KABLOSUZ ALGILAYICI AĞLARDA GİZLİ ANAHTAR ŞİFRELEMESİNDE ANAHTAR HAVUZU BÜYÜKLÜĞÜNÜN AĞ YAŞAM SÜRESİNE ETKİLERİ

BEKİR SAİT ÇİFTLER

YÜKSEK LİSANS TEZİ

ELEKTRİK VE ELEKTRONİK MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2013

ANKARA

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Hamza KURT

Anabilim Dalı Başkanı

Bekir Sait ÇİFTLER tarafından hazırlanan KABLOSUZ ALGILAYICI AĞLARDA GİZLİ ANAHTAR ŞİFRELEMESİNDE ANAHTAR HAVUZU BÜYÜKLÜĞÜNÜN YAŞAM SÜRESİNE ETKİLERİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____	_____
Doç. Dr. Bülent TAVLI	Doç. Dr. Kemal BIÇAKÇI
Tez Danışmanı	2. Tez Danışmanı

Tez Jüri Üyeleri

Başkan: Doç. Dr. Tolga GİRİCİ _____

Üye : Doç. Dr. Kemal BIÇAKÇI _____

Üye : Doç. Dr. Bülent TAVLI _____

Üye : Doç. Dr. Ali Cafer GÜRBÜZ _____

Üye : Yrd. Doç. Dr. Hakan GÜLTEKİN _____

TEZ BİLDİRİMİ

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

Bekir Sait ÇİFTLER

University : **TOBB Economics and Technology University**
Institute : **Institute of Natural and Applied Sciences**
Science Program : **Electrical and Electronics Engineering**
Supervisors : **Associate Professor Dr. Bülent TAVLI**
Associate Professor Dr. Kemal BIÇAKÇI
Degree Awarded and Date : **M.Sc. – May 2013**

Bekir Sait ÇİFTLER

IMPACT OF KEY POOL SIZE WITH SECRET KEY ENCRYPTION ON THE LIFETIME OF WIRELESS SENSOR NETWORKS

ABSTRACT

In Wireless Sensor Networks (WSN) system design, maximizing the network lifetime is one of the most important goals. Optimizing each node's lifetime does not result to the optimal network lifetime, network must be optimized altogether. The lifetime of wireless sensor networks is optimized if the traffic within the network is adjusted in a way that all nodes dissipate their energies in a balanced fashion. To balance the energy dissipation, nodes split their flows and these flows are forwarded to different nodes acting as relays. Security of wireless sensor networks is another important issue in system design. It is important to secure communication of the network against eavesdroppers, node capture attacks, etc. Secure data flow is provided with secret key distribution which enables hop-by-hop security and allows addition and deletion of nodes or keys. A Mixed Integer Programming (MIP) framework is constructed to characterize the impact of key distributions on the lifetime. The results show that the lifetime depends on the probability of sharing at least one key of two nodes due to key ring size and key pool size.

Keywords: Wireless Sensor Networks, Key Distribution, Lifetime Optimization, Linear Programming, Network Security

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Elektrik ve Elektronik Mühendisliği**
Tez Danışmanları : **Doç. Dr. Bülent TAVLI**
Doç. Dr. Kemal BIÇAKÇI
Tez Türü ve Tarihi : **Yüksek Lisans – Mayıs 2013**

Bekir Sait ÇİFTLER

KABLOSUZ ALGILAYICI AĞLARDA GİZLİ ANAHTAR ŞİFRELEMESİNDE ANAHTAR HAVUZU BÜYÜKLÜĞÜNÜN AĞ YAŞAM SÜRESİNE ETKİLERİ

ÖZET

Kablosuz algılayıcı ağların sistem tasarımında ağ yaşam süresini en büyük değerine ulaştırmak en önemli hedeflerden birisidir. Her bir düğümün yaşam süresini eniyilemek tüm ağın eniyi yaşam süresine ulaşmayı sağlamaz, eniyileme ağ üzerinde bütünüyle yapılmalıdır. Kablosuz algılayıcı ağların yaşam süresi ağ içerisindeki trafik düğümlerin tamamının enerjilerini dengeli bir şekilde harcayacak biçimde eniyilenmelidir. Enerji harcamasını dengelemek için, düğümler akımlarını bölmeli ve bu akımlar değişik düğümler röle olacak şekilde iletilmelidir. Kablosuz algılayıcı ağlarda güvenlik bir başka önemli sistem tasarım konusudur. Ağın iletişimini kulak misafirlerine, düğüm elegeçirme saldırıları ve benzeri saldırılara karşı korumak önemlidir. Güvenli veri akışı düğümden düğüme güvenlik sağlayan ve anahtar ya da düğüm eklenip çıkarılmasına olanak sağlayan gizli anahtar dağılımı kullanılarak sağlanmıştır. Anahtar dağılımının yaşam süresi üzerindeki etkilerini incelemek ve özelliklerini saptamak için bir Karışık Tamsayı Programlama sistemi oluşturulmuştur. Sonuçlar ağ yaşam süresinin iki düğümün en az bir ortak anahtar paylaşma olasılığına, bunun da anahtar halka büyüklüğü ve anahtar havuz büyüklüğüne bağlı olduğunu göstermiştir.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Anahtar Dağılımları, Yaşam Süresi Eniyilemesi, Doğrusal Programlama, Ağ Güvenliği

TEŞEKKÜR

Bu çalışmanın tamamlanmasında ilgi ve sabırla beni yönlendiren, akademik çalışmalarımda ve hayatın diğer alanlarında desteklerini her zaman yanımda hissettiğim değerli danışmanlarım Bülent Tavlı ve Kemal Bıçakçı'ya,

Bu süreçte bana yardımlarını esirgemeyen değerli hocalarım, çalışma arkadaşlarım ve TOBB ETÜ ailesinin tüm bireylerine,

Lisans ve Yüksek Lisans boyunca her zaman yanımda olan ev arkadaşlarıma,

Maddi ve manevi destekleri ile bugünlere gelmemde en büyük paya sahip annem, babam ve kardeşlerime,

Son olarak tez sürecinde bana desteğini esirgemeyen sevgili eşime,

Teşekkürü bir borç bilirim...

İçindekiler

1 GİRİŞ **1**

1.1 Kablosuz Algılayıcı Ağlar 1

1.1.1 Düğüm Yapısı 2

1.1.2 Kullanım Alanları 3

1.1.3 Enerji Verimliliği 4

1.1.4 İletişim Modeli 5

1.2 Ağ Güvenliği 6

1.2.1 Anahtar Dağılımı 7

1.3 Eniyileme 8

1.3.1 Doğrusal Programlama 8

1.3.2 Tamsayı Programlama 10

1.3.3 MATLAB ve GAMS 10

2 SİSTEM MODELİ **11**

2.1 Konuşlandırma 11

2.2 Eschenauer Anahtar Dağılımı 12

2.3 İletişim Modeli 15

2.4 Tamsayı Programlama Modeli 17

3 ANALİZLER **19**

3.1 Basit Örnekler 19

3.2 Simülasyon Verileri 21

3.2.1 Anahtar Halka Büyüklüğüne Göre 22

3.2.2 Anahtar Paylaşma Olasılığına Göre 25

4 SONUÇLAR **31**

ÖZGEÇMİŞ **34**

Şekil Listesi

1.1 Algılayıcı Düğümün Yapısı 3

2.1 100 Düğüm İçin Birim Yarıçapta Konuşlandırma Örneği 11

2.2 Anahtar Halka Büyüklüğüne göre Anahtar Paylaşma Olasılığı . . 13

2.3 İletim Güç Seviyeleri 15

2.4 Enerji Modeli 15

2.5 Tamsayı Programlama Modeli 17

3.1 Basit Örnek: Anahtar Kısıtının Olmadığı Durum 19

3.2 Basit Örnek: Anahtar Halka Büyüklüğünün 3 Olduğu Durum . . . 20

3.3 Basit Örnek: Anahtar Halka Büyüklüğünün 1 Olduğu Durum . . . 20

3.4 Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (100 Düğüm) 26

3.5 Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (200 Düğüm) 27

3.6 Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (300 Düğüm) 28

3.7 Anahtar Paylaşma Olasılığına Göre Yaşam Süresi Azalması 29

3.8 100, 200 ve 300 Düğümün Aynı Alanda Anahtar Paylaşma Olasılığına Göre 30

Tablo Listesi

0.1 Sembol Listesi xii

2.1 Anahtar Halka Büyüklüğüne Göre Anahtar Paylaşma Olasılığı [1] 14

2.2 CC1000 Radyosuna Sahip Mica2'nin Güç İletim Seviye Değerleri [2] 16

Sembol Listesi

Değişken	**Açıklaması**
t	Ağın yaşam süresi
A	Çizgedeki bütün kenarların kümesi
W	Bütün düğümlerin kümesi, baz istasyonu hariç
V	Bütün düğümlerin kümesi, baz istasyonu dahil
P veya H	Anahtar havuzu büyüklüğü (tüm ağdaki)
k veya AHB	Anahtar halkası büyüklüğü (düğüm başına)
KSP	İki düğümün ortak anahtara sahip olma olasılığı
f_{ij}	i-düğümünden j-düğümüne gönderilen veri paketi miktarı (tamsayı)
s_i	i-düğümünde üretilen veri paketi sayısı
b_{ij}	i-düğümü ile j-düğümü arasında veri gönderim imkanı (ikili değer)
e_i	i-düğümünün batarya enerjisi
$E^D_{tx,ij}$	i-düğümünden j-düğümüne gönderilen her bir veri paketi için harcanan enerji miktarı
E^D_{rx}	Alınan her bir veri paketi için harcanan enerji miktarı
$E^{ACK}_{tx,ij}$	i-düğümünden j-düğümüne gönderilen her bir teyit paketi için harcanan enerji miktarı
E^{ACK}_{rx}	Alınan her bir teyit paketi için harcanan enerji miktarı
d_{ij}	i-düğümü ve j-düğümü arasındaki mesafe
$R_{max}(l)$	l-seviyesinde iletim yapılabilecek en uzak mesafe
P_{DA}	Veri edinme için gereken güç
P_{PROC}	Veriyi işlemek için gereken güç
$P_{tx}(i,j)$	i-düğümünden j-düğümüne bir bit veri iletmek için gereken güç
P_{rx}	Bir bit veri almak için gereken güç
PS_{data}	Veri paketi büyüklüğü
PS_{ACK}	Teyit paketi büyüklüğü
BW	İletim için kullanılan bantgenişliği

Tablo 0.1: Sembol Listesi

1. GİRİŞ

Bu bölümde genel olarak, bu tezin içeriği olarak ifade edilebilecek;

- Kablosuz Algılayıcı Ağlar

  Düğüm Yapısı

  Kullanım Alanları

- Ağ Güvenliği

  Anahtar Paylaşımı

- Eniyileme

  Doğrusal Programlama

  Tamsayı Programlama

  GAMS ve CPLEX

konuları ele alınacak ve bu konular hakkında literatür bilgisi verilecektir.

1.1 Kablosuz Algılayıcı Ağlar

Fiziksel ve çevresel bir koşulu (sıcaklık, basınç, nem, vb.) algılamak üzere belli bir alana yayılmış müstakil düğümlerden oluşan, algıladığı durumu veri haline getirip birbiri üzerinden işbirliğiyle merkez istasyonuna ileten düğümler bütününe kablosuz algılayıcı ağ denmektedir. Enerji gereksinimlerini bataryalardan karşılayan ve dışardan enerji desteği olmayan bu düğümler, enerjilerini çok verimli bir şekilde kullanmak durumundadırlar. Kablosuz algılayıcı ağları Türkçe

yayınlarda kablosuz duyarga ağları ismiyle de anılmaktadır. Kablosuz algılayıcı ağlar altyapı elemanlarının (yöneltici ve erişim noktaları gibi) olmadığı ortamlarda kendi kendine örgütlenerek çalışabilen tasarsız ağlardır.

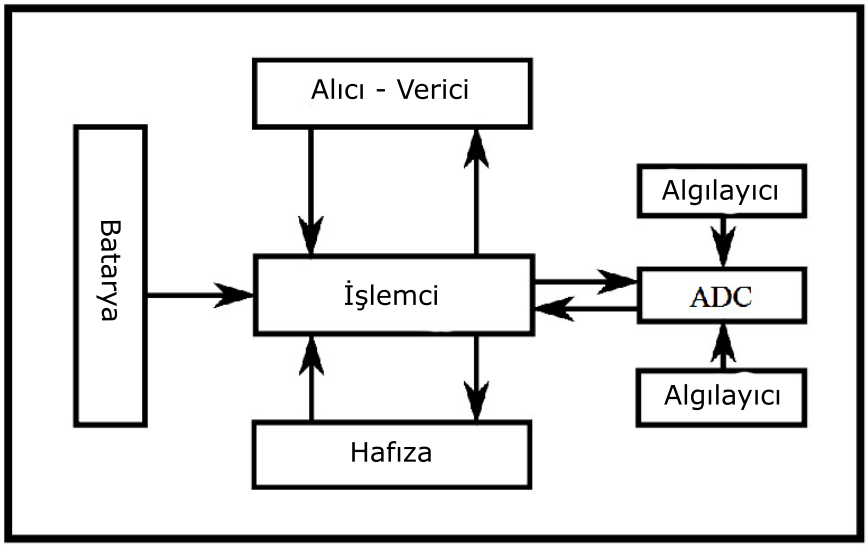
Kablosuz Algılayıcı Ağlar ilk olarak 1978'de DARPA'nın (Amerika Birleşik Devletleri Savunma Bakanlığı İleri Araştırma Projeleri Ajansı) yaptığı Dağıtık Algılayıcı Ağlar Çalıştayı'nda gündeme gelmiştir. 1980'lerde yine DARPA'nın Dağıtık Algılayıcı Ağlar grubunun çalışmaları sonucu çeşitli fikirler ortaya çıksa da uygulamaya geçmesi çok sonraları olmuştur [3]. 2000'li yılların başından itibaren kablosuz iletişimin gelişmesiyle beraber terminolojiye girmiş [4] ve o yıllardan itibaren ciddi bir ivme kazanıp bir çok alanda uygulamaya sahip olmuş bir teknolojidir.

2007 yılında Sohraby ve arkadaşları tarafından yapılan bir çalışmaya [4] göre bu alanda yapılan akademik çalışmaların büyük bir çoğunluğunu (yaklaşık olarak %9.7) konuşlandırma teknikleri oluşturmaktadır. Bu tezin alanı olan güvenlik ve yaşam süresi eniyilemesi ise sırasıyla %5.76 ve %3.33'lük bir pay almaktadır.

1.1.1 Düğüm Yapısı

Kablosuz algılayıcı düğümlerin iç yapısında bulunan temel elemanlar Şekil 1.1'de gösterilmiştir.

Kablosuz algılayıcı ağlarda düğümler yetenekleri açısından teknolojik sebeplerden ve maliyet açısından bir çok kısıtlara sahiptirler. Bunlar bataryada depolayabildikleri enerji miktarı, iletişim mesafeleri ve hızları, hesaplama hızı ve veri depolama miktarı gibi kısıtlardır [4]. Bundan dolayı kablosuz algılayıcı ağlarda algoritma ve protokol oluşturma çalışmaları çoğunlukla verimlilik üzerine yoğunlaşmaktadır. Kablosuz algılayıcı ağ uygulamalarında genellikle çok ciddi miktarda düğüm sayısı kullanıldığı için bir düğümün maliyeti olabildiğince düşürülmekte ve bu yapılırken de aynı şekilde düğümün var olan enerjisini de olabildiğince verimli kullanması gerekmektedir. Şekil 1.1'de görüldüğü gibi bir kablosuz algılayıcı ağ düğümü işlemci ve işlemciyi çevreleyen örneksel sayısal çevirici (ADC) ve ona bağlı algılayıcılar, diğer düğümlerle ve baz istasyonuyla haberleşmeyi sağlayan alıcı-verici, gerektiğinde veri depolamaya yarayan hafıza



Şekil 1.1: Algılayıcı Düğümün Yapısı

ve bataryadan oluşmaktadır.

1.1.2 Kullanım Alanları

Kablosuz algılayıcı ağları gelişen teknolojiyle yeteneklerinin artması ve maliyetinin de düşmesiyle bir çok uygulama alanı bulmuştur. Bu uygulama alanlarını beş ana başlık altında [4] [5] toplayıp bunlara örnekler verecek olursak bunlar;

- Askeri Uygulamalar

  Düşman birimlerin varlığını gözetleme

  Dost birimlerin varlığını gözetleme

  Hedef konumu belirleme

  Hasar ölçümleri

  Nükleer, biyolojik ve kimyasal saldırı tespiti

- Çevre Uygulamaları
  - Mikroklima
  - Orman yangınlarının tespiti
  - Sel ve fırtınaların tespiti
  - Tarımsal faaliyetlerde çevre koşullarının tespiti
- Sağlık Uygulamaları
  - Fizyolojik verilerin uzaktan görüntülenmesi
  - İlaç yönetimi
  - Hastanedeki bireylerin (doktor, hasta vb.) konumlarının takibi
- Ev Uygulamaları
  - Ev otomasyonu
  - Ev içi akıllı aletlerin yönetimi
- Ticari Uygulamalar
  - Envanter kontrolü
  - Araç takibi ve tespiti
  - Trafik akış izlemesi
  - Ofislerde ve fabrikalarda çevresel faktörlerin kontrolü

1.1.3 Enerji Verimliliği

Kablosuz algılayıcı ağlarda giriş bölümünde de belirttiğimiz gibi en büyük zorluklardan birisi enerjiyi verimli kullanmaktır. Kablosuz algılayıcı ağlar için enerjiyi verimli kullanmak demek işlevini yitirmeden ağın yaşam süresini olası en büyük değere ulaştırmak demektir. Ağ yaşam süresi ise ağ çalışmaya başladıktan sonra ağdaki herhangi bir düğümün enerjisini tam olarak bitirmesi, dolayısıyla işlevsiz hale gelmesine kadar geçen süredir. Bu doğrultuda ağın yaşam süresini uzatmak için çeşitli yöntemler vardır. Bunlar, aktarılacak verinin sıkıştırılması, verilerin doğrudan baz istasyonuna değil, düğümlerin beraber çalışarak birbirinin üzerinden aktarması sonucu aktarım sırasında oluşacak enerji kayıplarının en aza indirilmesi gibi tekniklerdir [6].

Kablosuz algılayıcı ağlarının düğüm yapısında dışarıdan enerji sağlayan bir parçası olmayıp, tüm enerjisini bünyesinde bulundurduğu bataryadan sağladığı için enerjinin verimli kullanımı çok önemlidir. Uygulamadan uygulamaya değişmekle birlikte bazı uygulamalarda her bir düğümün aylarca kendi bataryasıyla hem algılama işlemlerini gerçekleştirip, algıladığı bilgileri işleyip aktarılabilir veri haline getirip, gerektiğinde başka düğümlerden gelen verilerle bu verileri birleştirip düğümler üzerinden baz istasyonuna kadar aktarması gerekmektedir.

Algılayıcı düğümleri bünyelerinde çoğunlukla <500 mAh, 1.2 V bataryalar (AA boyutunda bir kalem pil) bulundurmaktadır. Yani bataryalarında mevcut olan enerji çok kısıtlı olmaktadır. Algılayıcı düğümlerin enerji harcamasını üç ana başlık altında toplayacak olursak algılama, iletişim ve veri işleme olarak belirtebiliriz. Bunların her birisinde ayrı eniyileme teknikleri kullanılarak verimlilik arttırılabilmektedir [4].

1.1.4 İletişim Modeli

Kablosuz algılayıcı ağların yaşam süresini eniyilemek için oluşturulan bir çok modelde basit iletişim modelleri kullanılmıştır [7]. Bu çalışmada deneysel sonuçlarla elde edilen parametler kullanılsa da, kablosuz algılayıcı ağların iletişim sırasında nasıl enerji harcadığını anlamak açısından basit modelden bahsedeceğiz.

Kablosuz algılayıcı ağları modellemek için kullanılan iletişim modelinde bir düğümden diğerine veri gönderilmesi için gereken enerji miktarı elektronik devrelerde kullanılan sabit enerji miktarı ve yolda oluşacak kaybı belirten iki düğüm arasındaki mesafenin üstel bir fonksiyonuyla gösterilmiştir.

$$P_{tx,ij} = \rho + \epsilon d_{ij}^{\alpha} \tag{1.1}$$

$$P_{rx,ij} = \rho \tag{1.2}$$

1.1 ve 1.2 ifadelerinde de görülen ρ bir düğümden diğerine 1 bit veri gönderilirken ve alınırken elektronik devrede harcanan sabit enerji miktarını ifade etmektedir. ϵ anten verimliliğini, d_{ij} i ve j düğümleri arasındaki mesafeyi ve

α ise yol boyunca oluşacak kaybı temsil etmektedir. En ideal durumda, yani elektromanyetik bir sönümleme olmadığı varsayıldığında $\alpha = 2$ alınır. Çeşitli engellerden dolayı sönümleme olan durumlarda da $\alpha = 4$ olarak seçilmiştir [7], [8].

Bu tez çalışmasındaki iletişim modeli ise Mica2 [2] algılayıcı düğümünün veri föyü ve deneysel sonuçları dikkate alınarak modellenmiştir. Problem tanımı bölümünün Sistem Modeli kısmında (2.1) detaylı olarak anlatılan bu modelde bir bit verinin gönderilmesi için gereken enerji mesafeye göre ayrık enerji seviyelerine sahiptir. Bu modelde Mica2 düğümlerinin özellikleri göz önünde bulundurulduğu için bir düğümün veri gönderebileceği mesafe sınırlıdır [2].

1.2 Ağ Güvenliği

Kablosuz algılayıcı ağların askeri uygulamalar gibi gizliliği ve dayanıklılığı çok önemli olan uygulama alanları olduğu için ağ güvenliği ayrı bir önem kazanmaktadır. Ayrıca ağ güvenliği diğer uygulama alanlarında ağın sorunsuz ve durmaksızın çalışmaya devam edebilmesi için de ayrıca bir öneme sahiptir. Güvenlik sistemine sahip olmayan kablosuz algılayıcı ağlar dinlemeden servis engellenmesine, düğümlerin ele geçirilmesinden sahte düğüm eklenmesine kadar değişik saldırılara karşı çaresiz kalabilirler.

Ağ güvenliği için kablosuz ağlar için çeşitli uygulamalar mevcuttur. Ancak normal kablosuz ağlar için geliştirilmiş güvenlik uygulamaları kablosuz algılayıcı ağların sınırlı kaynaklarıyla ya çalışmamakta ya da algılayıcı düğümlerin kendi işlevini yapmasını sağlayan enerjinin, veri depolama ünitesinin ya da işlemcisinin kaynaklarını büyük oranda tüketmektedir. Dolayısıyla kablosuz algılayıcı ağlarda kullanılabilecek güvenlik uygulamaları sınırlıdır. Bunlardan bir kaçı aşağıda listelenmiştir [3].

- Anahtar oluşturulması ve dağılımı
- Düğüm kimliği doğrulaması
- Gizlilik

Bu tezde ağ güvenliğinin bu yöntemlerden gizli anahtar dağılımı tekniği ile sağlandığı varsayılmış ve bu yöntem daha önce Eschenauer ve arkadaşlarının yaptığı çalışmaya [1] göre modellenmiştir.

1.2.1 Anahtar Dağılımı

Kablosuz algılayıcı ağların güvenliğini sağlamada kullanılan anahtar oluşturulması ve dağılımı yöntemi üzerine yapılan çalışmalara bakacak olursak, bu çalışmaların genellikle bağlanabilirlik üzerine yoğunlaştığını görebiliriz. Bu çalışmalarda değişik konuşlandırma koşullarıyla beraber çeşitli anahtar oluşturma ve dağıtım teknikleri denenmiş, birbirlerine olan üstünlükleri ve eksik kalan yönleri ortaya koyulmuştur. Çeşitli çalışmalarda ağ güvenliğinin bir noktada aksadığını varsayarak bir düğüm veya bir anahtarın düşman tarafından ele geçirilme durumu incelenmiştir.

Ruj ve arkadaşlarının çalışmasında [9] çeşitli anahtar dağıtım teknikleri incelenmiş (İkili, Q-karışık, PIKE) ve kendileri üçlü bir anahtar dağıtım tekniği öne sürmüşlerdir. Ruj ve arkadaşları çalışmalarında hesaplama karmaşıklığı, depolama imkanları ve düğüm kaybı karşısında ağın dayanıklılığı gibi durumlar incelenmiş ve kendi tekniklerinin üstün yönleri ortaya konmuştur.

Du ve arkadaşları yaptıkları çalışmda [10] konuşlandırma bilgilerini önceden bilindiğini varsayarak bağlanabilirlik, bellek kullanımı ve saldırıya karşı dayanıklılıkta gereksiz anahtar kullanımı yapmadan performansı yüksek tutmak için yeni bir anahtar dağılımı yöntemi önermişlerdir. Bu yöntemde anahtar dağılımı öncesinde düğüm konumlarının bilindiği varsayılmaktadır. Performans ölçütü olarak yerel ve genel bağlanabilirlik, iletişim yükü ve düğüm kaybına karşı dayanıklılık alınmıştır. Çalışmalarıyla Eschenauer'in ve arkadaşlarının çalışmasını [1] karşılaştırarak diğer anahtar dağıtımlarında bulunan anahtarların çok küçük bir azınlığıyla aynı derecede bağlanabilirliğin sağlanabildiğini göstermişlerdir.

Yu ve Guan'ın çalışmasında [11] düğüm kayıplarına karşı dayanıklı yüksek bağlanabilirlik sağlamak için grup temelli bir şema öne sürmüşlerdir. Bu yöntemde düğümler ağ alanında altıgen şeklinde alanlara bölünüp, bu alanlar dahilindeki her bir düğüm de gruplara bölünmüştür. Amaç az bellekle düğüm kaybına karşı

dayanıklılık ve yüksek bağlanabilirlik sağlamaktır. Yu ve Guan bu çalışmalarında altıgen alanların sınırlarının doğru seçilmesi durumunda az bellek kullanımıyla çok yüksek bir bağlanabilirlik ve düğüm kaybına karşı yüksek dayanıklılık gösterdiğini göstermişlerdir.

Bütün bu çalışmalarda görmekteyiz ki bu alanda çalışan bir çok insan daha çok bağlanabilirlik ve dayanıklılık üzerine çalışmaktadırlar [1], [9], [10], [11]. Bu çalışmalarda farklı farklı anahtar dağılımı teknikleri incelenmiş ve karşılaştırılmışlardır. Modelleme açısından en basit ve kolay anahtar dağıtım tekniklerinden olan Eschenauer ve arkadaşlarının dağıtım tekniğidir. Aynı zamanda bu teknik diğer teknikler için bir taban oluşturmaktadır. Diğer bir çok teknik bu teknikten yola çıkarak geliştirilmiştir.

1.3 Eniyileme

Eniyileme eldeki az miktardaki kaynağı olası en iyi şekilde kullanarak en iyi sonuçlara ulaşmaktır [12]. Eniyileme uygulamaları İkinci Dünya Savaşı'ndan bu yana lojistik uygulamalarıyla ciddi anlamda kullanılmaya başlanmış olup, havayolları planlaması ve petrol tedarik mekanizmaları gibi farklı alanlara yayılmış ve günümüz itibariyle neredeyse hayatımızdaki her alanda bir uygulamaya sahiptir. Büyük çaplı eniyileme uygulamalarının tarihi bayağı kısadır. Hatta bu konuda bir örnek belirtmek gerekirse Simplex metodunun mucidi George Dantzig 2005 yılında vefat etmiştir. Dantzig 1947 yılında İkinci Dünya Savaşının hemen sonrasında bulduğu Simplex metoduyla öncesinde elle ve düz bir yaklaşımkla yapılan bir çok eniyileme hesaplamasını algoritmik olarak ve daha basit bir şekilde yapabilme imkanı tanımıştır. Dantzig'in bulduğu Simplex hala bir çok uygulamanın altyapısında yatan algoritmadır.

1.3.1 Doğrusal Programlama

Doğrusal denklemlerle ifade edilmiş bir sistemde yararı gösteren bir doğrusal amaç fonksiyonunun varolan doğrusal kısıtlar dahilinde değişkenlerin en yararlı hale getirilmesi için oluşturulan modellere doğrusal (lineer) program denir.

Doğrusal programlar dört temel öğeden oluşurlar [12];

- **Değişkenler** Probleme başladığımızda bilmediğimiz, amaç fonksiyonunu olası en iyi değerine ulaştırmak için kontrol edebildiklerimizdir.
- **Amaç Fonksiyonu** Azami ya da asgari seviyeye indirmek istediğimiz sabit değerlerle ağırlıklandırılmış değişkenlerin oluşturduğu, hedefimizi gösteren, kâr ya da masraf gibi şeyleri ifade eden matematiksel fonksiyondur.
- **Kısıtlar** Değişkenlerin birbirine bağlı sınırlılıklarını ifade eden fonksiyonlardır.
- **Değişken Sınırları** Her bir değişkenin alabileceği azami ya da asgari değerler.

Her bir doğrusal program temelde şu şekilde ifade edilir;

$$c^T x \tag{1.3}$$

$$Ax \leq b \tag{1.4}$$

$$x \geq 0 \tag{1.5}$$

(1.4)'te gösterilen ifade doğrusal problemin amaç fonksiyonunu göstermektedir. x değişkenlerimizi bulunduran vektör, c ise amaç fonksiyonunda değişkenlerin katsayılarını bulunduran vektördür. (1.5)'teki ifade ise kısıtları göstermektedir. A kısıtlardaki x değişkenlerinin her bir kısıt için katsayılarını bulunduran matristir. b ise bu kısıtlara göre sabit değerlerin bulunduğu vektördür. Probleme göre (1.4) ifadesi azami (maksimum) veya asgari (minimum) değerine ulaştırılmak istenebilir, bu doğrultuda x değişkenleri kısıtlara göre değiştirilir. Standart bir doğrusal programda değişkenler sıfırdan küçük değer alamaz.

1.3.2 Tamsayı Programlama

Tamsayı programlama değişkenlerimizin tamsayı değerler alabildiği doğrusal programların adıdır. Çözümü değişkenlerin ayrık değerler üzerinden olacağı için çok daha karmaşıktır ve daha uzun sürer. Bazı problemleri modellemek için bazen daha gerçeğe yakın sonuçlar elde etmek için bazen de başka bir seçenek olmadığı için bu yöntem kullanılmak durumundadır.

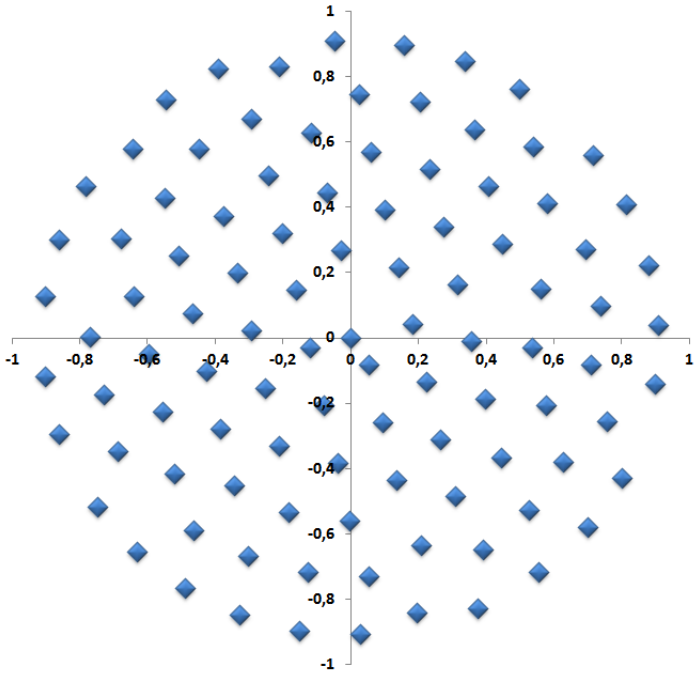
1.3.3 MATLAB ve GAMS

Eschenauer anahtar dağılım modelini oluştururken MATLAB'ın matrisler konusundaki hızlı işlem altyapısı kullanıldı. Sistem modeli ve anahtar dağılımları MATLAB'da [13] oluşturulurken, GAMS (Generic Algebraic Modeling Language) [14] programında ise bu modeli tamsayı programımıza parametre olarak işlendi ve GAMS'ın bünyesinde bulunan CPLEX çözücüsüyle eniyileme modeli çözülüp simülasyon verileri alındı.

2. SİSTEM MODELİ

2.1 Konuşlandırma

Gerçek hayatta kablosuz algılayıcı ağlar çok farklı şekillerde konuşlandırılabilmektedir. Akademik çalışmalarda genellikle belli bir dikdörtgen veya dairesel düzlem üzerine belli aralıklarla veya rastgele konuşlandırıldıkları varsayılmaktadır. Bu çalışmada ise dairesel bir topoloji oluşturuldu. Topolojiyi oluştururken bilinen en iyi dairesel istifleme geometrisini kullanıldı [15].



Şekil 2.1: 100 Düğüm İçin Birim Yarıçapta Konuşlandırma Örneği

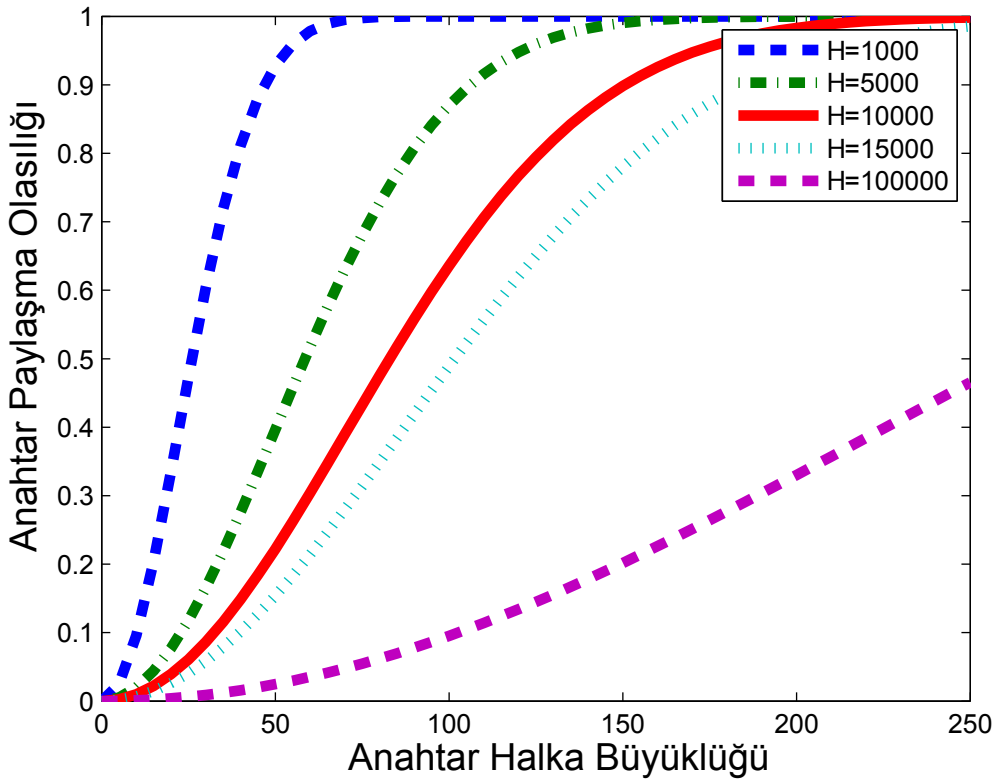
Şekil (2.1)'de görebileceğiniz üzere kullanılan dairesel istifleme geometrisi alanın en ideal şekilde algılayıcı düğümler tarafından taranmasını ve baz istasyonuna doğru veri iletimi yaparken en uygun veri atlamalarını yapmasına göre şekillenmiştir.

Konuşlandırmalarda düğümler arası mesafeler oluşturulurken yarıçap birim yarıçap halindeyken belli sabitlerle çarpılmış ve gerekli mesafeler oluşturulmuştur. Mesafelerin hesabında düğüm başına düşen alan hesabı uygulanmıştır. $50m^2, 100m^2$ ve $200m^2$'lik üç farklı değer atanıp, ona göre sonuçlar hesaplanmıştır.

2.2 Eschenauer Anahtar Dağılımı

Eschenauer'in anahtar dağılımı oldukça basit ve etkili bir yöntemdir. Ağ için merkezi bir otorite tarafından oluşturulan anahtarlar bir havuzda toplanır, bu havuz tez içerisinde Anahtar Havuzu olarak ifade edilmiştir. Ağın baz istasyonu tüm anahtarlara sahiptir, yani tüm düğümlerle iletişim kurabilmektedir. Ağda bulunan her düğüme yöneticinin belirlediği bir oranda ya da sayıda anahtar bu havuzdan rastgele seçilerek düğümlerin anahtar halkası oluşturulur. İki düğümün birbiriyle iletişim anahtar halkalarında en az bir ortak anahtara sahip olmaları gerekir. Eschenauer'in anahtar dağılım yönteminde iki düğümün en az bir anahtar paylaşma olasılığı matematiksel olarak hesaplanabilir [1]. Bu yönteme göre anahtar paylaşma olasılığı düğüm sayısından bağımsız olarak anahtar havuz büyüklüğü, yani havuzdaki anahtar sayısı (H) ve düğüm başına atanan anahtar halkasındaki anahtar sayısı (k) ile ilişkilidir.

$$P_{paylama} = 1 - \frac{k!(H-k)!(H-k)!}{H!k!(H-2k)!} \tag{2.1}$$



Şekil 2.2: Anahtar Halka Büyüklüğüne göre Anahtar Paylaşma Olasılığı

Eşitlik (2.1)'de anahtar paylaşma olasılığıyla anahtar havuzu büyüklüğü ve anahtar halkası büyüklüğü arasındaki ilişki verilmiştir. Şekil (2.2)'de havuz büyüklükleri 1000, 5000, 10000, 15000 ve 100000 olmak üzere 5 durum için anahtar halka büyüklüklerine göre anahtar paylaşma olasılıkları verilmiştir.

k	H=5000	H=10000	H=15000
5	0.00499	0.00249	0.00166
10	0.01983	0.00995	0.00664
15	0.04412	0.02228	0.01490
20	0.07717	0.03928	0.02634
25	0.11804	0.06073	0.04087
30	0.16562	0.08631	0.05834
35	0.21862	0.11566	0.07859
40	0.27570	0.14839	0.10142
45	0.33544	0.18405	0.12663
50	0.39649	0.22216	0.15398
55	0.45756	0.26225	0.18323
60	0.51745	0.30382	0.21412
65	0.57517	0.34639	0.24639
70	0.62985	0.38947	0.27977
75	0.68083	0.43262	0.31399

Tablo 2.1: Anahtar Halka Büyüklüğüne Göre Anahtar Paylaşma Olasılığı [1]

Tablo (2.1)'de anahtar halka büyüklüğüne göre 5000, 10000 ve 15000 anahtardan oluşan havuzlar için anahtar paylaşma olasılıkları verilmiştir. Bu değerler tezin deneysel kısmında oluşturulan sistemler için referans anahtar paylaşma olasılıklarını göstermektedir.

2.3 İletişim Modeli

İletişim modelimizi deneysel sonuçlardan ve ürünün veri föyünden yararlanarak Mica2 platformunun düğümlerine göre oluşturduk. Mica2 platformu Atmel 128L işlemcisi ve Chipcon CC1000 radyosunu içermektedir. Chipcon CC1000 radyosunun kullandığı bantgenişliği 38.4 Kilobittir. Bir düğümden diğer düğüme bir bitlik veri göndermek için gereken enerji mesafeye göre ayrık değerler içermekte ve belli bir mesafeden sonra veri gönderilememektedir. Ayrık enerji harcama verileri Mica2'nin deneysel olarak elde edilmiş olup, bu değerler ürün veri föyünde bulunmaktadır. Biz de modelimizi bu veri föyüne göre oluşturduk.

$$\begin{aligned} P_{tx}(i,j) &= \infty \quad if \quad d(i,j) > R_{max}(l_{max}) \\ & P_{tx}(l_{min}) \quad if \quad d(i,j) \leq R_{max}(l_{min}) \\ P_{tx}(l+1) \quad if \quad & R_{max}(l) < d(i,j) \leq R_{max}(l+1) \end{aligned} \tag{2.2}$$

Şekil 2.3: İletim Güç Seviyeleri

Mica2'nin mesafeye göre iletim güç seviyeleri Şekil (2.3)'de verildiği gibi mesafeye göre seviye seviye ayrık değerlere sahiptir. Mica2'nin hangi mesafede hangi güç seviyesinden iletim yapacağı Tablo (2.2)'de verilmiştir.

$$E^{D}_{tx(i,j)} = P_{tx}(i,j) \times PS_{Data}/BW \tag{2.3}$$

$$E^{ACK}_{tx(i,j)} = P_{tx}(i,j) \times PS_{ACK}/BW \tag{2.4}$$

$$E^{D}_{rx} = P_{rx} \times PS_{Data}/BW \tag{2.5}$$

$$E^{ACK}_{rx} = P_{rx} \times PS_{ACK}/BW \tag{2.6}$$

Şekil 2.4: Enerji Modeli

İletişim modelimizi algılanan verilerin paketler halinde iletildiğini ve alındığını, ayrıca alınan paketler için de alındı bilgisi, teyit (ing. Acknowledgement) paketlerinin gönderildiğini ve alındığını varsaydık. Bir veri paketinin büyüklüğünü 256 Bayt (ing. Byte) ve bir teyit paketinin büyüklüğünü 20 Bayt olarak belirledik. Modelimizde veri veya teyit paketi gönderirken harcanan enerji mesafeye göre değişirken veri veya teyit paketi almak sabit bir enerji harcamasına sahiptir. 2.3 ve 2.4 eşitliklerinde sırasıyla bir veri paketi veya bir teyit paketi göndermek için gerekli olan enerji hesaplanmaktadır. Bir veri paketi yollamak için gereken

Seviye	İletim Gücü (mW)	En Uzak Mesafe (m)
1	25.8	19.30
2	26.4	20.46
3	27.0	21.69
4	27.1	22.69
5	27.3	24.38
6	27.8	25.84
7	27.9	27.39
8	28.5	29.03
9	29.1	30.78
10	29.7	32.62
11	30.3	34.58
12	31.2	36.66
13	31.8	38.86
14	32.4	41.19
15	33.3	43.67
16	41.4	46.29
17	43.5	49.07
18	43.6	52.01
19	45.3	55.13
20	47.4	58.44
21	50.4	61.95
22	51.6	65.67
23	55.5	69.61
24	57.6	73.79
25	63.9	78.22
26	76.2	82.92

Tablo 2.2: CC1000 Radyosuna Sahip Mica2'nin Güç İletim Seviye Değerleri [2]

enerji, yollayan düğümle alıcı düğüm arasındaki mesafeye bağlı olan güç seviyesi ile paketin büyüklüğünün (veri paketindeki bit sayısının) çarpımının kullanılan bantgenişliğine bölümüne eşittir. Veri almak için gereken enerji ise daha basit bir şekilde, veri alımı için gereken güç sabit olduğu için aynı şekilde paket büyüklüğü ile güç değerinin çarpımının bantgenişliğine bölümüne eşittir.

2.4 Tamsayı Programlama Modeli

İletişim modelimiz veri iletiminin paketler halinde yapılması şeklinde oluşturulduğu için eniyileme modelimiz için Tamsayı Programlama modeli oluşturulmuştur. Bu model iletişim kısıtları, anahtar paylaşımından doğan kısıtlar ve enerji kısıtlarından yola çıkarak oluşturulmuştur.

Aşağıdakileri dikkate alarak
t'yi en büyük değerine çıkar:

$$f_{ij} \geq 0 \quad \forall (i,j) \epsilon A \tag{2.7}$$

$$f_{ij} = 0 \quad for \quad i = j \quad \forall (i,j) \epsilon A \tag{2.8}$$

$$f_{ij} = 0 \quad for \quad b_{ij} = 0 \quad \forall (i,j) \epsilon A \tag{2.9}$$

$$\sum_{j \epsilon W} f_{ji} + s_i t = \sum_{j \epsilon V} f_{ij} \quad \forall (i) \epsilon W \tag{2.10}$$

$$\begin{aligned} &\sum_{j \epsilon V} E^{D}_{tx(i,j)} f_{ij} + \sum_{j \epsilon W} E^{ACK}_{tx(i,j)} f_{ji} \\ &+ E^{D}_{rx} \sum_{j \epsilon W} f_{ji} + E^{ACK}_{rx} \sum_{j \epsilon V} f_{ji} \\ &+ t(P_{DA} + P_{PROC}) \leq e_i \quad \forall (i) \epsilon W \end{aligned} \tag{2.11}$$

Şekil 2.5: Tamsayı Programlama Modeli

Şekil (2.5)'de Tamsayı Programlama Modelinin denklemleri verilmiştir.

(2.7) kısıtında tüm veri akımlarının pozitif olduğunu, negatif akım olamayacağını belirtiyoruz.

(2.8) kısıtında ise düğümün kendi içerisinde akıma izin vermiyoruz.

(2.9) kısıtı anahtar paylaşma / paylaşmama durumuna göre iki düğüm arasındaki akımı kısıtlıyor. Eğer iki düğüm anahtar halkalarında en az bir ortak anahtara sahipse b değeri 1'e eşit oluyor ve düğümler birbirlerine paket yollayabiliyorlar. Eğer ortak bir anahtarları yoksa b değeri 0'a eşit oluyor ve aralarındaki akım da sıfıra eşit oluyor.

(2.10) kısıtında akım dengeleme denklemini görüyoruz. Bir düğüme gelen paket miktarı ve o düğümün ürettiği paket miktarı o düğümden çıkan paket miktarına

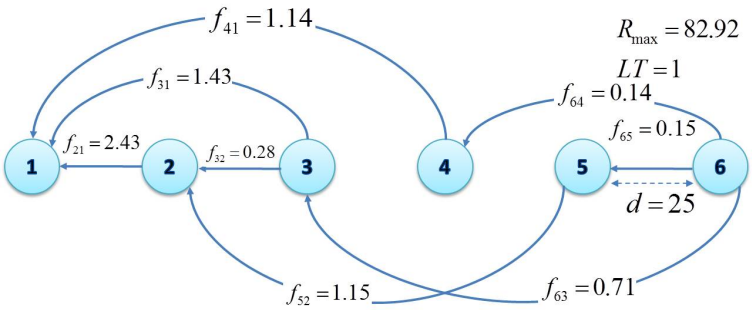
eşittir. Bu kısıt baz istasyonu hariç tüm düğümleri kapsıyor. Baz istasyonunu kapsamamasının nedeni, tüm veri paketlerinin baz istasyonunda son bulmasıdır.

(2.11) kısıtında baz istasyonu hariç her düğümün enerji kaynağı kısıtlıdır. Modelimizde her düğümün iki kalem pil (AA), yani 25 kJ kadar bir enerjiye sahip olduğunu varsaydık. Bu denklemde sırasıyla veri paketi iletimine, gelen veri paketleri için teyit paketi iletimine, gelen veri paketleri için veri paketlerini alırken harcanan enerjiye, alınan teyit paketlerine harcanan enerjiye, ve birim zamanda sabit enerji harcanan veri elde etme (algılama) ve işlemeye harcanan enerjinin toplamının düğümün toplam enerjisinden az olduğu gösterilmiştir.

3. ANALİZLER

3.1 Basit Örnekler

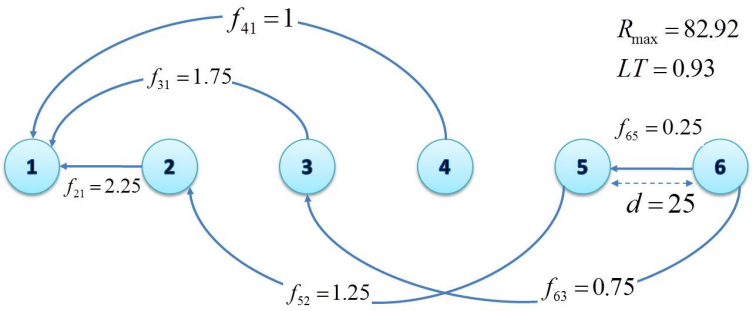
Şekil (3.1),(3.2) ve (3.3)'de oluşturduğumuz modeli basit örneklerle anlatıyoruz. Bu örnekta ağda 6 düğüm vardır ve ağ anahtar havuzu 10 anahtardan oluşmaktadır. Düğümler arası mesafe 25 metre olarak alınmıştır. Anahtar halka büyüklüğünün 10, 3 ve 1 olduğu durumlar için rastgele birer örnek oluşturulmuş ve şekillerde verilmiştir.



Şekil 3.1: Basit Örnek: Anahtar Kısıtının Olmadığı Durum

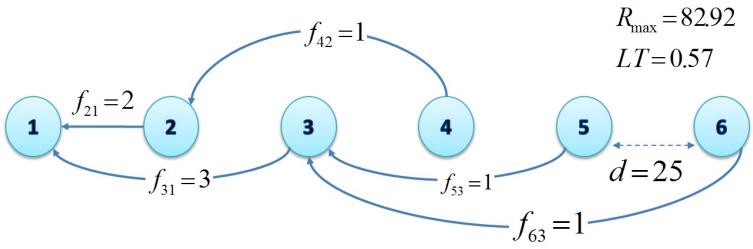
Şekil (3.1)'de anahtar kısıtının olmadığı durumda düğümler arası veri paketi akımlarının nasıl oluştuğunu görüyoruz. Düğümler istedikleri düğüm üzerinden baz istasyonuna veri aktarımı yapabilmektedir. Bu durumun yaşam süresini diğer durumlarla karşılaştırmak için birim zaman olarak kullandık. Yani bu durumun yaşam süresini 1 olarak kabul ettik.

Şekil (3.2)'de anahtar halka büyüklüğünü 3'e indirdik. Yani her bir düğüme 10 anahtardan oluşan anahtar havuzundan rastgele 3 anahtar seçerek anahtar



Şekil 3.2: Basit Örnek: Anahtar Halka Büyüklüğünün 3 Olduğu Durum

halkalarını oluşturmalarını sağladık. Bu durumda önceki durum gibi anahtar halkalarında tüm anahtarları bulundurmadıkları için bazı düğümler en az bir ortak anahtarlara sahip olamadılar. Dolayısıyla aralarındaki bağlantı koptu. Bu iletişimin kopmasıyla veri aktarımı olası eniyi halde kalamadı. Bağlantıların kopması dolayısıyla şekilde görülebileceği gibi ağ yaşam süresi 0.93'e indi (yani %7 azaldı). Kopan bağlantılara örnek vermek gerekirse mesela 6. düğüm ile 4. düğüm arasındaki ve 3. düğüm ile 2. düğüm arasındaki bağlantılar kopmuştur.



Şekil 3.3: Basit Örnek: Anahtar Halka Büyüklüğünün 1 Olduğu Durum

Şekil (3.3)'te anahtar halka büyüklüğünü 1'e indirdik. Şekil (3.2)'de olduğu gibi düğümler arasındaki bağlantıların ortak anahtara sahip olunamaması sonucu kopmasından dolayı ağ yaşam süresi kısıtsız hale göre %43 kayba uğrayıp 0.57'ye inmiştir. Ayrıca böyle bir durumda eğer 6. düğüm 5. ve 4. düğümlerle ortak anahtara sahip olamadığı gibi 3. düğümle de ortak bir anahtara sahip olmasaydı ağ yaşam süresi sıfıra inecekti. Çünkü bir düğümün yapısı itibariyle gönderebileceği en uzak mesafe 82.92 metredir. 2. Düğüm ise 6. düğüme 100 metre mesafede olduğu için, 6. düğüm en azından 5.,4. veya 3. birisiyle ortak bir anahtar paylaşmak durumundadır.

3.2 Simülasyon Verileri

Şekil (3.4),(3.5) ve (3.6)'da anahtar halka büyüklüğüne göre yaşam süresi azalma yüzdeleri hesaplanmış ve bu veriler grafikler halinde sunulmuştur.

Şekil (3.7)'de ise anahtar halka büyüklüğüne ve anahtar havuz büyüklüğüne göre oluşan anahtar paylaşma olasılığına göre yaşam süresi azalma yüzdeleri hesaplanmış ve bu veriler grafikler halinde sunulmuştur.

Son olarak Şekil (3.8)'de 100, 200 ve 300 düğüm için toplamda aynı alanı kapsayan bir sistemde (yani 100 düğüm için düğüm başına $150m^2$, 200 düğüm için düğüm başına $75m^2$ ve 300 düğüm için düğüm başına $50m^2$) sonuçlar hesaplanmış ve grafik halinde verilmiştir.

Sonuçlar ağ yaşam süresindeki azalmanın doğrudan anahtar halka büyüklüğüne bağlı olmadığı, ağ yaşam süresinin iki düğümün birbirine bağlanabilirliğine göre değiştiği, bunun da tekil olarak anahtar halka büyüklüğüne göre değil, aynı zamanda anahtar havuz büyüklüğüne bağlı bir değer olduğunu göstermiştir. Sonuç olarak ağ yaşam süresinde azalmalar olmaması için anahtar paylaşma olasılığının belli bir değerin üstünde olması gerektiği gösterilmiştir.

5000, 10000 ve 15000 anahtar havuz büyüklüğüne göre, anahtar halka büyüklükleri 0'dan 200'e kadar 5'er 5'er büyüterek sonuçlar aldık. Alınan sonuçlarda anahtar halka büyüklüğünün 200'den 75'e kadar (Anahtar havuz büyüklüğünün 15000 olduğunda anahtar paylaşma olasılığı 0.314) ağ yaşam yaşam süresinde ciddi azalmalar olmazken, sonrasında ciddi azalmalar görülmüştür. Bundan dolayı 75 anahtardan daha büyük durumlar için sonuçlar grafiklerde gösterilmemiştir.

3.2.1 Anahtar Halka Büyüklüğüne Göre

3.2.1.1 100 Düğüm İçin

Şekil (3.4)'de 100 düğüm için anahtar halka büyüklüğüne göre yaşam süresindeki azalma yüzdesi gösterilmiştir. Anahtar havuz büyüklükleri 5000, 10000 ve 15000'dir. Anahtar havuz büyüklükleri arttıkça grafik şeklini koruyarak sağa doğru genişlemektedir.

Düğümler baz istasyonu hariç birbiriyle görüşemezken ağ yaşam süresindeki düşüş yüzdesi $50m^2$ için 3.08, $100m^2$ için 12.88, $200m^2$ için 26.95'tir. H=15000 ve AHB=75 için (KSP=0.314) ağ yaşam süresindeki düşüş yüzdesi $50m^2$'de 0.42, $100m^2$'de 0.9 ve $200m^2$'de 1.37'dir.

100 düğüm için alınan sonuçlarda kırılma noktaları H=5000 için AHB=35 (KSP=0.219), H=10000 için AHB=50 (KSP=0.222), H=15000 için AHB=60 (KSP=0.214) olmak üzere anahtar paylaşma olasılıklarına göre neredeyse aynıdırlar. Bu kırılma noktalarından anahtar halka büyüklükleri bir parça dahi küçülse ağ yaşam süresinde ciddi azalmalar olmaktadır. Örneğin H=5000 ve AHB=35 için $50m^2$'de 1.04, $100m^2$'de 2.52 ve $200m^2$'de 3.35 iken, anahtar halka büyüklüğü 5 azaltıldığında (AHB=30) ağ yaşam süresindeki azalmalar $50m^2$'de 1.82'e, $100m^2$'de 5.67'e ve $200m^2$'de 7.94'e çıkmıştır.

Ağ yaşam süresindeki azalmalar H=5000 için AHB=15'te (KSP=0.044), H=10000 için AHB=20'de (KSP=0.039) ve H=15000 için AHB=25'te (KSP=0.041) doyuma ulaşmış ve sabit kalmıştır.

3.2.1.2 200 Düğüm İçin

Şekil (3.5)'de 200 düğüm için anahtar halka büyüklüğüne göre yaşam süresindeki azalma yüzdesi gösterilmiştir. Anahtar havuz büyüklükleri 5000, 10000 ve 15000'dir. Anahtar havuz büyüklükleri arttıkça grafik şeklini koruyarak sağa doğru genişlemektedir. Düğümleri konuşlandırırken düğüm başına alan modeli kullanıldığı için, 200 düğümde düğüm başına $200m^2$'lik durumda genel bağlanabilirliğin yitirildiği durumlar oluşmuştur. Çünkü iletişim modelinde bir düğümün erişebileceği en uzak mesafe 82.92 metre iken, en uzaktaki düğümlerin baz istasyonuyla arasındaki mesafe daha uzun olunca ve ortak anahtar yokluğu sebebiyle aradaki düğümlerden veri aktarımı da yapamadıkları için baz istasyonuna ulaşamamaktadırlar. $200m^2$ için bağlantıların koptuğu noktalar H=5000 için AHB=20 (KSP=0.077), H=10000 için AHB=30 (KSP=0.086), H=15000 için AHB=35'dir (KSP=0.079).

Düğümler baz istasyonu hariç birbiriyle görüşemezken ağ yaşam süresindeki düşüş yüzdesi $50m^2$ için 14.4, $100m^2$ için 28.89'dur. H=15000 ve AHB=75 için (KSP=0.314) ağ yaşam süresindeki düşüş yüzdesi $50m^2$'de 0.18, $100m^2$'de 0.47 ve $200m^2$'de 0.66'dır.

200 düğüm için alınan sonuçlarda kırılma noktaları H=5000 için AHB=30 (KSP=0.166), H=10000 için AHB=40 (KSP=0.148), H=15000 için AHB=50 (KSP=0.154) olmak üzere anahtar paylaşma olasılıklarına göre neredeyse aynıdırlar. Bu kırılma noktalarından anahtar halka büyüklükleri bir parça dahi küçülse ağ yaşam süresinde ciddi azalmalar olmaktadır. Örneğin H=5000 ve AHB=30 için $50m^2$'de 0.9, $100m^2$'de 1.88 ve $200m^2$'de 2.01 iken, anahtar halka büyüklüğü 5 azaltıldığında (AHB=25) ağ yaşam süresindeki azalmalar $50m^2$'de 2.8'e, $100m^2$'de 3.82'e ve $200m^2$'de 4.09'e çıkmıştır.

Ağ yaşam süresindeki azalmalar H=5000 için AHB=10'te (KSP=0.02), H=10000 için AHB=15'de (KSP=0.023) ve H=15000 için AHB=20'te (KSP=0.026) doyuma ulaşmış ve sabit kalmıştır.

3.2.1.3 300 Düğüm İçin

Şekil (3.6)'da 300 düğüm için anahtar halka büyüklüğüne göre yaşam süresindeki azalma yüzdesi gösterilmiştir. Anahtar havuz büyüklükleri 5000, 10000 ve 15000'dir. Anahtar havuz büyüklükleri arttıkça grafik şeklini koruyarak sağa doğru genişlemektedir. Düğümleri konuşlandırırken düğüm başına alan modelini kullanıldığı için, 300 düğümde düğüm başına $100m^2$ ve $200m^2$'lik durumda genel bağlanabilirliğin yitirildiği durumlar oluşmuştur. Çünkü iletişim modelinde bir düğümün erişebileceği en uzak mesafe 82.92 metre iken, en uzaktaki düğümlerin baz istasyonuyla arasındaki mesafe daha uzun olunca ve ortak anahtar yokluğu sebebiyle aradaki düğümlerden veri aktarımı da yapamadıkları için baz istasyonuna ulaşamamaktadırlar. $100m^2$ için bağlantıların koptuğu noktalar H=5000 için AHB=15 (KSP=0.044), H=10000 için AHB=20 (KSP=0.039), H=15000 için AHB=25'dir (KSP=0.041). $200m^2$ için bağlantıların koptuğu noktalar H=5000 için AHB=20 (KSP=0.077), H=10000 için AHB=25 (KSP=0.061), H=15000 için AHB=35'dir (KSP=0.079).

Düğümler baz istasyonu hariç birbiriyle görüşemezken ağ yaşam süresindeki düşüş yüzdesi $50m^2$ için 17.32'dir. H=15000 ve AHB=75 için (KSP=0.314) ağ yaşam süresindeki düşüş yüzdesi $50m^2$'de 0.09, $100m^2$'de 0.42 ve $200m^2$'de 0.57'dir.

300 düğüm için alınan sonuçlarda kırılma noktaları H=5000 için AHB=25 (KSP=0.118), H=10000 için AHB=35 (KSP=0.116), H=15000 için AHB=40 (KSP=0.101) olmak üzere anahtar paylaşma olasılıklarına göre neredeyse aynıdırlar. Bu kırılma noktalarından anahtar halka büyüklükleri bir parça dahi küçülse ağ yaşam süresinde ciddi azalmalar olmaktadır. Örneğin H=5000 ve AHB=25 için $50m^2$'de 1.14, $100m^2$'de 1.89 ve $200m^2$'de 4.92 iken, anahtar halka büyüklüğü 5 azaltıldığında (AHB=20) ağ yaşam süresindeki azalmalar $50m^2$'de 3.41'e, $100m^2$'de 3.79'e ve $200m^2$'de 10.22'ye çıkmıştır.

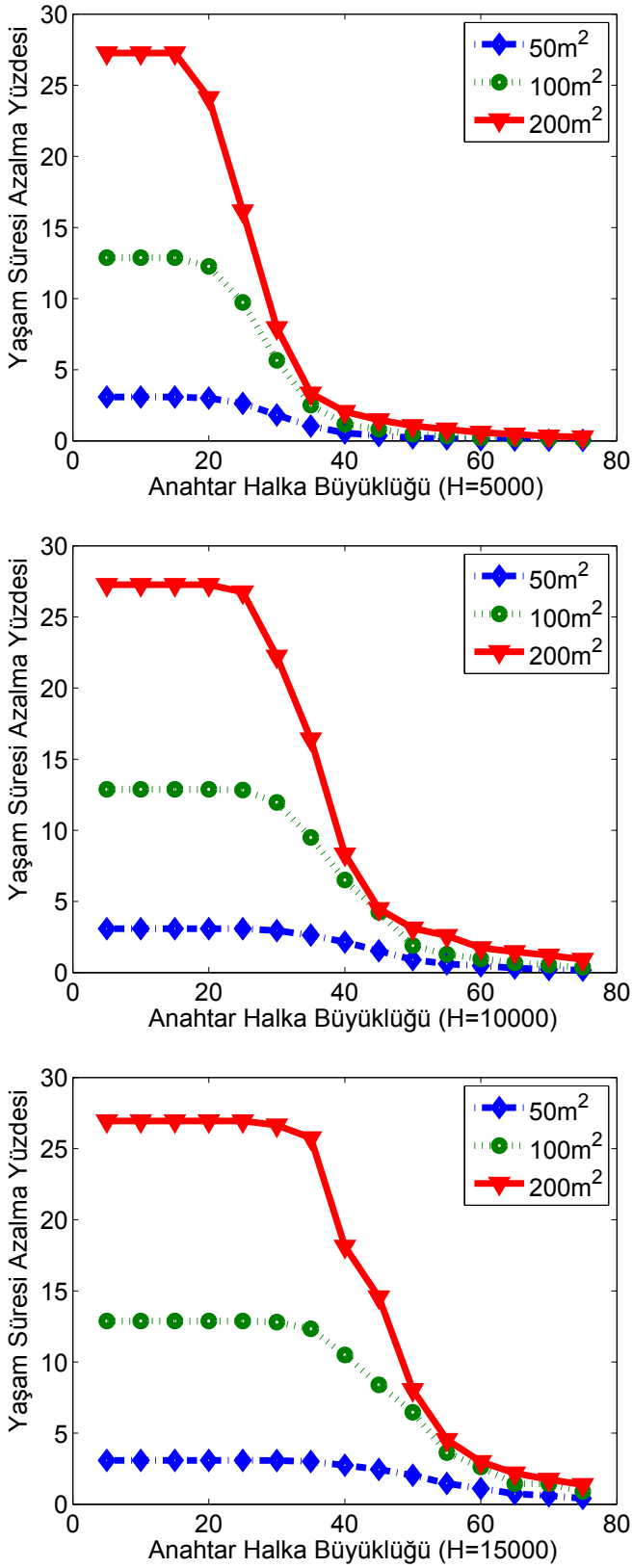
Ağ yaşam süresindeki azalmalar H=5000 için AHB=10'te (KSP=0.02), H=10000 için AHB=15'de (KSP=0.023) ve H=15000 için AHB=20'te (KSP=0.026) doyuma ulaşmış ve sabit kalmıştır.

3.2.2 Anahtar Paylaşma Olasılığına Göre

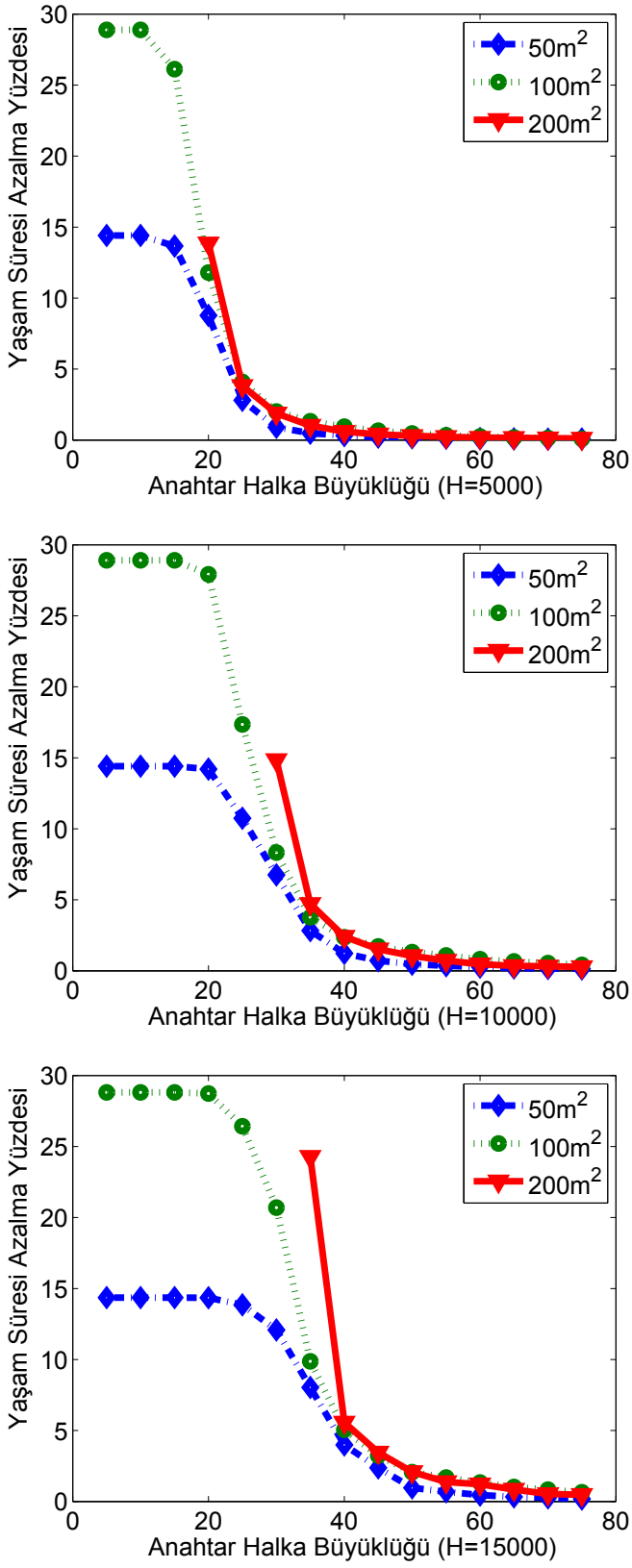
Anahtar halka büyüklüğüne göre yapılan simülasyon sonuçlarına göre ağ yaşam süresindeki azalmanın başlangıç, kırılma ve doyum noktaları anahtar havuz büyüklüğüne göre değişik anahtar halka büyüklüğüne sahiptirler. Ancak bu noktaların halka büyüklükleri için farklı havuz büyüklüklerine sahip de olsa anahtar paylaşma olasılık değerleri birbirine çok yakındır. Şekil (3.7)'de anahtar paylaşma olasılığına göre ağ yaşam süresindeki azalma yüzdesi verilmiştir. Bu grafikler 5000, 10000 ve 15000'lik havuz büyüklükleri için alınan sonuçların anahtar halka büyüklüğünün anahtar paylaşma olasılıklarına göre denk gelen değerlerin kombinasyonudur.

Grafiklerde görülen düğüm sayısı arttıkça daha düşük anahtar paylaşma olasılığına kadar değişime uğramayan ağ yaşam süresi, belli bir noktadan sonra çok daha ciddi kayıplara uğramaktadır. Ayrıca bu grafikler ağ yaşam süresindeki kaybın anahtar halka büyüklüğüne değil, anahtar paylaşma olasılığına bağlı olduğunu göstermektedir.

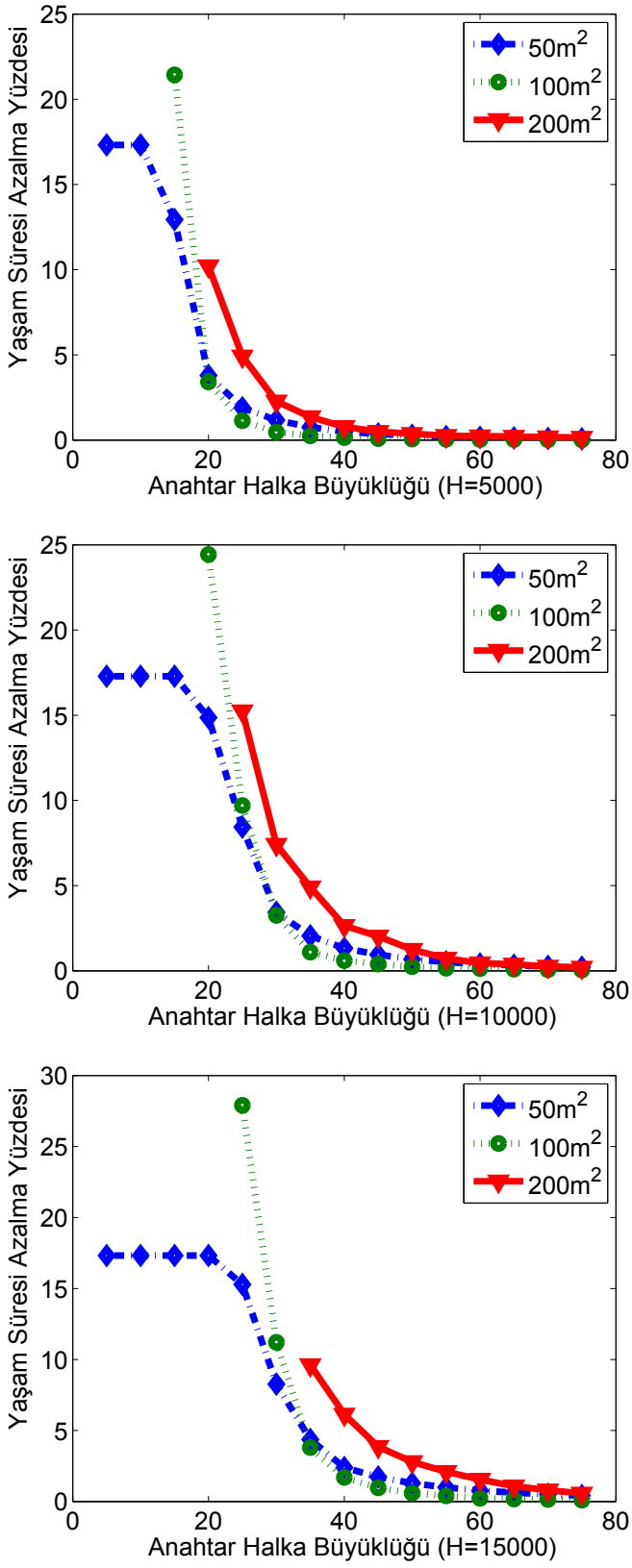
Şekil (3.8)'de 100, 200 ve 300 düğüm için toplamda aynı alanı kapsayan bir sistemde (yani 100 düğüm için düğüm başına $150m^2$, 200 düğüm için düğüm başına $75m^2$ ve 300 düğüm için düğüm başına $50m^2$) sonuçlar hesaplanmıştır. Düğüm sayısı daha azken önce daha büyük anahtar paylaşma olasılıklarında başlayan yaşam süresindeki azalma, daha büyük düğüm sayılarına göre daha az bir noktada doyuma ulaşmaktadır. 100 düğüm için KSP=0.5'te yaşam süresindeki azalma 0.5 civarındayken, 200 düğüm için 0.05, 300 düğüm için ise 0'a yakın bir değerdir. Kırılma noktası 100 düğüm için KSP=0.23 civarına denk gelirken, 200 düğüm için KSP=0.15, 300 düğüm için KSP=0.11'e denk gelmektedir. Doyum noktasında ise yaşam süresindeki kayıp yüzdesi 100 düğüm için %15 civarı, 200 düğüm için %16 civarı, 300 düğüm için %17.5 civarındadır.



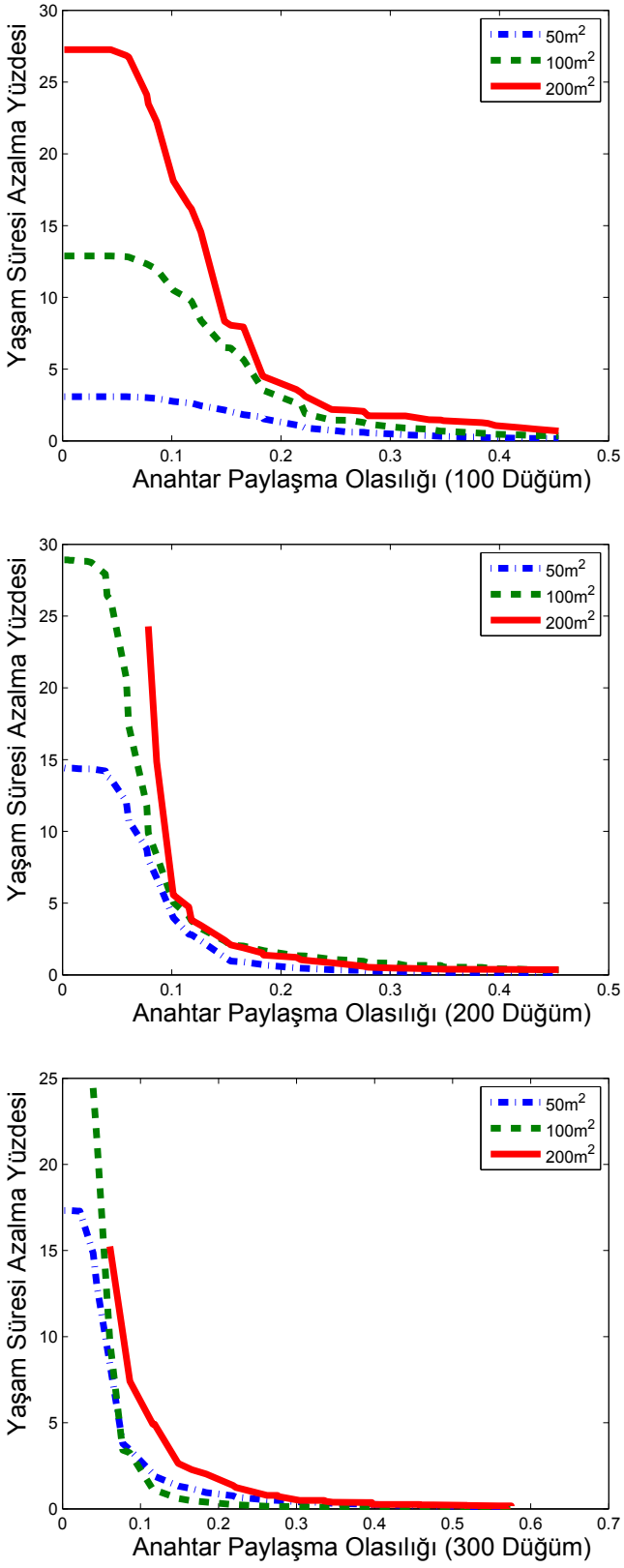
Şekil 3.4: Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (100 Düğüm)



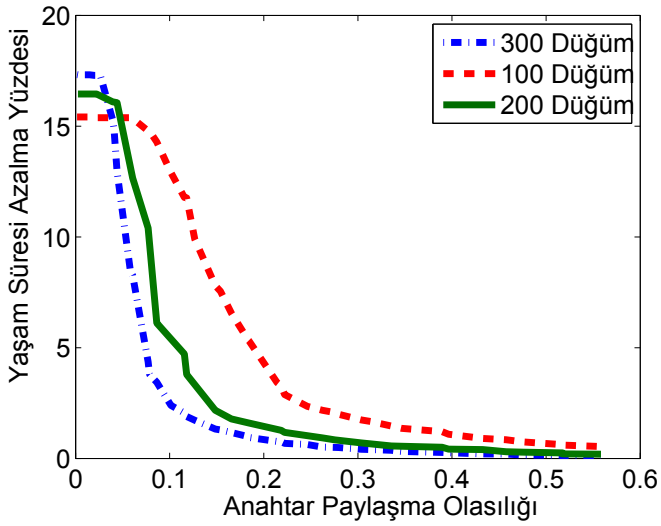
Şekil 3.5: Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (200 Düğüm)



Şekil 3.6: Anahtar Halka Büyüklüğüne Göre Yaşam Süresi Azalma Yüzdesi (300 Düğüm)



Şekil 3.7: Anahtar Paylaşma Olasılığına Göre Yaşam Süresi Azalması



Şekil 3.8: 100, 200 ve 300 Düğümün Aynı Alanda Anahtar Paylaşma Olasılığına Göre

4. SONUÇLAR

Bu çalışmada gizli anahtar şifrelemesinde anahtar havuzu ve anahtar halka büyüklüğünün ağ yaşam süresine etkileri incelenmiştir. Dairesel topolojide düğüm başına farklı alanlar ve farklı düğüm sayıları kullanılarak yapılan incelemelerde ağ yaşam süresinde azalma olmaması için gerekli parametreler elde edilmiştir.

Çalışmada elde edilen sonuçlara göre, anahtar havuzu ve anahtar halkası büyüklüğünün doğrudan kendi başlarına ağ yaşam süresine etkileri yoktur. Bu ikilinin beraber oluşturduğu anahtar paylaşma olasılığı, dolayısıyla iki düğüm arasındaki bağlanabilirlik durumuna bağlı olarak ağ yaşam süresindeki düşüş belirlenmiştir.

Ayrıca düğüm sayısına bağlı olarak ağ yaşam süresindeki düşüşün kırılma noktası ve doyuma ulaştığındaki ağ yaşam süresindeki azalma yüzdesinin değiştiği ortaya çıkmıştır. Düğüm sayısı arttıkça daha düşük anahtar paylaşma olasılıklarına dayanabilen ağ yaşam süresi, kırılma noktasından sonra ise çok daha dik bir şekilde ağ yaşam süresini kaybetmektedir.

Verilere göre ağ yaşam süresindeki kayıp anahtar paylaşma olasılığı 0.044 (H=5000 AHB=15) iken (100 düğüm için) %26.5'e kadar çıkabilmektedir. Ancak anahtar paylaşma olasılığı 0.3'e (H=5000 AHB=45) kadar çıkarılırsa ağ yaşam süresindeki kayıp (100 düğüm için) %1'in altına inmektedir.

Sonuç olarak ağ yaşam süresi anahtar paylaşma olasılığına, düğüm sayısına ve düğüm başına alana göre değişir. Düğüm başına alan artarsa anahtar paylaşma olasılığı da arttırılmalıdır ki düğümün iletişim kurabileceği alandaki bağlanabileceği düğüm sayısı değişmesin. Eğer alandaki düğüm sayısı artırılırsa yaşam süresinden kaybetmeden bellekten kazanmak için daha az anahtar kullanılabilir.

Kaynakça

[1] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, (New York, NY, USA), pp. 41–47, ACM, 2002.

[2] K. Bilinska, M. Filo, and R. Krystowski, "Mica2 http://wwwpub.zih.tu-dresden.de/ dargie/wsn/slides/students/mica.ppt," 2007.

[3] W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*. Wireless Communications and Mobile Computing, Wiley, 2010.

[4] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*. Wiley, 2007.

[5] C.-Y. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[6] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *Wireless Communications, IEEE Transactions on*, vol. 1, pp. 660 – 670, oct 2002.

[7] Z. Cheng, M. Perillo, and W. Heinzelman, "General network lifetime and cost models for evaluating sensor network deployment strategies," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 4, pp. 484–497, 2008.

[8] B. Tavli, M. Akgun, and K. Bicakci, "Impact of limiting number of links on the lifetime of wireless sensor networks," *Communications Letters, IEEE*, vol. 15, no. 1, pp. 43–45, 2011.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications," *Computers, IEEE Transactions on*, vol. PP, no. 99, p. 1, 2012.

[10] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 1, pp. 4 vol. (xxxv+2866), march 2004.

[11] Z. yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 4, pp. 1915 – 1920 Vol. 4, march 2005.

[12] J. Chinneck, *Practical Optimization: A Gentle Introduction*. Carleton University, 2003.

[13] "Mathworks' matlab, http://www.mathworks.com/products/matlab."

[14] "Gams, general algebraic modeling system, http://www.gams.com/."

[15] E. Specht, "The best known packings of equal circles in the unit circle. http://hydra.nat.uni-magdeburg.de/packing/," 2010.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: ÇİFTLER, Bekir Sait
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 16.10.1989 İskenderun
Medeni hali	: Evli
Telefon	: 05556461988
Faks	:
e-mail	: bsciftler@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Orta Doğu Teknik Üniversitesi	2011
Yüksek Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2013

İş Deneyimi

Yıl	**Yer**	**Görev**
2011-2013	TOBB Ekonomi ve Teknoloji Üniversitesi	Araştırma Görevlisi

Yabancı Dil

İngilizce (Çok iyi)
Arapça (Az)