümelerle Şekil 3.3' deki gibi gösterilebilir.

Şekil 3.3'de görüldüğü gibi 160 cm'den 170 cm'ye doğru büyüyen değerler için K kümesine ait olma derecesi düşerken O kümesine ait olma derecesi artmaktadır. Üyelik derecesi olarak adlandırılan bu değerler 170 cm ile 180 cm arasında değişen değerler içinde O ve U kümesine aitlik seviyesini göstermektedir.



Şekil 3.3. Boy uzunlukları bulanık kümeleri

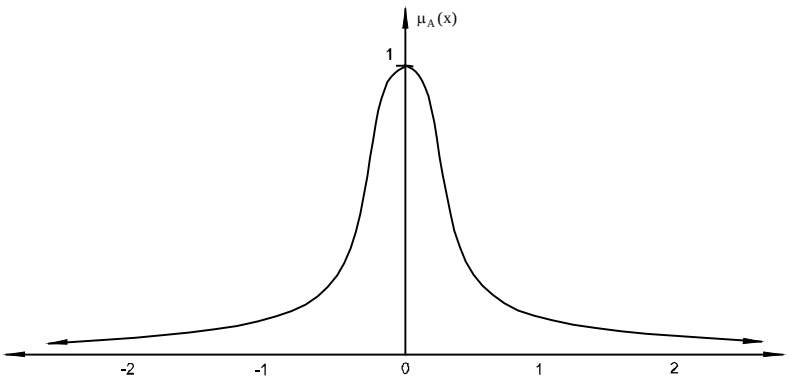
X evrensel kümesinde tanımlanan, bulanık küme A için μ_A üyelik fonksiyonu şöyle ifade edilir [38];

$$\mu_A : X \rightarrow [0,1] \tag{3.1}$$

μ_A üyelik fonksiyonu $[0,1]$ kapalı aralığında gerçek bir sayıyı göstermektedir. Örnek olarak gerçek sayılar kümesinde üyelik fonksiyonu $\mu_A(x)$ aşağıdaki gibi tanımlanabilir;

$$\mu_A(x) = \frac{1}{1+10x^2} \tag{3.2}$$

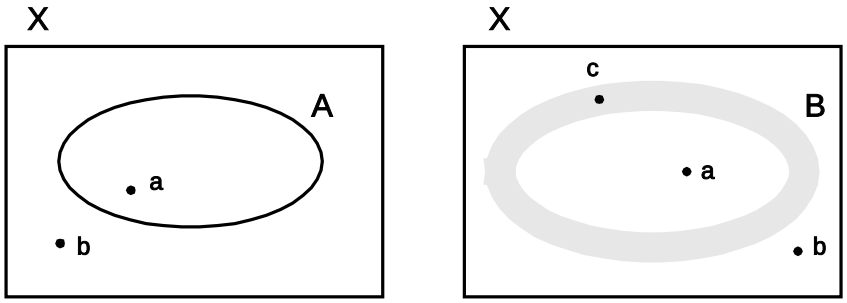
Bu fonksiyonun grafiği Şekil 3.4' de görülmektedir [40].



Şekil 3.4. Örnek üyelik fonksiyonu grafiği

A bulanık kümesine ait olan herhangi bir gerçek sayının üyelik derecesi bu fonksiyon kullanılarak bulunabilir. Örneğin 3 sayısının üyelik derecesi 0.01, 1 sayısının 0.09, 0.25 sayısının üyelik derecesi 0.62 ve 0 sayısının üyelik derecesi de 1 olarak bulunur.

X evrensel kümesinde tanımlanmış A keskin kümesi ile B bulanık kümesi Şekil 3.5'de görülmektedir.



(a) (b)

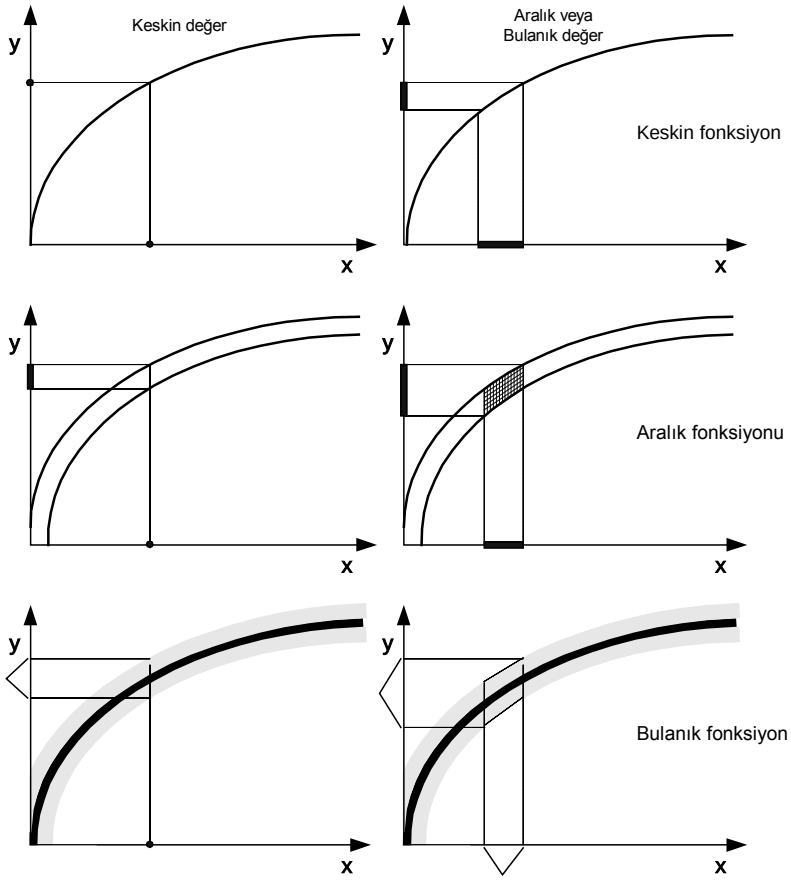
Şekil 3.5. (a) A keskin kümesi (b) B bulanık kümesi

Şekil 3.6'da ise keskin, aralıklı ve bulanık fonksiyonlar verilmiştir.

Bulanık kümeler ilk olarak 1965 yılında Lütfi A. Zadeh tarafından kesin değere sahip olmayan bulanık bilgilerin gösterimi ve işlemlerini ifade etmek için ortaya atılmıştır [38]. Daha sonra Mamdani [39], Takagi ve Sugeno [40] ile Tsukamoto [41] farklı bulanık modeller geliştirmişlerdir. Bulanık mantığın genel karakteristik özellikleri Zadeh tarafından şu şekilde ifade edilmiştir [42];

- Bulanık mantıkta, kesin değerlere dayanan düşünme yerine yaklaşık düşünme kullanılır.
- Bulanık mantıkta her şey [0,1] aralığında belirli bir derece ile gösterilir.
- Bulanık mantıkta bilgi büyük, küçük, çok az gibi dilsel ifadeler şeklindedir.
- Bulanık çıkarım işlemi dilsel ifadeler arasında tanımlanan kurallar ile yapılır.
- Her mantıksal sistem bulanık olarak ifade edilebilir.
- Bulanık mantık matematiksel modeli çok zor elde edilen sistemler için çok uygundur.

- Bulanık mantık tam olarak bilinmeyen veya eksik girilen bilgilere göre işlem yapma yeteneğine sahiptir.



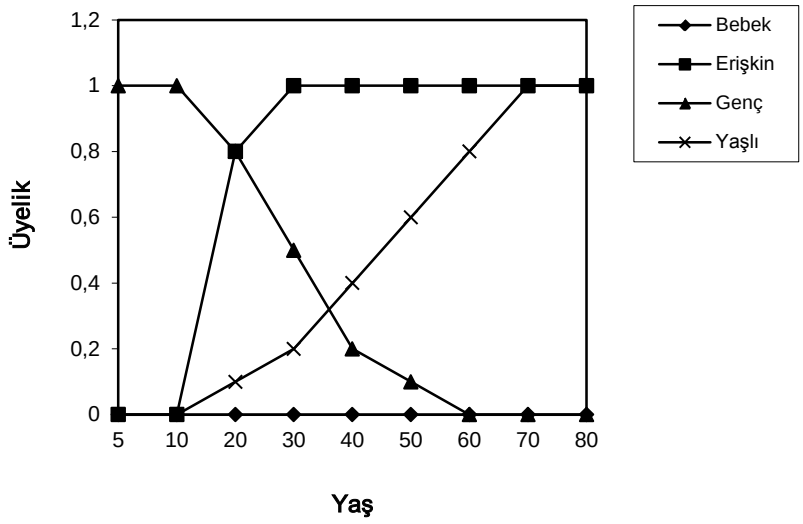
Şekil 3.6. Keskin, aralık ve bulanık fonksiyonlar

3.1.1. Bulanık küme kavramları

Bulanık kümelerde kullanılan semboller ve ifadeler ile keskin kümelerde kullanılan ifadelerin büyük bir bölümü benzemektedir. Küçük bir keskin evrensel kümenin elemanlarının dört farklı bulanık kümeye üyelik dereceleri Çizelge 3.1'de ve grafiği de Şekil 3.7'de gösterilmiştir. Burada $X=\{5,10,20,30,40,50,60,70,80\}$ bütün yaşların kümesini ve bebek, erişkin, genç, yaşlı bulanık kümeleri de X evrensel kümesinden seçilen değerlerin üyelik derecelerini göstermektedir [43].

Çizelge 3.1. Bulanık kümeler

Yaş	Bebek	Erişkin	Genç	Yaşlı
5	0	0	1	0
10	0	0	1	0
20	0	0.8	0.8	0.1
30	0	1	0.5	0.2
40	0	1	0.2	0.4
50	0	1	0.1	0.6
60	0	1	0	0.8
70	0	1	0	1
80	0	1	0	1



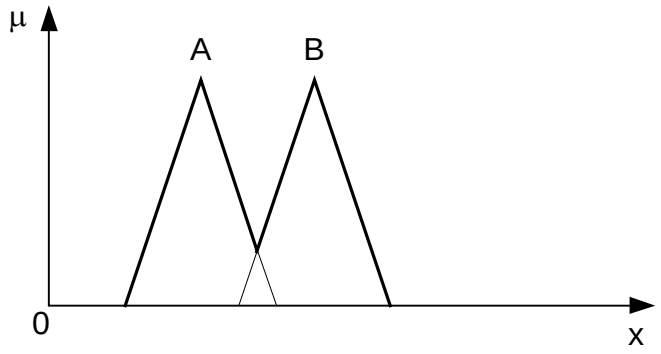
Şekil 3.7. Çizelge 3.1' de tanımlanan bulanık kümelerin grafik gösterimi

3.1.2. Birleşim kümesi

Her $x \in X$ için A ve B bulanık kümelerinin, bulanık birleşim kümesi şöyle ifade edilir;

$$\mu_{A\cup B}(x) = \max\left[\mu_A(x), \mu_B(x)\right] \tag{3.3}$$

$A \cup B$ kümesinin, herhangi bir x∈X için elemanlarının üyelik derecesi, A ve B kümelerinden üyelik derecesi büyük olana eşittir. Bu tanımlamadan anlaşılacağı gibi A ve B kümelerinin her biri $A \cup B$ kümesinin alt kümesidir. Şekil 3.8'de A ve B olarak tanımlanan iki bulanık kümenin birleşimi görülmektedir.



Şekil 3.8. Bulanık kümelerde birleşim

Genç ve yaşlı kümelerinin birleşim kümesinin

Genç ∪ Yaşlı= 1/5+1/10+0.8/20+0.5/30+0.4/40+0.6/50+0.8/60+1/70+1/80,

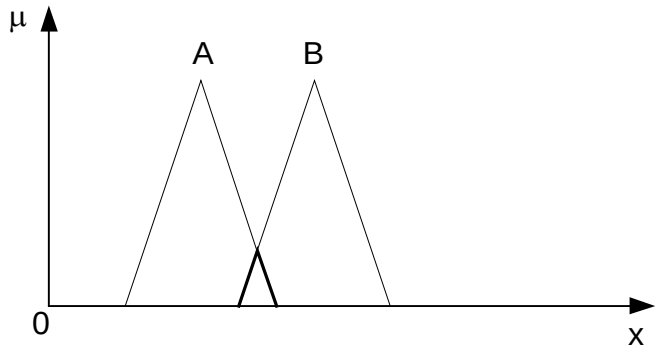
olduğu görülmektedir.

3.1.3. Kesişim kümesi

A ve B bulanık kümelerinin kesişim kümesindeki bir x elemanının üyelik derecesi, x'in A ve B kümelerindeki üyelik derecelerinden küçük olana eşittir.

$$\mu_{A\cap B}(x) = \min\left[\mu_A(x), \mu_B(x)\right] \tag{3.4}$$

Bu tanımlamadan da görüleceği gibi $A \cap B$ kümesi, A ve B kümelerinin alt kümesidir. Şekil 3.9'da A ve B olarak tanımlanan iki bulanık kümenin kesişimi görülmektedir.



Şekil 3.9. Bulanık kümelerde kesişim

Çizelge 3.1' deki genç ve yaşlı kümelerinin kesişim kümesi,

Genç $\cap$ Yaşlı = 0.1/20 + 0.2/30 + 0.2/40 + 0.1/50,

olmaktadır [44].

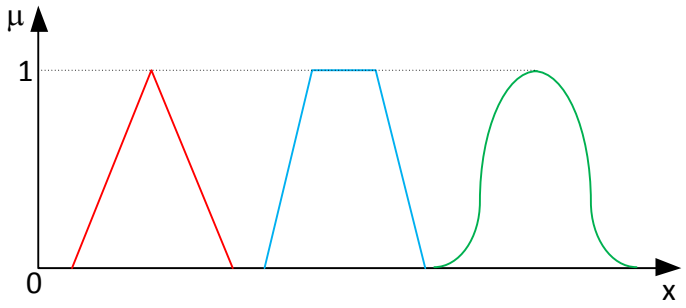
3.1.4. Bulanık mantık

Boolean mantık tabanlı kümelerde bir nesne, kümenin ya tam elemanı veya hiç elemanı değildir. Nesnenin üyelik değeri 1 ise tam eleman, 0 ise hiç elemanı olmamaktadır. Bulanık mantık, insanın günlük yaşantısında nesnelere verdiği üyelik değerlerini, dolayısıyla insan davranışlarını taklit eder [45]. Örneğin elini suya sokan bir kişi hiçbir zaman tam olarak ısısını bilemez, onun yerine sıcak, az sıcak, soğuk, çok soğuk gibi dilsel niteleyiciler kullanır.

Bulanık mantık denetleyici herhangi bir $x \in X'$ e [0, 1] kapalı aralığında bir üyelik derecesi belirler. Bulanık mantık kesin olmayan yada matematiksel olarak tam

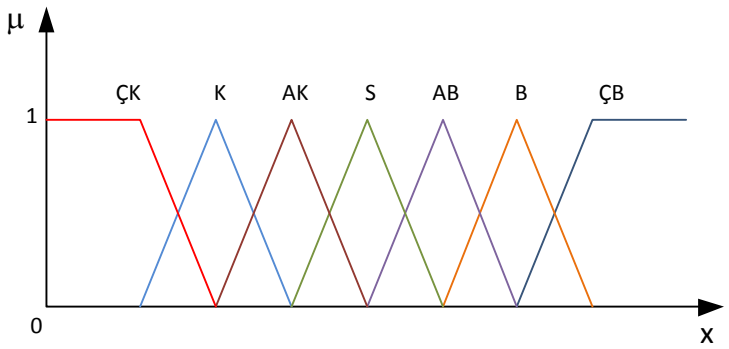
modellenemeyen bilgilerle ilgilenmesine rağmen, sözel nitelikli matematiksel teoriye dayanmaktadır.

Bulanık mantık sisteminin temeli, üyelik fonksiyonlarından ortaya çıkarılan dilsel değişkenlerin oluşturduğu girişleri karar verme sürecinde kullanmaktır. Bu değişkenler, dilsel EĞER-ÖYLE İSE kuralların ön şartları tarafından birbirleriyle eşleşirler [46]. Her bir kuralın sonucu, girişlerin üyelik derecelerinden, durulaştırma metoduyla sayısal bir değer elde edilmesiyle belirlenir. Bulanık mantık sistemin kural listesi ve üyelik fonksiyonu dizaynı için genellikle uzman operatörden sağlanan bilgiler kullanılmaktadır. Üyelik fonksiyonları Şekil 3.10' te görüldüğü gibi üçgen, yamuk, çan eğrisi olarak kullanılmaktadır. Denetimi yapılan sistemin özelliğine göre bunların dışında uygun bir fonksiyonda kullanılabilir.



Şekil 3.10. Üçgen, yamuk ve çan eğrisi üyelik fonksiyonları

Üyelik fonksiyonları genellikle küçük, orta, büyük olarak 3, küçük, orta küçük, orta, orta büyük, büyük olarak 5 veya çok küçük, küçük, az küçük, sıfır, az büyük, büyük, çok büyük olarak 7 etiketle tanımlanmaktadır. En yaygın kullanılan 7 etiketli üyelik fonksiyonu Şekil 3.11' de görülmektedir.



Şekil 3.11. Yedi etiketli üyelik fonksiyonu

X evrensel kümesindeki A bulanık kümesi sıralı çiftler halinde gösterilebilir. Her bir çift eleman x' i ve üyelik derecesini ifade etmektedir.

$$A = \{(x, \mu_A(x)) \mid x \in X\} \tag{3.5}$$

3.1.5. Bulanık sistemlerin avantajları ve dezavantajları

Bulanık sistemlerin literatürde en çok yayınlanmış avantajları, oluşturulma aşamasında matematiksel modele ihtiyaç duyulmaması ve sistemin basit bir şekilde dilsel ifadelerle yorumuna bağlı olarak denetiminin yapılabilmesidir. Bunun yanısıra en sık belirtilen dezavantajları ise üyelik fonksiyonlarının ayarlanmasının uzun zaman alması ve öğrenme kabiliyeti olmamasıdır [47]. Ayrıca denetlenen sistemin kararlılık analizi için kesin bir yöntem olmaması bulanık sistemlerin temel sorunudur [48]. Bulanık sistemlere ait avantajlar ve dezavantajlar Çizelge 3.2'te verilmiştir [44].

Çizelge 3.2. Bulanık sistemin avantajları ve dezavantajları

Avantajlar
Matematiksel modele ihtiyaç duyulmaz
Uzman kişiden elde edilen kural tabanı bilgisi kullanılabilir
Sistemin basit yorumlamasına dayanarak bulanık sistem oluşturulabilir
Dezavantajlar
Mutlaka kural tanımlaması gerekir
Öğrenme kabiliyeti yoktur
Üyelik fonksiyonlarının parametrelerinin ayarlanmasında belirli metod yoktur
Değişik sistemlere adaptasyon çok zordur

3.2. Genetik Algoritmalar

Önerilen protokolde yol kurulumu için genetik algoritma kullanılmaktadır. Yol kurulumunun gerçek zamanlı olarak oluşturulmasından dolayı deterministik yöntemler daha iyi sonuç bulsalar bile nondeterministik yöntemlere göre uzun zaman gerektirmektedir. Bu yüzden belirli bir seviyede uygunluğa sahip yol kurulumu sistem için gerekli ve yeterli olmaktadır.

Genetik algoritmalar; doğal seleksiyon prensibinden yola çıkılarak geliştirilmiş *arama* algoritmalarıdır. Algoritma, belirli bir uzunluğa sahip dizilerden oluşmuş bir veri yığınına sahiptir. Yığın içindeki her bir dizi, çözüm uzayında bir noktayı temsil eder. Bu diziler aynı zamanda üreme yolu ile varlığını sürdürmeye aday olan birer bireydir. Algoritmanın temel işleyişi, çözüme uygun olmayan bireyleri elemek, çözüme daha uygun bireyleri seçmek ve seçilen bireylerden yeni bireyler üretmek doğrultusundadır. Algoritmanın işleyişi aşamalı olarak düşünüldüğünde temel prensibinin eleme olduğu anlaşılmaktadır. İkinci prensip ise, elemeyi aşan bireylerden yararlanılarak olası yeni çözümler elde etmektir. Bu da bireyler arasındaki bilgi alışverişi ile sağlanır. Bireyler arası rassal bilgi alışverişi, arama işleminin, çözüm uzayının daha uygun noktalarında devam etmesini sağlar [49, 50].

Genetik Algoritma (GA) stokastik bir arama yöntemidir. Darwin'in öne sürdüğü evrim teorisinin, "en uygun olan yaşar" ilkesine dayanmaktadır. Biyolojik sistemlerin gelişim sürecini modelleyen GA, ilk olarak Holland tarafından önerilmiştir [51]. Sezgisel bir yöntem olan GA, problem için en optimum sonucu bulamayabilir, ancak bilinen metotlarla çözülemeyen veya çözüm zamanı çok büyük olan problemlerde optimuma çok yakın çözümler vermektedir. Holland'ın araştırmasının amacı iki yönlüdür:

i. Doğal sistemlerde görülen adaptasyon (ortama uyum yeteneği) kavramını açıklamak.
ii. Doğal sistemlerin temel işleyişini, yapay yazılım sistemleri aracılığı ile modellemek.

Doğal sistemler, oldukça sağlam ve kararlı yapıdadırlar. Uyum yeteneğinin nasıl gelişip işlediğini öğrenmenin en iyi yolu, biyolojik sistemler üzerindeki çalışmalardır. Genetik algoritmaların karmaşık arama uzaylarına uygulandığında, kararlı çözümlere ulaştıkları, bu çalışmanın gerçekleşmesinde yararlanılan kaynaklarda da görüleceği üzere, kuramsal ve deneysel çalışmalar ile kanıtlanmıştır. Etkili ve verimli bir yöntem olduğu kanıtlandıktan sonra çeşitli bilim dallarının yanısıra iş dünyası ve mühendislikte geniş bir uygulama alanı bulmuştur [52].

Genetik algoritmaların geniş bir uygulama alanı bulmasının en önemli nedeni, kuşkusuz hesaplamalarda sağladığı basitlik ve arama işlemlerindeki iyileştirme gücüdür. Ayrıca klasik yöntemlerde karşılaşılan, arama uzayında süreklilik, türevin alınabilirliği gibi sınırlayıcı özellikler gerektirmeyişi de avantajlarını ve tercih edilirliğini artırmaktadır.

Genetik algoritmalar belirli sayıda çözümden oluşan bir çözüm kümesiyle başlar (başlangıç popülasyonu). Biyolojik modellerde her çözüm önerisi bir bireye, bireylerin oluşturduğu küme ise popülasyona karşılık gelmektedir. Algoritmanın her iterasyonunda önce çözüm açısından daha uygun bireyler seçilir, daha sonra yeni bir

kuşak oluşturacak bireyler arasında rassal olarak bilgi alışverişi yapılarak, yeni popülasyona ulaşılır. Bireylerin, çiftleşme ve üreme kapasiteleri, hayatta kalma olasılıkları ve yaşama sürelerinin belirlenmesine dayanan popülasyon denetimi, genetik algoritmanın esasını oluşturmaktadır. Her iterasyon sonunda, çözüme daha uygun bireyler elde edilir. Yeni bireylerin üretilmesinde çaprazlama, mutasyon gibi operatörler rassal işlem yaptığından, her iterasyon sonucunda elde edilen çözüm kümesi de rassaldır. Bu nedenle GA, yönlendirilmiş rassal arama yöntemi olarak da adlandırılmaktadır.

Bilgisayar terminolojisi ile bir GA, mümkün çözümlerin kodlandığı dizilerin oluşturduğu populasyon ile biyolojik özellikleri taklit eden operatörlerin oluşturduğu bir kümeden oluşur. Çizelge 3.3'de verilen ve basit GA olarak adlandırılan algoritma, yapısal programlama diline uygun, biyolojik özelliklerle modellenmiş ve GA' nın temel işleyiş prensibini açıklayıcı niteliktedir [52].

Çizelge 3.3. Basit GA

Başla n elemanlı başlangıç yığınını (popülasyon) oluştur. Popülasyon içindeki bireyleri belirle
Bireylerin uygunluk değerlerini belirle Başla *1'den n'* e kadar *tekrarla* *n.* bireyi seç gerekiyorsa *n.* bireyi değişikliğe (genetik operatörlerle) uğrat *n.* bireyi değerlendir Bitir (Eleme ve hata kriterlerini işlet) *olmadıkça başa dön* Bitir.

Basit bir GA' nın ilk aşamasında, varolan bütün çözümlerin bir alt kümesi olacak

biçimde bir başlangıç popülasyonu oluşturulur. Popülasyon içindeki bireyler birer dizi biçiminde kodlanır. Her dizi biyolojik olarak bir kromozoma eşdeğerdir. GA'nın herhangi bir adımındaki popülasyon, nesil veya kuşak (generation) olarak adlandırılır. Popülasyon içindeki dizilere birer uygunluk değeri (fitness value) atanır. Uygunluk değeri bir bireyin genlerinin, bir sonraki nesile taşınma şansını belirlemek üzere atanan değerdir. Bir dizinin uygunluk değeri aynı zamanda, problemin uygunluk fonksiyonu (fitness function) değerini belirler. Problemin yapısına göre seçilecek amaç fonksiyonu ile elde edilecek uygunluk değerleri algoritmanın matematiksel tabanını kolaylaştırmak amaçlıdır. Algoritma içinde yer alan yeni nesil üretme, eleme ve en uygun çözümü belirleme aşamalarında seçilecek kriterler, güçlü olanın şansını rastsal olarak artıran fonksiyonlar ile ifade edildiğinde hem yöntemin asıl mantığından uzaklaşılmamış, hem de algoritmanın ihtiyacı olan matematiksel dayanak üretilmiş olur.

Tipik bir GA uygulamasında, her iterasyonda sırası ile şu temel işlemler gerçekleştirilmektedir:

1. Yeniden Üretim İşlemi (Reproduction): Varolan populasyondan bir sonraki nesile taşınacak bireylerin seçilmesi işlemidir. Yeni nesile taşınacak bireyler, genetik olarak daha üstün özelliklere sahip olanlardır.

2.Genetik Operatörler (Çaprazlama ve/veya Mutasyon): Seçme işlemi ile elde edilen populasyonda bireylerin herbirinin belli bir bölümüne uygulanan genetik operatörler, çaprazlama ve mutasyon operatörleridir. Bu operatörler yardımı ile önceki neslin genetik bilgilerinden yararlanılarak yeni bir nesil, diğer bir deyişle yeni çözüm adayları üretilmiş olur. Çaprazlama operatörü ile önceki populasyondan seçilen bireyler arasında bilgi değişimi sağlanır. Mutasyonun amacı ise dizilerin bir kısmında yapılacak rassal değişimler ile çözüm çeşitliliğini artırmak ve olası tehlikeler karşısında populasyonun devamlılığını garanti altına almaktır.

3. Uygunluk Değeri Atama: Uygunluk değeri, yeni nesilde yer alacak bireylerin

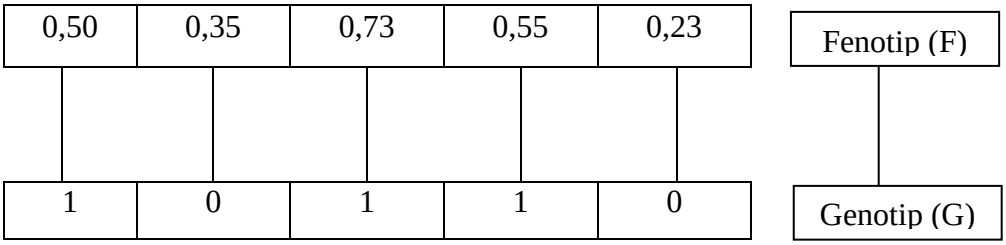
uygunluk değerlerinin belirlenmesinde kullanılır. Algoritmanın her iterasyonunda bireylerin uygunluk değeri hesaplanarak üreme kapasiteleri ve gen aktarımlarına ilişkin bilgiler elde edilir.

3.2.1. Basit genetik algoritma işlemleri

GA'yı diğer arama yöntemlerinden ayıran en önemli özellik, parametrelerin kendileri yerine farklı özelliklere sahip bireyler olarak gösterilmesi ve bu bireylerin kendilerini temsil eden diziler aracılığıyla ifade edilmeleridir. Bu nedenle, problemin çözümünde ilk adım, arama uzayını temsil edecek uygun bir kodlama yapısının seçilmesidir. Literatürde en yaygın kullanılan kodlama "1" ve "0" değerlerinden oluşan bir dizi tanımlamaktır. Dizinin uzunluğu problemin içerdiği parametre sayısı ile kısıtlanmalıdır [53].

Dizi gösterimi; *fenotip* (Phenotype) olarak adlandırılan olası çözümlerin algoritma içinde kullanılacak kodlanmış bilgilere, yani *genotiplere* (Genotype) dönüştürülmesidir [54]. Çoğu problemde fenotip ve genotipler aynı alınabilmektedir. Ancak özellikle nümerik problemlerin çözüm kümeleri için fenotipleri genotiplere dönüştürecek fonksiyonların tanımlanmasına ihtiyaç duyulmaktadır. Şekil 3.12'de fonksiyonuna göre bu dönüştürmenin nasıl yapıldığı basitçe gösterilmiştir.

$$f(u) = \begin{cases} 1 & u => 0,5 \\ 0 & u < 0 \end{cases} \qquad (3.6)$$



Şekil 3.12. Fenotiplerin genotiplere dönüştürülmesi

GA'yı diğer yöntemlerden ayıran bir başka önemli özellik ise, çözümü noktadan noktaya değil, noktalardan oluşan bir dizi içinde aramasıdır. Başlangıç popülasyonunu oluşturan bireyler genellikle rassal olarak seçilir. Böylece problemin olası çözümlerinin çoğunluğunun içerilmesi sağlanır. Kısıtlı optimizasyon problemleri gibi bazı özel problemlerde, başlangıçta rastsal olarak seçilen populasyon, çözüm uzayının istenmeyen bölgeleri olan lokal minimumlar çevresinde çözümlerde takılmasından dolayı çalışma performansı düşebilir. Bu nedenle problemin özelliğine göre uygun başlangıç değerlerinin programcı tarafından seçilmesi gerekebilir.

Her iterasyonda, bir değerlendirme fonksiyonu yardımıyla yığın içindeki dizilerin uygunluk değerleri bulunur. Amaç fonksiyonu denilen bu fonksiyonun seçimi kullanıcının amacına ve problemin yapısına göre çok değişik biçimlerdedir. Gözden kaçırılmaması gereken en önemli unsur bu fonksiyonun eleme kriteri oluşturmada programcıya matematiksel kolaylık sağlayıcı nitelikte olması gereğidir. Çözümlerin global minimuma yönelişini verimli ve hızlı bir seviyede tutarken, çözüm seçeneklerini kısıtlamayacak ve rastgele seçim mantığına aykırı düşmeyecek bir fonksiyon seçilmelidir.

Aşağıda verilen örnekte f (x) = x^2 olarak seçilen değerlendirme fonksiyonu ile popülasyonu oluşturan bireylerin değerlendirildiği varsayılmıştır; popülasyonun sayısı n=4 olmak üzere, bireyler *(i =1,2,...,n)*;

p_1 = 1 1 0 1
p_2 = 1 0 0 1
p_3 = 0 1 0 1
p_4 = 1 0 1 1

olarak ifade edilmektedir. Her bireyin ikili olarak kodlandığı ve tamsayı olarak bir değeri gösterdiği düşünülürse, bireylerin gerçek değerlerinin,

p_1=1 + 4 + 8 = 13

p_2=1 + 8 = 9

p_3=1 + 4 = 5

p_4=1 + 2 + 8 = 11 olduğu görülür.

f fonksiyonuna göre her bir genotipin değeri $f_i(x)$ hesaplanarak;

$f_1(13) = 169$, $f_2(9) = 81$, $f_3(3) = 25$, $f_4(11) = 121$ elde edilir.

Algoritmanın her iterasyonunda yeni nesli oluşturan bireyleri ifade eden diziler, bir önceki nesilden hayatta kalanlar ve/veya üretilenlerdir. Üretim sürecinden önce seçim süreci işletilir. Seçimin amacı doğrultusunda diziler, uygunluk değerleri oranına veya uygunluk değeri ile orantılı bir olasılık değerine göre seçilirler. Böylece "doğal seleksiyon" yapay yolla gerçekleştirilmiş olur; uygun bireyler hayatta kalırlar.

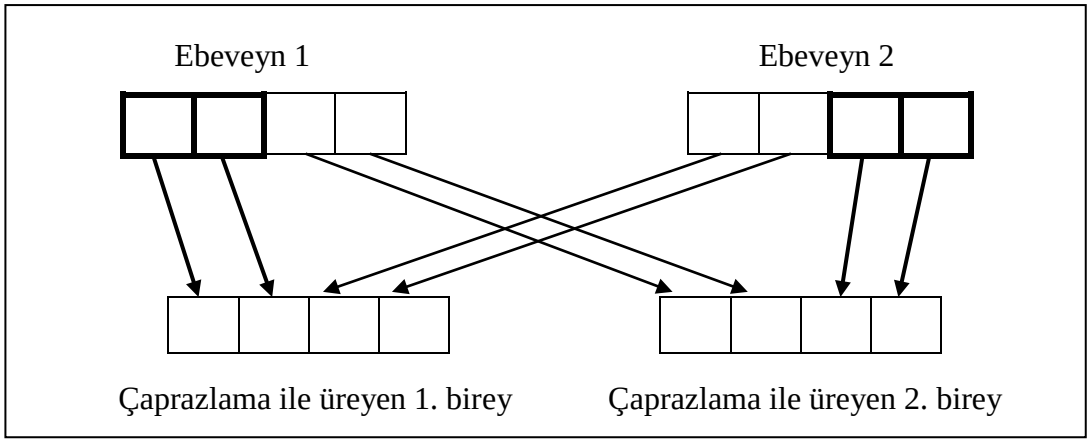
Genetik algoritmalarda yeniden üretim operatörü ile, yüksek uygunluk değerlerine sahip bölgelere yönelim sağlanmaktadır. Böylece problemin global minimum veya en yakınındaki lokal minimum civarında yer alan optimum çözümüne yönelimi sağlanmış olur.

3.2.2. Genetik operatörler

Çaprazlama operatörü

Çaprazlama, farklı çözümler arasında bilgi değişimini sağlayarak arama uzayının benzer fakat araştırılmamış bölgelerine yönelmeyi mümkün kılan bir arama operatörüdür [54]. Ebeveyn olarak seçilen bireylerden belirlenen bir yönteme göre uygun sayılarda genler alınarak yeni çözümler elde edilir (Şekil 3.13). Ebeveynin üreme kapasitesi ile aktaracağı genlerin sayısı, ilgili ebeveynin uygun çözüme yakınlığı ile doğru orantılıdır. Çaprazlama her yeni nesilde en iyi çözüme daha çok yaklaşan bireyler elde etmek için ideal bir yöntemdir. Ancak, oldukça ender de olsa,

sistemde kararsızlığa yol açabilecek genlerin yeni nesillere aktarılması tehlikesine yol açabilmektedir. Benzer biçimde sistemin istenmeyen bir lokal minimum etrafında odaklanan çözümler üretmeye başlayarak algoritmanın verimsiz sonuçlandırılması da olasıdır. Bunun nedeni GA' nın rastsal tabanlı bir yaklaşım olmasıdır.



Şekil 3.13. Çaprazlamaya bir örnek

İkili düzen kodlama için literatürde bilinen çaprazlama operatörlerinden üçü şunlardır;

1. Tek Noktalı Çaprazlama Operatörü: Bu operatörde, çaprazlama noktası 1 ile L-1 arasında rassal olarak seçilir. Eşleşen iki dizide, bu çaprazlama noktasından sonraki bölümler yer değiştirerek yeni iki dizi seçilir. Çizelge 3.4'de yığına ait B1 ve B2 gibi iki bireyin 5 noktasındaki çaprazlanması örnek olarak verilmiştir.

2 .İki Noktalı, Çaprazlama Operatörü: Bu operatörde 1 ile L-1 arasında rassal olarak iki kesme noktası seçilir. Çizelge 3.5'da B1 ve B2 bireylerinin 3 ve 7 noktalarında 2 noktalı çaprazlanması örnek olarak verilmiştir.

Çizelge 3.4. Tek noktalı çaprazlama

	1	2	3	4	5	6	7	8	9	10	11
B1 :	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**1**
B2 :	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**
B1’:	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**0**
B2’:	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**

Çizelge 3.5. İki noktalı çaprazlama

	1	2	3	4	5	6	7	8	9	10	11
B1 :	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**
B2 :	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**1**
B1’:	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**
B2’:	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**

3. Düzenli (Uniform) Çaprazlama Operatörü: Bu operatörde önce ikili düzende geçici bir dizi oluşturulur. Uzunluğu, yığındaki dizilerin uzunluğuna eşit olan bu dizide, 0 ve 1 değerleri önceden belirlenen bir olasılık değerine göre elde edilir. Bu dizinin her noktasında aldığı 0 ve 1 değerlerine göre, çiftleştirilecek bireylerin ilgili noktalardaki değerleri yer değiştirir. Çizelge 3.6'da verilen örnek, 2,5,6,8 ve 9. noktaları üzerindeki değerleri 1 olan geçici diziye göre B1 ve B2 dizilerinin yer değiştiren değerlerini, başka bir deyişle B1 ve B2 dizilerinin geçici dizi uyarınca 2,5,6,8 ve 9 noktalarında nasıl bir çaprazlama işlemine tabi tutulduklarını göstermektedir.

Çizelge 3.6. Düzenli çaprazlama

	1	2	3	4	5	6	7	8	9	10	11
B1 :	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**1**
B2 :	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**
Geçici dizi:	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**
B1˚:	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**
B2˚:	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**

Mutasyon operatörü

Biyolojik sistemlerde mutasyon, türün değişen doğal şartlar karşısında uyum yeteneğini artırarak devamlılığını sağlayan genetik bir önlem niteliğindedir. Mutasyon GA uygulamalarında, kararsızlık veya yanlış yönelim gibi durumlarda algoritmayı koruyacak bir tür emniyet birimidir. Ancak gereğinden fazla kullanılması durumunda, çözümde çeşitlemeler oluşturması nedeniyle işlem sürecinde de gereğinden fazla bir uzamaya yol açabilir. Bu olgunun da GA' nın en önemli tercih nedenlerinden ve avantajlarından birini dezavantaja dönüştürebileceği unutulmamalıdır.

Kısaca mutasyonun amacı dizilerin bir kısmında rassal değişimler yaparak çözüm uzayında yeni noktalar elde etmek, çözüm çeşitliliği oluşturarak olası tehlikeler karşısında popülasyonun devamlılığını garanti altına almaktır. Biyolojik sistemlerde türün değişen çevresel koşullara uyumunu sağlayan mutasyondur [54]. GA modellemelerinde mutasyonun önem derecesi değişen çok sayıda parametre karşısında sistemin çözüm üretme olasılığını artırmasına yardımcı olmaktadır.

GA uygulamalarında mutasyon ikili düzende kodlanmış bir dizinin üzerindeki değerleri rassal olarak tersleyerek diziyi mutasyona uğratmış olur. Matematiksel bir kontrolde, genin mutasyona uğrama olasılığı oldukça küçük değerlerde seçilmelidir. Bir başka yöntem ise, kendisini tekrar eden çözümlerin çoğalması durumunda

mutasyona başvurulmasıdır. Çizelge 3.7'de 8. noktası mutasyona uğrayan bir dizi, örnek olarak verilmiştir.

Çizelge 3.7. Mutasyon işlemi

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
B1:	1	0	0	1	1	0	0	0	1	1	1
B2:	1	0	0	1	1	0	0	1	1	1	1

Mutasyon, değişik çözüm arayışları türeten bir operatördür. Bireylerin birbirine çok benzemeye başladığı, yani algoritmanın yakınsamak üzere olduğu durumlarda etkisi oldukça artmaktadır.

3.2.3. Genetik algoritmaların avantajları ve dezavantajları

Genetik algoritmaların sahip olduğu avantajlar kısaca şöyle sıralanabilir:

- Çözüm uzayı hakkında herhangi bir bilgiye ihtiyaç duymazlar.
- Yerel optimum noktada takılı kalmaya direnç gösterirler.
- Geniş çaplı optimizasyon problemlerinin çözümünde iyi sonuçlar verir.

Görüldüğü gibi genetik algoritmaların genel yöntemlere üstünlük oluşturacak birçok avantajı vardır. Yöntemin basitliği, problem çözümüne yönelik sezgiselin kolay ve çabuk şekilde geliştirilmesini sağlar. Buna karşılık genetik algoritmaların, uygun değerlere sahip ailelerin yüksek uyum derecesine sahip ancak mümkün olmayan çocuklar üretmesi veya çaprazlama işlemi sonucu aileyi oluşturan bireylerin iyi özelliklerinin bozularak çocuklara geçmemesi gibi bazı durumlarda daha kötü sonuçlar verdiği bilinmektedir.

Genetik algoritmaların diğer başlıca avantajlarından biri global optimizasyon metodu olmasıdır. Yeterli büyüklükte bir nüfusla başlandığında, araştırmalar genetik

algoritmaların bu nüfusu oluşturan bölümler arasında rahatlıkla yüksek uyum değerine sahip bölümlere geçebildiğini göstermiştir.

Ayrıca genetik algoritmalar optimizasyon problemlerinde diğer yöntemlerin sorun yaşadığı, değişkenlerin kontrolünde esneklik sağlamaktadır. Ek olarak genetik algoritmalar herhangi bir iterasyonda belli sayıda mümkün çözüm içerir. Gerçek yaşamda optimum sağlayan tek bir çözümü incelemek yerine alternatif çözümlerden oluşan belli bir grubu analiz etmek daha yararlı olabilir.

Bütün bu avantajlarına karşılık genetik algoritmalar bazı dezavantajlara da sahiptir. Bunlar kısaca özetlenecek olursa;

- Çok fazla uyum fonksiyonu hesaplaması gerektirir.
- Global olarak tam optimum noktanın saptanmasında problem yaşamaktadır.
- Kullanılan konfigürasyon genel değil, probleme özgü bir yapı taşımaktadır.
- Nesiller arasında iyi özelliklerin kaybolma ihtimali vardır.

Bunlardan ilki çözümün herhangi bir aşamasında eldeki mümkün bireylerin her biri için uyum fonksiyonu değeri hesaplandığı için işlem zamanının ve gerekli hesaplama maliyetinin yüksek olmasıdır. Ayrıca her ne kadar global bir yaklaşıma sahip olsa da global olarak tam optimum noktanın yakalanmasında problem yaşamaktadır.

Bahsedilen bu dezavantajlara ek olarak yukarıda bahsedildiği gibi uygun değişken değerlere sahip bireylerden uygulanması mümkün olmayan yeni bireyler oluşma olasılığı vardır. Ayrıca üreme süreci boyunca anne ve babanın genlerinde yapılan çaprazlamalar sonucu iyi özelliklerini kaybedebilmeleri, oluşturulan yeni nesiller için problem oluşturmaktadır. Bu tip sorunların üstesinden gelmek için genetik algoritmalar çeşitli sezgisel yöntemlerle beraber kullanılarak "Melez Algoritmalar" adlı yöntemler oluşturulmakta ve arama performansları yükseltilmeye

çalışılmaktadır.

3.2.4. Kontrol parametreleri

GA' da aşağıda sıralanan 6 kontrol parametresi kullanılır:

- Popülasyonun genişliği
- Çaprazlama oranı
- Mutasyon oranı
- Nesil Aralığı
- Seçim stratejisi
- Ölçeklendirme fonksiyonu

GA'nın performansı, yukarıda sıralanan parametrelerin değerlerine bağlıdır. Bu nedenle programlamada bu parametrelerin en uygun kombinasyonla ilişkilendirilmesi önemlidir. Bu parametreler ve algoritmanın performansına etkileri aşağıda sırasıyla kısaca açıklanmıştır:

1.*Popülasyonun genişliği (N):* Algoritmanın yakınsaması ile doğrudan ilgilidir. Özellikle başlangıç popülasyonu küçük seçildiğinde GA'nın performansı düşer. Küçük genişlikte seçilen popülasyon, arama uzayının çözüm önerilerini sınırlar. Bu durumda arama uzayından yapılan örnekleme yetersiz kalır, zamansız yakınsama ortaya çıkar. Popülasyon genişliğinin büyük seçilmesi ise, çözüm uzayının oldukça iyi örneklenmesini sağladığından aramanın etkinliğini artırır. Böylece zamansız yakınsamanın önüne geçilir. Ancak yığın genişliğinin çok büyük seçilmesi, çözüm önerilerinin değerlendirilmesi süresini artıracağından, programın işleyişinin uzayacağı ve uygun çözüme yakınsamanın yavaşlayacağı unutulmamalıdır.

2.*Çaprazlama katsayısı (p_c):* Çaprazlama operatörünün sıklığını kontrol eden parametredir. Her yeni kuşakta p_c*N adet birey üzerinde çaprazlama işlemi gerçekleşir. Çaprazlama katsayısının büyük olması popülasyonda hızlı bir

değişkenliğe, küçük olması da arama işleminin yavaşlamasına yol açar.

3. *Mutasyon oranı (p_m):* Eleme sonucunda hayatta kalarak popülasyonu oluşturan bireyler, genellikle, seçilecek p_m katsayısı ile orantılı bir olasılıkla, rassal değişime uğratılırlar. Mutasyonun amacı ve gereğinden fazla kullanımının yol açacağı dezavantajlar ilgili başlık altında belirtilmişti. GA' da mutasyon ancak gereği ortaya çıktığında uygulanması gerektiğinden iki yönteme başvurulabilir. Birinci yöntem p_m katsayısının küçük seçilmesi, ikinci yöntem ise program içinde kullanılan bir karşılaştırma işlemi doğrultusunda, iterasyonun bazı adımlarında mutasyon operatörünün işletilmesidir.

4.*Nesil aralığı (g):* Her iterasyonda popülasyonda oluşacak değişimin yüzdesini kontrol eden bir parametredir. Bu parametrenin belirlediği, bir sonraki kuşakta, bir önceki kuşaktaki bireylerden kaçının hayatta kalacağıdır. Her yeni kuşak oluştuğunda, diğer bir deyişle t. iterasyon sonucunda, oluşan popülasyonun N*(1-g) adet bireyi, (t+1). iterasyonda da hayatta kalacaktır.

Örneğin; g = 1 => N*(1-1) = 0 olacağından, bir önceki kuşaktan hiç bir birey sonraki kuşağa taşınmayacaktır.

g=0,5 => N*(1-0,5) = 0,5*N olacağından, bireylerin yarısı sonraki kuşakta hayatta kalacaklardır.

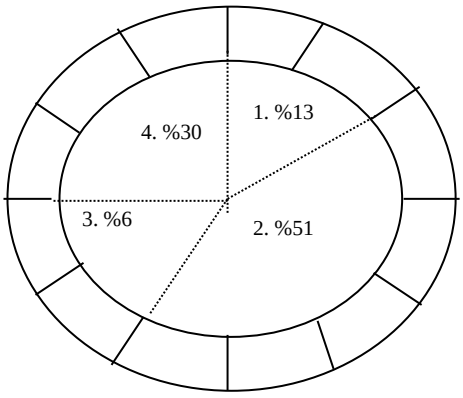
Görülmektedir ki; nesil aralığının küçülmesi, çözüm değişkenliğini de küçültmektedir. Bu da algoritmanın yakınsama hızını düşürmektedir.

5.*Seçim stratejisi:* GA' nın rassal bir arama yöntemi olduğu daha önce de belirtilmiş, popülasyondaki bireylerin üreme ve hayatta kalma şansının atanan uygunluk değeri ile orantılı olduğu açıklanmıştı. Uygunluk değeri, çaprazlama ve nesil aralığı, sonraki popülasyona hangi bireylerin ve bireylerin hangi genetik bilgilerinin taşınacağını belirlemede yeterli olmayabilir. Ayrıca, uygunluk değerinin eleme kriteri ile

ilişkilendirilmesi, programlamayı kolaylaştırır. Seçim stratejisi hangi bireyler dışında kalanların öleceğine karar vermeyi sağlar. Diğer bir deyişle, doğal seleksiyonun gerçekleşmesi için gereken eleme kriterinin belirlenmesine yarar.

GA'da en çok kullanılan eleme mekanizması Goldberg'in önerdiği rulet çemberi (roulette wheel) yöntemidir [52]. Bu yöntemde çember, N eşit aralığa bölünür. Aralığın genişliği ilgili bireyin seçilme olasılığına eşittir. Seçim aşamasında çember, N defa çevrilir. Her çevrimde 0-1 aralığında bir değer üretilir. Eleme aralığına karşılık gelen aralıkta yer alan bireyler yeni popülasyonda da yer alır.

Şekil 3.14'de rulet çemberine göre hayatta kalacak bireylerin belirlenmesi örneklenmiştir. Buna göre, başlangıçta eşit şansa sahip 24 bireyin, 24 çevrim sonunda hayatta kalma yüzdeleri dört bölgeye farklı yüzdeler ile dağılmıştır. 2. bölgede yer alan bireylerin hayatta kalma şansı %51 iken, 3. bölgedekilerin % 6 gibi oldukça düşük bir değere düştüğü görülmektedir. Bu değerler diğer kontrol parametreleri ile ilişkilendirilerek, bireylerin kaçının hayatta kalacağına, ne oranda üreyeceklerine veya sadece uygunluk fonksiyonu değerlerinin saptanmasına karar vermek üzere kullanılabilir.



Şekil 3.14. Rulet çemberine dizilen bireylerin, N çevrim sonucu hayatta kalma şanslarının dağılımı

6.*Ölçeklendirme fonksiyonu:* GA'da kullanılan eleme kriteri belirleme yöntemlerinin çoğu, belli bir hata aralığına sahiptir. İterasyon sayısı arttıkça, hata her adımda daha

da artar. Bireylerin uygunluk değerleri, eleme kriteri ile ilişkilendirildiğinden, hatanın her iterasyonda artması sonucu, eleme zorlaşabilir veya amacından sapabilir. Çünkü artan hata değeri, bireylerin uygunluk değerlerinin birbirine yaklaşmasına veya sistemin erken yakınsamasına yol açacak doğru olmayan uygunluk değerleri atamasına neden olur. Bu durumun önüne geçebilmek için uygunluk değerlerinde belli aralıklarla düzenleme yapılması gerekir [55]. Düzenleme işlemini gerçekleştiren, ölçeklendirme fonksiyonudur.

3.3. Saldırı Tespit Sistemleri

Bir bilgi varlığının bütünlüğünü, gizliliğini, güvenilirliğini veya erişilebilirliğini engelleme amaçlı tüm davranışlar saldırının tanımını oluşturur. Saldırı tespit sistemleri, tüm tedbirlere karşın bilgisayar sistemlerine yapılan saldırıları gerçekleşirken ya da gerçekleştikten sonra tespit etmek, İnternet veya yerel ağdan gelebilecek, ağdaki sistemlere zarar verebilecek, çeşitli paket ve verilerden oluşan bu saldırıları fark etmek üzere tasarlanmış sistemlerdir ve bu saldırılara yanıt vermeyi amaçlayan bir güvenlik teknolojisidir [56]. Saldırı tespit sistemleri bir nevi alarm sistemi olarak düşünülebilir. Bunları pek çok farklı şekillerde kategorilere ayırmak mümkündür. Bir saldırı tespit sistemi öncelikle aktif ya da pasif olabilir. İkincisi anasistem-tabanlı (host-based) ya da ağ-tabanlı (network-based) olabilir. Bu ikisini birleştirdiğimizde saldırı tespit sistemleri aktif/anasistem-tabanlı, aktif/ağ-tabanlı, pasif/anasistem-tabanlı, pasif/ağ-tabanlı olarak gruplandırılabilir [57]. Bir sistemin aktif olması tespit edilen bir saldırıya gerçek-zamanlı veya buna yakın cevap vermesi gerekirir. Örnek olarak güvenlik duvarı kurallarını saldırıya göre şekillendirmek veya kullanıcıyı komut konsolundan uyarmak vb. gösterilebilir. Pasif sistemler genelde saldırıyı kaydederler ve daha sonra incelenmek üzere saklarlar. Anlaşıldığı üzere saldırıların tespit edilebilmesi için tetikleme mekanizmalarına başka bir deyişle sistem ve ağ kaynaklarının yanlış ve normal olmayan kullanımlarının neler olduğunun bilinmesine ihtiyaç vardır. Saldırı tespiti iki analiz metoduna göre sınıflandırılabilir [56]. Bunlar kötüye kullanım saldırıları ile anormallik saldırılarıdır.

3.3.1. Kötüye kullanım saldırı tespiti

İç ağdan kaynaklı saldırılar tespit edilir. Bu yöntemde, STS edindiği bilgileri analiz eder ve büyük boyutlu imza (signature) veritabanlarıyla karşılaştırır. Esasen STS önceden belgelenmiş saldırılardan yola çıkarak güvenliği sağlamaya çalışır [58].

Avantajları

- İmza tanımlarının bilinen saldırı durumlarına göre modellenmesi
- Kullanıcıların imza veritabanını denetleyebilmesi ve sistem yöneticisi tarafından hangi saldırı tiplerinin alarma neden olacağının kolaylıkla anlaşılabilmesi
- Kurulumdan hemen sonra işlerlik kazanması
- Sistemin kolay anlaşılırlığı

Dezavantajları

- Saldırı aktivitelerinin birbirinden ayrık pek çok olayı kapsaması
- Bir saldırganın yapabileceği tüm saldırılar için ayrı imza tanımlanmasının gerekliliği
- İmza veritabanının sürekli güncel tutulmasının gerekliliği

Burada asıl önemli olan imza ölçütlerinin iyi bir şekilde tanımlanabilmesi ve veritabanının büyüklüğünün ayarlanmasıdır. Veritabanı gereğinden fazla büyürse yanlış uyarı verme olasılığı yükselebilir. Benzer şekilde, veritabanındaki imzalar yetersiz kalırsa bu da güvenlik sorunları oluşturabilir.

3.3.2. Anormallik saldırı tespiti

Bu yöntemde kullanıcı grubu ya da her bir kullanıcı için ayrı ayrı olmak üzere profil belirlenir. Profiller dinamik olarak veya elle oluşturulabilir ve normal kullanıcı aktivitesini tanımlayabilmek için taban çizgisi (baseline) olarak kullanılırlar. Eğer

ağda yapılan bir işlem taban çizgisinden çok fazla sapma gösterirse alarm tetiklenir. Bu STS profiller üzerinden çalıştığından aynı zamanda profil tabanlı STS olarak da adlandırılır [58] .

Avantajları

- İçten gelen saldırılar ve kullanıcı hesabı hırsızlığının tespitinde çok etkili olması
- Profillerin özelleştirilmiş olmasının, saldırganın hangi faaliyetlerde bulunduğunda alarm üretilmeyeceğini bilmesini zorlaştırması
- İlk defa meydana gelen saldırıların tespitinin daha kolay olması

Dezavantajları

- Uygun profillerin oluşturulabilmesi için ağın dinlenmesinin ve analiz edilmesinin gerekliliği
- Analiz süresince ağın normal trafiği anlaşılmaya çalışıldığından bu süre içinde ağın güvenliksiz oluşu
- Profillerin yönetiminin ve bakımının zahmetli ve zaman kaybına neden olması
- Sistemin karmaşıklığı ve her bir farklı saldırıyla alarmı tetikleyecek olay arasında bağlantı kurmanın zorluğu
- Saldırının normal kullanıcı etkinliklerine çok yakın olduğu durumlarda alarm üretilememesi
- Kullanım süresi uzadıkça, hangi saldırıların alarm üreteceğini kestirmenin zorlaşması

3.3.3. Ağ tabanlı saldırı tespit sistemleri

Ağ tabanlı saldırı tespit sistemleri ağın kendi segmenti üzerinden geçen trafiği veri kaynağı biçiminde görüntüler. Bunun için genelde ağ kartı geçirgen (promiscuous) moda getirilerek üzerinden geçen tüm trafiği yakalaması sağlanır. Ağın diğer segmentlerine ve telefon hatları gibi diğer iletişim çeşitlerine ait trafik yakalanamaz

ve görüntülenemez. Ağ tabanlı STS temelde ağda dolaşan paketlerin bir algılayıcı (sensor) üzerinden geçenleriyle ilgilenir. Algılayıcıya gelen paket mevcut imzalarla karşılaştırılır ve pakete ne yapılacağına karar verilir. Başlangıç seviyesindeki filtre hangi paketlerin kabul edilip hangilerinin atılacağını veya saldırı tanıma modülüne gönderileceğini belirler. Saldırı belirlenirse cevap modülü saldırıya karşılık olarak alarm üretilmesini tetikler. Algılayıcı ile görüntüleyici (monitor) arasındaki trafiğin şifrelenmesi veya algılayıcı ve görüntüleyicilerin ayrı bir ağa dahil edilmesi güvenlik açısından önemlidir. Bilgili ve deneyimli bir saldırgan için algılayıcı ve görüntüleyici arasındaki trafik (alarmlar, durum kayıtları, diğer paketler vb.) ağa saldırmak için çok önemli bilgiler içermektedir [59].

4. ÖNERİLEN PROTOKOL

Güvenli bir kablosuz ağ haberleşme sisteminin tasarımı sırasında karşılaşılan önemli problemler bulunmaktadır. Bu problemler kısaca;

- Güvensiz kablosuz haberleşme hatları,
- Altyapının sabit olmaması,
- Kaynak kısıtları (pil gücü, bant genişliği, bellek, işlemci gücü) ve
- Düğüm hareketliliğinden kaynaklanan dinamik ağ topolojisi

olarak sıralandırılabilir.

Güvenli yönlendirme protokolünün ana ihtiyaç ve problemleri ise [1];

- Zararlı düğümlerin tespiti; bu tür düğümler yönlendirme işlemi sırasında kullanılmamalıdır.
- Doğru yol keşfinin garanti edilmelidir.
- Ağ topolojisinin gizliliği. Eğer saldırgan ağ topolojisini öğrenebilirse darboğaz düğümlere saldırabilir.
- Saldırılara karşı kararlılık. Yönlendirme protokolü saldırılardan sonra sonlu bir zaman aralığında normal çalışmasına geri dönebilmelidir.

Bu problemlerin çözümü için hali hazırda literatürde bulunan yönlendirme protokolleri her anlamda yeterli güvenliği sağlayamamaktadırlar [60]. Çizelge 2.1'de görüldüğü gibi çoğu protokol sadece tek bir saldırıya cevap verebilmek amacıyla tasarlanmıştır. Bazıları ise aşırı bant genişliği kullandığı için verimli değildir. Bazı protokollerin ise çok yüksek işlemci gücü gereksinimleri vardır.

Bu sebeple kablosuz ağlarda güvenliği arttırmak için güvenlik bilinçli bir yönlendirme protokolüne ihtiyaç bulunmaktadır. Bu doktora çalışmasında genişbant kablosuz ağlar için güvenlik bilinçli zeki yönlendirme protokolü geliştirilmiştir.

Protokolün temel amacı, paketleri önerilen güvenlik seviyesinde bir rota üzerinden yönlendirmektir. Paketlere eklenen güvenlik seviyesi etiketi ile paketlerin takip etmesi gereken yolun hesaplanması sağlanmaktadır. Sağlıklı bir yönlendirmenin yapılabilmesi için paketlerin üzerinde ilerleyeceği düğümler arası bağların güvenlik seviyelerinin doğru hesaplanması gerekmektedir. Bu amaçla, her düğüm kendisiyle veri alışverişi yapabildiği düğümler arasındaki bağları, bir STS ile dinleyerek, bağdan gelen saldırılar ve türlerine göre o bağı puanlandırır. Ardından bu puanları diğer düğümlere bildirir. Bildirim işlemi paket yayınımları yardımıyla yapılmaktadır. Ayrıca her yapılan yayınıma bir sağlama numarası verilerek olası yayınım fırtınalarının önüne geçilmiştir.

Herhangi bir düğümden bir başka düğüme saldırı gerçekleştiğinde saldırıya maruz kalan düğümde bulunan STS bunu algılar ve saldırının tipine göre o yolun güvenlik değerini tekrar puanlar. Bağların güvenlik seviyeleri zamana bağlı olarak sürekli değişmektedir. Bu nedenle paketlerin düğümlerde ve düğümler arası bağlarda ilerlerken dinamik olarak uygun şartlar altında yönlendirilmeleri gerekmektedir. Bu amaçla bağların puanları bulanık mantıkla dilsel değişkenlere çevrilerek basitleştirilmiş ve rotayı hesaplayacak algoritmaya girdi olarak verilmiştir.

Paketlerin kaynak düğümden hedef düğüme kadar hangi düğümlerden ve bağlardan geçeceğinin hesaplanması gerekmektedir. Bu hesaplamanın zamanla bağlar arasında hareket ve güvenlikten kaynaklanan değişimler de göz önüne alınarak ziyaret edilen her düğümde tekrar edilmesi gerekmektedir. Böylece düğümlerin güvenlik seviyelerinin güncelliği ve hesaplamanın güncel veriler üzerinden yapılması sağlanmış olur.

4.1. Zamanla Değişen Yönlendirme Problemi

$G(V,E,W)$ dinamik ağında, V düğüm kümesi, $E \subseteq V \times V$ kenar (bağ) kümesi ve $W(t) = \{ w_{uv}(t) \mid (u,v) \in E \}$ zaman bağımlı kenar güvenlik değerleri kümesi olsun. Gerçek $w(t)$ değeri ancak t anında bilinebilir. Fakat yönlendirme algoritması bu

değere yaklaşık bir değeri kullanarak yönlendirme işlemini gerçekleştirmektedir. Bu amaçla en uygun kontrol *t* zamanına en yakın zamanda, yani kenar kullanılmadan hemen önceki zaman dilimidir. Bu amaçla güvenlik değerlerini hesaplayacak bulanık mantık tabanlı güvenlik seviyesi hesaplama modülü (GSHM) tasarlanmıştır. Her düğümde bulunan GSHM; t_0 şimdiki zaman ve c bir sabit olmak üzere zamanı $t_0 \le t \le t_0 + c$ olarak kullanacak bir kara kutu sistemidir. GSHM bir düğümün kenarlarının güvenlik değerlerini belirli zaman aralıklarında güncellemekte ve çevresine bu yeni değerleri bildirmektedir. Eğer iletim yapacak düğümün bağlarının güvenlik seviyelerinde bir değişiklik varsa ve iletimde kullanılacak kenar minimum güvenlik seviyesinin altına düşmüşse, kalan yol tekrar hesaplanmaktadır.

Problemi matematiksel olarak göstermek amacıyla; paketleri *u* düğümünden *v* düğümüne iletmek için, *n* uzunluğunda A güzergâhı üzerinden $A = (a_1, a_2, ..., a_{n-1}, a_n)$ şeklinde ve *m* uzunluğunda B güzergâhı üzerinden $B = (b_1, b_2, ..., b_{m-1}, b_m)$ şeklinde gönderebileceğimiz iki yol bulunsun. *n* değerinin *m* değerinden daha küçük olduğunu varsayarsak *A* güzergahı tercih edilecektir. *A* yolundan ilerlerken y düğümüne geldiğimizde a_{y+1} yolunun güvenlik seviyesinin azalarak değiştiği ve kullanım için uygun olmadığını varsayalım. Bu durumda güzergahın değiştirilerek başka bir güzergah üzerinden yola devam etmek gereği ortaya çıkar. Eğer *B* güzergâhı halen minimum güvenlik şartlarını sağlıyor ise *y* düğümünden *v* düğümüne giderken *B* güzergâhını kullanmak daha uygun olacaktır. Bu durumda $a_k = b_h = y$ ise, bu yeni durumda daha iyi bir çözüm olan

$$C = (a_1, a_2, ..., a_{k-1}, a_k, b_{h+1}, ..., b_{m-1}, b_m) \tag{4.1}$$

kullanılacaktır.

t anında *x* düğümünden *y* düğümüne bir güzergah tanımlamasının genel ifadesi

$$G_{x,y}(t) = (x, v_2, ..., v_i, ..., v_j, ..., v_{n-1}, y) \tag{4.2}$$

olsun. Başlangıç anı t_0 olan, *s* ile *d* düğümleri arasında hesaplanmış en kısa atlama sayısına sahip güzergah

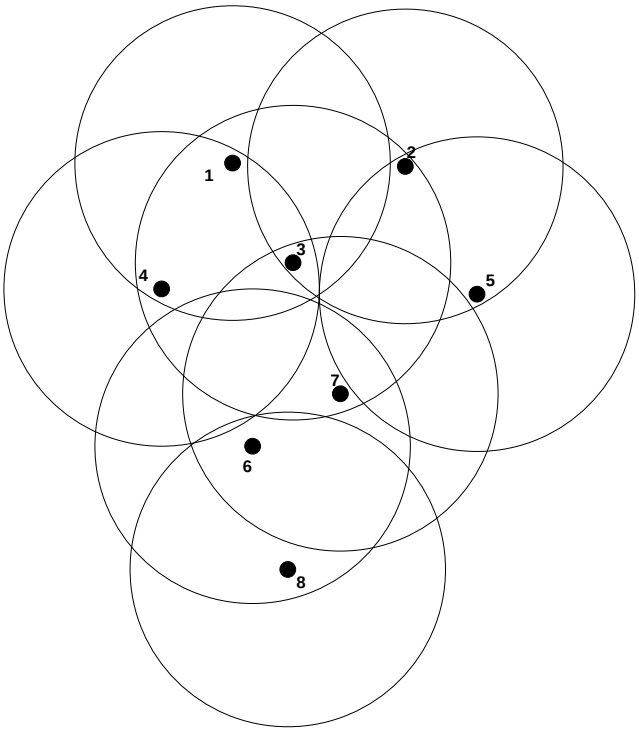
$$G_{s,d}(t_0) = (s, v_2, ..., v_i, ..., v_j, ..., v_{n-1}, d) \tag{4.3}$$

olsun. Paketler $G_{s,d}(t_0)$ güzergahında ilerlerken v_i düğümünde kullanılacak bir bağda beklenmedik bir güvenlik sorunu oluşsun. Böyle bir durumda o bağ güvensiz olduğu için kullanılamaz. Bu durumda $G_{v_i,v_j}(t_0)$ güzergahı da kullanılamayacaktır. Böylece daha uygun bir altgüzergah olan $G_{v_i,v_j}(t_1)$ güzergahı t_1 anında hesaplanarak kullanılır.

$$G_{v_i,d}(t_1) = G_{v_i,v_j}(t) + (v_{j+1}, ..., v_{n-1}, d) = (v_i, v'_{i+1}, ..., v'_{j-1}, v_j, v_{j+1}, ..., v_{n-1}, d) \tag{4.4}$$

Burada t_0 ve t_1 anlarındaki iki bilgi kontrollü olarak çaprazlanarak yeni güzergah elde edilmiş olur. Bu tür bir kontrollü çaprazlama her bilgi güncellemesinde gerekmeyebilir.

$G_{s,d}(t_0)$ başlangıç güzergahı ve $G_{y,z}(t_k)$ altgüzergahlar olsun. Her alt uzayda $W(t)$ değişeceğinden çözüm uzayı da farklılık gösterecektir. GSHM $t_0 \le t \le t_0 + c$ zaman aralığı için bulunduğu düğümün bağlarının $W(t)$ değerlerini hesaplayarak yönlendirme tablosunda gerekli değişiklikleri yapmaktadır. Ayrıca bu değişiklikler belirli zaman aralıklarında diğer düğümlere iletilmektedir.



Şekil 4.1. Sekiz düğümden oluşan örnek bir genişbant kablosuz ağı

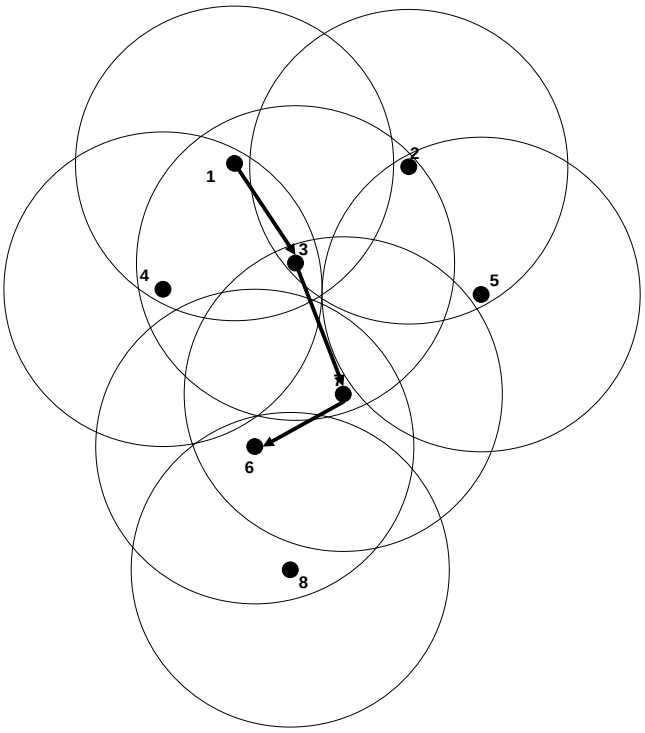
Burada bir numaralı düğüm "3" ve "4" numaralı düğüm ile haberleşebilmektedir. Çizelge 4.1 düğümlerin haberleşebildikleri komşu düğümleri göstermektedir. Düğümlerin aynı tipte ve haberleşme mesafelerinin de aynı olduğu kabul edilmiştir.

Çizelge 4.1. Düğümlerin doğrudan haberleşebildikleri düğümler

Düğüm no	Doğrudan haberleşebildiği düğüm no
1	3 ve 4
2	3 ve 5
3	1, 2, 4 ve 7
4	1 ve 3
5	2
6	7 ve 8
7	3 ve 6
8	6

Çizelge 4.2. Düğümlerin komşuluk tablosu

Düğüm No	1	2	3	4	5	6	7	8
1			1	1				
2			1		1			
3	1	1		1			1	
4	1		1					
5		1						
6							1	1
7			1			1		
8						1		



Şekil 4.2. "1" numaralı düğümün "6" numaralı düğüm ile haberleşmesinde minimum atlama sayısının kullanıldığı yönlendirme metodu

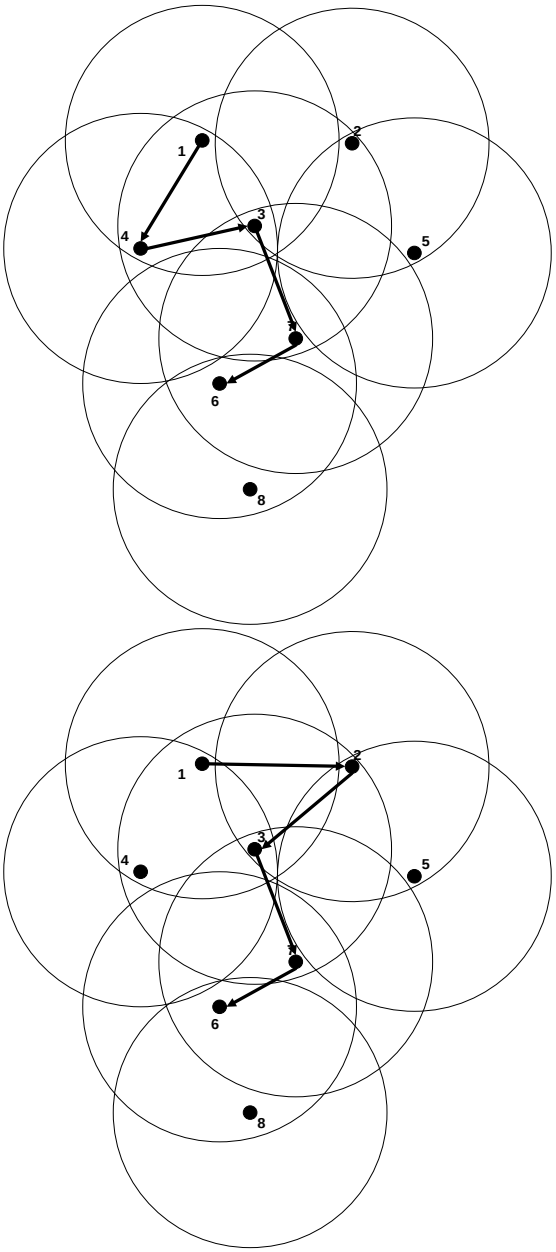
Örnek bir yönlendirme olması açısından "1" numaralı düğüm "6" numaralı düğüme bilgi göndermek isterse paketlerin oluşturulacak sanal gidiş yolu üzerinde en kısa atlama sayısı 1-3-7-6 olacaktır. Fakat yönlendirme işlemine düğümlerin ve gidiş yollarının güvenlik durumlarını da katacak olursak farklı gidiş yolları ortaya çıkabilir. Çünkü en kısa gidiş yolu en güvenilir yol olmayabilir [28].

Çizelge 4.3. Düğümlerin komşuluk tablosuna dilsel güvenlik bilgilerinin eklenmiş hali

Düğüm No	1	2	3	4	5	6	7	8
1	Kendisi	0,Güvenilmez	1,Güvenilmez	1,Çokgüvenilir	0,Tamgüvenilir	0,Tamgüvenilir	0,Çokgüvenilir	0,Güvenilir
2	0,Güvenilmez	Kendisi	1,Güvenilir	0,Güvenilir	1,Tamgüvenilir	0,Güvenilmez	0,Tamgüvenilir	0,Çokgüvenilir
3	1,Güvenilmez	1,Güvenilir	Kendisi	1,Çokgüvenilir	0,Çokgüvenilir	0,Güvenilmez	1,Güvenilir	0,Güvenilir
4	1,Çokgüvenilir	0,Güvenilir	1,Çokgüvenilir	Kendisi	0,Güvenilir	0,Tamgüvenilir	0,Güvenilmez	0,Tamgüvenilir
5	0,Tamgüvenilir	1,Tamgüvenilir	0,Çokgüvenilir	0,Güvenilir	Kendisi	0,Güvenilmez	0,Güvenilmez	0,Güvenilmez
6	0,Tamgüvenilir	0,Güvenilmez	0,Güvenilmez	0,Tamgüvenilir	0,Güvenilmez	Kendisi	1,Çokgüvenilir	1,Güvenilmez
7	0,Çokgüvenilir	0,Tamgüvenilir	1,Güvenilir	0,Güvenilmez	0,Güvenilmez	1,Çokgüvenilir	Kendisi	0,Güvenilir
8	0,Güvenilir	0,Çokgüvenilir	0,Güvenilir	0,Tamgüvenilir	0,Güvenilmez	1,Güvenilmez	0,Güvenilir	Kendisi

Bazı yolların güvenli olmaması durumunda yapılması gereken işlem, yolun değiştirilerek daha güvenli bir yol üzerinden iletişime devam edilmesidir. Çizelge 4.3 herhangi bir t zamanında düğümlerin birbirleri ile haberleşebilme ve güvenlik ilişkilerinin dilsel olarak oluşturulmuş tablosunu göstermektedir. Yol değişikliği haberleşme başlangıcında sanal yol oluşturulurken veya haberleşme devam ederken sanal yol üzerinde meydana gelen bir güvenlik açığı sonucunda yolun değiştirilmesi şeklinde olabilir. Bu amaçla, hazırlanan protokolde iletişim yolları onları kullanan düğümler tarafından kontrol edilerek puanlanmıştır. Elde edilen puanlama listeleri düğümlerde dağıtık olarak saklanacağından daha güvenli bir yapının oluşması sağlanmıştır.

Şekil 4.3'te görüldüğü gibi "1" numaralı düğüm ile "6" numaralı düğüm arasında Çizelge 4.3.'de verilen komşuluk tablosu kullanılarak minimum güvenlik seviyesi "güvenilir" olmak üzere belirlenen güvenlik seviyesinde sanal bir yol oluşturulmuştur. Bu sanal yol için "1-3" yolu daha kısa olacağı halde yeterli güvenlik seviyesinin altında olduğu için kullanılmamıştır. Böylece güvenli yol "1-4","4-3","3-7","7-6" yolları üzerinden veya "1-2","2-3","3-7","7-6" yolları üzerinden oluşturulmuştur. Belirli bir güvenlik seviyesi için her iki yol da doğru olduğu için, en iyi yol söz konusu değildir. Bu durumda çözümün daha hızlı yapılabilmesi için herhangi bir doğru yolu bulabilen bir algoritma kullanılması çok uygun olacaktır. Bu amaçla sezgisel bir yöntem olan genetik algoritma bu yolların belirlenmesi amacıyla kullanmaktadır. Çünkü yollar ve güvenlik değerleri dinamik olarak sürekli değiştiği için Dijikstra'nın en kısa yol gibi algoritmaları iletim yollarının hesaplamalarında uygun olmamaktadır [61, 62]. Protokolün işleyişinde iki önemli yapı bulunmaktadır. Bunlar yolların güvenlik değerlerinin bulanık kümeler yardımıyla hesaplanması ve elde edilen bu değerlere göre genetik algoritma yardımıyla uygun iletim yolunun elde edilmesidir.



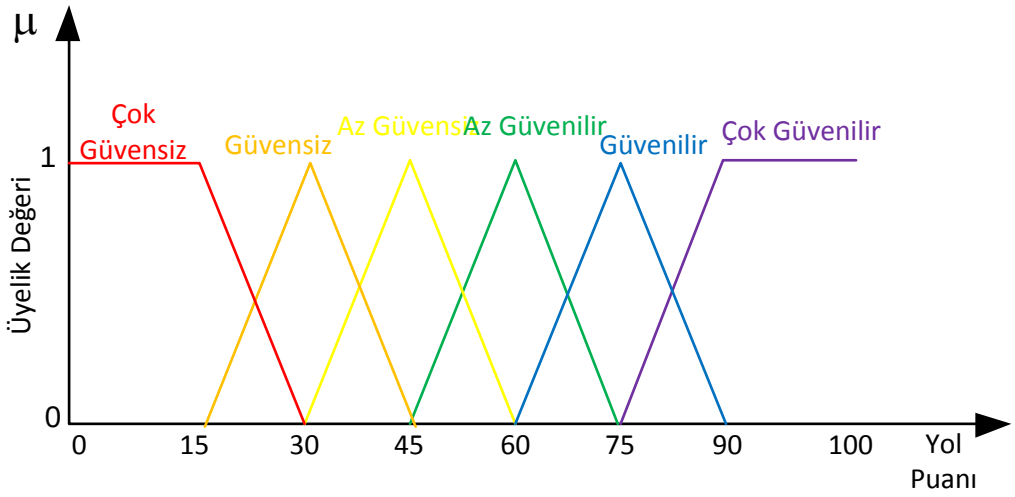
Şekil 4.3. Bir numaralı düğümün altı numaralı düğüm ile haberleşmesinde [1-3] yolu güvenli olmadığı için farklı bir yol tercih edilen iki yol örneği

4.2. Bağların Güvenlik Değerlerinin Hesaplanması

Düğümler arasında kurulan yolların güvenlik seviyeleri tespit edilirse kurulacak olan sanal yolların hesaplanması için gereken girdi elde edilmiş olur. Bu amaçla yolların puanlamasının yapılabilmesi için bulanık kümelerden yararlanılmaktadır.

4.2.1. Bulanık mantığın protokolde uygulanması

Geliştirilen protokolde, her yol için güvenlik değeri her düğümün kendisinden sonraki yolların her birine puan vermesiyle hesaplanmaktadır. Bu puanlar 0 ile 1 aralığında dinamik olarak değişmektedir. Başlangıçta komşu yolların güvenlik seviyesi 50 olarak alınmıştır. Güvenlik seviyeleri dilsel ifadelerden oluşmaktadır. Bu amaçla Şekil 4.4'de görülen 6 seviyeli üçgen üyelik fonksiyonu kullanılmıştır.



Şekil 4.4 Protokolde kullanılan üçgensel bulanık üyelik fonksiyonu ve sınırları

Hazırlanan protokolde puanlama için her düğümde bir atak sınıflandırma listesi, bu atakların tespiti için o ataklara ait imzalar ve atakların ciddilik durumlarına göre eksiltme puanlamalarını içeren bakseç tablosu bulunmaktadır. Puanlama sırasında iki fonksiyon görev yapmaktadır. Bu fonksiyondan birincisi olan düşürücü fonksiyon çeşitli olaylara göre bakseç tablosu üzerinden yolların güvenlik puanlarını azaltmakta, diğer fonksiyon olan yükseltici fonksiyon ise yine bakseç tablosu üzerinden yolların güvenlik seviyelerini arttırmaktadır. Örneğin, düğümünün bir bağından saldırı tespit edildiğinde o bağın puanı tehdidin türüne ve ciddiyetine göre düşürülmektedir. Güvenlik seviyesi paketlerin durumuna ve önceliğine göre belirli bir seviyenin altına düştüğünde ise bu yol kullanıma kapatılmaktadır. İletişime

kapatılan yol yükseltici fonksiyon tarafından güvenlik seviyesi yükseltilerek tekrar kullanıma açılırsa yol hesaplamalarında kullanılmaktadır.

Her düğüm kendisine bağlı yolları bulanık olarak değerlendirmekte ve bu değerler yol kurulumu sırasında genetik algoritmanın uygunluk fonksiyonuna giriş olarak kullanılmaktadır.

Değerlendirme kriterleri güvenlik parametrelerine göre karşılaşılan güvenlik sorunlarına bağlı olarak sürekli değişmekte ve yeni bir yol kurulumu sırasında gerçek zamanlı bilgilerle işlemler gerçekleşmektedir.

4.3. Yol Kurulumu

İki düğüm arasında güvenlik bilinçli sanal bir yol oluşturulmakta ve haberleşme bu sanal yol üzerinden gerçekleştirilmektedir. Burada amaç en kısa yol yerine paketin gönderilmek istendiği uygun güvenlik seviyesindeki yolun tespit edilmesinin sağlanmasıdır. Bu nedenle maliyet hesabı yapılmaktadır. Maliyet hesabında atlama sayısı (hop count), iletişim süresi, düğümlerin birbirlerine olan uzaklığı ve bulanık üyelik fonksiyonu ile elde edilen puan kullanılabilir. Girdilerin çok fazla olması sebebiyle en iyi yolun hesaplanması uzun zaman alabilir. Fakat sistemin çalışması için olabildiğince uygun bir yol oluşturulması yeterli olacaktır. Bu amaçla sezgisel (heuristic) bir yöntem olan genetik algoritma kullanılmaktadır. Çünkü yollar ve güvenlik değerleri dinamik olarak sürekli değiştiği için Dijikstra'nın en kısa yol gibi algoritmaları iletim yollarının hesaplamalarında uygun olmamaktadır [61]. Protokolün işleyişinde iki önemli yapı bulunmaktadır. Bunlar yolların güvenlik değerlerinin bulanık kümeler yardımıyla hesaplanması ve elde edilen bu değerlere göre genetik algoritma yardımıyla uygun iletim yolunun elde edilmesidir. Genetik algoritmanın protokole uygulanması aşağıda anlatılmıştır.

4.3.1. Genetik algoritmanın protokolde uygulanması

İki düğüm arasında en uygun yolun bulunması ağ analizinde en bilinen problemlerden biridir. Bu konuda en basit çözüm yöntemi, düğümler arasındaki ağırlıkların sabit alınarak çözüldüğü Dijkstra'nın ortaya koyduğu algoritmadır. Bu algoritma $O(n^2)$ zamanda çözüme ulaşmaktadır [63]. Fakat pratik uygulamalarda bir bağın ağırlığı haberleşme sırasında çoğunlukla zamanın bir fonksiyonu olarak değişmektedir [64].

Örneğin, iş çıkışı saatinde, geniş bir ana arterde trafik kazası meydana gelsin. Böylece yol ancak tek şeritten akmaya başlayacaktır. Bu yolu kullanan sürücüler evlerine daha çabuk ulaşabilmek için doğal olarak başka yollar üzerinden gitmeye çalışacaklardır. Sürücüler yolculuk başladığında kazadan ve yolun yavaş ilerlediğinden haberdar değildir. Fakat öğrendiklerinde dinamik olarak yollarını daha hızlı gidebilecekleri güzergâhlara yönlendirerek yeni duruma adapte olmaktadırlar. Bu tür ağlar dinamik ve stokastik ağ olarak adlandırılmaktadır [65].

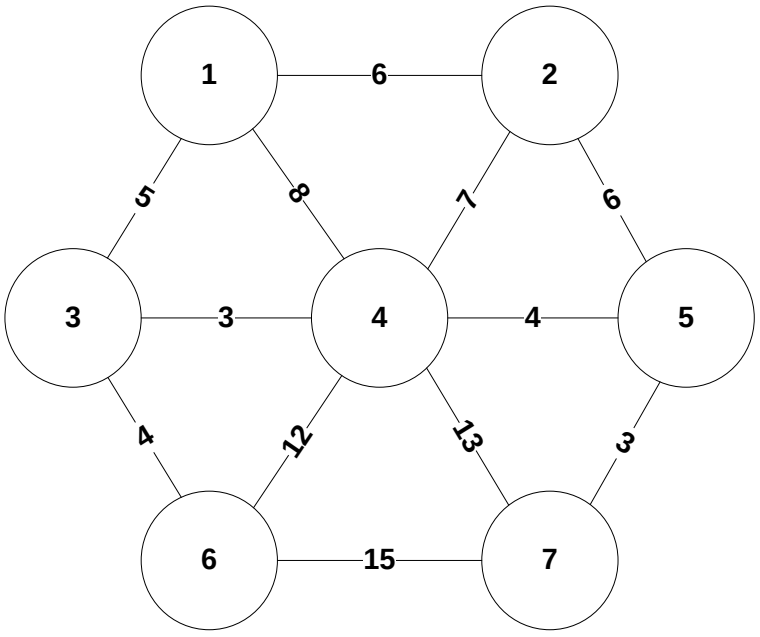
G yönlendirilmiş grafı, sonlu sayıda *V* düğümünden ve bu *V* düğümlerinden oluşan ikili çiftlerden oluşsun. Bu ikili çiftler *E* kenar kümesini oluştursun. Herhangi bir (*u*,*v*) kenarı *u* düğümünden *v* düğümüne bir bağlantı göstermektedir. w_{uv} o kenarın güvenlik seviyesini göstersin. Verilen iki düğüm arasında belirli bir güvenlik seviyesinin altına inmeden kısa bir güzergah bulunması, çözülmesi gereken problem olarak karşımıza çıkmaktadır. Bu tür bir problemin literatürde çeşitli çözüm yöntemleri vardır [63, 66, 67]. Fakat güvenlik seviyesi $w_{uv}(t)$ şeklinde zamanın bir fonksiyonu olarak değişiyor ise bu tür ağlara dinamik ağlar denilmektedir.

Fu [68], Dijkstranın algoritmasının daha genel olan bu yeni yapıya uyarlanabileceğini göstermiştir. Fakat değişecek ağırlık fonksiyonlarının önceden bilindiğini ve daha sonra değişmeyeceğini öngörmektedirler. Bu durum çoğu gerçek yaşam uygulamaları ile uyumsuz bir çözüm olmaktadır. Şekil 4.19'da görülen ağ göz önüne alındığında 1 ile 5 düğümleri arasında güvenlik seviyesi 6 olan bir haberleşme

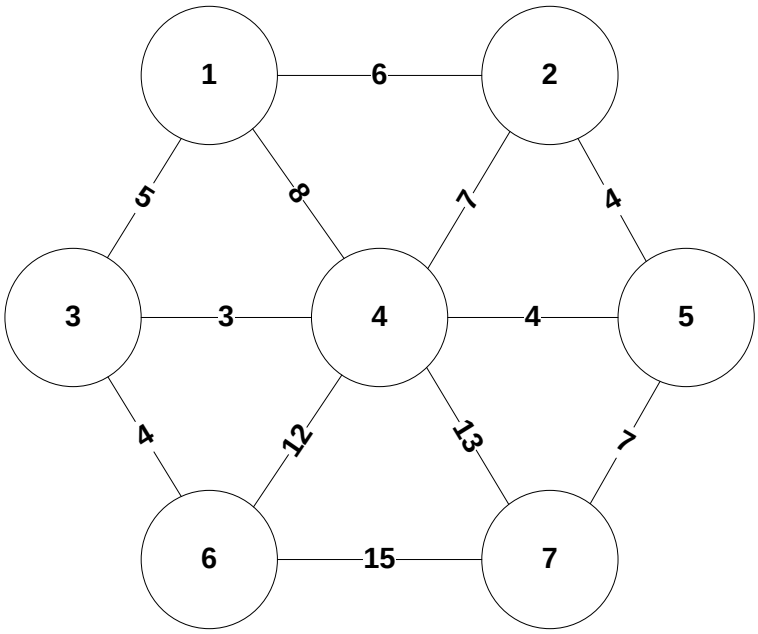
gerçekleştirilmek istenirse (1,2,5) olarak atlama düğümleri hesaplanır. Fakat 2 numaralı düğüme gelindiğinde w_{25}=4 ve w_{75}=7 olarak değişirse, bu durumda yollar tekrar hesaplanmalıdır. Hesaplanan yeni yol (2,4,7,5) olacaktır. Eğer diğer adımlarda da kenarlardan biri istenen güvenlik seviyesi değerinin altında olursa yeni bir hesaplama ile güzergah tekrar hesaplanır.

Gen [69] genetik algoritma ile sabit ağırlıklı bir graf üzerinde en kısa yolu bulan bir yöntem önermiştir. Cedric [61] ise dinamik ve stokastik ağlarda en kısa yolu bulan bir genetik algoritma önermiştir.

Geliştirilen protokolde iki düğüm arasında paketlerin gideceği güvenli ve dinamik bir yol genetik algoritma ile belirlenmektedir. Daha sonra bu dinamik yol üzerinden paketler iletilirken gerektiğinde yeni yollar üzerinden yönlendirilerek hedef düğüme ulaşmaktadırlar.



Şekil 4.5. t_0 anında ağdaki kenarların güvenlik ağırlıkları



Şekil 4.6. t_1 anında ağdaki kenarların güvenlik ağırlıkları

Genetik algoritmanın temeli Holland'ın [51] çalışmalarına dayanmaktadır. Geliştirilen protokolde en uygun yol, Açık En Kısa Öncelikli (OSPF-Open Shortest Path First) protokolüne benzer bir metot ile bulunmaktadır. Bu yapıda yönlendirme ve güvenlik ile ilgili bilgiler dağıtık bir şekilde ara düğümlerde (router) hesaplanarak saklanmaktadır. Bu bilgiler belirli aralıklarla dinamik olarak paylaşılarak güncellenmektedir.

Genetik algoritma evrim kurallarından biri olan doğal seleksiyon prensibine dayanmaktadır. Bireylerden oluşan bir toplum bilgisi (çözüm uzayı) vardır. Çoğunlukla bu bireyler kromozomlarla ifade edilirler. Kromozomlar ise n boyutunda bir vektör olarak ifade edilirler.

$$C = (c_i \mid 1 \le i \le n) \tag{4.5}$$

Burada c_i gen olarak adlandırılmaktadır. Genetik algoritmada bilgi kromozomlara kodlanarak fenotip çözümler oluşturulabilir. Böylece değişik kromozom çözümleri aynı fenotip ile çözümlenebilir. Bu çalışmada kullanılacak kromozomlar ile fenotip

arasında ayrık bir kodlama sistemi bulunmamaktadır. İki terim de aynı bilgiyi ifade etmektedirler.

Bir grup bireye popülasyon denilmektedir. Arka arkaya gelen popülasyonlara nesil denilmektedir. Genetik algoritma G(0) başlangıç nesli ile başlar ve her G(t) nesli, yeni bir G($t+1$) neslini oluşturur. Protokolde yeni nesil G($t+1$), eski nesil G(t)'nin yerini alacaktır.

Yeni nesildeki yeni bireylerin oluşturulması iki temel evrim konseptine dayanmaktadır [70];

a) Bireyin yaşama kabiliyetini gösteren uyum yeteneği,
b) Şimdiki neslin genetik bilgisi ve bu bilgilerle bir sonraki nesil için temel oluşturacak genetik operatörler.

Genetik işlemler çoğunlukla çaprazlama ve mutasyon işlemleridir. Çaprazlama operatörü ebeveyn olarak adlandırılan iki bireyin genetik bilgileri kullanılarak yavru bireyler olarak adlandırılan yeni bireyler oluşturmaktadır. Yüksek uyum puanlarına sahip bireylerin ebeveyn olup genetik bilgilerinin bir kısmını bir sonraki nesillere geçirmeleri ihtimali daha yüksektir. Çaprazlama işlemi çözüm uzayının başarılı bir alt uzayına erişim sağlamaktadır. Mutasyon operatörü bireydeki bir veya daha fazla geni rastgele değiştirmektedir. Mutasyonlar popülasyonun genetik değişimini arttırmaktadır. Mutasyon sayesinde genetik algoritmada çözüm uzayının daha önce keşfedilmemiş bölgelerinde tarama yapılmaktadır. Genetik algoritmada çaprazlama ve mutasyon operatörleri ile kuşaklar ilerledikçe sonuca yaklaşan yeni alt uzaylar araştırılmaktadır. Çizelge 4.4'de önerilen protokolde kullanılan genetik algoritmanın genel yapısı verilmiştir.

Çizelge 4.4. Kullanılan genetik algoritmanın genel yapısı

```
G(0) başlangıç popülasyonunu oluştur.
      G(0)'ın uygunluğunu kontrol et.
      for (t=1; sonlanma kriterine kadar; t++)
            {
                  G(t-1)'den G(t) oluştur.
                  G(t)'nin uygunluğunu kontrol et.
            }
```

Hazırlanan genetik algoritmada aşağıda ifade edilen parametreler için en uygun olan değerler simülasyonlar ile parametre taraması yapılarak araştırılmış ve sonuçları, Sonuçlar bölümünde sunulmuştur.

a) Popülasyon boyutu (N)
   Popülasyon boyutu popülasyondaki bireylerin sayısıdır.
b) Nesil sayısı (k)
   Nesil sayısı kaç nesil sonra sonuçların alınacağına dair durdurma kriteridir.
c) Çaprazlama oranı (p_c)
   Çaprazlama oranı p_c iki ebeveynden yeni iki çocuk oluşturma oranıdır. (1-p_c) ise bu iki ebeveynden çocuk oluşturmak yerine yeni nesle direkt kopyalanma oranlarıdır.
d) Mutasyon oranı (p_m)
   Mutasyon oranı p_m bir sonraki nesilin her yeni bireyinin genetik mutasyona tabi olma oranıdır.

4.3.2. Protokolde uygulanan genetik gösterim ve operatörler

Başlangıç operatörü

Başlangıç operatörü popülasyon boyutu (N) kadar başlangıç ve varış düğümleri arasında rastgele başlangıç güzergahları oluşturur.

Çaprazlama operatörü

n uzunluğa sahip A kromozomu, $A=(a_i \mid 1 \le i \le n)$ ile m uzunluğa sahip B kromozomu, $B=(b_i \mid 1 \le i \le m)$ olsun. Tek noktalı çaprazlama ile yeni oluşacak yeni kromozom

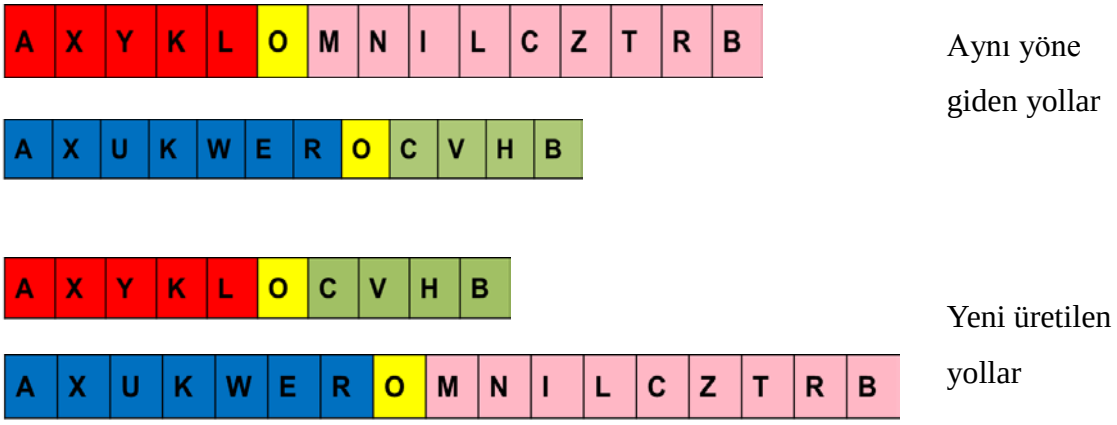
$$C=(a_1, a_2, ..., a_j, b_k, ..., b_{m-1}, b_m) \tag{4.6}$$

olacaktır. Fakat çoğunlukla $(a_j, b_k) \notin E$ olacaktır. Bu durum kopuk bir güzergah anlamına gelmektedir. Bu nedenle işleme özel çaprazlama operatörü (İÖÇO) tanımlanarak yeni bireylerin çözüm uzayında tanımlı noktalar olarak gösterimi sağlanmıştır.

İÖÇO iki ebeveynde de bulunan ortak noktalardan yapılan tek veya çok noktalı çaprazlama operatörüdür. Yukarıdaki örnekte İÖÇO bize $a_j = b_{k-1}$ olan j ve k verir. Böylece $(a_j, b_k) \in E$ olacaktır. Eğer iki noktalı çaprazlama yapılacaksa bu durumda $a_j = b_{k-1}$ ve $a_i = b_{h-1}$ olacaktır. Eğer $j < i$ ve $k > h$ veya $j > i$ ve $k < h$ olursa altgüzergah ters yönde hareket gösteriyor demektir. Eğer $j < i$ ve $k < h$ ise İÖÇO iki noktadan çaprazlama işlemini şu şekilde yapmaktadır;

$$C=(a_1, a_2, ..., a_j, b_k, b_{k+1}, ..., b_{h-1}, a_{i+1}, ..., a_{n-1}, a_n) \tag{4.7}$$

Örnek bir İÖÇO Şekil 4.7'de gösterilmiştir. Burada aynı başlangıç ve varış noktalarına sahip iki yol sarı ile gösterilen ortak "O" düğümü üzerinden çaprazlanmıştır. Böylece ortaya "A" düğümünden "B" düğümüne ulaşılabilen iki yol daha türetilmiş olur.

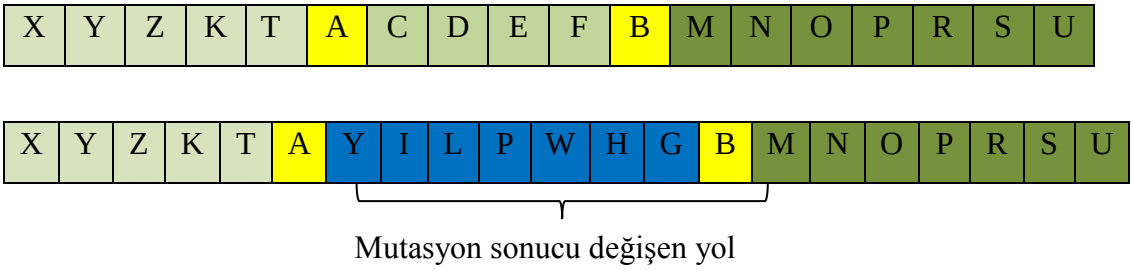


Şekil 4.7. Tek noktadan işleme özel çaprazlama operatörü

Mutasyon operatörü

Mutasyon operatörü, genetik algoritmada genlerin değerlerini rastgele değiştirmek amacıyla kullanılmaktadır. Fakat bu problemde, eğer mutasyon operatörü genlerin değerini rastgele değiştirirse oluşacak sonuç çözüm uzayının dışında olacaktır. Bu nedenle işleme özel mutasyon operatörü (İÖMO) tanımlanmıştır. Bu operatör rastgele iki gen seçer ve bu iki gen arasını rastgele bir güzergah ile doldurur. Başlangıç operatörü rastgele güzergahın elde edilmesinde kullanılabilir. Mutasyon operatörü kromozomun boyutunu yani atlama sayısını değiştirmektedir.

İÖMO'nün nasıl çalıştığı Şekil 4.8'de gösterilmiştir. Sarı ile gösterilen genler Mutasyon operatörü tarafından rastgele seçilen iki düğümdür. Mavi ile gösterilen düğümler rastgele seçilen bu iki beyaz düğüm arasında oluşturulmuş rastgele uygun bir güzergahı temsil etmektedir.



Şekil 4.8. İşleme özel mutasyon operatörü

Uygunluk fonksiyonu

Problemde kısıtlar minimum atlama sayısı ve güzergâh üzerindeki kenarların minimum güvenlik seviyesinde tutulmasının sağlanmasıdır. Bu amaçla ebeveynlerin seçiminde rulet fonksiyonu kullanılacaktır. Ayrıca seçilen ebeveynler üzerinde kesişim noktası bulunmaması durumunda uygun bir prop fonksiyonu ile yeni ebeveyn seçilerek denenecektir. Bu durum ortak nokta bulununcaya kadar devam edecektir. Böylece rastgelelik bozulmamaktadır. Çünkü rastgele seçilen bir bireyden bir sonraki birey de rastgeledir. Şekil 4.9'da rulet fonksiyonu rastgele iki ebeveyn belirlesin. Bu ebeveynler 3 ve 5 numaralı bireyler olsun. Fakat 3 numaralı bireyin kromozomları ile 5 numaralı bireyin kromozomları arasında yapılan incelemede ortak düğümlerinin olmadığı görülmektedir. Bu durumda belirli bir prop fonksiyonu kullanılarak yeni bir birey seçilmekte ve ortak düğüm noktalarının varlığı kontrol edilmektedir. Bu işlem ortak düğümü olan iki ebeveyn bulununcaya kadar devam etmektedir. Prop fonksiyonu olarak $F(x) = x + 1$ kullanılabilir. Böylece yeni bulunan birey; yani 6 numaralı birey ebeveyn olarak denenecektir. 3 numaralı birey ile 6 numaralı birey arasında 12 numaralı düğüm ortak olduğu için prop fonksiyonu durdurulmuş ve bu iki birey arasında çaprazlama yapılmıştır. Eğer ortak bir düğüm bulunmasaydı arama işlemimiz prop fonksiyonuna göre (burada bir sonraki) yeni birey numarası elde edilerek devam edecektir.

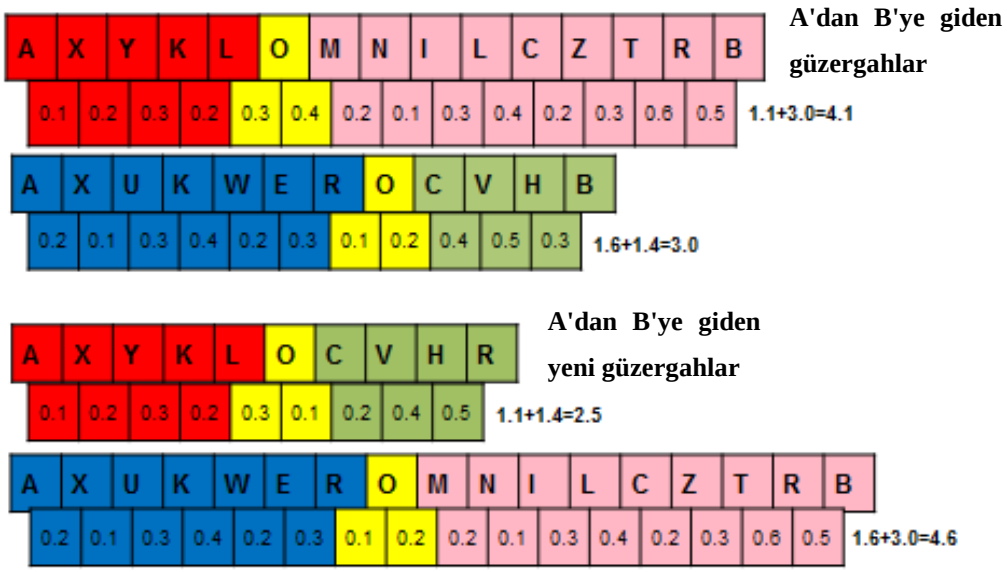
Birey numarası	Kromozomları
0	3,6,8,12,4,35
1	3,6,7,12,35
2	3,6,4,5,7,15,21,35
3	3,2,8,7,12,13,5,35
4	3,45,13,35,44,56,75,35
5	3,24,14,23,26,28,35
6	3,7,12,45,65,25,35
7	3,8,16,13,25,33,35
8	3,44,3,32,23,74,88,13,35
.....	.....

Şekil 4.9. Bireyler ve bireylerin kromozomlarının göstericileri

Çizelge 4.5. Uyum fonksiyonunun genel yapısı

```
for(sayaç=1;sayaç<genboyu;sayaç++)
      {
      if(gshm(gen(sayaç),gen(sayaç+1))<güvenlik)
            güvenlik=gshm(gen(sayaç),gen(sayaç+1))
      }
return "yol güvenlik değeri"
```

Uyum fonksiyonu ile elde edilen sonuçların en küçük olanı en uygun olacak şekilde sıralanarak belirli bir nesil sonunda çözüme ulaşılır. Örnek uyum fonksiyonu sonuçları Şekil 4.10'de verilmiştir.



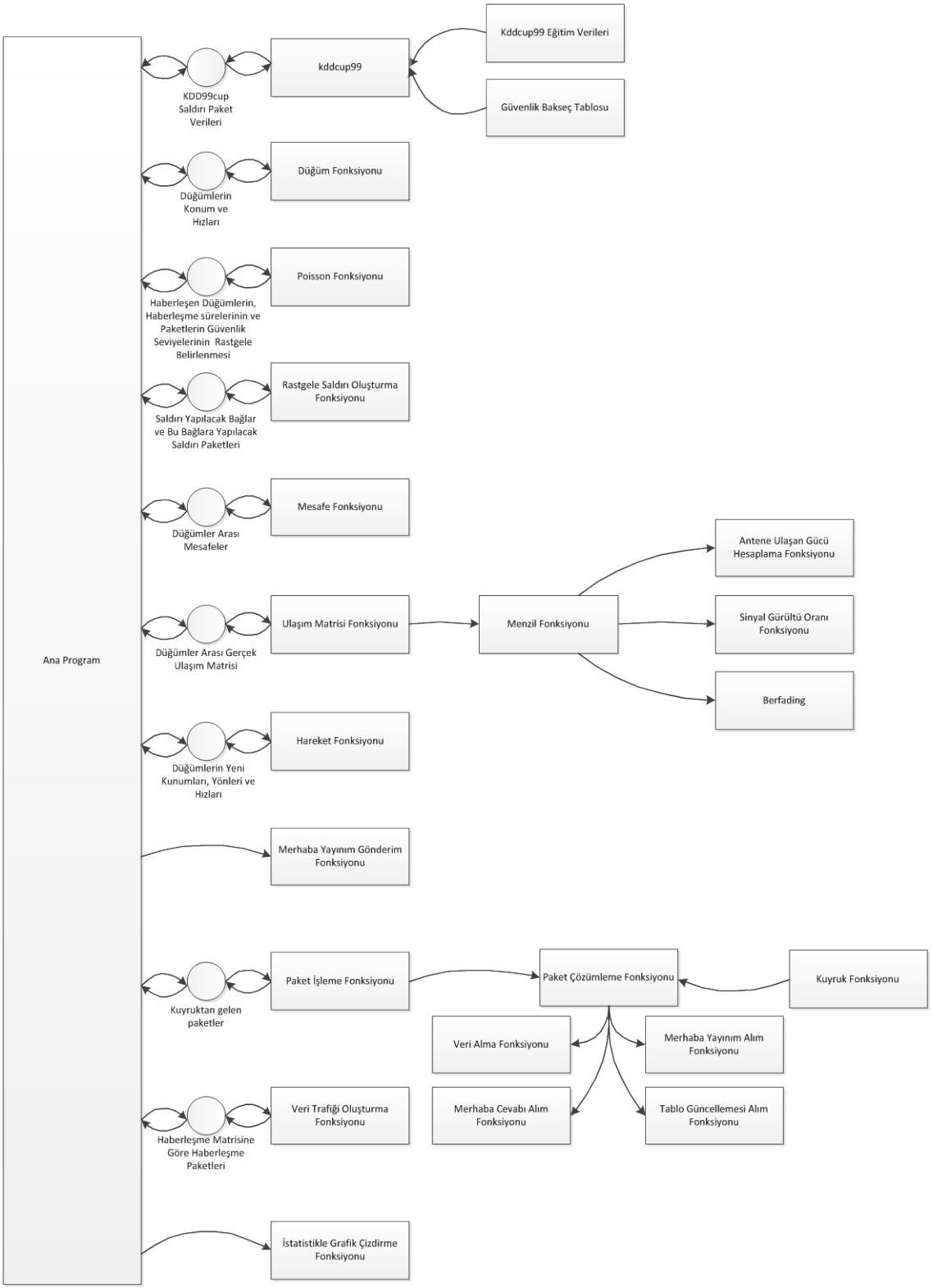
Şekil 4.10. İki güzergah ve bu güzergahların uyum fonksiyonu (güvenlik değeri) değerleri. Güzergahların çaprazlanması sonucu elde edilen yeni güzergahlar ve bu yeni güzergahların uyum fonksiyonu (güvenlik değeri) değerleri ve bireylerin kromozomlarının göstericileri

5. GELİŞTİRİLEN PROTOKOLÜN BENZETİMİ VE ANALİZİ

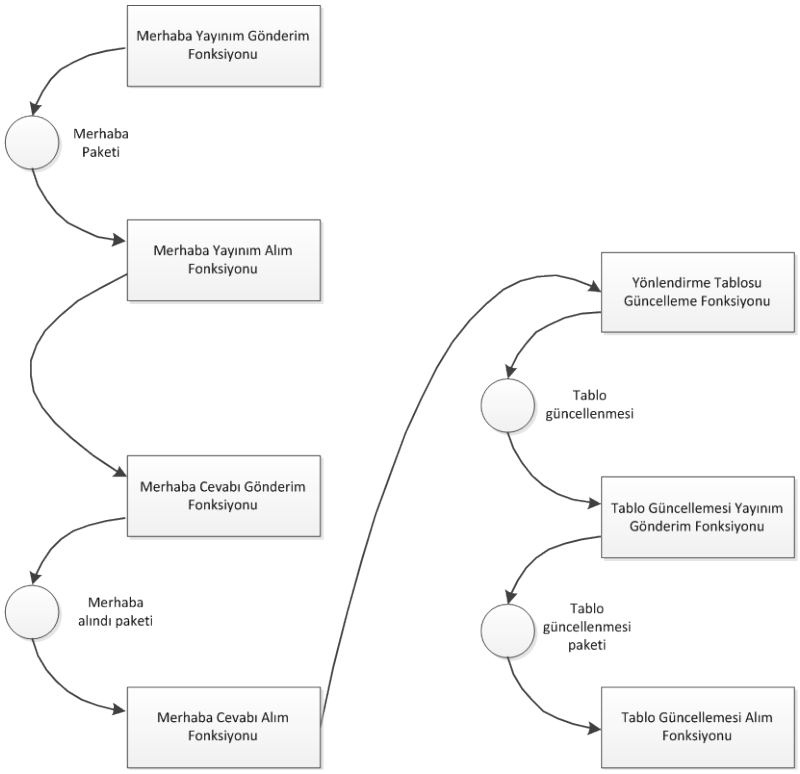
Literatürde geliştirilen diğer protokollerin ağ benzetim aracı olarak kullanılan olay tabanlı benzetim araçları, geliştirilen protokolün benzetimi için de kullanılmaktadır. Çünkü düğümler gerçek hayatta ayrı yerlerde ve birbirlerinden bağımsız çeşitli görevleri yerine getirmek amacıyla üretilmişlerdir. Bu nedenle geliştirilen protokolün benzetimi Matlab programlama dili ile gerçekleştirilmiştir. Benzetim programı fonksiyonel bir yapıdadır. Ayrıca benzetim parçalı ve birbirinden bağımsız düğümlerden oluştuğu için nesne yönelimli programlama yaklaşımı uygulanmıştır. Benzetimde, baz istasyonları ve hareketli düğümler olmak üzere iki çeşit düğüm kullanılmıştır. Program çeşitli görevleri yerine getiren fonksiyon parçalarından oluşmaktadır.

5.1. Benzetim Akış Fonksiyonları

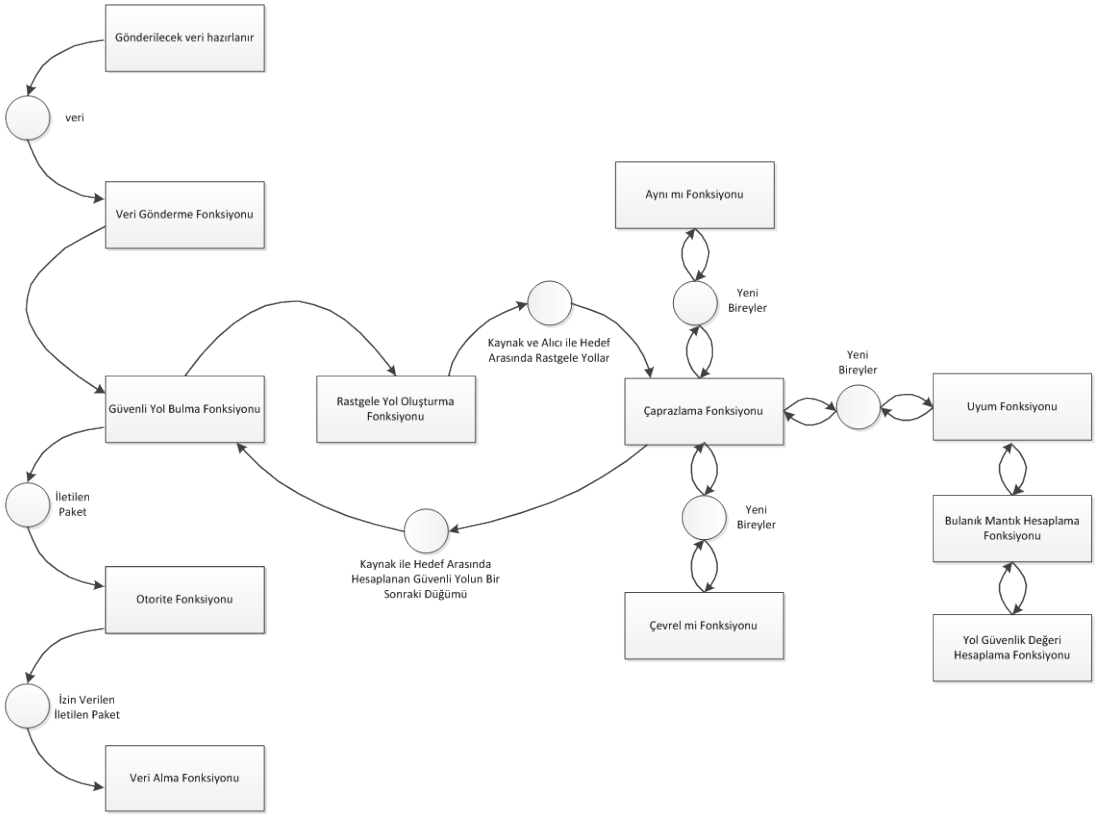
Benzetimi gerçekleyen fonksiyon ve programlar aşağıda anlatılmaktadır. Geliştirilen protokolde yapılan benzetim işlemleri Şekil 5.1-5.4'de verilmiştir.



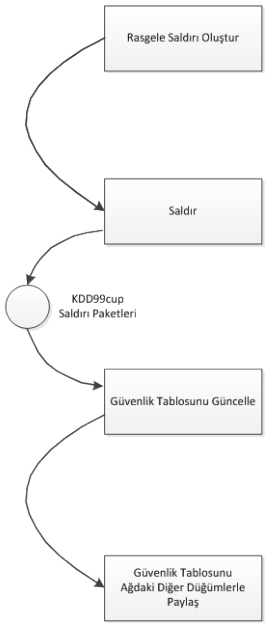
Şekil 5.1. Benzetim programının ana akış ve fonksiyonlar arası iletişim şeması



Şekil 5.2. Yönlendirme tablosu oluşturma fonksiyonları ve aralarındaki iletişim şeması



Şekil 5.3. Paket iletimi fonksiyonları ve aralarındaki iletişim şeması



Şekil 5.4. Güvenlik tablosu fonksiyonları ve aralarındaki iletişim şeması

Ana Program: Benzetim programının ana fonksiyonudur. Bu fonksiyonda; benzetimi yapılacak düğümlerin sayısı, baz istasyonu sayısı, düğümlerin dağıldıkları alanın bir kenarının metre cinsinden değeri, düğümlerin başlangıç hızları ve ivmeleri, düğümlerde bulunan paket kuyruğunun maksimum uzunluğu, düğümlerden gönderilen merhaba yayınımları arasındaki bekleme zamanı tanımlanmaktadır.

Oluşturulan düğümlerin başlangıç pozisyonlarının hesaplanması için gerekli fonksiyon olan düğüm fonksiyonu çağırılır. Birbirleri arasında veri haberleşmesi yapan düğümler ve verilerin iletileceği güvenlik seviyesi de bu fonksiyonda tanımlanmaktadır. Düğümlerin hareketlerini kontrol edip düzenleyen fonksiyonlar çağırılmaktadır. Ayrıca benzetim devam ederken elde edilen verilerin görüntülenmesi ve kayıt altına alınması için gerekli fonksiyonlar da çağırılır.

Erişim Fonksiyonu: Düğümlerin ulaşım matrisinin hesaplanmasında kullanılan fonksiyondur. Bu fonksiyonda; düğümlerin anten kazançları, iletim güçleri ve ortam gürültüsü tanımlanmaktadır. Bu tanımlamalar ışığında iki düğüm arasındaki maksimum haberleşme mesafesi hesaplanmaktadır.

Antene Ulaşan Gücü Hesaplayan Fonksiyon: Alıcı ve verici düğümün anten kazancı G_r ve G_t, aradaki mesafe d, ve iletim gücü P_t, alıcı düğüme iletilen güç P_r'nin hesaplandığı fonksiyondur. İletim gücünün denklemi Eş. 5.1'de verilmiştir.

$$P_r = \frac{G_t \bullet G_r \bullet P_t}{d^4} \tag{5.1}$$

Sinyal Gürültü Oranı Fonksiyonu: Ortamın sinyal gürültü oranını hesaplayan fonksiyondur. Fonksiyonun denklemi Eş. 5.2'de verilmiştir. P_r alıcı düğümün anteninin aldığı güç, P_n antenin bulunduğu ortam gürültüsüdür.

$$SNR = 10\log\left(\frac{P_r}{P_n}\right) \tag{5.2}$$

Menzil Fonksiyonu: Düğümlerin sinyal gürültü oranlarına göre karşılıklı haberleşme yeteneklerini hesaplayan fonksiyondur.

Ulaşım Matrisi Fonksiyonu: Menzil fonksiyonundan elde edilen bilgiler kullanarak sanal evren içindeki düğümlerin birbirleri arasında bir ulaşım matrisi elde edilir. Elde edilen bu matris anlık gerçek komşuluk matrisidir. Bu matris otorite fonksiyonu tarafından düğümler arasındaki paket iletimlerinin yapılmasında iletim izinleri için kullanılmaktadır.

Otorite Fonksiyonu: Bu fonksiyon paketler için sanal evrenin benzetimini yapan kısımdır. Erişim fonksiyonundan alınan anlık gerçek komşuluk matrisine göre düğümlerin birbirlerine gönderdikleri paketleri yönetir. Bir düğüm tarafından gönderilen paket bu fonksiyona iletilir. Bu fonksiyon anlık gerçek komşuluk matrisine göre gerekli kontrolleri yapar ve iki düğüm arasında haberleşme varsa söz konusu paketi iletir. Eğer iki düğüm arasında haberleşme yoksa paket günlüğe kaydedilir ve gönderilen paketin alıcısı olmadığı için kayıp paket olarak kabul edilir.

Düğüm Fonksiyonu: Düğümlerin başlangıç konumlarını, başlangıç yönlerini ve hızlarını Ana Programda girilen başlangıç değerlerine göre hesaplayıp belirlenen alana rastgele dağıtan fonksiyondur.

Hareket Fonksiyonu: Düğümlerin verilen alan içinde rassal fakat gerçekçi hareketlerinin sağlanması için hazırlanmış fonksiyondur. Fonksiyonda düğümlerin hızları ve yönleri Ana Programda verilen sınırlar dahilinde yeniden hesaplanır. Ardından arazideki konumları hesaplanan yeni hız ve yönlerine göre tespit edilir.

Mesafe Fonksiyonu: Düğümler arasındaki mesafenin hesaplandığı fonksiyondur. Bu tablo sinyal gürültü oranının hesaplanmasında kullanılmaktadır. İki düğüm arasındaki mesafenin hesabı Eş. 5.3 ile hesaplanmaktadır.

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{5.3}$$

Kuyruk Fonksiyonu: Düğümlerin haberleşme kuyruğu işlemlerini gerçekleştiren fonksiyondur. Düğümlerde bulunan paket kuyruklarına paket eklenmesi, çıkarılması ayrıca kuyruğun dolması gibi hata yönetimi işlemlerini yöneten fonksiyondur. Ana Programda belirtilen kuyruk uzunluğuna göre kuyruğun boyutu belirlenmektedir.

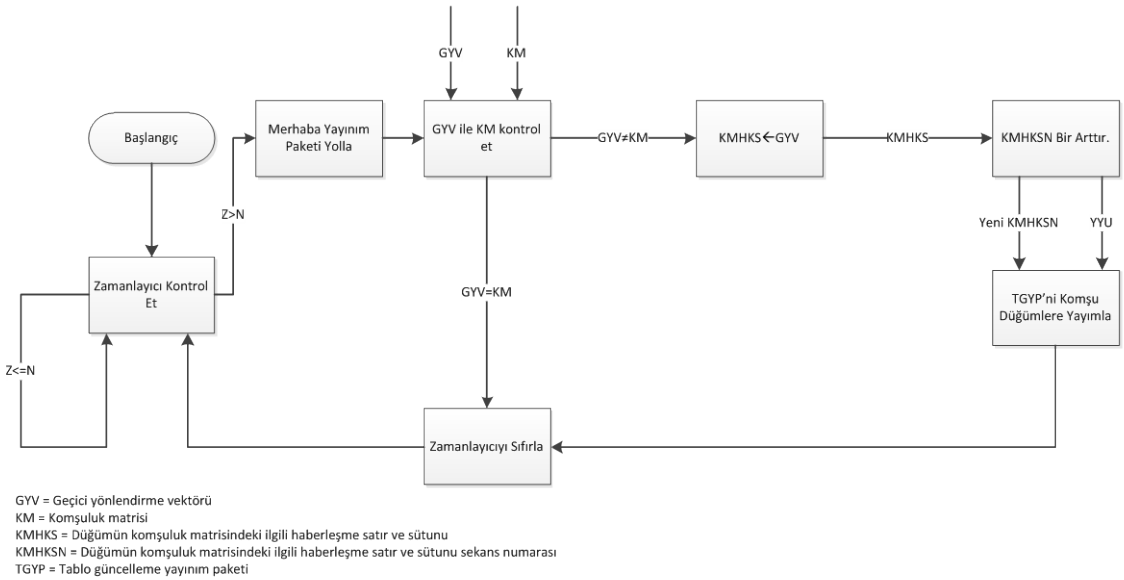
Paketleri İşleme Fonksiyonu: Bu fonksiyonun görevi kuyruk fonksiyonu ile kuyruktan paket okuyup, onu Paket Çözümleme Fonksiyonu ile çözümledikten sonra, paketin tipine göre sınıflandırarak gerekli fonksiyonlara iletmektir. Paket, merhaba yayınım paketi ise Merhaba Yayınımı Alım Fonksiyonu, merhaba cevap paketi ise Merhaba Cevap Alım Fonksiyonu, tablo güncelleme paketi ise Tablo Güncelleme Alım Fonksiyonu, veri paketi ise Veri Alım Fonksiyonuna iletilmektedir. Eğer paket bunların hiçbiri değilse, o zaman paket ihmal edilir, paket günlüğe yazılır ayrıca paket STS'ye bildirilir.

Merhaba Yayınım Gönderim Fonksiyonu: Düğümlerin çevrelerine belirli aralıklarla merhaba mesajı yayımlamalarını sağlayan fonksiyondur. Böylece çevre düğümler yayım yapan düğümle komşu olduklarını anlayarak tablolarında gerekli düzenlemeyi yapacaklardır. Her düğümde bulunan zamanlayıcılar sıfırlandığında bu fonksiyon çevresine merhaba yayınımı yapar ve zamanlayıcıyı başlangıç değerine getirir. Şekil 5.5'de merhaba yayınım paketi zaman sayacı olayında yapılan işlemler gösterilmiştir.

Merhaba yayınım paketi zaman sayacı olayı için kulanılan adımlar aşağıda verilmiştir.

1) Merhaba yayınım paketi yolla.
2) Geçici yönlendirme vektörü (GYV) ile düğümün komşuluk matrisindeki (KM) satır ve sütun değerlerini karşılaştır. Farklılık yoksa 6. adıma atla.

3) Düğümün komşuluk matrisindeki haberleşme satır ve sütunu (KMHKS), GYV ile değiştir.
4) Düğümün KMHKS sekans numarası bir arttır.
5) Yeni yönlendirme vektörü, yeni sekans numarası ile beraber komşu düğümlere tablo güncelleme yayınım paketi olarak yayımla.
6) Sayaçı sıfırla.
7) Son



Şekil 5.5. Merhaba yayınım paketi zaman sayacı olayında yapılan işlemler

Merhaba Yayınım Alım Fonksiyonu: Düğüm haberleşme kuyruğundan işlenmek üzere merhaba yayınım paketi çıktığında, çıkan paket bu fonksiyona iletilerek paketin işlenmesi sağlanmaktadır. Fonksiyon paketi çözer ve kendi yönlendirme tablosunu günceller. Ayrıca geri merhaba yayınım paketi aldığı düğüme merhaba cevap paketi gönderir.

Merhaba yayınım paketi alınması olayı;

1) Merhaba yayınım paketini yollayan düğüme merhaba cevap paketi gönder.
2) Son

Merhaba Cevabı Gönderim Fonksiyonu: Bu fonksiyon, düğüm merhaba yayınım paketi aldığında merhaba cevap paketinin hazırlanarak geri gönderilmesini sağlayan fonksiyondur.

Merhaba Cevabı Alım Fonksiyonu: Düğüm haberleşme kuyruğundan işlenmek üzere merhaba cevap paketi çıktığında, çıkan paket bu fonksiyona iletilerek paketin işlenmesi sağlanmaktadır. Fonksiyon paketi çözer ve kendi yönlendirme tablosunu günceller.

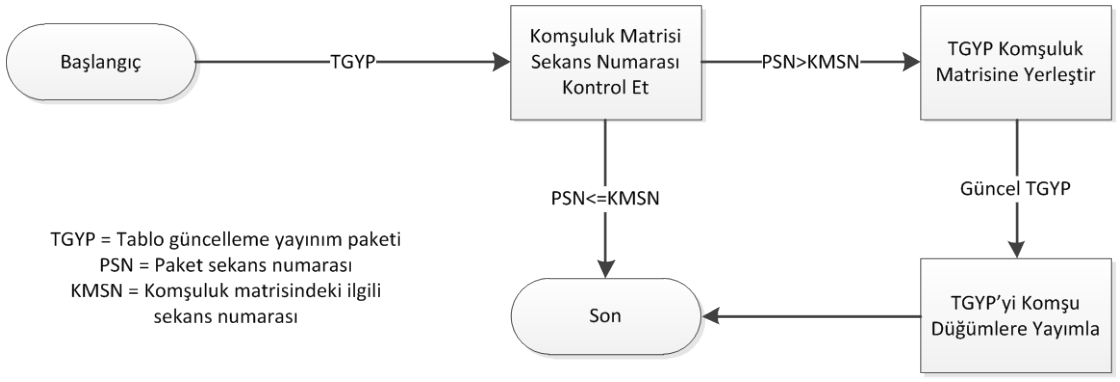
Merhaba cevap paketi alınması olayı için kullanılan adımlar aşağıda verilmiştir.

1) Merhaba cevap paketinin geldiği düğüm, geçici yönlendirme vektörüne haberleşebiliyor olarak işle.
2) Son

Yönlendirme Tablosu Güncelleme Fonksiyonu: Bu fonksiyon düğümün yönlendirme tablosu güncellenmesi gerekebileceği durumlarda çağırılır. Fonksiyon tablo ile gelen güncelleme bilgisini karşılaştırır. Tabloda bir değişiklik yapılması gerekiyorsa gerekli değişikliği yapar ve yapılan bu değişikliği komşularına yeni bir sağlama sayısıyla beraber bildirilmesi için Tablo Güncellemesi Yayınım Gönderim Fonksiyonu çağırılır. Yönlendirme tablosu güncelleme paketine eklenen bu sağlama sayısı, yayınım fırtınası oluşumunun engellenmesi amacıyla oluşturulmuştur. Fonksiyon tabloda bir değişiklik gerekmiyorsa veya tablo zaten bu bilgiyi içeriyorsa herhangi bir düzenleme yapmaz.

Tablo Güncellemesi Yayınım Gönderim Fonksiyonu: Bu fonksiyon, düğümün yönlendirme tablosunda bir değişiklik meydana geldiğinde bunu komşu düğümlere bildirmek için hazırlanan paketi yayınlayan fonksiyondur.

Tablo Güncellemesi Alım Fonksiyonu: Bu fonksiyon düğümün tablosundaki ilgili satır ve sütunun sağlama sayısı ile gelen paketin içerdiği sağlama sayısını karşılaştırır. Paket ile gelen yeni bilginin sağlama sayısı tabloda bulunan sağlama sayısından büyükse tablo yeni paketteki yeni bilgilerle güncellenir ve komşulara Tablo Güncellemesi Yayınım Gönderim Fonksiyonu ile dağıtılır. Eğer paketle beraber gelen sağlama sayısı tablodaki ilgili satır ve sütunun sağlama değerinden küçükse, bu o paketin eski olduğunu göstermektedir. Bu durumda paket ihmal edilir ve hiçbir işlem yapılmaz. Şekil 5.6'da tablo güncelleme yayınım paketi alınması olayında yapılan işlemler gösterilmiştir.



Şekil 5.6. Tablo güncelleme yayınım paketi alınması olayında yapılan işlemler

Tablo güncelleme yayınım paketi (TGYP) alınması olayı için kulanılan adımlar aşağıda verilmiştir.

1) Paketin sekans numarası, paketi alan düğümün komşuluk matrisindeki ilgili sekans numarasına eşit veya küçükse 4. adıma git.
2) TGYP ile gönderilen vektör, düğümün komşuluk matrisindeki ilgili satır ve sütun ile değiştir.
3) TGYP komşu düğümlere yayımla.
4) Son

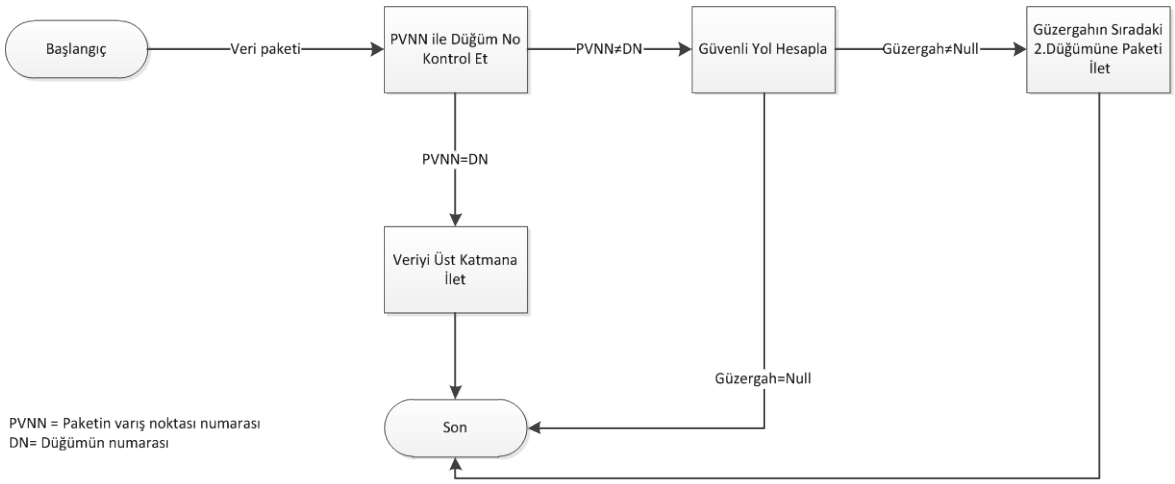
Paket Hazırlama Fonksiyonu: Fonksiyona gönderilen değişkenleri paketleyerek düğümler arası gönderilebilecek paketler halinde algoritmaya uygun veriyapısı oluşturur.

Paket Çözümleme Fonksiyonu: Paketin içindeki verileri ayıklayan fonksiyondur. Bu fonksiyona giren paket üyelerine ayrılır. Paketlerin içindeki değişkenlere erişilmesini sağlar.

Veri Hazırlama Fonksiyonu: Düğümlerin birbirlerine veri paketleri hazırlayıp göndermeleri için gerekli verinin hazırlandığı fonksiyondur. Veri olarak herhangi bir görüntü, ses, veya metin bilgisi kullanılabilir. Bu amaçla benzetimde hafıza kaplamaması açısından '0' katarı iletilen veri olarak kullanılmıştır.

Veri Gönderme Fonksiyonu: Bu fonksiyon öncelikle kaynaktan hedefe iletilecek veri paketinin bir sonraki adımda hangi düğüme gönderilmesi gerektiği bilgisini hesaplamak için Güvenli Yol Bulma Fonksiyonunu çalıştırır. Bulunan en uygun ve güvenli yolun bir sonraki atlama düğümü, veri ve diğer bilgiler Paket Hazırlama Fonksiyonu ile veri paketi haline dönüştürülür. Elde edilen paket sonraki atlama düğümüne iletilmek üzere Otorite Fonksiyonuna gönderilir.

Veri Alma Fonksiyonu: Kuyruktan alınan paket eğer veri paketi ise paket Veri Alma Fonksiyonu tarafından işlenir. Bu fonksiyon öncelikle paketin TTL değerini bir yükseltir. Ardından paketin hedefinin kendisi olup olmadığını kontrol eder. Eğer hedef düğüm kendisi ise günlüğe paket başarılı bir şekilde hedefe ulaştı bilgisini yazar. Eğer hedef kendisi değilse, yeni hesaplanan TTL değerini, maksimum atlama değeriyle karşılaştırır ve hesaplanan TTL değeri Maksimum atlama değerine eşitse veya üzerindeyse paketi atıp, günlüğe paket maksimum TTL değerini aştığı için atılmıştır bilgisiyle beraber kayıt eder. Eğer hesaplanan TTL değeri maksimum atlama sayısının altında ise paket hedefe gönderilmek üzere Veri Gönderme Fonksiyonuna iletilir. Şekil 5.7 veri paketi alma olayında yapılan işlemleri göstermektedir.



Şekil 5.7. Veri paketi alma olayında yapılan işlemler

Veri paketi alınması olayı için kulanılan adımlar aşağıda verilmiştir.

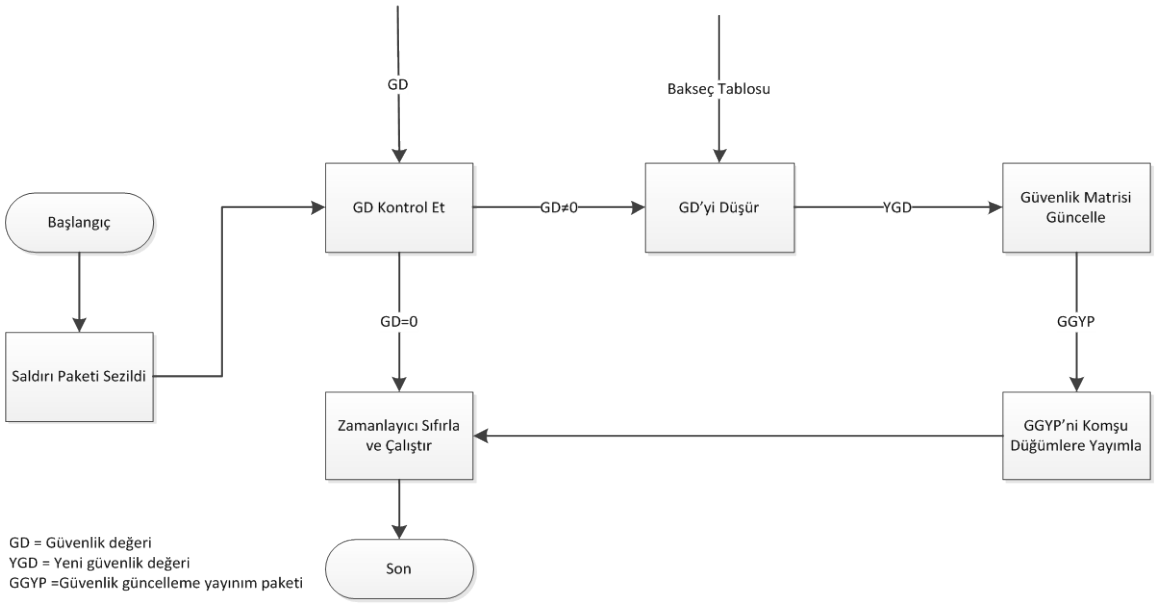
1) Paketin varış noktası numarası ile düğümün numarası aynı ise paketin içindeki veriyi üst katmanlara ilet ve 5. adıma git.
2) Veri paketi içindeki güvenlik seviyesine göre, bu düğüm ile varış düğümü arasında uygun güzergahı hesapla.
3) Uygun bir güzergah bulunamaz ise paketi düşür ve 5. adıma git.
4) Hesaplanan güzergahın 2. düğümüne paketi ilet.
5) Son

Güvenlik Tablosu Oluşturma Fonksiyonu: Bu fonksiyon saldırı bilgisini, Saldırı Bilgisi Al Fonksiyonundan alır. Güvenlik tablosunu günceller ve kendisi ile ilgili değişiklikleri komşu düğümlere yayımlar.

Saldırı Bilgisi Al Foksiyonu: Bu fonksiyon KDDCUP99 eğitim veritabanından aldığı verilerle, düğümün komşuluğunda olan düğümler ve onlarla olan bağları hakkında anormal aktiviteye sahip bağların puanlarının düşürülmesi, diğerlerinin ise süreölçer vasıtasıyla zaman içinde yükseltilmesini hesaplamaktadır.

Saldırı paketleri alma olayı için kulanılan adımlar aşağıda verilmiştir.

1) Saldırının geldiği bağın güvenlik değeri 0 ise 5. Adıma git.
2) Saldırının geldiği bağın güvenlik seviyesi, saldırının türüne göre bakseç tablosuna bakılarak düşür.
3) Güvenlik matrisindeki değişen bağın olduğu satır ve sutununun sekans numarası bir arttır.
4) Yeni bağ değeri ve sekans numarası güvenlik güncelleme yayınım paketi olarak paketlenerek komşu düğümlere ilet.
5) O bağ için zamanlayıcı sıfırlanarak çalıştır.
6) Son

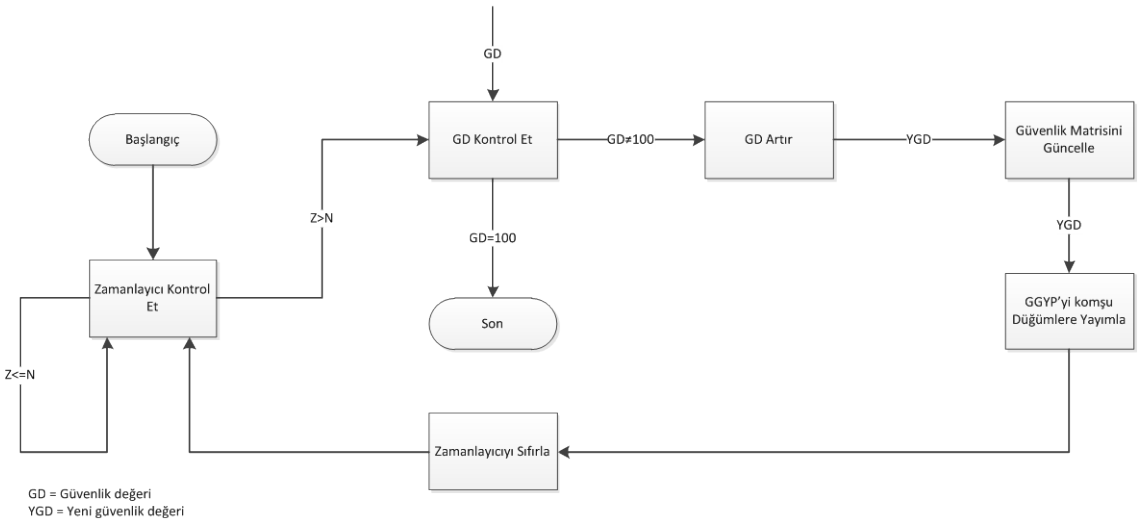


Şekil 5.8. Saldırı paketleri alma olayında yapılan işlemler

Saldırı paketi alma zaman-aşımı olayı için kullanılan adımlar aşağıda verilmiştir.

1) Bağın güvenlik değeri 100 ise zamanlayıcıyı durdur ve 5. adıma git.
2) Bağın güvenlik değeri belirlenen değerde arttır.

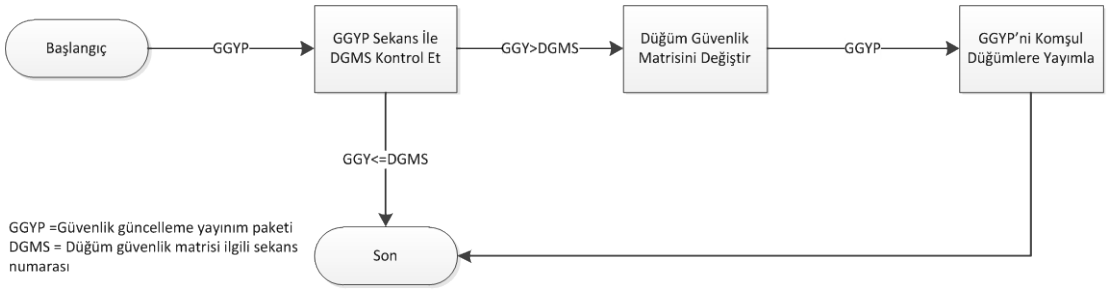
3) Güvenlik matrisindeki değişen bağın olduğu satır ve sütununun sekans numarası bir arttır.
4) Yeni bağ değeri ve sekans numarası güvenlik güncelleme yayınım paketi olarak paketlenerek komşu düğümlere ilet.
5) Son



Şekil 5.9. Saldırı paketi alma zaman aşımı olayında yapılan işlemler

Güvenlik güncelleme yayınım paketi (GGYP) alma olayı için kulanılan adımlar aşağıda verilmiştir.

1) Paketin sekans numarası, paketi alan düğümün güvenlik matrisindeki ilgili sekans numarasına eşit veya küçükse 4. adıma git.
2) GGYP ile gönderilen vektör, düğümün komşuluk matrisindeki ilgili satır ve sütun ile değiştir.
3) GGYP komşu düğümlere yayımla.
4) Son



Şekil 5.10. Güvenlik güncelleme yayınım paketi gönderilmesi olayında yapılan işlemler

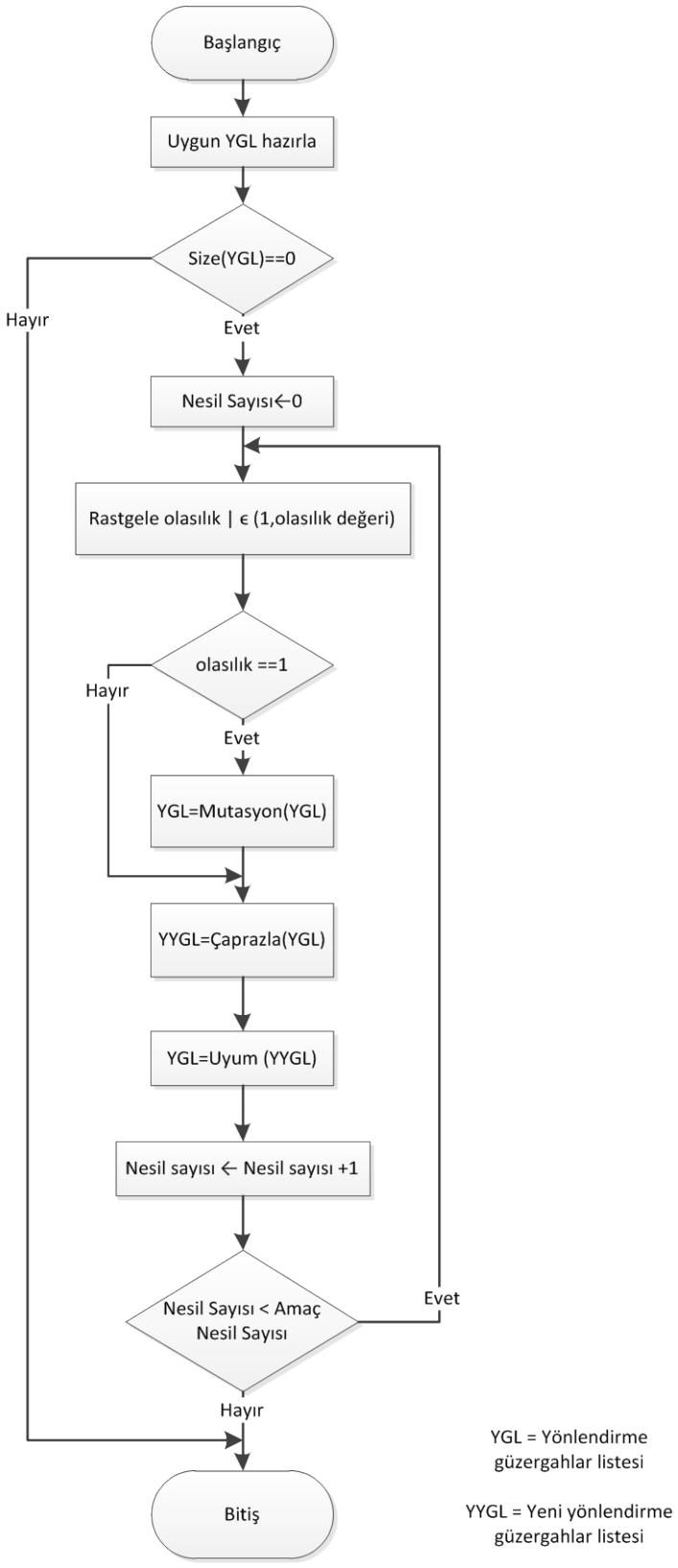
Bulanık Mantık Hesaplayıcı Fonksiyon: Bu fonksiyon belirli iki düğüm arasındaki bağı, dilsel yargılar kullanılarak puanlamaktadır. Bu puanın hesaplanması için gerekli diğer bilgiler oluşturulan güvenlik tablosundan alınmaktadır. Fonksiyon bu amaçla bulanık kümeler ve onlara olan üyelik değerlerini kullanmaktadır. Problem bir minimizasyon problemi olduğu için üyelik değerleri 0 en iyi üye, bir ise en kötü üye olarak ifade edilecek şekilde hesaplanmaktadır. Bu amaçla benzetimde kullanılan ve Şekil 4.4'de verilen grafikte kullanılan dilsel ifadeler ve onların bulanık üyelik fonksiyonları gösterilmektedir. Ayrıca Şekil 4.4'de de görüldüğü gibi dilsel ifadelerin üyelik değerleri hesaplanırken üçgen üyelik fonksiyonları kullanılmıştır.

Bulanık güvenlik üyelik kümesi değerlerinin hesaplanması için kulanılan adımlar aşağıda verilmiştir.

1) Düğümde bulunan güvenlik matrisinden, pakette bildirilmiş güvenlik seviyelerine göre üyelik değerleri hesaplayarak bulanık güvenlik seviyesi üyelik matrisini elde et.
2) Son

Yolun Güvenlik Değerini Hesaplayan Fonksiyon: Bu fonksiyon verilen bir yol için belirli bir güvenlik seviyesinde o yolun güvenlik puanını hesaplamaktadır. Bu amaçla yol üzerindeki düğümlerin arasındaki bağların güvenlik puanını Bulanık Mantık Hesaplayıcı Fonksiyon ile hesaplayıp toplar.

Güvenli Yol Bul Fonksiyonu: Bu fonksiyon belirli bir dilsel güvenlik seviyesiyle kaynak ve hedef düğümleri arasında uygun yolun hesaplanmasını sağlayan fonksiyondur. Yolun hesaplanması için öncelikle kaynakla hedef arasında Rastgele Yol Oluştur Fonksiyonu ile sayısı Ana Programda belirtilen bir başlangıç popülasyonu oluşturulur. Oluşturulan bu populasyon Çaprazlama Fonksiyonuna gönderilerek İÖÇO yardımıyla çaprazlanır. Ayrıca belirli bir yüzde ile bazı yolların bazı genleri Mutasyon Fonksiyonuna gönderilerek İÖMO yardımıyla mutasyona uğratılır. Ardından yeni populasyon Uyum Fonksiyonuna gönderilir. Bu işlem Ana Programda belirlenen miktarda tekrarlanarak yeni nesiller oluşturulduktan sonra en uygun bireyin ikinci elemanı bir sonraki atlama elemanı olarak seçilerek çağıran fonksiyona geri gönderilir. Şekil 5.11'de Güvenli yol bulma fonksiyonunun akış diagramı gösterilmiştir.



Şekil 5.11. Güvenli yol bulma fonksiyonu akış şeması

Güvenli yol bulunması için kulanılan adımlar aşağıda verilmiştir.

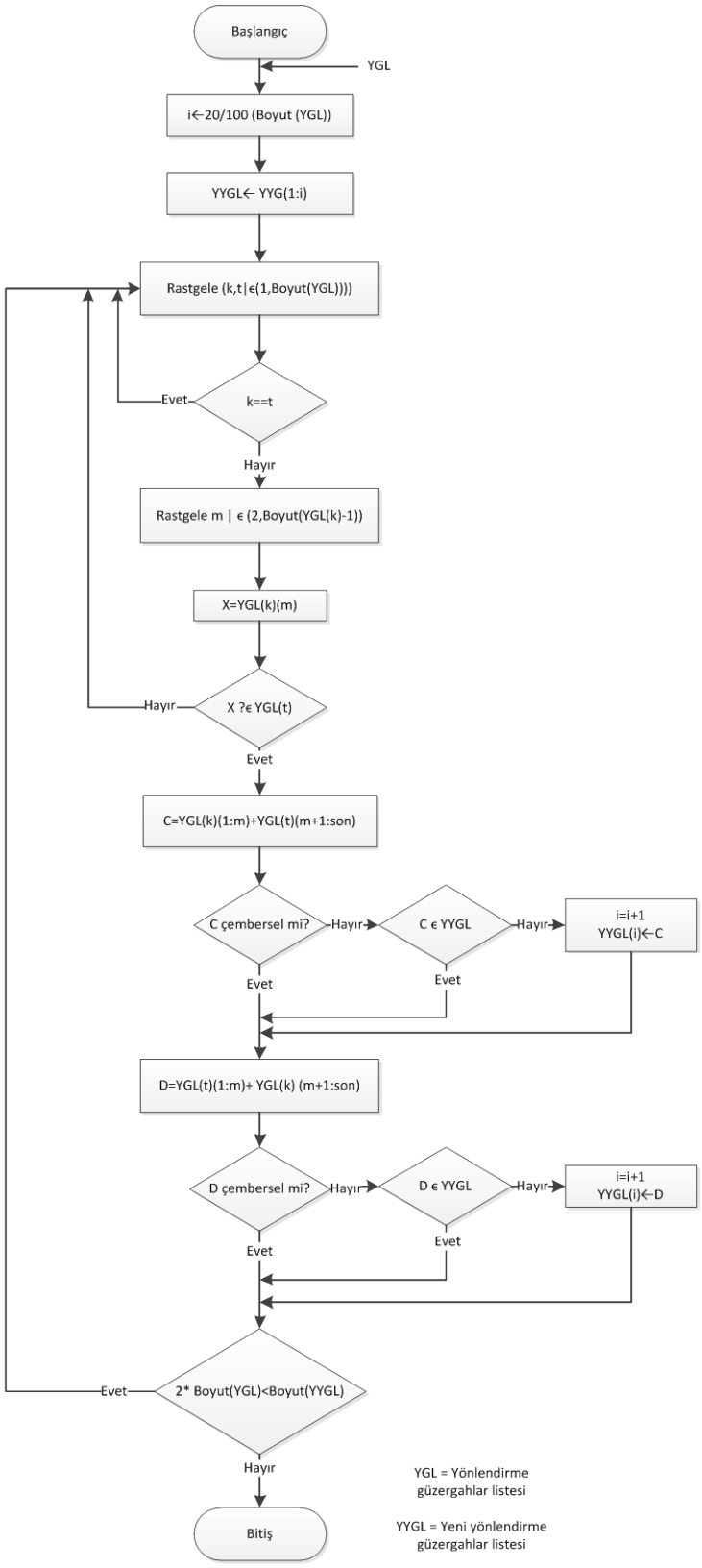
1) Başlangıçtan varışa kadar rastgele başlangıç popülasyon sayısı kadar bir güzergahlar listesi (GL) hazırla
2) GL 0 ise yol yoktur ve 9. adıma git.
3) Nesil sayısını sıfırla
4) GL'yi belirli bir olasılık oranı ile mutasyon fonksiyonundan geçir.
5) GL'yi çaprazlama fonksiyonundan geçir.
6) GL'yi uyum fonksiyonundan geçir.
7) Nesil sayısını bir arttır.
8) Nesil sayısı ulaşılacak nesil sayısından küçükse 4. adıma git.
9) GL'nin en üstündeki güzergahı uygun güzergah olarak ilet.
10) Son

Çaprazlama Fonksiyonu: Bu fonksiyon kendine gelen yollardan birini sırayla seçer ve üzerinde rastgele belirlediği bir düğümü belirler. Belirlenen bu düğümün sıradaki diğer düğümde bulunup bulunmadığına bakılır. Eğer bulunmazsa bir sonraki düğümde aranır. Aynı düğüm bulunca bu iki yol bu düğüm üzerinden çaprazlanarak yeni yol elde edilir. Ardından yavru yol, döngü kontrolü için Çevrel mi Fonksiyonuna gönderilir. Ardından yeni üretilen tüm yolların birbirleri ile aynı olup olmadığının kontrolü için Aynı mı Fonksiyonuna gönderilir. Aynı olanlardan biri çıkarılır. Bu işlem toplam popülasyonunun iki katı kadar nüfus elde edilinceye kadar devam eder. Şekil 5.12'de çaprazlama fonksiyonunun akış diyagramı gösterilmiştir.

Çaprazlama fonksiyonu için kullanılan adımlar aşağıda verilmiştir.

1) Yönlendirme güzergahları listesinin (YGL) ilk %20'sini yeni yönlendirme güzergahları listesine (YYGL) doğrudan aktar.
2) YGL'den rastgele iki güzergah seç (A ve B güzergahları).
3) A ve B güzergahları aynı ise 2. adıma git.
4) A güzergahından rastgele bir düğüm al (X düğümü).

5) B güzergahında X düğümü yoksa 2. adıma git.
6) A güzergahının başlangıcından X düğümüne kadar olan parçası ile B güzergahının X düğümünden varışa kadar olan parçasını birleştirerek yeni bir güzergah oluştur (C güzergahı).
7) C güzergahı çembersel ise 10. adıma git.
8) C güzergahı YYGL'de zaten varsa 10. adıma git.
9) C güzergahını YYGL'ye ekle.
10) B güzergahının başlangıcından X düğümüne kadar olan parçası ile A güzergahının X düğümünden varışa kadar olan parçasını birleştirerek yeni bir güzergah oluştur (D güzergahı).
11) D güzergahı çembersel ise 14. adıma git.
12) D güzergahı YYGL'de zaten varsa 14. adıma git.
13) D güzergahını YYGL'ye ekle.
14) YYGL, YGL'nin iki katından küçük ise 2. adıma geri dön.
15) Son



Şekil 5.12. Çaprazlama fonksiyonu akış şeması

Rastgele Yol Oluştur Fonksiyonu: Bu fonksiyon belirtilen iki düğüm arasında, sayısı Ana Programda başlangıç popülasyon sayısında belirtildiği kadar ve uzunluğu TTL değerini aşmayacak adımda rastgele yollar üretmektedir.

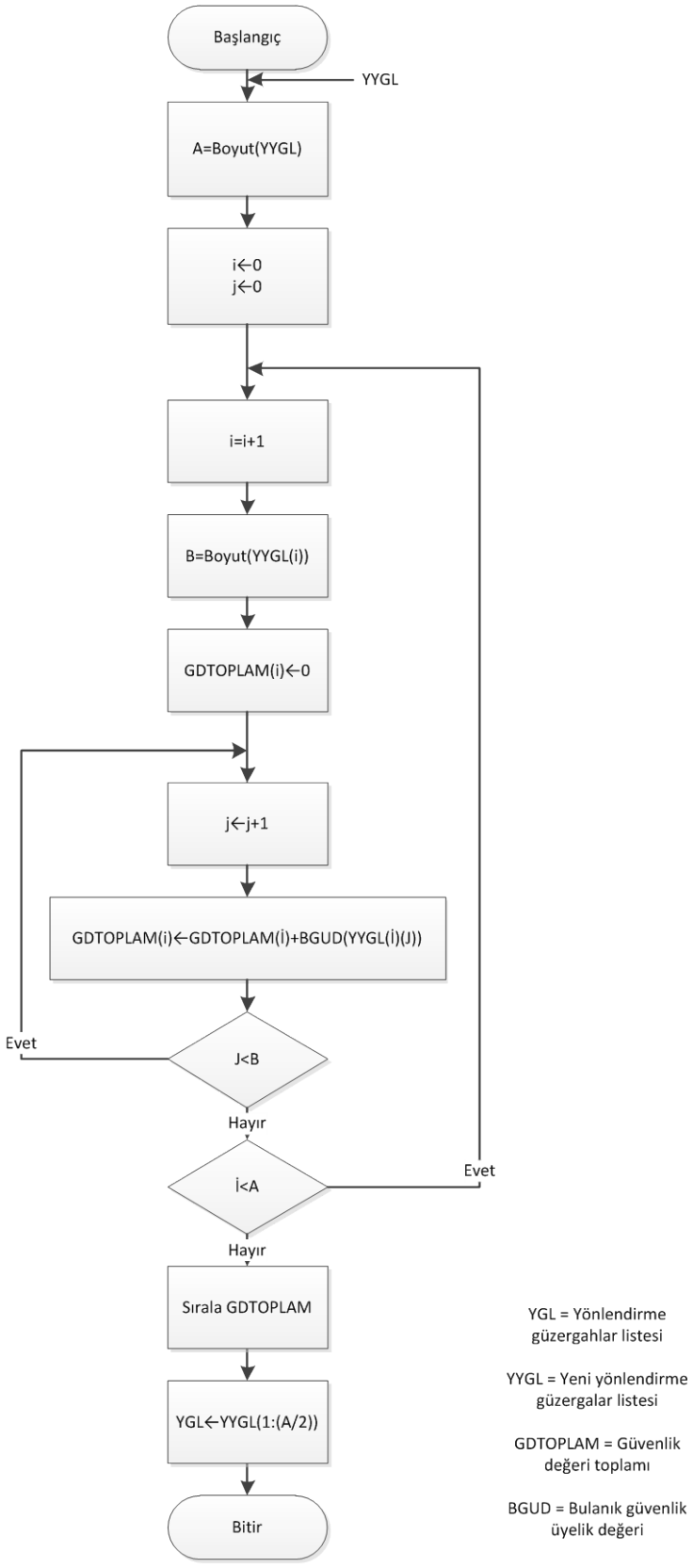
Çevrel mi Fonksiyonu: Bu fonksiyon yol üzerindeki döngüleri kontrol etmektedir.

Aynı mı Fonksiyonu: Bu fonksiyonda, verilen iki yolun aynı olup olmadığının kontrolü yapılmaktadır.

Uyum Fonksiyonu: Bu fonksiyon, dilsel ifade ile verilen güvenlik seviyesi için yol üzerindeki düğümler arası bağları güvenlikhesapla fonksiyonu ile hesaplar. Elde edilen değerler arasından en küçük olandan başlanarak popülasyon sayısı kadar birey seçilir ve geri kalanlar elenir. Şekil 5.13'de uyum fonksiyonunun akış diyagramı gösterilmiştir.

Uyum fonksiyonu için kullanılan adımlar aşağıda verilmiştir.

1) Güzergah listesindeki her bir güzergah için düğümleri arasındaki bulanık güvenlik üyelik kümesi değerlerini aralarında topla.
2) Bulunan değerlere göre listeyi küçükten büyüğe sırala.
3) Listenin üst yarısını yeni liste olarak döndür.
4) Son



Şekil 5.13. Uyum fonksiyonu akış şeması

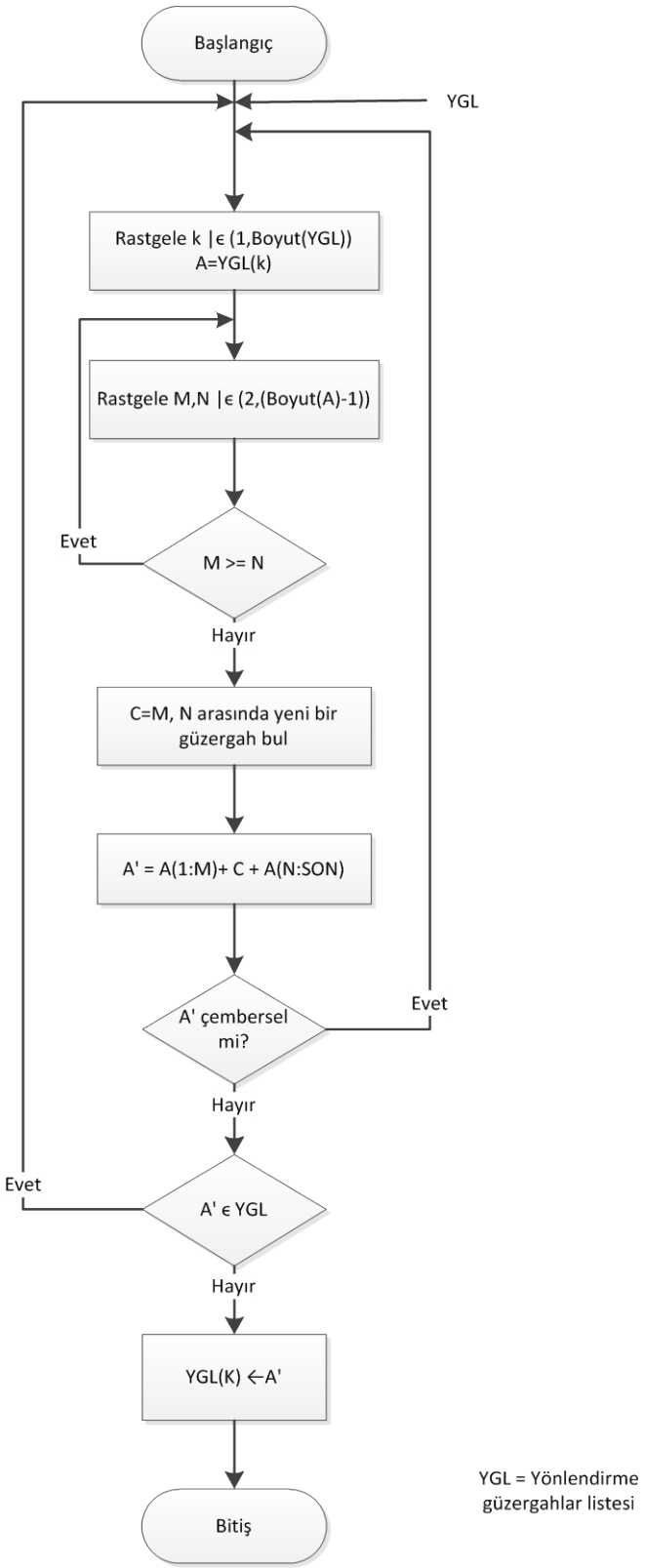
Mutasyon Fonksiyonu: Bu fonksiyon işleme özel mutasyon operasyonunu gerçekleştirir. Öncelikle belirli yol seçilir ve bu yolun üzerinde belirlenen iki düğüm arasındaki yol tekrar hesaplanarak değiştirilir. Şekil 5.14'de İşleme Özel Mutasyon Fonksiyonunun akış diyagramı gösterilmiştir.

Mutasyon fonksiyonu için kullanılan adımlar aşağıda verilmiştir.

1) Listedeki güzergahlardan birini rastgele seç (A güzergahı).
2) Seçilen güzergahdan iki düğümü rastgele seç (X ve Y düğümü).
3) X'den Y'ye yeni bir güzergah (B güzergahı) oluştur.
4) A güzergahında X ve Y arasını çıkarıp yerine B güzergahını ekleyerek yeni bir erişim güzergahı (A' güzergahı) oluştur.
5) A' güzergahı çembersel ise 1. adıma git.
6) A' güzergahı listede bulunan diğer güzergahlarla aynı ise 1. adıma git.
7) Listedeki A güzergahını A' güzergahı ile değiştir.
8) Son

Paket Günlüğü Kayıt Fonksiyonu: Bu fonksiyon kendisine iletilen paketleri ve onların hata kodlarını zaman etiketi ile beraber "packetlog.txt" dosyasına kayıt etmektedir.

İstatistik Grafiklerini Çizen Fonksiyon: Bu fonksiyon günlük dosyasından verileri okuyup, paketleri hata kodlarına göre sınıflandırıp istatistik grafiklerini çizdirmektedir.



Şekil 5.14. Mutasyon fonksiyonu akış şeması

5.2. Örnek Benzetim

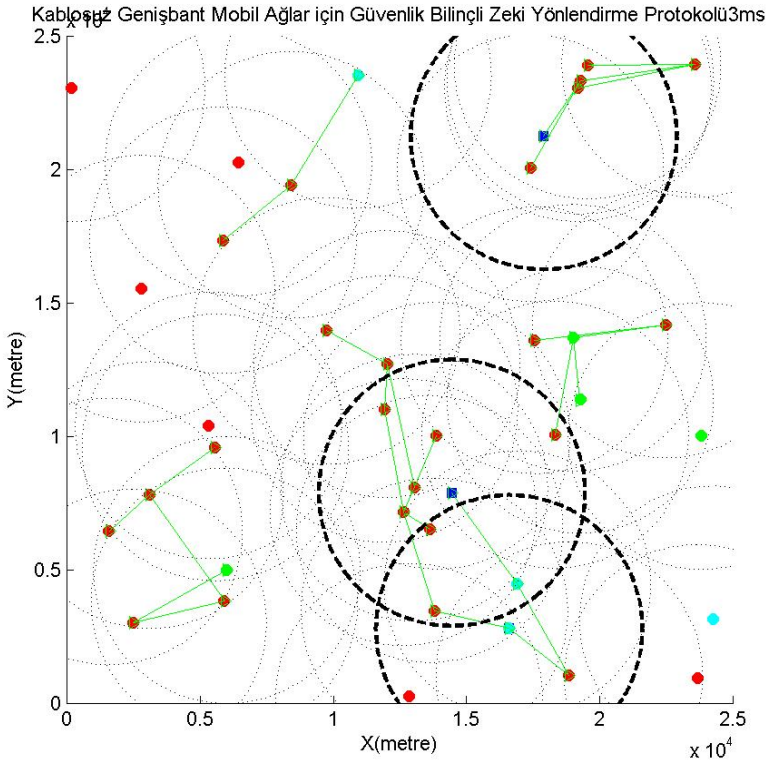
Hazırlanan örnek senaryonun genel özellikleri aşağıda verilmiştir.

- Toplam düğüm sayısı = 50 düğüm
- Toplam baz istasyonu sayısı = 3 kule
- Hareket halindeki düğümün başlangıç hızı = 5.0 m/s
- Hareket halindeki düğümün maksimum açısal yön değişim hızı = 20 ^{o}/s
- Hareket halindeki düğümlerin maksimum ivmelenmesi = 1 m/s^2
- Toplam simülasyon süresi = 3000 adım
- Simülasyon alanının boyutları = 25000 m X 25000 m
- Düğümler arasında maksimum bağlantı sayısı =1
- Maksimum atlama sayısı (TTL) = 10 düğüm
- Düğümler arası maksimum haberleşme mesafesi = 5000 m
- Düğüm kuyruk uzunluğu = 1000
- Düğüm yayınım zamanlayıcısı = 500 adım

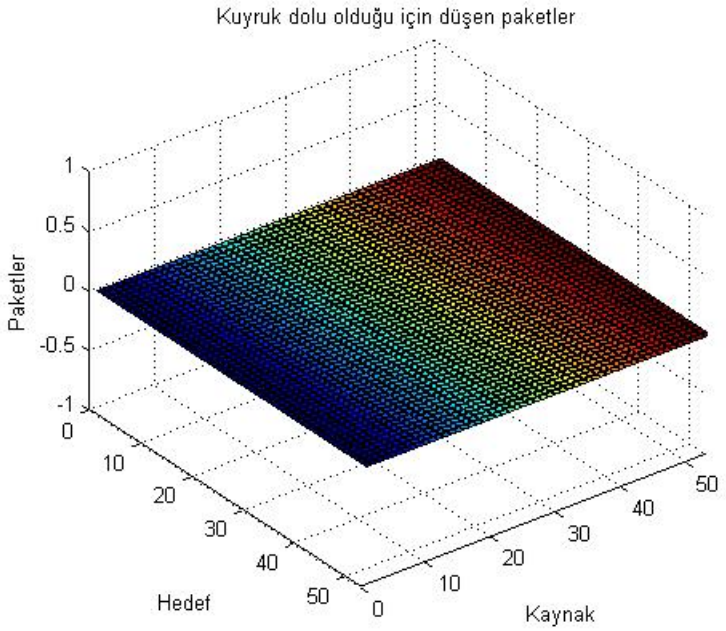
Düğümlerin başlangıç hızları ve yönleri verilen değişkenler yardımıyla hesaplanmaktadır. Ardından 100. adım ile 500. adım arasında

1. Düğüm → 5. Düğüme ‘az güvenilir’ damgalı paketler gönderilmektedir.

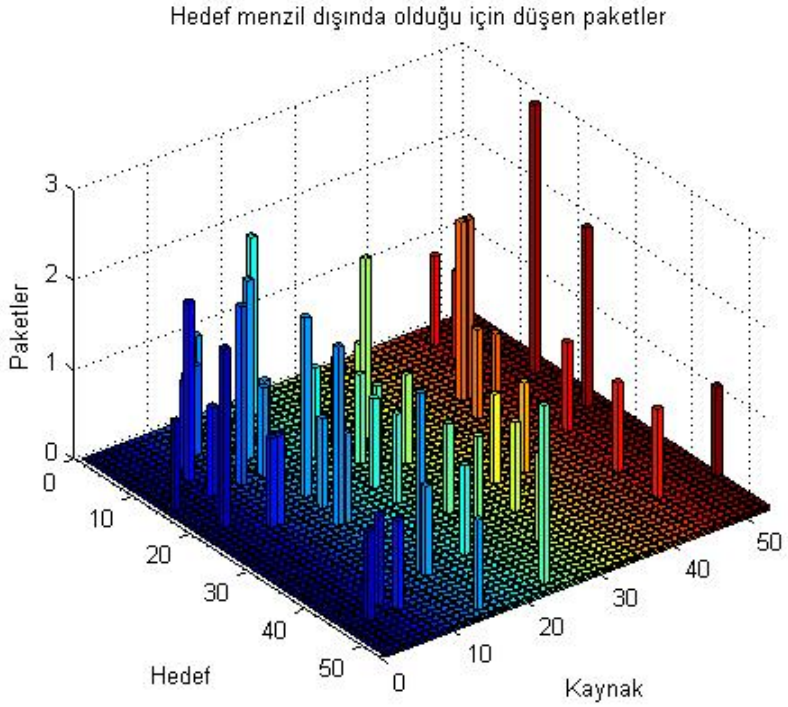
Benzetimin 3 ms sırasında alınan görüntüsü Şekil 5.15’de verilmiştir. Benzetim süresince kırmızı daire ile gösterilen düğümler rastgele hareket etmektedir. Mavi kare ile gösterilen düğümler ise baz istasyonları olup benzetim süresince konumları sabittir. Ayrıca düğümlerin haberleşme yarıçapları çizgili dairelerle gösterilmiştir. Baz istasyonlarının haberleşme yarıçapları kalın çizgili dairelerle gösterilmiştir. Düğümler arasında bulunan yeşil çizgiler düğümlerin birbirlerine ilettikleri paketlerdir. Benzetim sonucunda düşen ve hedefine ulaşan paket sayıları ile bunların noktalara göre dağılımları (Şekil 5.16 – 5.19) elde edilmiştir.



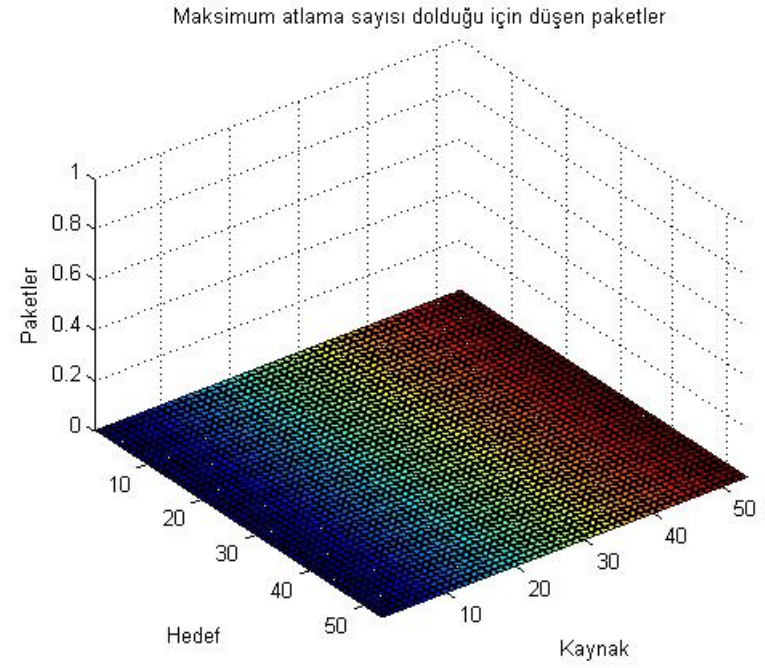
Şekil 5.15. Baz istasyonlarının ve hareketli düğümlerin iletim mesafeleri ve birbirlerine gönderdikleri paketler ve renk kodlu paket türleri



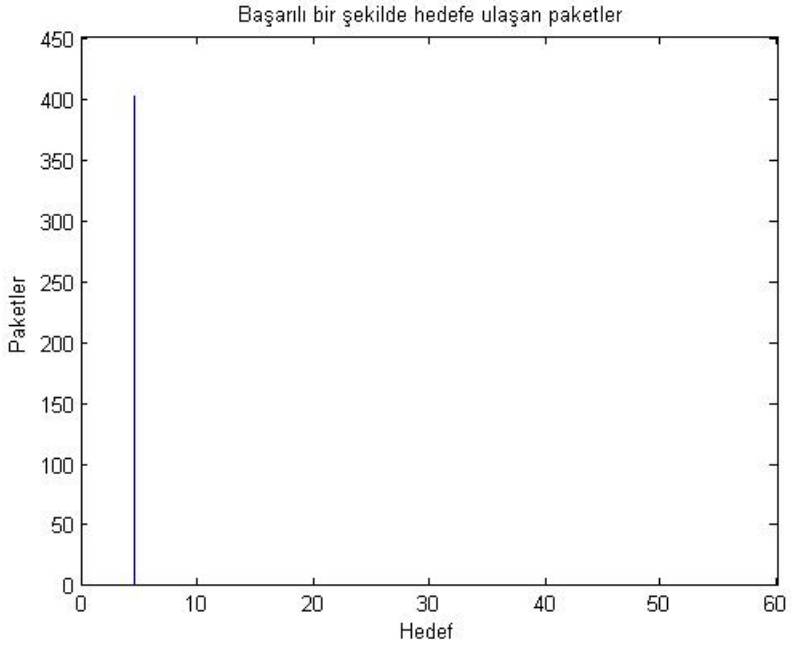
Şekil 5.16. Düğümlerin kuyruğu dolduğu için düşen paketler



Şekil 5.17. Hedef düğüm menzil dışında olduğu için düşen paketler



Şekil 5.18. Paket maksimum TTL sayısını aştığı için düşen paketler



Şekil 5.19. Başarılı bir şekilde hedefine ulaşan paket sayısı ve düğümlere göre dağılımları

5.3. Protokolün Performans Analizleri

Yönlendirme protokollerinin belirli bir standarda kavuşmasının sağlanması ve birbirleri ile karşılaştırılmalarını sağlamak amacıyla 1991 yılında Internet Engineering Task Force RFC 2501 (Request for comments) yayınlanmıştır. Bu belgede yönlendirme protokollerinin hangi kriterlere göre yapılacağı hakkında bilgi verilmiştir [3].

Performans metrikleri olarak da adlandırılan bu özellikler kalitatif ve kantitatif olmak üzere iki temel çatı altında incelenebilir. Hazırlanan protokolün kantitatif özellikleri şu şekilde sıralanabilir.

1) Paket dağıtım oranı: Toplam alınan veri paketlerinin (P_r), toplam iletilen veri paketlerine (P_s) oranı olarak ifade edilmektedir. Eş. 5.4'de gösterildiği gibi hesaplanmaktadır.

$$Pdr = \frac{P_r}{P_s} \tag{5.4}$$

2) Paket iletim kapasitesi(throughput): Alınan verinin (P_r) geçen zamana (t) oranıdır. Eş. 5.5'de gösterildiği gibi hesaplanmaktadır.

$$T = \frac{P_r}{t} \tag{5.5}$$

3) Yönlendirme ek yükü: Yönlendirme paketlerinin (P_{ro}), iletilen toplam paket sayısına (P_t) oranı olarak ifade edilmektedir. Eş. 5.6'da gösterildiği gibi hesaplanmaktadır.

$$R_o = \frac{P_{ro}}{P_t} \tag{5.6}$$

Protokolün performansı, Matlab programı yardımıyla oluşturulan senaryolar ve benzetim yazılımı ile hesaplanmış ve elde edilen veriler kullanılmıştır.

5.3.1. Benzetim parametreleri

Yapılan benzetimlerde, geliştirilen protokolün çeşitli parametreleri incelenmiş bunların yönlendirmeye ve performansa olan etkileri saptanmaya çalışılmıştır. Bu parametreler aşağıda verilmiştir.

Düğümlere Yapılan Ataklar

Düğümlerin %50'sine KDD99 eğitim veritabanından alınan saldırı paketleri ile değişik tehlike seviyelerinde rastgele saldırılar düzenlenmiştir. Böylece düğümlerdeki güvenlik tablolarının değişimi gerçekleştirilmiştir. Performans değerlendirmesinde saldırılar var yada yok şeklinde kullanılmıştır. Ayrıca düğümlerin %10, %20, %30, %40 ve %50'sine KDD99 eğitim veritabanından alınan

saldırı paketleri ile değişik tehlike seviyelerinde rastgele saldırılar düzenlenmiştir. Böylece çeşitli saldırı düzeyleri karşısında protokolün performansı incelenmiştir.

Maksimum TTL

Paketlerin maksimum yaşama süresinin yani maksimum atlama sayısının haberleşmeye olan etkisinin incelenmesi amacıyla 5, 10 ve 15 olarak seçilmiştir.

Nesil Sayısı

Genetik algoritmada nesil sayısının yol bulunmasına ve dolayısıyla haberleşmeye olan etkisinin incelenmesi amacıyla 10 ve 20 nesil parametre olarak belirlenmiştir.

Mutasyon Oranı

Yol bulmak amacıyla kullanılan genetik algoritmada bulunan mutasyonun haberleşmeye olan etkisinin incelenmesi amacıyla 1/100 ve 1/10000 oranları seçilmiştir.

Popülasyon Birey Sayısı

Genetik algoritmada yol bulmak amaçlı üretilen başlangıç popülasyonunun etkilerinin incelenmesi amacıyla 30, 60 ve 90 yol olarak belirlenmişlerdir.

Ortam Boyutu

5 km x 5 km, 10 km x 10 km, 15 km x 15 km, 20 km x 20 km ve 25 km x 25 km olmak üzere farklı büyüklükteki alanlara dağılmış düğümlerin haberleşme performansları incelenmiştir.

Düğüm Sayısı

Benzetim için 10, 20, 30 ve 40 düğümlü ağlar kullanılmıştır.

Baz İstasyonu Sayısı

Benzetimlerde kullanılan sabit ve hareket etmeyen baz istasyonu sayısı 3 olarak belirlenmiştir.

Düğümler Arasındaki Maksimum Bağlantı Sayısı

Düğümler arasındaki bağlantı full-duplex ve sayısı bir olarak alınmıştır.

Düğümler Arası Haberleşebilme Maksimum Mesafesi

İki düğümün birbiri ile atlamasız maksimum haberleşme menzili mobil 802.16 ağları için fizibıl olan 5 km alınmıştır [17].

Ham Fiziksel Bantgenişliği

IEEE 802.11 haberleşme standardında 5 km menzil için uygun bant genişliği olan 30 Mbyte/s alınmıştır [17].

Düğüm Kuyruk Uzunluğu

Düğümlerde bulunan paket kuyruğunun uzunluğu 1000 paket olarak belirlenmiştir.

Hareketsizlik Zamanı

0, 100, 200, 300, 400, 500 ve 600 saniye hareketsizlik zamanları kullanılmıştır. Hareketsizlik zamanı düğümlerin hareket etmeden sabit durdukları zamandır. 0 sn

durumunda düğümler rastgele belirlenmiş bir hız ve ivme ile sürekli hareket ederler. 100 sn durumunda, 100 sn bekledikten sonra belirlenen yeni bir noktaya belirli bir hız ve ivme ile gittikten sonra o noktada tekrar 100 sn beklediğini göstermektedir. Hareket etme ve bekleme simülasyon süresince devam etmektedir.

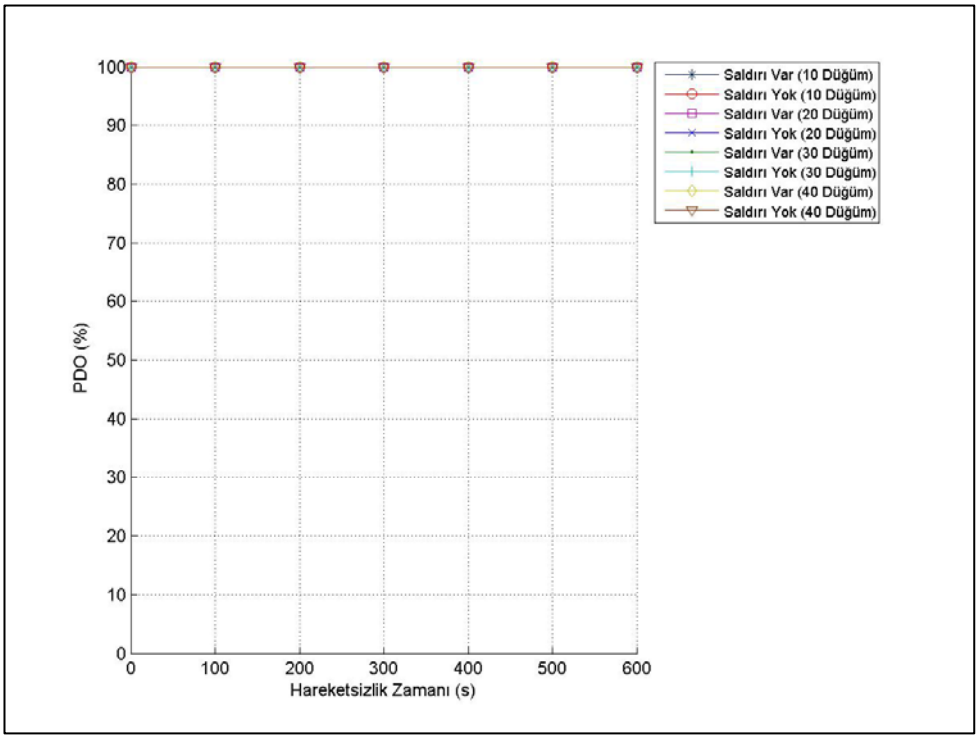
Benzetim Süresi

Benzetim modelleri 900 sn çalıştırılmaktadır.

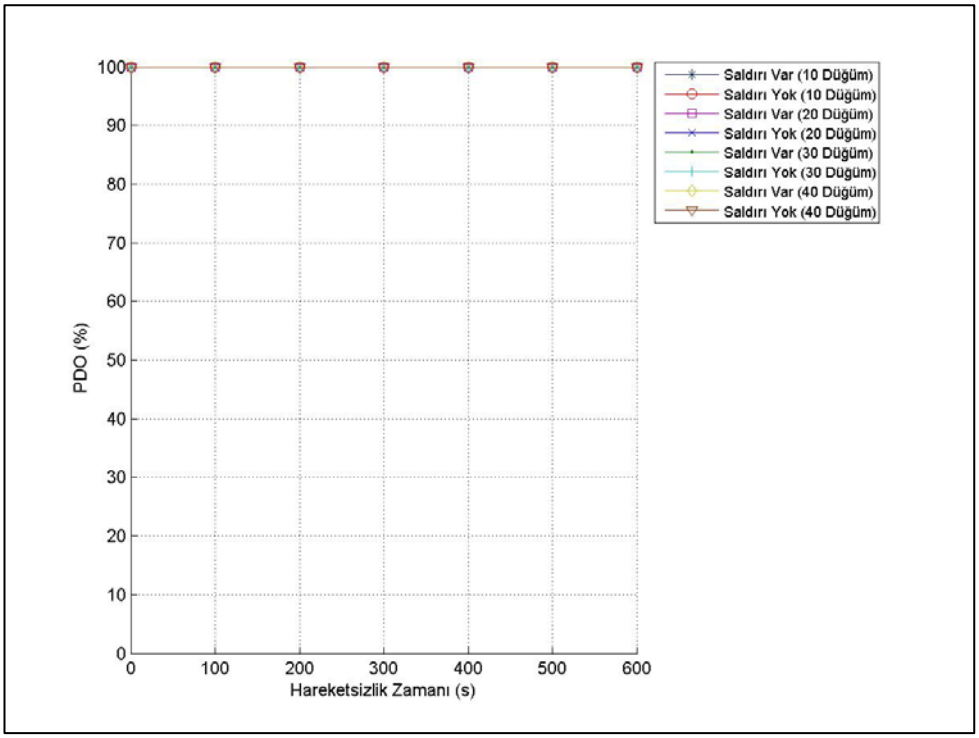
5.3.2. Ağa yapılan saldırıların haberleşmeye olan etkisi

Ağa yapılan saldırıların haberleşmeye etkisinin incelenmesinde düğümlerin paket dağıtım oranlarının, paket iletim kapasitelerinin ve normalize yönlendirme ek yüklerinin saldırılı ve saldırısız durumlar için, düğüm sayısına bağlı olarak düğüm hareketsizlik zamanı ile değişim grafiklerinden yararlanılmıştır. Düğümlerin yarısının diğer yarısına saldırı paketi gönderdiği senaryo "Saldırı Var" olarak kabul edilmiştir. Bu durumda kötücül düğüm sayısı %50'dir.

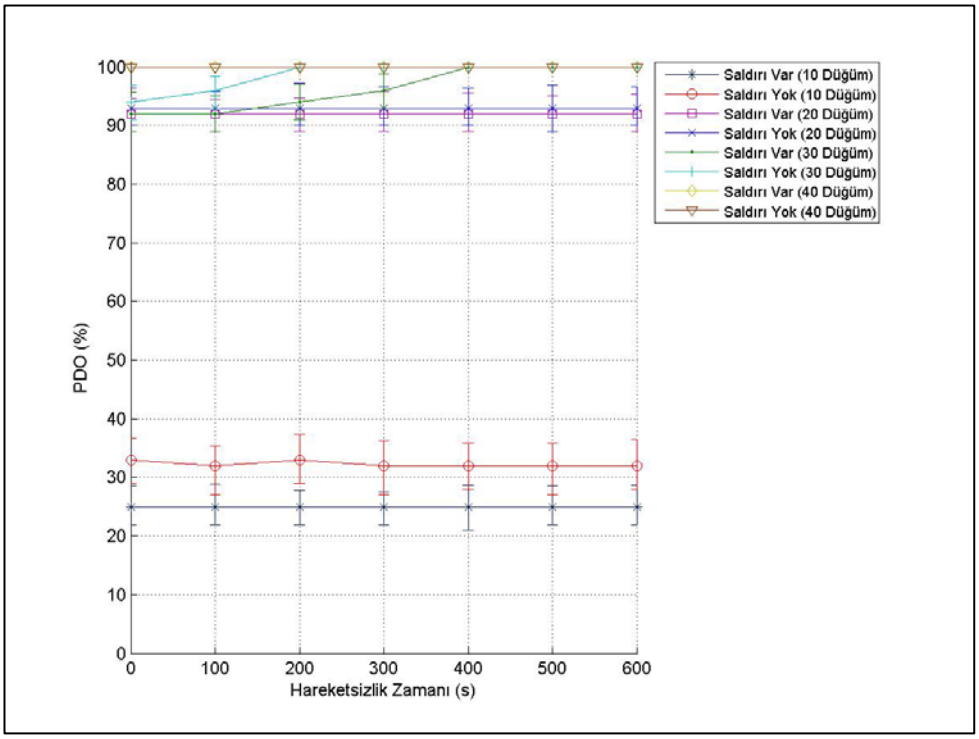
Paket dağıtım oranlarının alanlara göre dağılımları Şekil 5.20-5.24’ de gösterilmiştir.



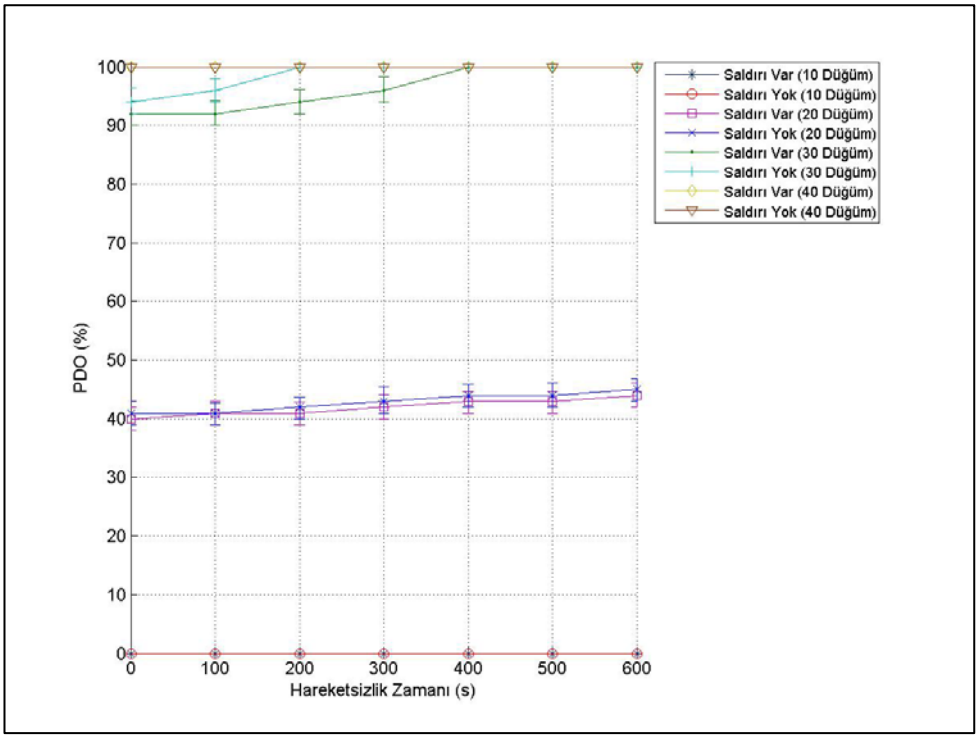
Şekil 5.20. 5 km x 5 km alana dağılmış düğümlerin paket dağıtım oranları



Şekil 5.21. 10 km x 10 km alana dağılmış düğümlerin paket dağıtım oranları



Şekil 5.22. 15 km x 15 km alana dağılmış düğümlerin paket dağıtım oranları

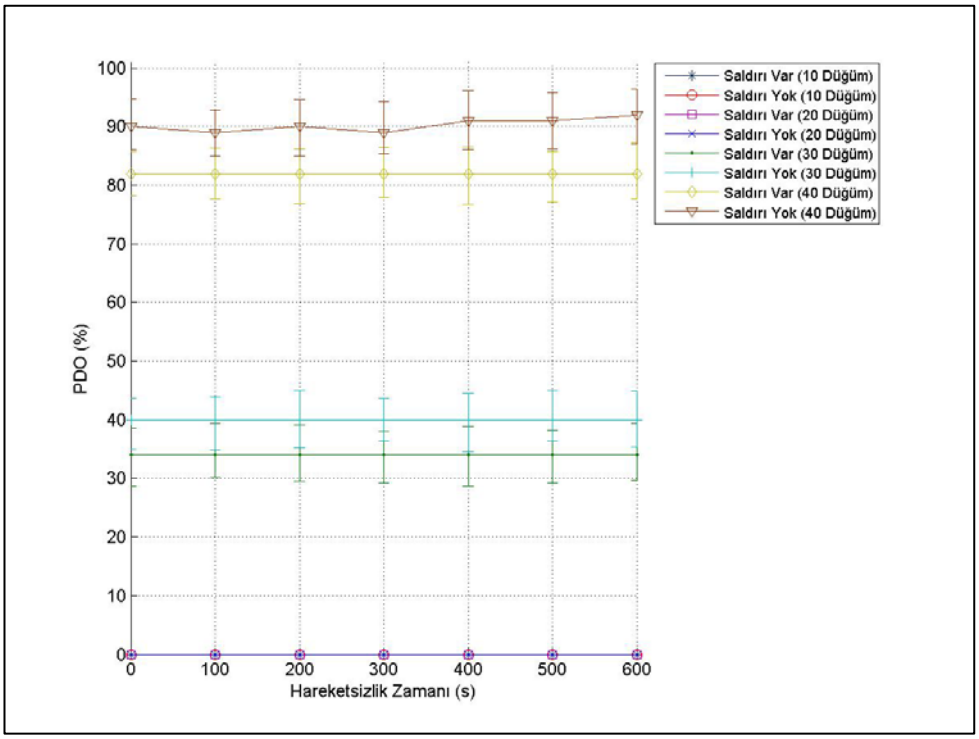


Şekil 5.23. 20 km x 20 km alana dağılmış düğümlerin paket dağıtım oranları

Çizelge 5.1'de örnek olarak 20 km x 20 km alana dağılmış düğümlerin paket dağıtım oranlarının ortalamaları alınmış sayısal değerleri gösterilmiştir.

Çizelge 5.1. 20 km x 20 km alana dağılmış düğümlerin paket dağıtım oranları (%)

Hareketsizlik Zamanı (s)	Saldırı Var (10 Düğüm)	Saldırı Yok (10 Düğüm)	Saldırı Var (20 Düğüm)	Saldırı Yok (20 Düğüm)	Saldırı Var (30 Düğüm)	Saldırı Yok (30 Düğüm)	Saldırı Var (40 Düğüm)	Saldırı Yok (40 Düğüm)
0	0	0	40	41	92	94	100	100
100	0	0	41	41	92	96	100	100
200	0	0	41	42	94	100	100	100
300	0	0	42	43	96	100	100	100
400	0	0	43	44	100	100	100	100
500	0	0	43	44	100	100	100	100
600	0	0	44	45	100	100	100	100



Şekil 5.24. 25 km x 25 km alana dağılmış düğümlerin paket dağıtım oranları

Çizelge 5.2'de örnek olarak 25 km x 25 km alana dağılmış düğümlerin paket dağıtım oranlarının ortalamaları alınmış sayısal değerleri gösterilmiştir.

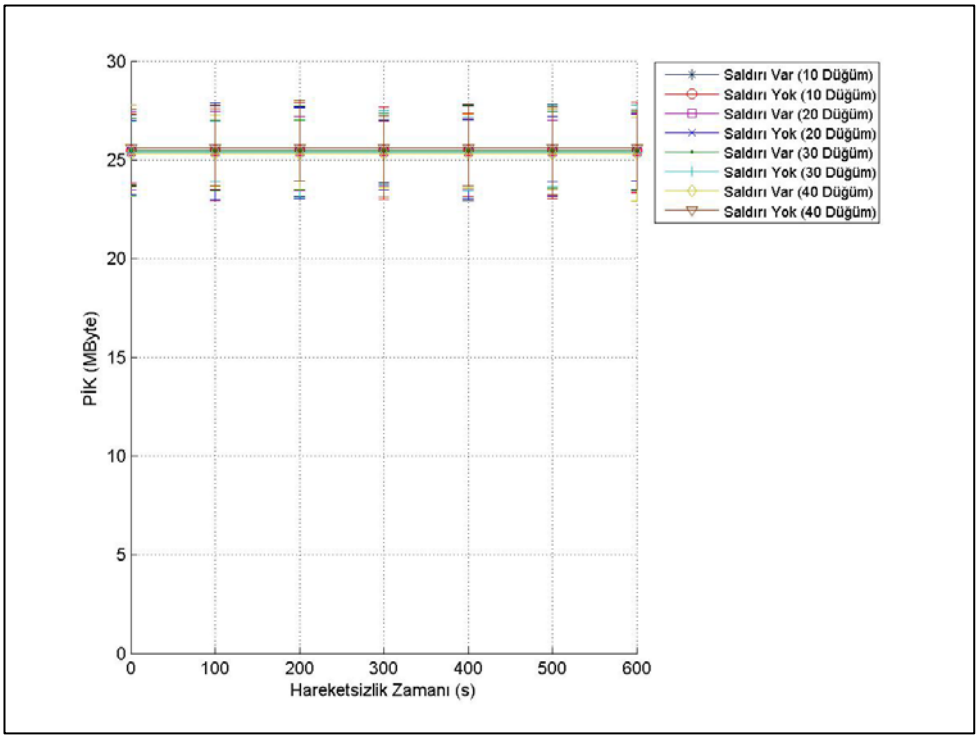
Çizelge 5.2. 25 km x 25 km alana dağılmış düğümlerin paket dağıtım oranları (%)

Hareketsizlik Zamanı (s)	Saldırı Var (10 Düğüm)	Saldırı Yok (10 Düğüm)	Saldırı Var (20 Düğüm)	Saldırı Yok (20 Düğüm)	Saldırı Var (30 Düğüm)	Saldırı Yok (30 Düğüm)	Saldırı Var (40 Düğüm)	Saldırı Yok (40 Düğüm)
0	0	0	0	0	34	40	82	90
100	0	0	0	0	34	40	82	89
200	0	0	0	0	34	40	82	90
300	0	0	0	0	34	40	82	89
400	0	0	0	0	34	40	82	91
500	0	0	0	0	34	40	82	91
600	0	0	0	0	34	40	82	92

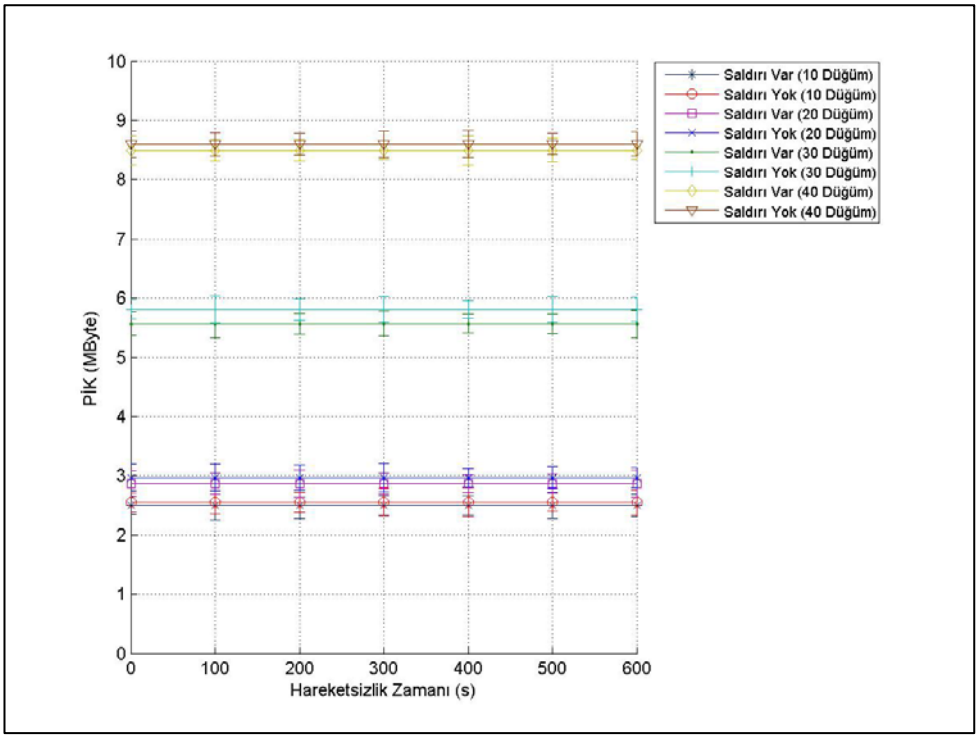
5 km x 5 km (Şekil 5.20) ve 10 km x 10 km (Şekil 5.21) büyüklüğündeki alanlarda düğümler birbirleri ile direk haberleşebilmekte ya da arada tek düğümün olması haberleşme için yeterli olmaktadır. Bu nedenle saldırı olsa bile haberleşme güvenli uygun yollar kullanılarak yapılabilmekte dolayısıyla gönderilen paketler hedefine ulaşabilmektedir (PDO= %100).

15 km x 15 km (Şekil 5.22) büyüklüğündeki alanda ise düğüm sayısına da bağlı olarak hiçbir düğüm ile haberleşemeyen veya çok az düğüm ile haberleşebilen elemanlar ortaya çıkmaktadır. Bu nedenle paket dağıtım oranları düşmektedir. 20 km x 20 km (Şekil 5.23) ve 25 km x 25 km (Şekil 5.24) büyüklüğündeki alanlarda bu durum daha bariz görünmekte hatta bazı düğüm sayılarında hiç haberleşme olmamaktadır. Hareketsizlik zamanının artması ise düğümün konumuna bağlı olarak paket dağıtım oranları üzerinde olumlu (haberleşemeyen düğümün başka bir düğüme yaklaşarak haberleşmeye başlaması ve o konumda uzun süre bekleyerek haberleşmeyi tamamlayabilmesi) ya da olumsuz (haberleşebilen bir düğümün diğer düğümlerden uzaklaşarak haberleşme yapamadığı bir konuma gelmesi ve o konumda uzun süre beklemesi) etki yapmaktadır. Bu nedenle ortalama alınmış olduğu halde PDO değerlerinde hareketsizlik zamanına bağlı olarak salınımlar görülmektedir.

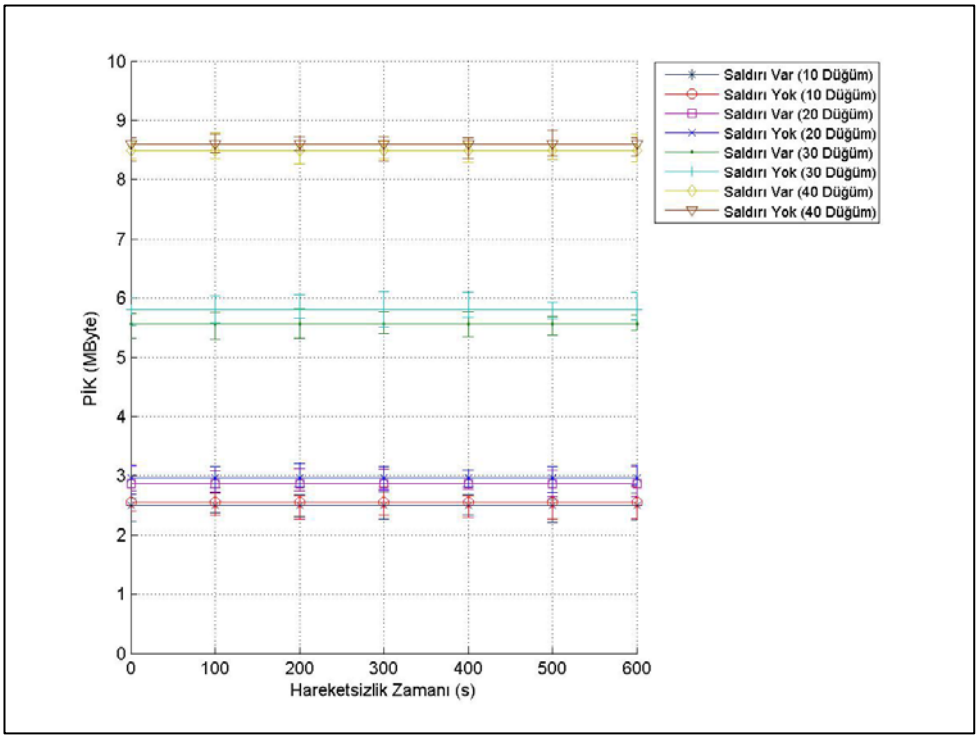
Paket iletim kapasitelerinin alanlara göre dağılımları Şekil 5.25-5.29'da gösterilmiştir.



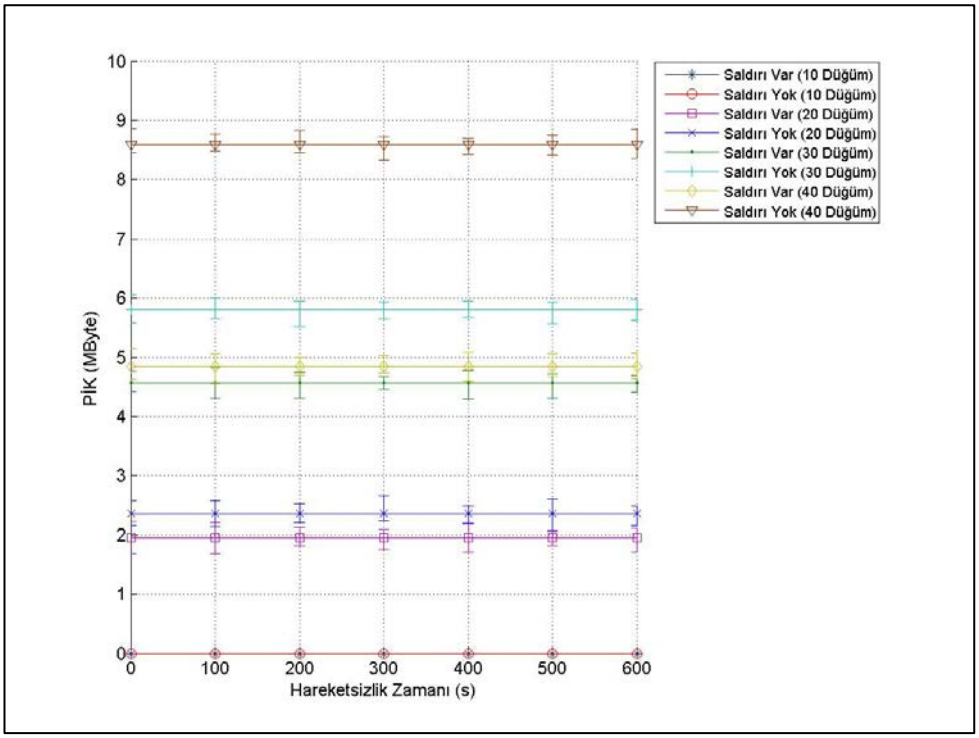
Şekil 5.25. 5 km x 5 km alana dağılmış düğümlerin paket iletim kapasitesi



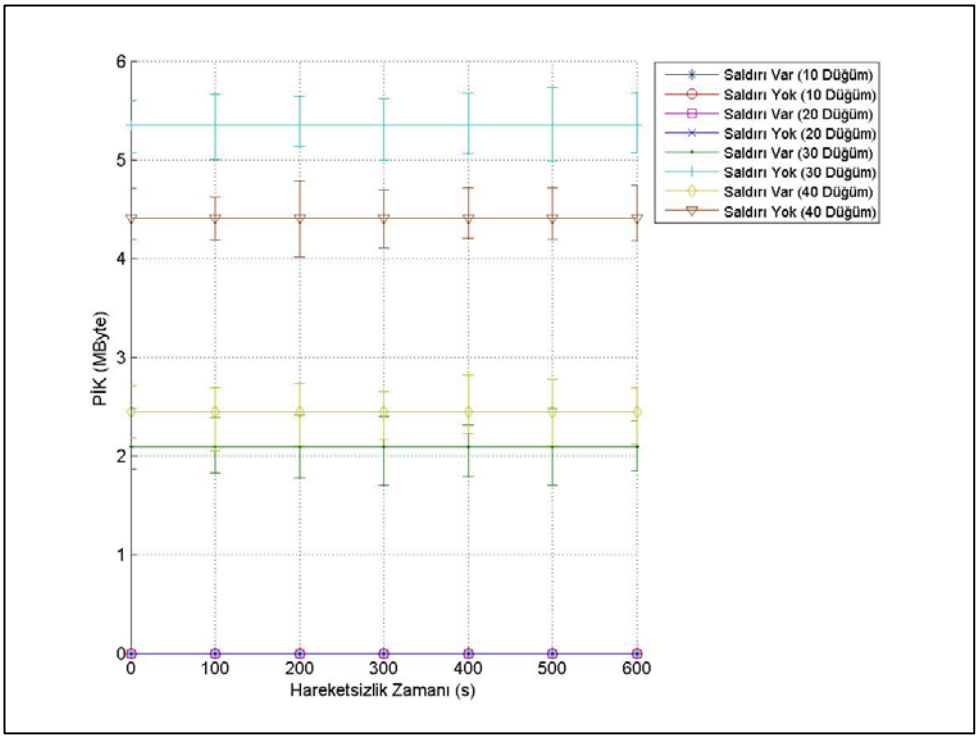
Şekil 5.26. 10 km x 10 km alana dağılmış düğümlerin paket iletim kapasitesi



Şekil 5.27. 15 km x 15 km alana dağılmış düğümlerin paket iletim kapasitesi



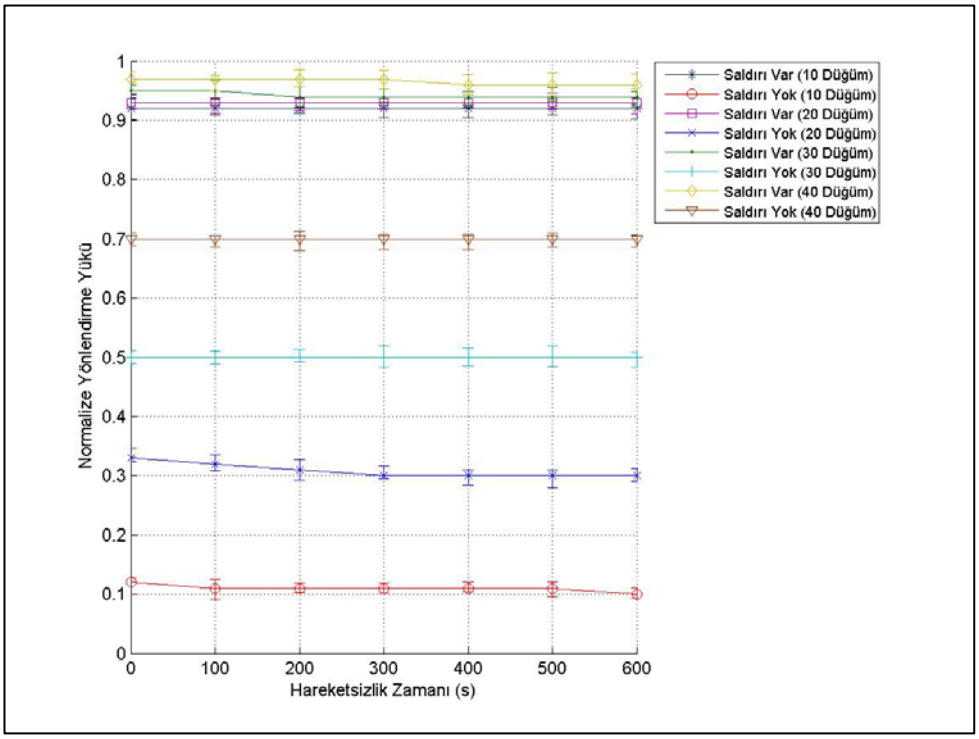
Şekil 5.28. 20 km x 20 km alana dağılmış düğümlerin paket iletim kapasitesi



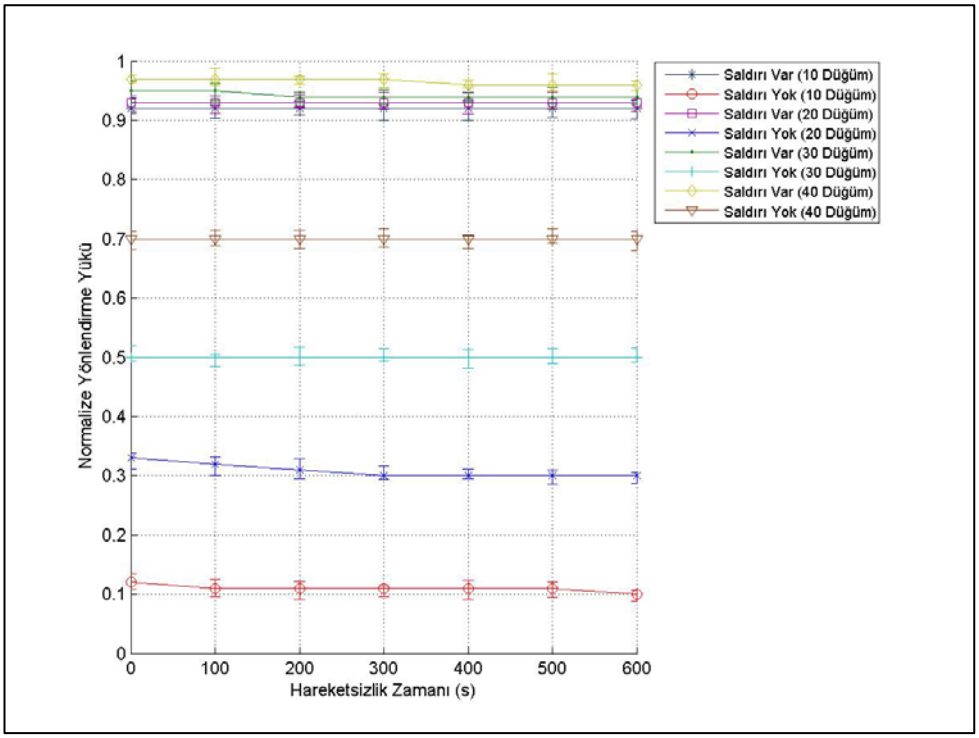
Şekil 5.29. 25 km x 25 km alana dağılmış düğümlerin paket iletim kapasitesi

5 km x 5 km (Şekil 5.25) büyüklüğündeki alanda düğümler birbirleri ile direk haberleşebilmekte, dolayısıyla da gönderilen paketler teorik hıza yakın bir hızda iletilmektedir. 10 km x 10 km (Şekil 5.26) ve daha büyük alanlarda ise paketler başka düğümler kullanılarak istenilen düğüme iletilmektedir. Burada oluşan paket kuyrukları ve yapılan yol hesaplamaları nedeniyle paket iletim kapasiteleri de düşmektedir. Alanın büyümesi ve düğüm sayısının azalması ile atlama sayısı artmakta ve paket iletim kapasitesi bundan olumsuz etkilenmektedir. Saldırı olduğunda ise bazı yollar da kullanılamadığı için atlama sayıları daha da artmaktadır. Bir başka deyişle saldırının olması durumu paket iletim kapasitelerini düşürmektedir. Hareketsizlik zamanının değişimi ise paket iletim kapasitesini etkilememektedir. Çünkü düğümlerin iletişim yarıçapları çok geniş olduğu için hareket etseler dahi komşuluk tablolarında çok hızlı bir değişim olmamaktadır.

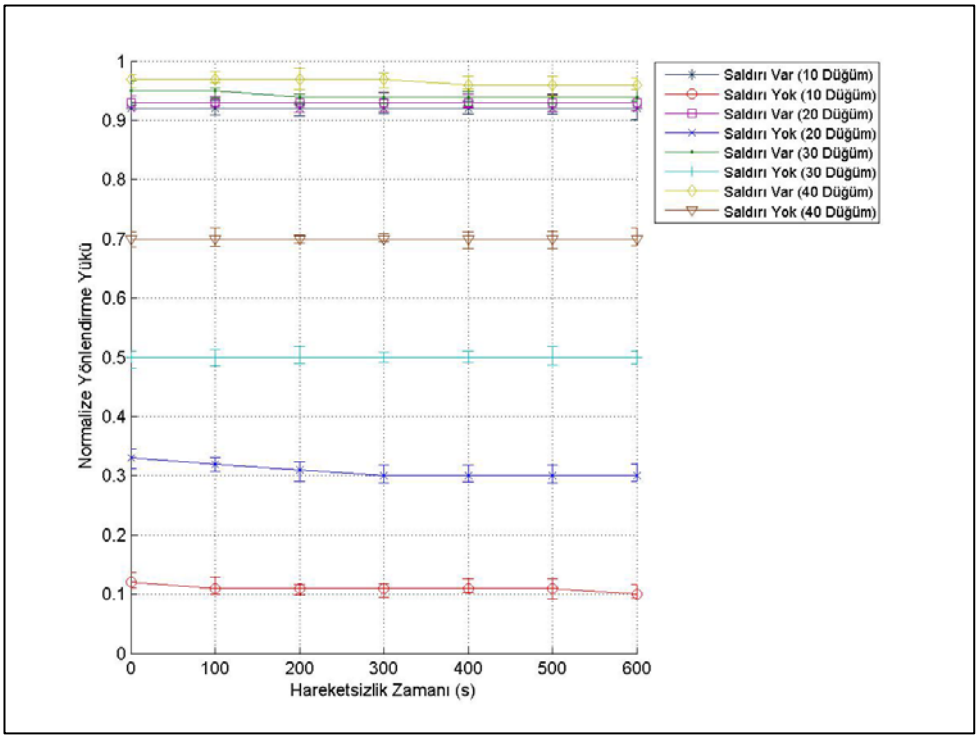
Normalize yönlendirme ek yükünün alanlara göre dağılımları Şekil 5.30-5.34'de gösterilmiştir.



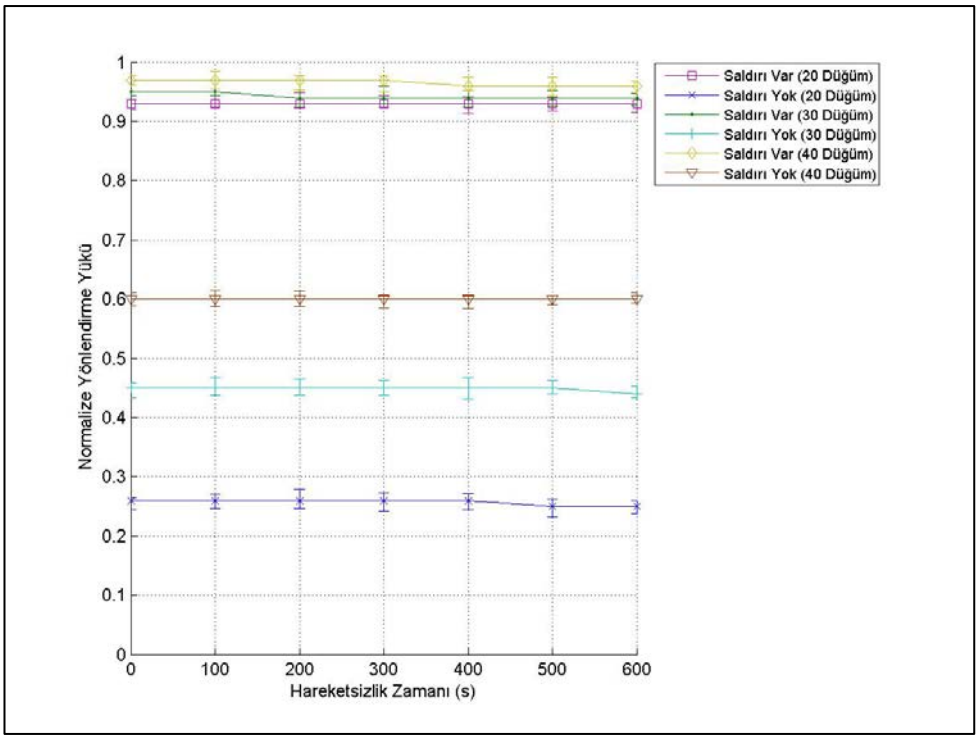
Şekil 5.30. 5 km x 5 km alana dağılmış düğümlerin normalize yönlendirme ek yükü



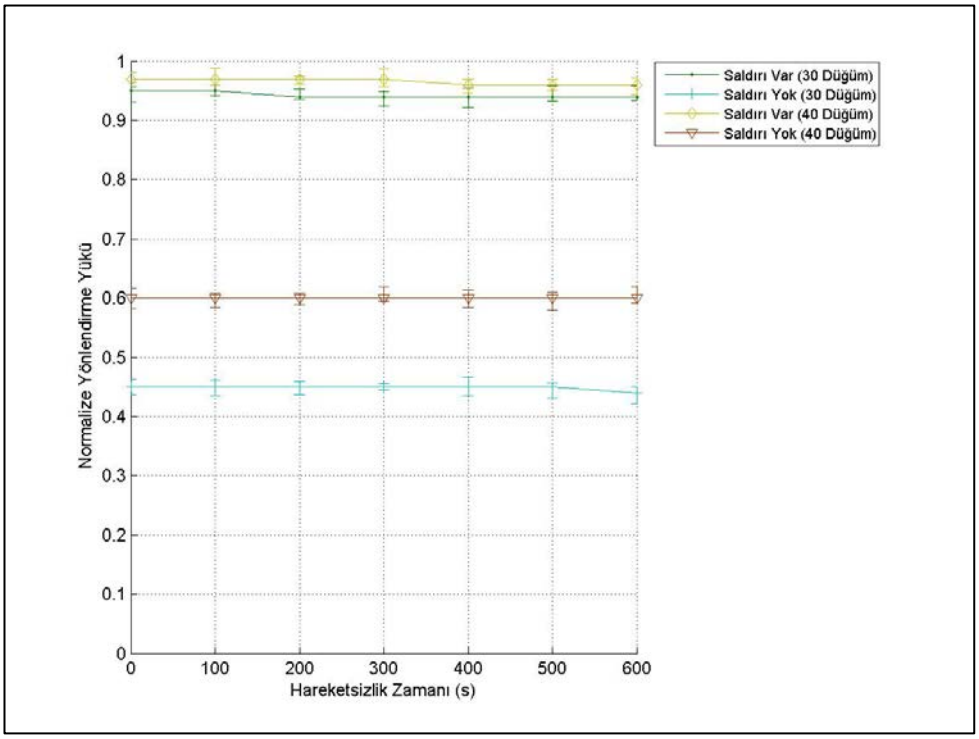
Şekil 5.31. 10 km x 10 km alana dağılmış düğümlerin normalize yönlendirme ek yükü



Şekil 5.32. 15 km x 15 km alana dağılmış düğümlerin normalize yönlendirme ek yükü



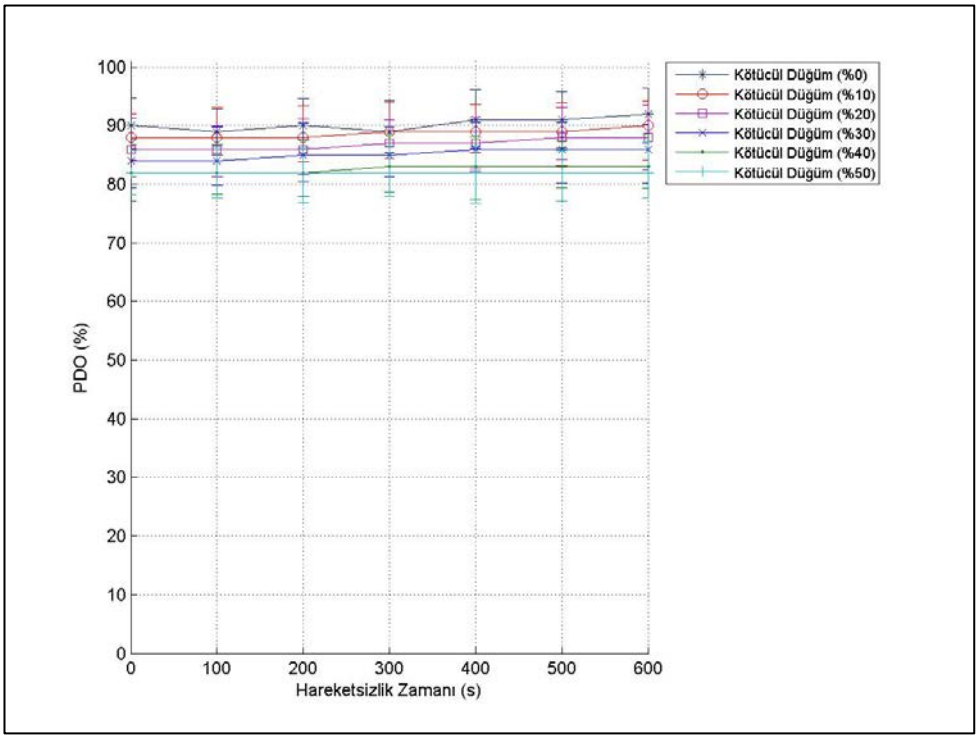
Şekil 5.33. 20 km x 20 km alana dağılmış düğümlerin normalize yönlendirme ek yükü



Şekil 5.34. 25 km x 25 km alana dağılmış düğümlerin normalize yönlendirme ek yükü

Normalize yönlendirme ek yükü, düğümlerin komşuluk ve güvenlik tablolarını hazırlayabilmek için gönderdikleri paketlerin toplam gönderilen pakete oranı olarak ifade edilmektedir. Küçük alanda az sayıda düğüm ile haberleşildiği saldırısız durumlarda, düğümler birbirlerinin durumları hakkında çok az bir haberleşme ile haberdar olmakta ve veri paketlerini gönderip alabilmektedir. Bu nedenle bu durumda NYY değeri en iyi olmaktadır. Alanın ve/veya düğüm sayısının artışı ile düğümlerin birbirleri hakkında bilgi almak için yaptıkları haberleşmeler artmakta dolayısıyla NYY değeri kötüleşmektedir (artmaktadır). Saldırının olduğu durumlarda ise sürekli olarak düğümlerin birbirleri ile olan bağlarının güvenlik seviyelerinin değişmesi nedeniyle haberleşmedeki güncelleme paketlerinin sayısı artmaktadır. Bu da NYY değerinin artarak kötüleşmesine neden olmaktadır.

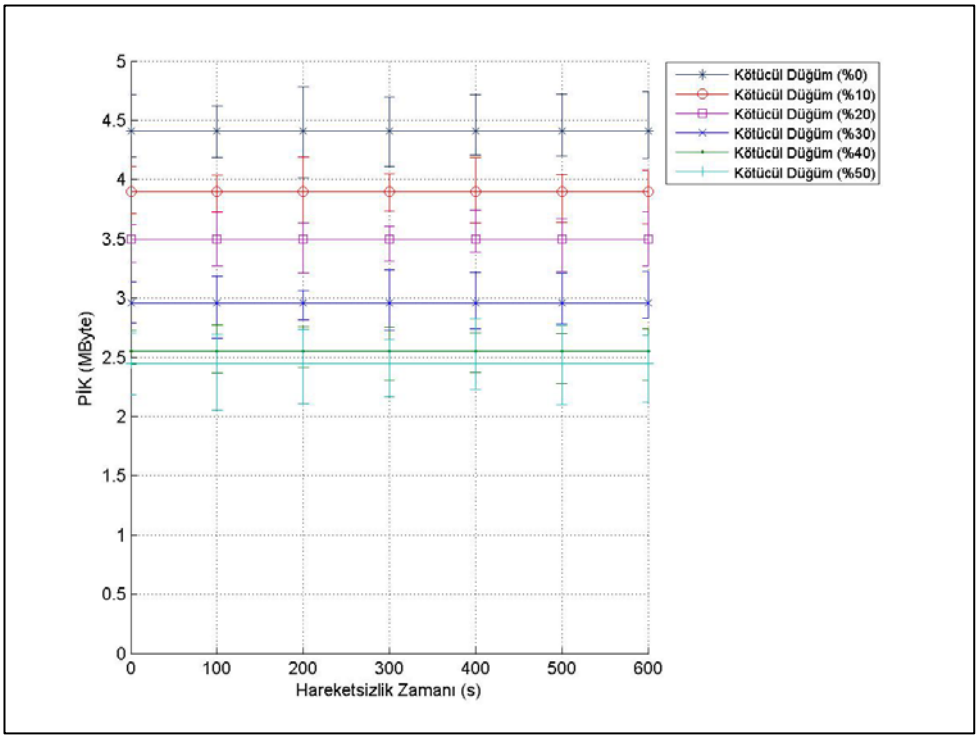
25 km x 25 km alana dağılmış 40 adet düğümün çeşitli saldırı senaryolarına göre paket dağıtım oranları Şekil 5.35'de verilmiştir.



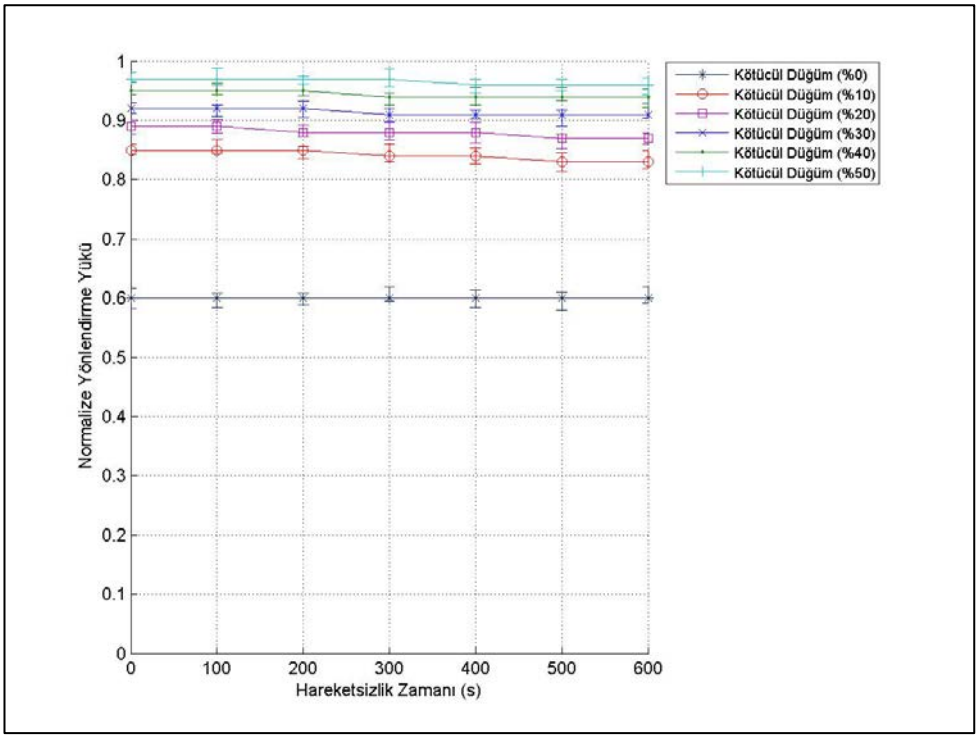
Şekil 5.35. 25 km x 25 km alana dağılmış düğümlerin paket dağıtım oranları

25 km x 25 km alana dağılmış 40 adet düğümün çeşitli saldırı senaryolarına göre paket iletim kapasiteleri Şekil 5.36'da verilmiştir.

25 km x 25 km alana dağılmış 40 adet düğümün çeşitli saldırı senaryolarına göre normalize yönlendirme ek yükleri Şekil 5.37'de verilmiştir.



Şekil 5.36. 25 km x 25 km alana dağılmış düğümlerin paket iletim kapasitesi



Şekil 5.37. 25 km x 25 km alana dağılmış düğümlerin normalize yönlendirme ek yükü

Şekil 5.35'de görüldüğü gibi ağdaki kötücül düğüm sayısı arttıkça paket dağıtım oranı düşmektedir. Fakat bu düşüş çok fazla değildir. Bu durum önerilen yönlendirme protokolünün görevini çok iyi yerine getirdiğini göstermektedir.

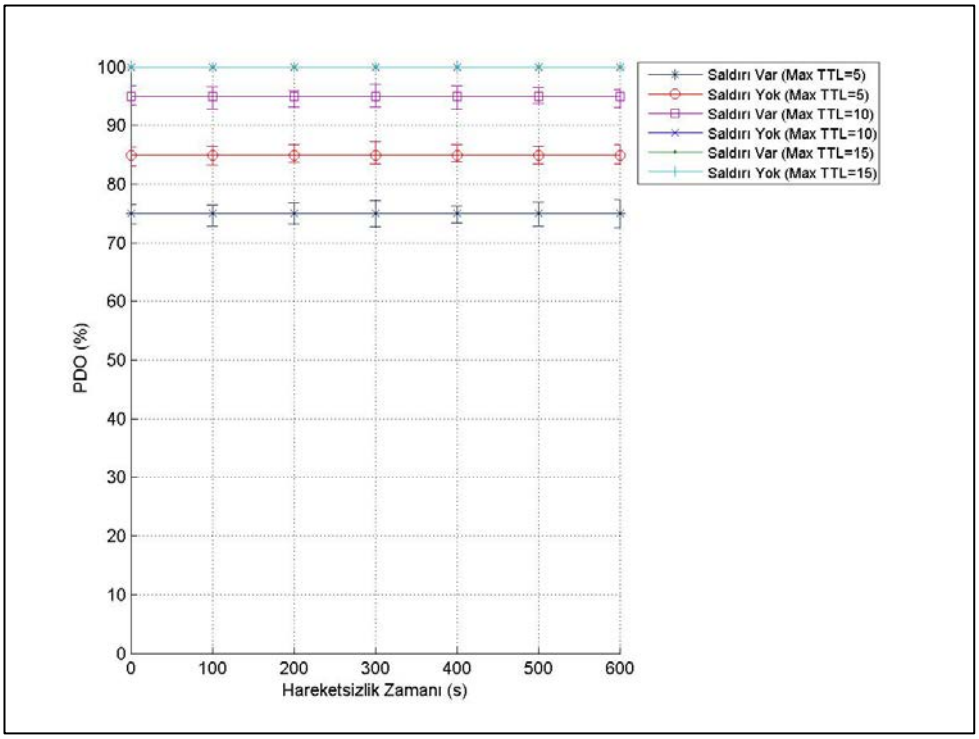
Ağdaki kötücül düğüm sayısı arttıkça, paket iletim kapasitesi Şekil 5.36'da görüldüğü gibi düşmektedir. Çünkü saldırı olmadığı durumlarda oluşan ideal güzergahlar yerine saldırılar nedeniyle yeni güvenli fakat uzun yollar tercih edilmektedir. Bu durum paket iletim kapasitesini düşürmektedir.

Saldırı olmadığı durumlarda normalize yönlendirme yükü 0,6 iken saldırı olduğunda bu değer kötücül düğüm sayısıyla yükselmektedir. Çünkü düğümler birbirlerinin yerlerinin tespitinin yanısıra değişen güvenlik değerlerini de paylaşmaya başlamışlardır.

5.3.3. Maksimum TTL değerinin haberleşmeye olan etkisi

Maksimum TTL (atlama sayısı) değişiminin haberleşmeye etkisinin incelenmesinde düğümlerin paket dağıtım oranlarının, paket iletim kapasitelerinin ve normalize yönlendirme ek yüklerinin saldırılı ve saldırısız durumlar için maksimum TTL sayısına bağlı olarak düğüm hareketsizlik zamanı ile değişim grafiklerinden yararlanılmıştır.

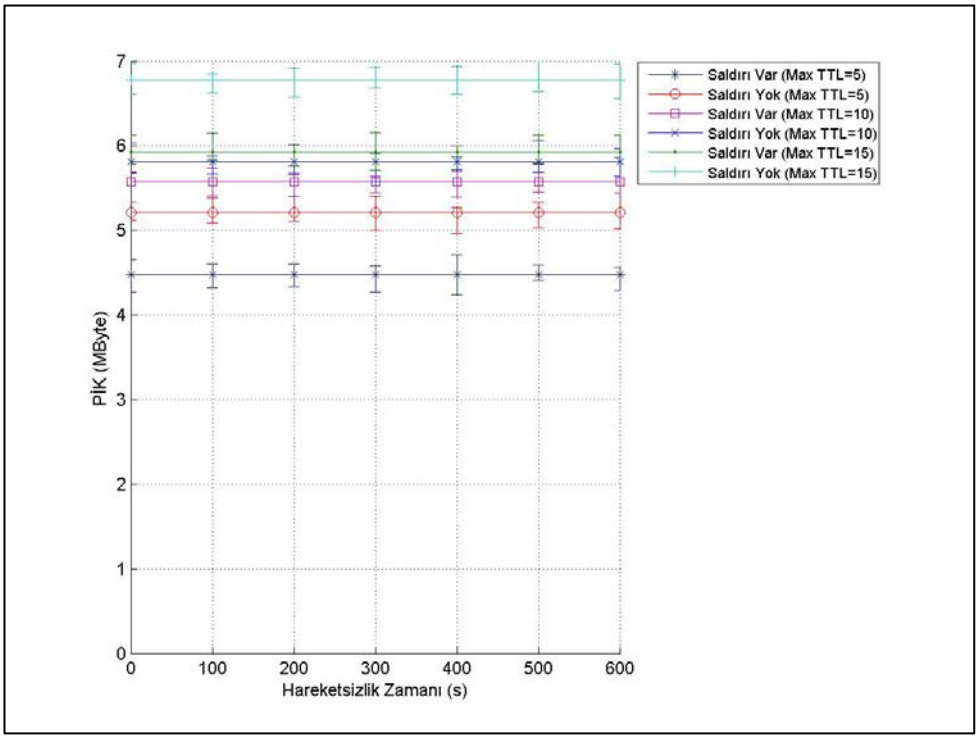
Paket dağıtım oranlarının maksimum TTL'e göre dağılımları Şekil 5.38'de gösterilmiştir.



Şekil 5.38. Maksimum TTL değerinin paket dağıtım oranına etkisi

Maksimum TTL değeri paketin atılmadan önce gidebileceği maksimum düğüm sayısını belirlemektedir. Küçük bir TTL değeri bazı durumlarda paketin ulaşabileceği düğüme erişimini engellemektedir. Bu durum PDO değerlerinin düşmesine neden olmaktadır. Aynı şekilde TTL değeri çok yüksek olursa hem hesaplama zamanı artacak hem de kaybolan paketler (gideceği düğüme artık ulaşamıyor ise) ağda gereksiz yere dolaşmaya devam edecekler ve ağı meşgul edeceklerdir. Şekil 5.38'de görüldüğü gibi maksimum TTL değeri artarken PDO oranı da artmaktadır. Fakat belli bir değerin üzerinde eğer her düğümün en az iki bağı varsa PDO değeri %100 olmaktadır. Bu değer grafikte 10 iken sağlanmaktadır. Bu nedenle 10 TTL değeri 40 elemanlı ağ için yeterli olmaktadır.

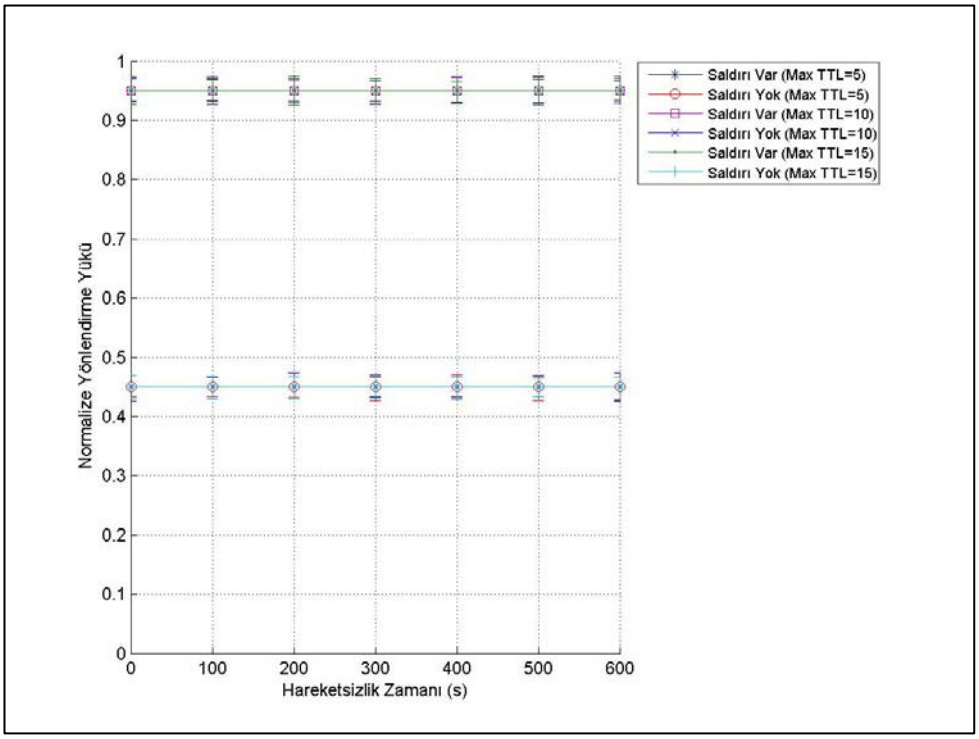
Paket iletim kapasitesinin maksimum TTL'e göre dağılımları Şekil 5.39'da gösterilmiştir.



Şekil 5.39. Maksimum TTL değerinin paket iletim kapasitesine etkisi

Başlangıç ve hedef düğümleri arasında rastgele yeni yollar hesaplanırken sınırlayıcı kısıt olarak Maksimum TTL ve nesil sayısı kullanılmaktadır: çünkü yol uzunluğu maksimum TTL değerinden daha uzun olamaz. Ayrıca maksimum TTL değeri çok düşük olduğunda birey sayısı kadar yol bulunamayabilir. Yeterli birey sayısı olmadığı durumlarda genetik algoritma bazen yanlış sonuçlar üretebilmektedir. Bu nedenle paket iletim kapasitesi maksimum TTL değeri ile artmaktadır. Max TTL değeri arttıkça, üretilebilecek maksimum güzergah sayısı da artmaktadır.

Normalize yönlendirme ek yükünün maksimum TTL'e göre dağılımları Şekil 5.40'da gösterilmiştir.



Şekil 5.40. Maksimum TTL değerinin normalize yönlendirme yüküne etkisi

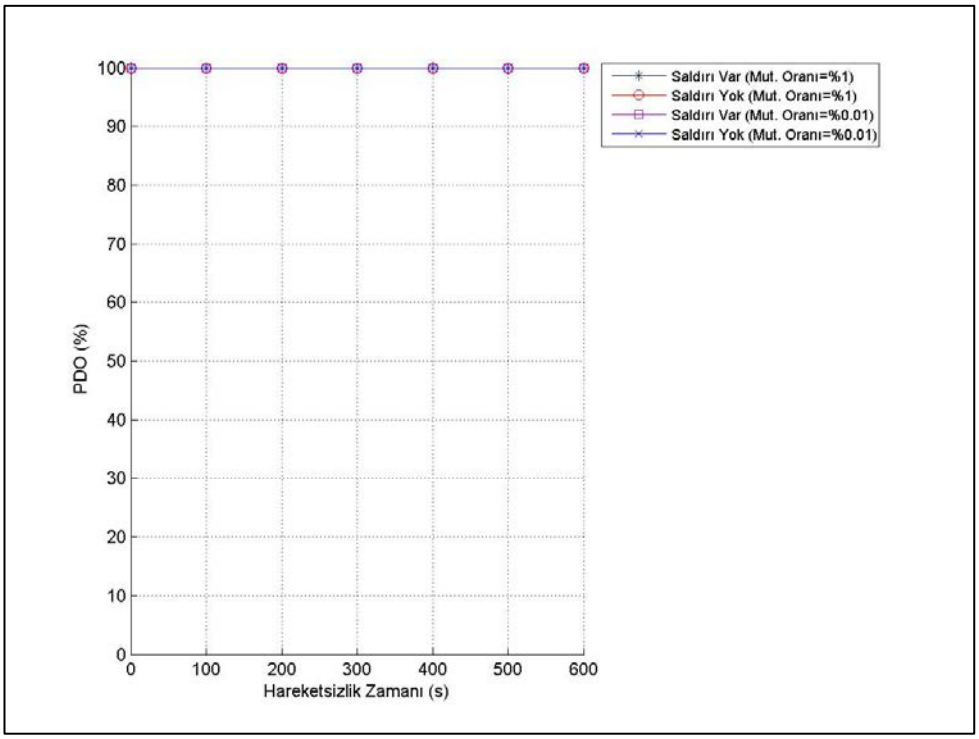
Küçük alanda az sayıda düğüm ile haberleşildiği saldırısız durumlarda, düğümler birbirlerinin durumları hakkında çok az bir paket alışverişi ile haberdar olmakta ve ardından veri paketlerini gönderip alabilmektedir. Bu nedenle bu durumda NYY değeri 0.44 gibi daha iyi bir değer olmaktadır. Alanın ve/veya düğüm sayısının artışı ile düğümlerin birbirleri hakkında bilgi almak için yaptıkları haberleşmeler artmakta dolayısıyla NYY değeri kötüleşmektedir (artmaktadır). Saldırının olduğu durumlarda ise sürekli olarak düğümlerin birbirleri ile olan bağlarının güvenlik seviyelerinin değişmesi nedeniyle haberleşmedeki güncelleme paketlerinin sayısı artmaktadır. Bu da NYY değerinin artarak daha da kötüleşmesine neden olmaktadır. Bu nedenle Maksimum TTL değerinin değişiminin NYY'e etkisi yok denecek kadar azdır.

5.3.4. Mutasyon oranının haberleşmeye olan etkisi

Mutasyon oranının değişiminin haberleşmeye etkisinin incelenmesinde düğümlerin paket dağıtım oranlarının, paket iletim kapasitelerinin ve normalize yönlendirme ek

yüklerinin saldırılı ve saldırısız durumlar için mutasyon oranına bağlı olarak düğüm hareketsizlik zamanı ile değişim grafiklerinden yararlanılmıştır.

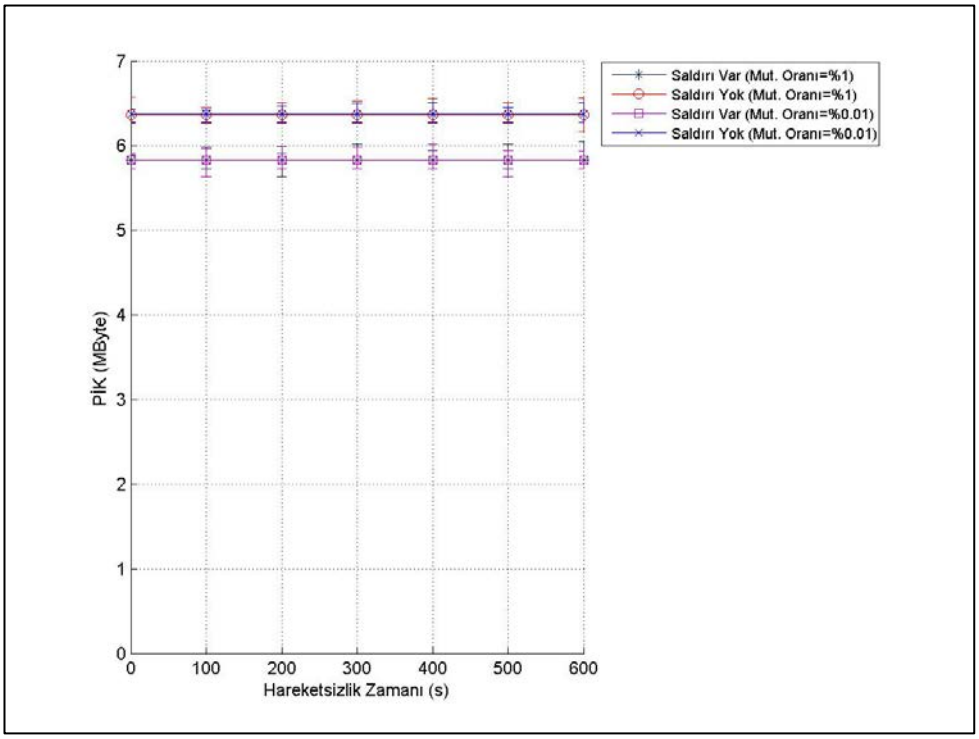
Paket dağıtım oranının mutasyon oranına göre dağılımları Şekil 5.41'de gösterilmiştir.



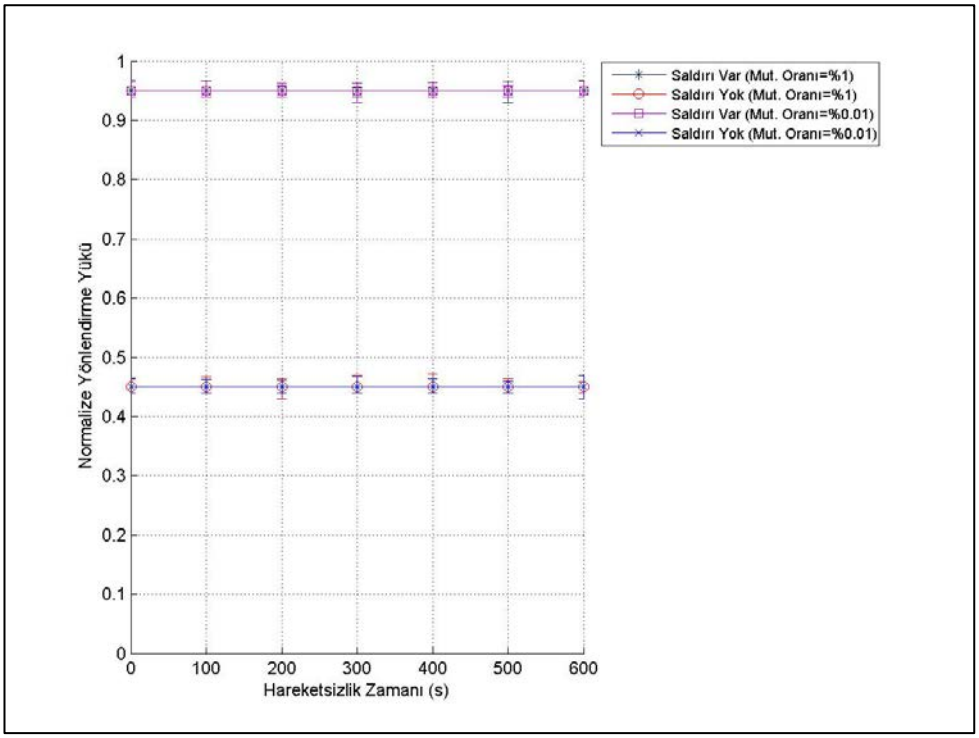
Şekil 5.41. Mutasyon oranının paket dağıtım oranına etkisi

Paket iletim kapasitesinin mutasyon oranına göre dağılımları Şekil 5.42'de gösterilmiştir.

Normalize yönlendirme ek yükünün mutasyon oranına göre dağılımları Şekil 5.43'de gösterilmiştir.



Şekil 5.42. Mutasyon oranının paket iletim kapasitesine etkisi



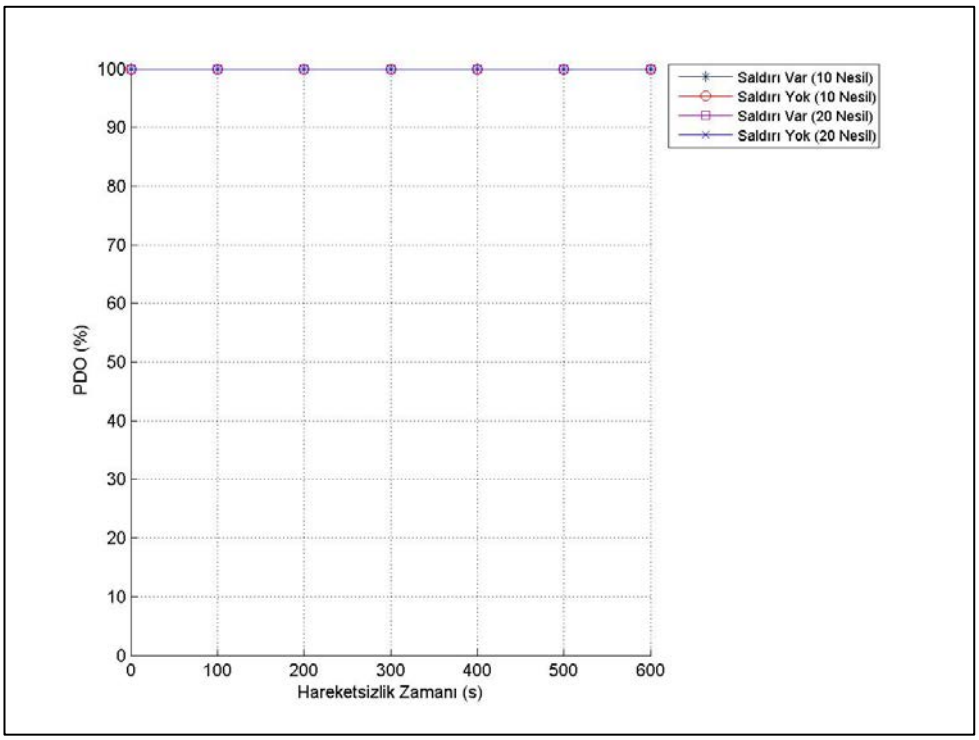
Şekil 5.43. Mutasyon oranının normalize yönlendirme yüküne etkisi

Mutasyon fonksiyonu genetik algoritmada yolların bulunması sırasında çözüm kümesini çeşitlendirmek için ek yeni yolların oluşturulması amacıyla kullanılmaktadır. Şekil 5.41-5.43'de mutasyon oranının değişiminin trafik değerlerini etkilemediği görülmektedir. Çünkü mutasyon ile güzergahı değişen paketlerin, tüm veri paketlerine oranı çok küçüktür.

5.3.5. Nesil sayısının haberleşmeye olan etkisi

Nesil sayısının değişiminin, haberleşmeye etkisinin incelenmesinde düğümlerin paket dağıtım oranlarının, paket iletim kapasitelerinin ve normalize yönlendirme ek yüklerinin saldırılı ve saldırısız durumlar için nesil sayısına bağlı olarak düğüm hareketsizlik zamanı ile değişim grafiklerinden yararlanılmıştır.

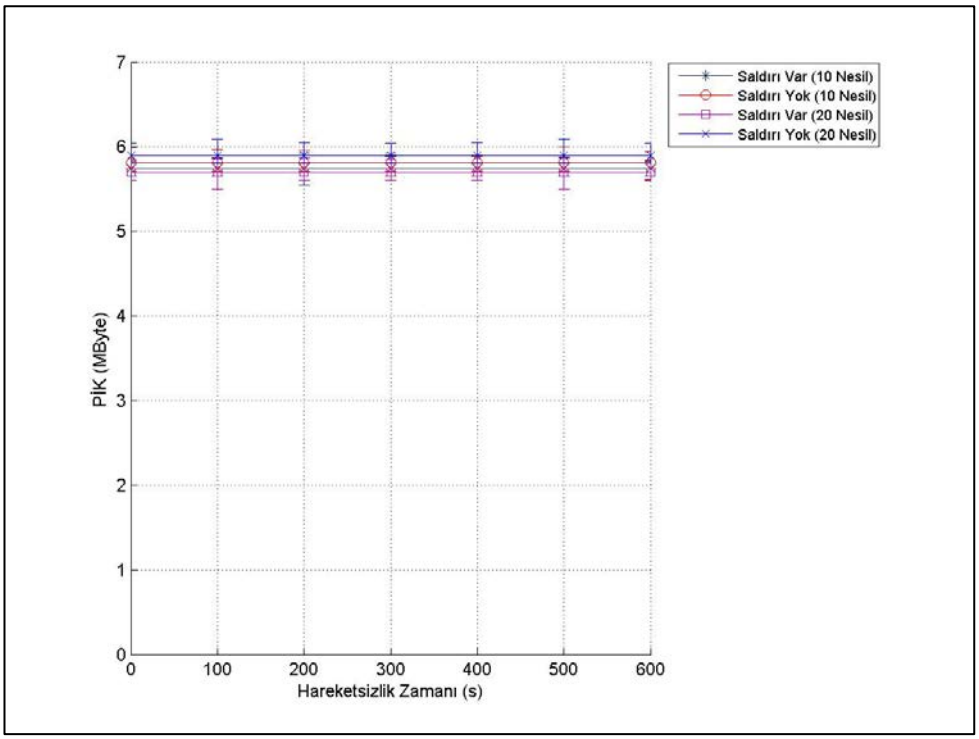
Paket dağıtım oranının nesil sayısına göre dağılımları Şekil 5.44'de gösterilmiştir.



Şekil 5.44. Nesil sayısının paket dağıtım oranına etkisi

Genetik algoritmada nesil sayısı sonuca daha yaklaşık bir değer bulunması amacıyla yükseltilmektedir. Çünkü çoğunlukla nesil sayısı arttıkça daha doğru sonuçlar elde edilmektedir. Amaç fonksiyonumuz iki düğüm arasında güvenli ve kısa bir yol bulunması olduğu için nesil sayısının PDO ile değişmediği görülmektedir. Çünkü tüm paketler her dört durumda da yerine ulaşabilmektedir.

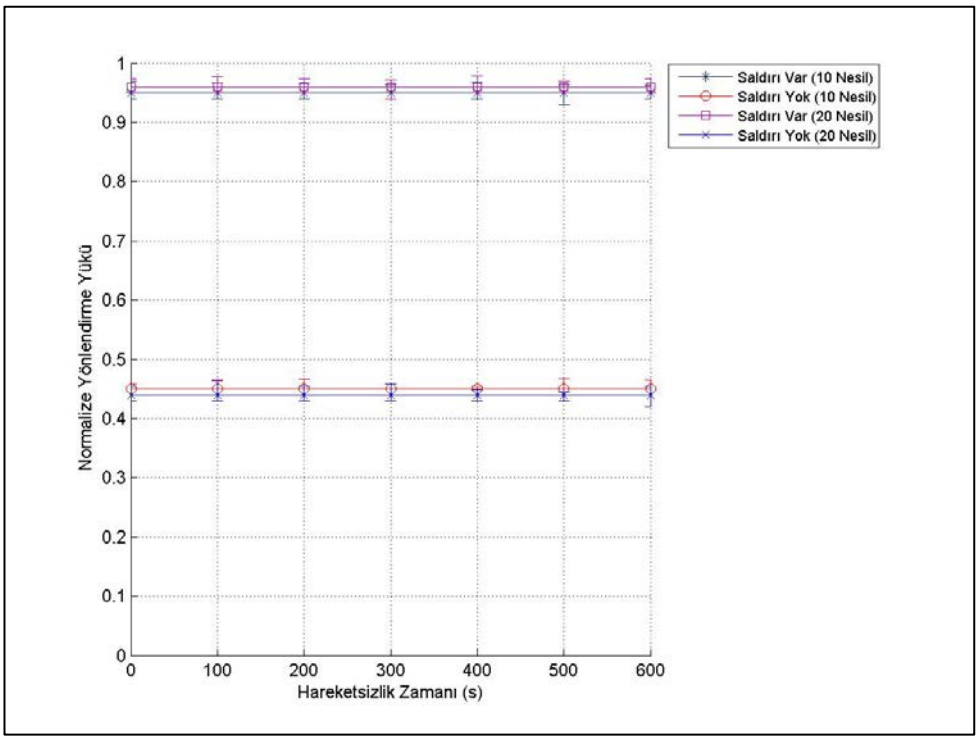
Paket iletim kapasitesinin nesil sayısına göre dağılımları Şekil 5.45'de gösterilmiştir.



Şekil 5.45. Nesil sayısının paket iletim kapasitesine etkisi

Nesil sayısının doğru çözüme ulaşıldıktan sonra devam etmesinin optimum çözüm olan sonucu etkilemeyeceği için nesil sayısının paket iletim kapasitesine etkisinin az olduğu Şekil 5.42'de görülmektedir. Çok az olan etkilenmenin nedeni ise nesil sayısının artmasından kaynaklanan yönlendirme sırasındaki hesaplamalardaki artışlardan kaynaklanmaktadır.

Normalize yönlendirme ek yükünün nesil sayısına göre dağılımları Şekil 5.46'da gösterilmiştir.



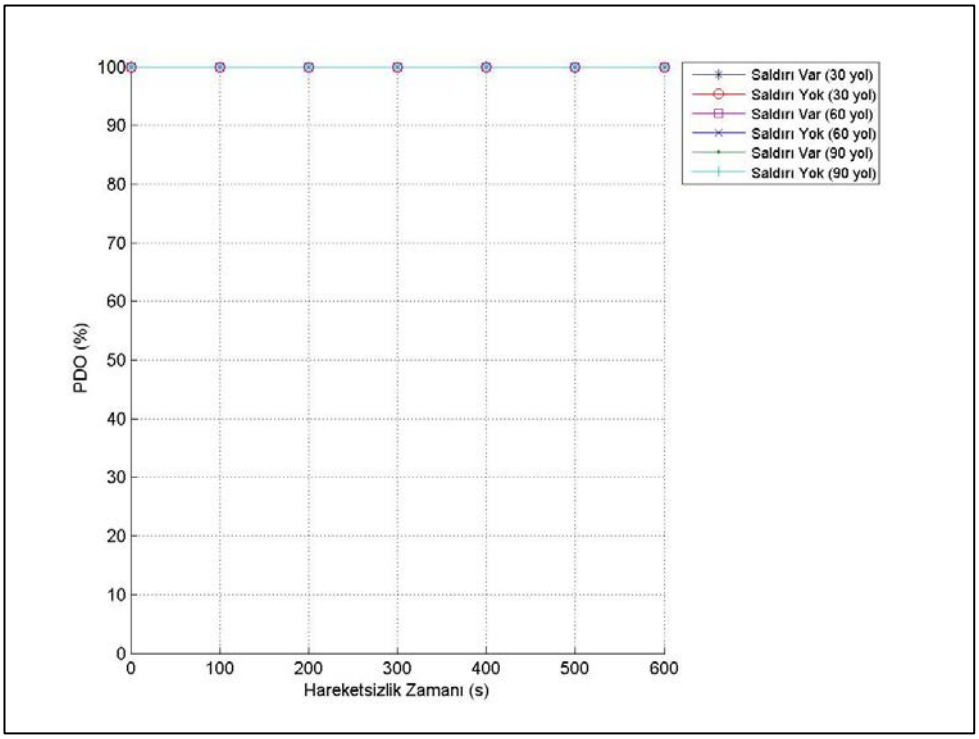
Şekil 5.46. Nesil sayısının normalize yönlendirme yüküne etkisi

Şekil 5.46'da nesil sayısının değişiminin normalize yönlendirme ek yükünü etkilemediği görülmektedir. Çünkü nesil sayısı paketlerin daha etkin güzergah bulmalarında etkili olur. NYY üzerinde etkisi yoktur.

5.3.6. Birey sayısının haberleşmeye olan etkisi

Birey sayısının değişiminin haberleşmeye etkisinin incelenmesinde düğümlerin paket dağıtım oranlarının, paket iletim kapasitelerinin ve normalize yönlendirme ek yüklerinin saldırılı ve saldırısız durumlar için birey sayısına bağlı olarak düğüm hareketsizlik zamanı ile değişim grafiklerinden yararlanılmıştır.

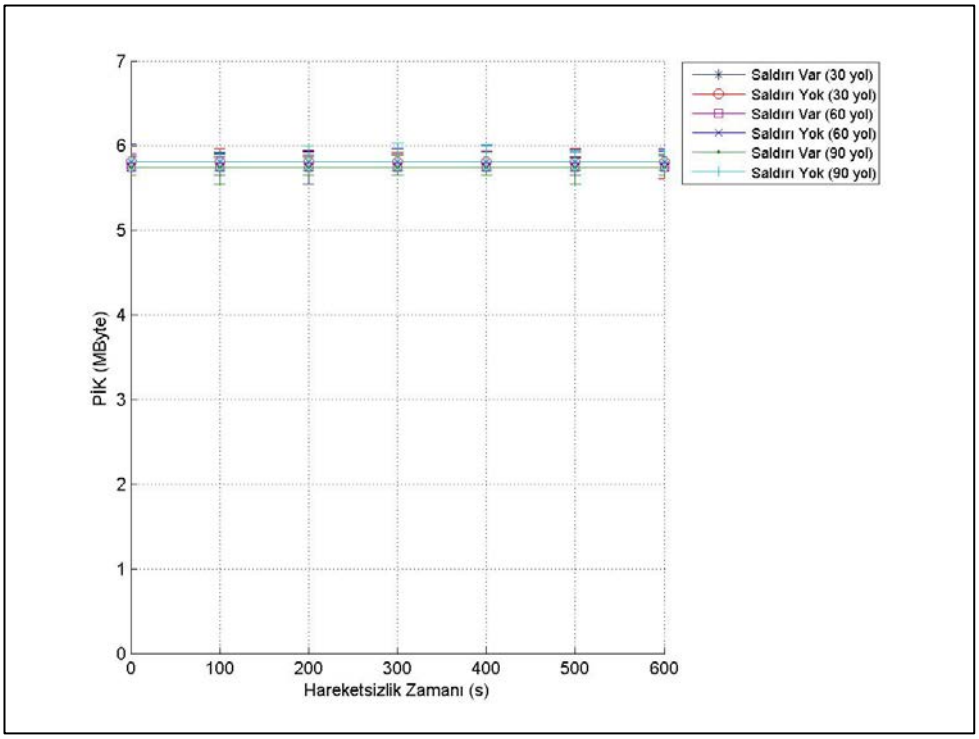
Paket dağıtım oranının birey sayısına göre dağılımları Şekil 5.47'de gösterilmiştir.



Şekil 5.47. Birey sayısının paket dağıtım oranına etkisi

Birey (rastgele yol) sayısının değişimi ile paket dağıtım oranı arasında bir ilişki görülmemiştir. Çünkü paketler varış düğümüne ulaşabilmek için en az bir güzergaha ihtiyaç duymaktadırlar. Bu sayının birden fazla olması paketlerin varış noktasına gidebilme yeteneklerini etkilememektedir.

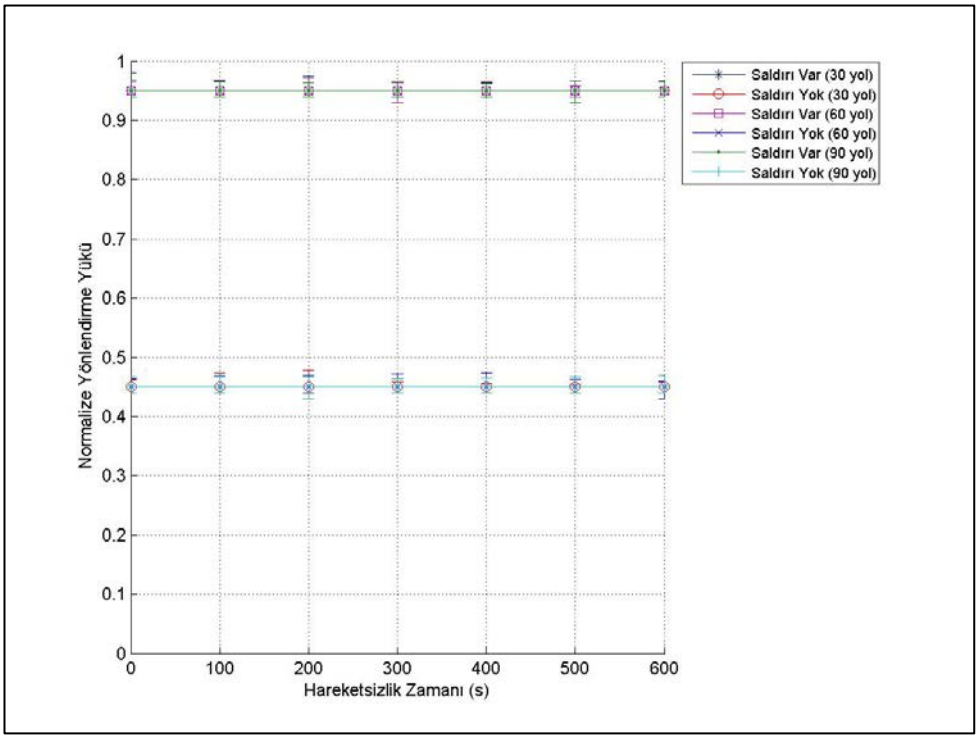
Paket iletim kapasitesinin birey sayısına göre dağılımları Şekil 5.48'de gösterilmiştir.



Şekil 5.48. Birey sayısının paket iletim kapasitesine etkisi

Başlangıç ve hedef düğümleri arasında rastgele yeni yollar hesaplanırken sınırlayıcı kısıt olarak Maksimum TTL ve birey sayısı kullanılmaktadır. Birey sayısının değişimi ile paket iletim kapasitesi arasında bir ilişki Şekil 5.48'de görüldüğü gibi bulunmamaktadır. Çünkü protokolde kullanılan rastgele güzergah bulma algoritmasında kısa güzergahların öncelikli olarak bulunma olasılığı daha yüksek olduğu için başlangıç güzergah sayısı paket iletim kapasitesini etkilememektedir.

Normalize yönlendirme ek yükünün birey sayısına göre dağılımları Şekil 5.49'da gösterilmiştir.



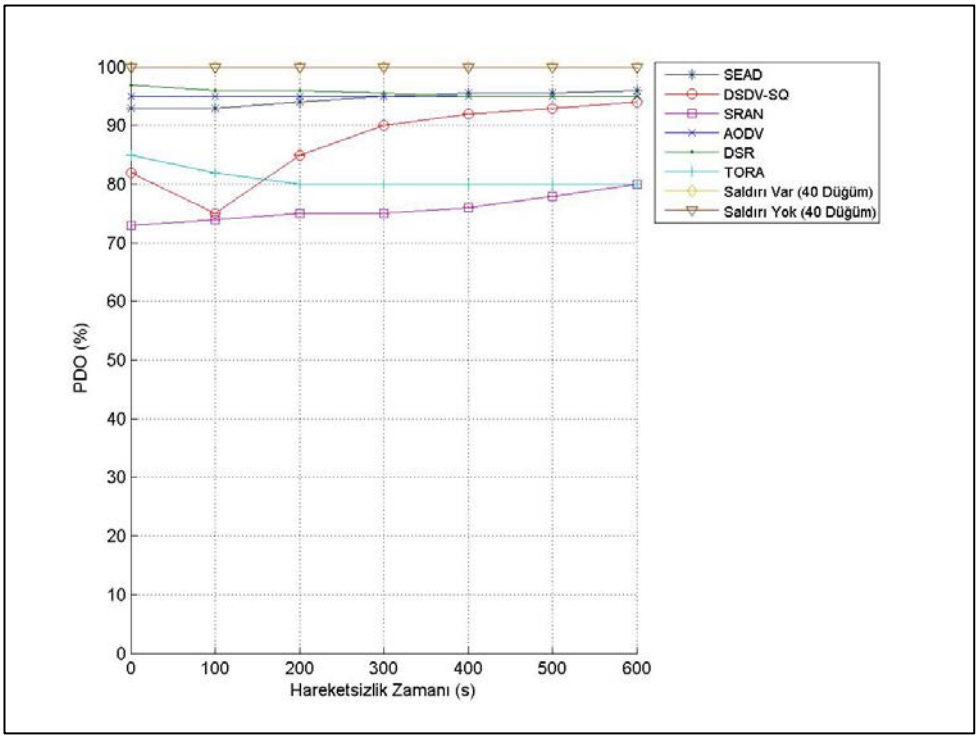
Şekil 5.49. Birey sayısının normalize yönlendirme yüküne etkisi

Birey sayısının değişimi normalize yönlendirme yüküne etki etmemektedir. Çünkü birey sayısı paketlerin daha etkin güzergah bulmalarında etkili olur. NYY üzerinde etkisi yoktur.

5.4. Protokolün Literatürde Bulunan Örnek Protokoller ile Karşılaştırılması

Geliştirilen protokol için Matlab benzetimi sonucunda elde edilen performans değerleri literatürde sıklıkla geçen bazı algoritmalarla karşılaştırılmıştır. DSR, DSDV, AODV, TORA ve SEAD yönlendirme protokollerinin performans verileri geliştirilmiş protokolün verileri ile karşılaştırılmıştır.

Şekil 5.50 ve Çizelge 5.3'de yönlendirme algoritmaları paket dağıtım oranları bakımından karşılaştırılmıştır.



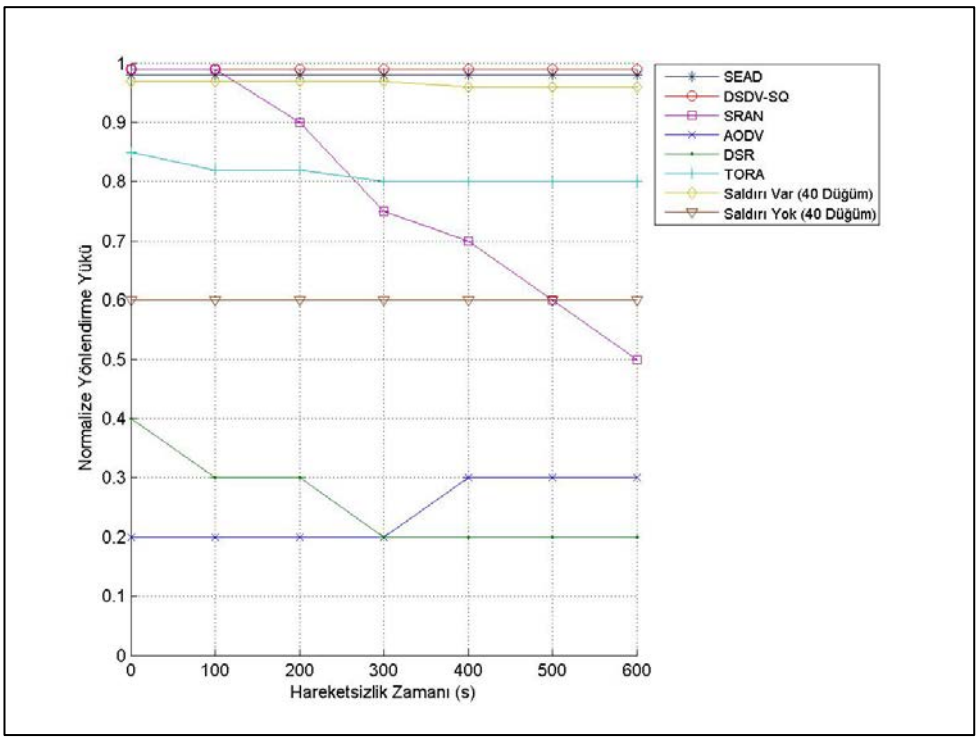
Şekil 5.50. Protokolün diğer protokollere göre paket dağıtım oranları

Çizelge 5.3. Protokolün diğer protokollere göre paket dağıtım oranları (%)

Hareketsizlik Zamanı (s)	SEAD	DSDV-SQ	SRAN	AODV	DSR	TORA	Saldırı Var (40 Düğüm)	Saldırı Yok (40 Düğüm)
0	93	82	73	95	97	85	100	100
100	93	75	74	95	96	82	100	100
200	94	85	75	95	96	80	100	100
300	95	90	75	95	95,5	80	100	100
400	95,5	92	76	95	95	80	100	100
500	95,5	93	78	95	95	80	100	100
600	96	94	80	95	95	80	100	100

Hazırlanan protokolün genişbant kablosuz mobil ağ olmasından ötürü bazı avantajları vardır. Bunlardan birisi menzili, bir diğeri de haberleşme bantgenişliğidir. Bu iki özelliği çok iyi kullanan protokol halihazırda literatürde bulunan diğer protokollere eşdeğer performans değerleri sunmuştur. Ayrıca diğer protokollere ek olarak paketlere istedikleri güvenlik seviyesinde güvenli optimum yol sunulmasını sağlamaktadır ve diğer protokollere göre paket dağıtım oranı %100'dür.

Şekil 5.51 ve Çizelge 5.4'de yönlendirme algoritmaları normalize yönlendirme ek yükleri bakımından karşılaştırılmışlardır.



Şekil 5.51. Protokolün diğer protokollere göre normalize yönlendirme yükü

Çizelge 5.4. Protokolün diğer protokollere göre normalize yönlendirme yükü

Hareketsizlik Zamanı (s)	SEAD	DSDV-SQ	SRAN	AODV	DSR	TORA	Saldırı Var (40 Düğüm)	Saldırı Yok (40 Düğüm)
0	0,98	0,99	0,99	0,2	0,4	0,85	0,97	0,6
100	0,98	0,99	0,99	0,2	0,3	0,82	0,97	0,6
200	0,98	0,99	0,9	0,2	0,3	0,82	0,97	0,6
300	0,98	0,99	0,75	0,2	0,2	0,8	0,97	0,6
400	0,98	0,99	0,7	0,3	0,2	0,8	0,96	0,6
500	0,98	0,99	0,6	0,3	0,2	0,8	0,96	0,6
600	0,98	0,99	0,5	0,3	0,2	0,8	0,96	0,6

Hazırlanan protokol saldırı durumunda, ağda diğer çoğu protokolden daha fazla yönlendirme yükü oluşturmaktadır. Güvenli yol hesabı için her düğümde bulunan güvenlik tablolarının güncellenmesi gerekmektedir. Normalize yönlendirme ek yükü

bakımından Şekil 5.48 incelendiğinde bu durum görülmektedir. Saldırının olmadığı durumlarda NYY değeri 0,6 gibi bir değerde iken saldırı durumunda güvenlik tablosu güncelleme paketleri nedeniyle 0,96 gibi bir değere yükselmektedir. Fakat yine de geliştirilen protokol SEAD, DSDV-SQ, SRAN ve TORA'dan daha iyi normalize yönlendirme yükü değerlerine sahiptir. Ayrıca sadece AODV ve DSR gibi güvenlik özelliği bulunmayan protokollerden daha kötü NYY değerleri bulunmaktadır.

Hazırlanan protokol 802.16 standardını kullandığı halde karşılaştırıldığı diğer protokoller 802.11 standardını kullanmaktadırlar. Bu nedenle protokoller paket iletim kapasiteleri bakımından aynı kategoride olmadıkları için karşılaştırılamamışlardır.

6. SONUÇLAR

Bu doktora tez çalışmasında kablosuz genişbant mobil ağlar için güvenlik bilinçli zeki yönlendirme protokolü tasarlanmış, benzetimi gerçekleştirilmiş ve parametreleri optimize edilmiştir. Ayrıca diğer güvenlik protokolleri ve benzetim araçları incelenmiştir.

Deterministik yöntemlerle yapılan yönlendirmenin hesaplanmasının büyük ağlar için çok zaman aldığı ve ağın dinamik yapısının sürekli değişmesi sebebiyle paketler ilerlerken hatalı ve güvensiz yönlendirmelerin olabileceği yapılan araştırmalarda görülmüştür.

Cravetz tarafından önerilen Security Aware Routing (SAR) protokolünde yer alan entegre güvenlik metriği kavramı ağ kurulurken oluşturulan ve sabit bir yapıdır. Ayrıca güvenlik ilişkisinin zamana bağlı olarak değişmediği kabul edilmiştir. Fakat bu ilişki gerçek hayatta zamana bağlı olarak değişebilir. Bu yapı sabit olduğu için SAR protokolünün zaman içinde değişen ağlarda verimi azalır. Çünkü ağdaki güvenlik ilişkisi zamanla değiştiği halde düğümler üzerine kayıtlı sabit güvenlik ilişkisi zamanla geçerliliğini yitirebilir. SAR protokolünde bulunan sabit güvenlik ilişkisi yapısının dinamik hale getirilmesi amaçlanan bu yönlendirme protokolünde, mevcut literatürde bulunan SAR yapısının bu iş için uygun olmadığı gözlemlenmiştir.

Zamana bağlı dinamik bir yönlendirme yapısının oluşması nedeniyle mevcut SAR protokolünün kullandığı AODV tabanlı yönlendirme yerine link state routing (LS) tabanlı bir yönlendirme algoritması tasarlanmıştır.

Hazırlanan bu algoritmada belirlenen bir güvenlik seviyesini karşılayan yol çözümü karşıladığı için, çözüme daha hızlı ulaşabilmek amacıyla genetik algoritma kullanılmıştır. Ayrıca genetik algoritmaya giriş olacak dinamik güvenlik seviyeleri

için bulanık mantık kümelerinde kullanılan dilsel ifadeler tercih edilmiştir. Böylece saldırılara karşı uyum sağlayarak adapte olabilen bir protokol elde edilmiştir.

Bu amaçla deterministik olmayan bir yöntem olan genetik algoritma incelenmiş ve dinamik yönlendirme için uygun olabileceğine karar verilmiştir. Ayrıca kablosuz ağların güvenliğini ön planda tutan bir yönlendirme yapılabilmesi amacıyla düğümler arasındaki yollar puanlandırılmıştır. Bu amaçla her düğüm iletim yaptığı yola, yolun kalitesi ve güvenliği için puan vermektedir. Bu puanlar her düğümde kendisini ilgilendiren yollar için olacağından güvenlik bilgisi dağıtık bir şekilde korunmaktadır. Puanlandırma saldırı tespit sistemi ve o sisteme bağlı bir bakseç tablosu yardımıyla yapılmaktadır. Elde edilen puanlamalar dilsel ifadeler yardımıyla genetik algoritmanın hesaplama performansını arttırması nedeniyle bulanık mantık yardımıyla hesaplanmaktadır.

Hazırlanan yönlendirme protokolünün çalışma performansının hesaplanması amacıyla Matlab ile ağ benzetim programı yazılmıştır. Yazılan bu benzetim programı ile protokolün parametreleri optimize edilmiş çeşitli koşullar, stres ve saldırılar altında verdiği tepkiler, benzetim ve analiz çalışmaları yapılarak incelenmiştir.

Bu tez çalışmasından elde edilen sonuçlar aşağıda maddeler halinde sunulmuştur. Bunlar;

- Yapılan benzetim çalışmaları ve parametre taramalarında seçilen başlangıç popülasyon sayısının, protokolün paketleri kaynaktan hedefe verimli ve istenilen güvenlik seviyesinde iletebilmesinde çok büyük etken olmadığı gözlemlenmiştir.

- Düğümlerin kuyruk uzunlukları ile ağın büyüklüğü ve kararlılık durumuna ulaşma zamanı arasında doğru orantı olduğu gözlemlenmiştir.

- Haberleşme ağ kararlılık durumuna ulaşmadan başlarsa, haberleşme paketlerinde de kayıplar oluşabileceği görülmüştür.

- Haberleşmede paket iletim oranı, ağda bulunan aynı güvenlik seviyesindeki bağların miktarı ile doğru orantılı olduğu gözlemlenmiştir.

- Ağa yapılan saldırılar, güvenlik seviyelerini etkilediğinden saldırının yoğunluğuna göre bağlar arasındaki güvenlik seviyeleri değişmekte, bu durum ise haberleşme hızını etkilemektedir.

- Nesil sayısının doğru çözüme ulaşıldıktan sonra devam etmesinin optimum çözüm olan sonucu etkilemeyeceği için nesil sayısının paket iletim kapasitesine etkisinin az olduğu gözlemlenmiştir.

- Paket iletim kapasitesi maksimum TTL değeri ile artmaktadır.

- Hareketsizlik zamanının değişimi paket iletim kapasitesini etkilememektedir.

- Mutasyon oranının değişimin trafik değerlerini etkilememektedir.

- İletilecek veri paketleri kötücül düğümler yerine güvenli düğümler üzerinden iletildiğinden geliştirilen protokol literatürde bulunan diğer protokollerden daha iyi paket dağıtım oranına sahiptir.

- Geliştirilen protokol güvenlik protokolleri arasında normalize yönlendirme yükü bakımından eşdeğer bir özellik sergilemektedir.

- Protokol hazırlanırken, hali hazırda açık kaynak kodlu IEEE 802.16 haberleşme standardını destekleyen ağ benzetim yazılımları bulunmadığı için protokol ile beraber ağ benzetim yazılımı da Matlab programlama dilinde yazılmıştır. Böylece gelecekte her türlü ağ benzetim çalışmalarında kullanılmak üzere genel bir altyapı oluşturulmuştur.

- Geliştirilen protokol ile, zamanla değişen, hareketli ve saldırılara açık olan bir ağda, bulanık mantık ve genetik algoritma kullanılarak, düğümlerin gönderdikleri paketlerin güvenliklerini ön planda tutup, adapte olarak iletebildikleri bir haberleşme ortamı elde edilmiştir.

- Genetik Algoritma ile yol bulunurken rastgele yol seçimi geniş ağlarda yüksek işlemci gücü gerektirdiği gözlemlenmiştir.

- Dilsel ifadeler için kullanılan fonksiyonlar değiştirilerek değişik güvenlik politikaları elde edilmektedir.

- Geliştirilen protokol, KDD99 veritabanında bulunan sınırlı sayıdaki ve bilinen saldırı türleri için yapılan saldırılarda başarılı olmuştur.

İlerde bu geliştirilen bu protokol dağıtık yapı yerine, merkezi tabanlı uygulanabilir. Ya da geniş ağlarda, ağ alt ağlara bölünebilir. Ayrıca uygulanan bulanık mantık fonksiyonları değiştirilerek değişik güvenlik türleri ve yaklaşımları tatbik edilebilir.

KAYNAKLAR

1. Murthy, C.S.R., Manoj, B.S., "Ad Hoc Wireless Networks: Architectures and Protocols", ***Prentice Hall PTR***, 1-880 (2004).

2. Canbek, G., Sağıroğlu, S., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", ***Politeknik Dergisi***, 9(3): 165-174 (2006).

3. Vural, Y., Sağıroğlu, Ş., "E-Devlet Güvenliği: Güncel Tehditler", ***17. İstatistik Araştırma Sempozyumu***, Ankara, 19-31 (2008).

4. Abramson, N., "Development of the Alohanet", ***IEEE Transactions on Information Theory***, 31(2): 119-123 (1985).

5. Crow, B.P., Widjaja, I., Kim, J.G., Sakai, P.T., "IEEE 802.11 wireless local area networks", ***IEEE Communications Magazine***, 35(9): 116-126 (1997).

6. Kuran, M.S., Tugcu, T., "A survey on emerging broadband wireless access technologies", ***Computer Networks***, 51(11): 3013-3046 (2007).

7. "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements", ***IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)***: C1-1184 (2007).

8. "IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications", ***IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)***: i-67 (2003).

9. "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements", ***IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition)***: 1-189 (2005).

10. "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6:

Medium Access Control (MAC) Security Enhancements", ***IEEE Std 802.11i-2004***: 1-175 (2004).

11. Cleary, K., "Internet via MMDS", ***International Broadcasting Convention***, 79-82 (1997).

12. Fong, B., Ansari, N., Fong, A.C.M., Hong, G.Y., "On the scalability of fixed broadband wireless access network deployment", ***Communications Magazine, IEEE***, 42(9): S12-S18 (2004).

13. "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", ***IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001)***: 1-857 (2004).

14. Cao, M., Ma, W.C., Zhang, Q., Wang, X.D., "Analysis of IEEE 802.16 mesh mode scheduler performance", ***IEEE Transactions on Wireless Communications***, 6(4): 1455-1464 (2007).

15. "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1", ***IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004)***: 1-822 (2006).

16. "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems- Amendment 1: Management Information Base", ***IEEE Std 802.16f-2005 (Amendment to IEEE Std 802.16-2004)***: 1-245 (2005).

17. "IEEE Standards for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 3: Management Plane Procedure and Services", ***IEEE Std 802.16g 2007 (Amendment to IEEE Std 802.16-2004)***: 1-202 (2007).

18. "IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Bridges Amendment 5: Bridging of IEEE 802.16", ***802.16k-2007 (Amendment to IEEE Std 802.1D-2004)***: 1-14 (2007).

19. Bolton, W., Yang, X., Guizani, M., "IEEE 802.20: mobile broadband wireless access", ***IEEE Wireless Communications***, 14(1): 84-95 (2007).

20. "IEEE Draft Standard for Local and Metropolitan Area Networks - Standard Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification", ***IEEE Unapproved Draft Std 802.20/D4.1m***: 1-104 (2008).

21. Cole, E., Krutz, R., Conley, J.W., "Network Security Bible", ***Wiley Pub.***, 849 (2005).

22. Li, H., Chen, Z., Qin, X., Li, C., Tan, H., "Secure routing in wired networks and wireless ad hoc networks", ***Technical Report***: 25-36 (2002).

23. Johnson, D.B., Maltz, D.A., "Dynamic Source Routing in Ad Hoc Wireless Networks", ***Mobile Computing***, 353: 153-181 (1996).

24. Hu, Y.-C., Johnson, D.B., Perrig, A., "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", ***Ad Hoc Networks***, 1(1): 175-192 (2003).

25. Charles, E.P., Pravin, B., "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers", ***SIGCOMM Comput. Commun. Rev.***, 24(4): 234-244 (1994).

26. Hu, Y.C., Perrig, A., Johnson, D.B., "Ariadne: A secure on-demand routing protocol for ad hoc networks", ***Wireless Networks***, 11(1-2): 21-38 (2005).

27. Perrig, A., Canetti, R., Tygar, D., Song, D., "The TESLA Broadcast Authentication Protocol", ***In CryptoBytes***, 5(2): 2-13 (2002).

28. Seung, Y., Prasad, N., Robin, K., "Security-aware ad hoc routing for wireless networks", ***Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking and computing***, Long Beach, CA, USA, 299-302 (2001).

29. Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing", ***Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on***, 90-100 (1999).

30. Papadimitratos, P., Haas, Z.J., "Secure routing for mobile ad hoc networks", ***SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)***, 01.27-31 (2002).

31. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M., "A secure routing protocol for ad hoc networks", ***Network Protocols, 2002. Proceedings. 10th IEEE International Conference on***, 78-87 (2002).

32. Nie, J., Wen, J., Luo, J., He, X., Zhou, Z., "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks", ***Fuzzy Sets and Systems***, 157(12): 1704-1712 (2006).

33. Buchegger, S., Le Boudec, J.Y., "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes—Fairness In Dynamic Ad-hoc NeTworks", ***Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing***, 226–236 (2002).

34. Sthultz, M., Uecker, J., Berghel, H., "Wireless insecurities", ***Advances in Computers***, 67: 225-251 (2006).

35. Hu, Y.C., Perrig, A., Johnson, D.B., "Rushing attacks and defense in wireless ad hoc network routing protocols", ***Proceedings of the 2nd ACM workshop on Wireless security***, 30-40 (2003).

36. Hu, Y.C., Perrig, A., Johnson, D.B., "Wormhole attacks in wireless networks", ***IEEE Journal on Selected Areas in Communications***, 24(2): 370-380 (2006).

37. Newsome, J., Shi, E., Song, D., Perrig, A., "The sybil attack in sensor networks: analysis & defenses", ***Proceedings of the 3rd international symposium on Information processing in sensor networks***, 259-268 (2004).

38. Zadeh, L.A., "Fuzzy sets", ***Information and Control***, 3(8): 338-353 (1975).

39. Mamdani, E., "Application of fuzzy logic to approximate reasoning using linguistic synthesis", ***IEEETransactions on Computers***: 1182-1191 (1977).

40. Takagi, T., Sugeno, M., "Fuzzy identification of systems and its applications to modeling and control", ***IEEE Transactions on Systems, Man, and Cybernetics***, 15: 116-132 (1985).

41. Tsukamoto, Y., "An approach to fuzzy reasoning method", ***Advances in fuzzy set theory and applications***: 137-149 (1979).

42. Zadeh, L., "Fuzzy logic and soft computing: Issues, contentions and perspectives", ***Third Int. Conf. on Fuzzy Logic***, Lizuka, Japan, 1-2 (1994).

43. Klir, G., Folger, T., Kruse, R., "Fuzzy sets, uncertainty, and information", ***Prentice Hall Englewood Cliffs***, 1-347 (1988).

44. Akcayol, M.A., "Bir Anahtarlamalı Reklüktans Motorun Sinirsel-Bulanık Denetimi", Doktora Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 204 (2001).

45. Yager, R., "A note on probabilities of fuzzy events", ***Information Sciences***, 18(2): 113-129 (1979).

46. Zimmermann, H., "Fuzzy set theory--and its applications", ***Springer Netherlands***, 1-507 (2001).

47. Nauck, U., Kruse, R., "Design and implementation of a neuro-fuzzy data analysis tool in Java", ***Manual. Technical University of Braunschweig. Germany***: 8-112 (1999).

48. Deperlioğlu, Ö., "Bir anahtarlama kipli konvertörün sinirsel-bulanık denetimi", Doktora Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 1-186 (2001).

49. Gen, M., Cheng, R., "Genetic Algorithms and Engineering Design", ***Wiley-Interscience***, 1-380 (1997).

50. Altıparmak, F., "Genetik algoritmalar ile haberleşme şebekelerinin topolojik optimizasyonu", Doktora Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 39-46 (1996).

51. Holland, J.H., "Adaptation in natural and artificial systems", ***University of Michigan Press Ann Arbor***, 280 (1975).

52. Goldberg, D.E., "Genetic Algorithms in Search, Optimization and Machine Learning", ***Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA***, 403 (1989).

53. Davis, L., "Handbook of genetic algorithms", ***Van Nostrand Reinhold***. New York, 320 (1991).

54. Michalewicz, Z., "Genetic Algorithms+ Data Structures= Evolution Programs", ***Springer***, 383 (1996).

55. Darwen, P., Yao, X., "A dilemma for fitness sharing with a scaling function", ***IEEE International Conference on Evolutionary Computation***, 166 (1995).

56. Güven, E.N., "Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi", Yüksek Lisans, ***Gazi Üniversitesi***, Ankara, 128 (2007).

57. Barnard, R., "Intrusion detection systems", ***Gulf Professional Publishing***, 454 (1988).

58. Bace, R., "Intrusion detection systems", ***US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology***, 322 (2001).

59. Liang, B., Jian, K., Kuo, Z., Fan-er, M., "Intrusion detection systems", ***Journal of Changchun Post and Telecommunication Institute***: 75-112 (2002).

60. Ünal, M., Akcayol, M.A., "Kablosuz Ağlarda Güvenli Yönlendirme Protokolleri", ***Bilişim Teknolojileri Dergisi***, 1(3): 7-13 (2008).

61. Davies, C., Lingras, P., "Genetic algorithms for rerouting shortest paths in dynamic and stochastic networks", ***European Journal of Operational Research***, 144(1): 27-38 (2003).

62. Şimşek, M., Akcayol, M.A., "A Heuristic Routing Protocol and Congestion Control at Wireless Networks", ***Journal of the Faculty of Engineering and Architecture of Gazi University***, 23(1): 57-63 (2008).

63. Dijkstra, E.W., "A note on two problems in connexion with graphs", ***Numerische Mathematik***, 1(1): 269-271 (1959).

64. Doğru, İ.A., Şimşek, M., Akcayol, M.A., "Hareketli Ad-Hoc Ağlarda Bir Hareketlilik Yönetimi Protokolü", ***G.Ü. Politeknik Dergisi***, 11(4): 313-318 (2008).

65. Toklu, S., Akcayol, M.A., "Congestion Control in WAP Traffic and Transport Layer Protocols", ***Journal of the Faculty of Engineering and Architecture of Gazi University***, 24(3): 397-408 (2009).

66. Floyd, R.W., "Algorithm 97: Shortest path", ***Communications of the Acm***, 5(6): 75-108 (1962).

67. Eppstein, D., "Finding the k Shortest Paths", ***35th Annual Symposium on Foundations of Computer Science***, Santa Fe, NM, USA, 154-154 (1994).

68. Fu, L., "Real-time Vehicle Routing and Scheduling in Dynamic and Stochastic Traffic Networks", Doktora Tezi, ***University of Alberta***, Alberta, 20-176 (1996).

69. Gen, M., Cheng, R., Wang, D., "Genetic algorithms for solving shortest path problems", ***IEEE International Conference on Evolutionary Computation***, Indianapolis, USA 401-406 (1997).

70. De Jong, K., "Learning with genetic algorithms: An overview", ***Machine Learning***, 3(2): 121-138 (1988).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: ÜNAL, Muhammet
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 07.06.1976 Samsun
Medeni hali	: Bekar
Telefon	: 0 (312) 582 31 21
e-mail	: muhunal@gazi.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek Lisans	Gazi Ü./Elektrik Elektronik Mühendisliği	2003
Lisans	Gazi Ü./Elektrik Elektronik Mühendisliği	2001
Lise	Gazi Anadolu Lisesi	1994

İş Deneyimi

Yıl	Yer	Görev
2002-2005	Gazi Üniversitesi	Araştırma Görevlisi
2005-2010	Gazi Üniversitesi	Öğretim Görevlisi

Yabancı Dil

İngilizce, Almanca

Yayınlar

1. Taplamacıoğlu M.C., Ünal M., "Yüksek Gerilim Dc Hatlarda Korona Analizi" Elektrik Mühendisleri IX. Ulusal Kongresi, Kocaeli, 2001
2. Ünal M., Yüncü S., "Choosing the Right Hardware for Beowulf Clusters Considering Price /Performance Ratio", International Conferance on Electrical and Electronics Engineering, Page 361-364, 3-7 December, Bursa, 2003
3. Ünal M., Akcayol M. A. "Kablosuz Ağlarda Güvenlik Bilinçli Yönlendirme Protokolleri" Bilişim Teknolojileri Dergisi, Sayfa 7-13, Eylül 2008 Vol 1, Sayı 3