KABLOSUZ ALGILAYICI AĞLARDA İNKÂR-EDEMEME MEKANİZMALARININ VE BAZ İSTASYONU GÖZLEMLENEMEZLİĞİNİN SAĞLANMASININ AĞ ÖMRÜNE OLAN ETKİLERİNİN İNCELENMESİ

İBRAHİM ETHEM BAĞCI

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

NİSAN 2011

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Erdoğan Doğdu

Anabilim Dalı Başkanı

İbrahim Ethem BAĞCI tarafından hazırlanan KABLOSUZ ALGILAYICI AĞLARDA İNKÂR-EDEMEME MEKANİZMALARININ VE BAZ İSTASYONU GÖZLEMLENEMEZLİĞİNİN SAĞLANMASININ AĞ ÖMRÜNE OLAN ETKİLERİNİN İNCELENMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Kemal Bıçakcı	Doç. Dr. Bülent Tavlı
Tez Danışmanı	2. Tez Danışmanı

Tez Jüri Üyeleri

Başkan: Yrd. Doç. Dr. M. Fatih Demirci _____

Üye : Doç. Dr. Kemal Bıçakcı _____

Üye : Doç. Dr. Bülent Tavlı _____

Üye : Yrd. Doç. Dr. Hakan Gültekin _____

Üye : Yrd. Doç. Dr. Tansel Özyer _____

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.

……..……..

İbrahim Ethem Bağcı

Üniversitesi : TOBB Ekonomi ve Teknoloji Üniversitesi

Enstitüsü : Fen Bilimleri

Anabilim Dalı : Bilgisayar Mühendisliği

Tez Danışmanı : Doç. Dr. Kemal Bıçakcı, Doç. Dr. Bülent Tavlı

Tez Türü ve Tarihi : Yüksek Lisans – Nisan 2011

İbrahim Ethem Bağcı

KABLOSUZ ALGILAYICI AĞLARDA İNKÂR-EDEMEME MEKANİZMALARININ VE BAZ İSTASYONU GÖZLEMLENEMEZLİĞİNİN SAĞLANMASININ AĞ ÖMRÜNE OLAN ETKİLERİNİN İNCELENMESİ

ÖZET

Enerji kısıtlı kablosuz algılayıcı ağlarda gizlilik, bütünlük, doğrulama ve inkâr-edememe güvenlik servislerinin ilk üçü genellikle ya simetrik şifreleme ile ya da açık anahtar ve gizli anahtar algoritmalarının birlikte kullanılması ile gerçekleştirilmiştir. İnkâr-edememe, sadece açık anahtar algoritmaları ile gerçekleştirilen dijital imzalar ile yerine getirildiği için ayrı bir karaktere sahiptir. Bu yüzden bu servisin uygulanabilirliğinin kablosuz algılayıcı ağlar için genellikle mümkün olmadığı düşünülmüştür. Bu tez çalışmasının ilk kısmında inkâr-edememe servisinin gerçekleştirilmesinin kablosuz algılayıcı ağların ağ ömrüne olan etkilerini incelemek için doğrusal programlama modeli geliştirildi. RSA, ECDSA ve tek-zamanlı imzalama (OTS) algoritmaları kullanıldı ve bu algoritmalar çeşitli topolojilerde ve çalıştırma koşullarında karşılaştırıldı. Çalışmalar, uygun algoritma seçildiğinde dijital imzaların kullanılmasıyla meydana gelen ağ ömründeki azalmanın 80-bit ve 112-bit güvenlik seviyeleri için sırasıyla %10 ve %20'den daha az olabileceğini gösterdi.

Kablosuz algılayıcı ağlarda baz istasyonuna yapılan bir saldırı bütün ağı kullanışsız hale getirilebilir. Bu yüzden belirli durumlarda baz istasyonunun fiziksel konumunu gizlemek gerekebilir. Bundan önce bu problem üzerinde çalışanlar, tüm ağda global bilgiye sahip olan bir saldırganın varlığını göz önüne almamışlardır. Bu tez çalışmasının ikinci kısmında basit bir çözüm olarak, sahte baz istasyonları oluşturarak bir düğümün verilerinin sadece baz istasyonuna değil, aynı zamanda diğer düğümlere de gönderilmesi düşünüldü. Daha az masraflı alternatif bir çözüm bütün düğümlerin gelen ve giden verilerinin miktarının eşitlenmesi ile sağlandı. Bu sayede tüm ağdaki iletişimin gözlemlenmesine rağmen baz istasyonunun konumu hakkında bir bilginin elde edilememesi mümkün oldu. Bu tez çalışmasının ikinci kısmında doğrusal programlama modelleri sayesinde bahsedilen bu iki çözümün ağ ömrüne olan etkileri incelendi. Yaptığımız analiz ile baz istasyonu

gözlemlenemezliğini sağlamanın ağ ömrüne olan etkisinin dikkate değer olduğu ve en iyi ihtimalle ağ ömründe yarı yarıya düşüş gerçekleştiği sonucuna ulaşılmıştır.

Anahtar Kelimeler: Kablosuz algılayıcı ağlar, İnkâr-edememe, Ağ ömrü, Doğrusal programlama, Konum mahremiyeti, Sayısal imzalar

University : **TOBB University of Economics and Technology**

Institute : **Institute of Natural and Applied Sciences**

Science Programme : **Computer Engineering**

Supervisor : **Assoc. Prof. Kemal Bıçakcı, Assoc. Prof. Bülent Tavlı**

Degree Awarded and Date : **M. Sc. – April 2011**

İbrahim Ethem BAĞCI

THE IMPACT OF NON-REPUDIATION AND PRESERVING PERFECT SINK UNOBSERVABILITY ON THE LIFETIME OF WIRELESS SENSOR NETWORKS

ABSTRACT

In energy-limited wireless sensor networks, first three of confidentiality, integrity, authentication and non-repudiation security services are typically implemented by either using pure symmetric crypto primitives or with a hybrid public key and secret key algorithm combination. Non-repudiation requirement has a unique characteristic in the sense that it can be met only by digital signatures which is usually implemented with public key algorithms. Hence this service has been traditionally considered to be infeasible in wireless sensor networks. In the first part of this thesis, we construct a linear programming framework to analyze the impact of implementing a non-repudiation service on the lifetime of wireless sensor networks. Feeding the model with published results of RSA and ECDSA algorithms and parameters derived for a modified communication-efficient version of one-time signatures, we compare these algorithms with respect to their effect on network lifetime in different topologies and operating conditions. We have shown that with proper algorithm selection and for a wide range of network parameters, the lifetime reduction due to the utilization of digital signatures can be less than 10 % and 20 % for security levels of 80-bit and 112-bit respectively compared to a network not utilizing digital signatures.

In wireless sensor networks an attack to the base station (sink) can render the whole network useless hence concealing the physical location of the sink may be necessary in certain circumstances. Previous studies addressing this challenging problem do not study in the presence of an eavesdropper who has global knowledge for the entire network. In the second part of this thesis, a naive solution is to employ fake sinks so that nodes send their data not only to the real sink but also other locations. An alternative solution with less overhead could be provided when all

nodes including base station equalize the values of their total incoming and outgoing flows as well as their energy expenditure. By this way, no information about sink location is revealed when all communication within the network is monitored. . In the second part of this thesis, through a Linear Programming framework we analyze and compare impact of these solutions on the lifetime of wireless sensor networks.

Key Words: Wireless Sensor Networks, Non-repudiation, Network lifetime, Linear programming, Location privacy, Digital signatures

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren çok değerli hocalarım Kemal Bıçakcı, Bülent Tavlı ve Hakan Gültekin'e, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, desteklerini esirgemeyen asistan arkadaşlarıma ve bana verdikleri manevi destekten dolayı ailem ve arkadaşlarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

KISALTMALAR

Kısaltmalar	Açıklama
KAA	Kablosuz Algılayıcı Ağlar – Wireless Sensor Networks
DP	Doğrusal Programlama – Linear Programming
RSA	Geliştiricileri Rivest, Shamir ve Adleman'nın baş harfini alan açık anahtar şifrelemesi
ECDSA	Eliptik Eğri Dijital İmzalama Algoritması - Elliptic Curve Digital Signature Algorithm
OTS	Tek-zamanlı Şifreleme – One-time Signature
Dİ	Dijital İmzalama – Digital Signature
SBİ	Sahte Baz İstasyonları
DA	Dengeli Akışla
GAMS	Matematiksel programlama ve en iyileme için kullanılan yüksek seviye modelleme sistemi - General Algebraic Modeling System

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
$E_{tx,ij}$	i düğümünden j düğümüne 1 bit veri iletimi için harcanan enerji
E_{rx}	1 bit veri almak için harcanan enerji
E_{Elec}	algılayıcı düğümünün elektronik donanımında harcanan enerji
ε_{amp}	alıcı-vericinin verimlilik faktörü
α	yol kayıp faktörü
d_{ij}	i düğümü ve j düğümü arasındaki mesafe
f_{ij}	i düğümünden j düğümüne veri akışı
f_{ij}^{k}	i düğümünden j düğümüne giden ve hedefinde k düğümü olan veri akışı
d_i	inkâr-edememe probleminde birim zamanda i düğümde üretilen veri miktarı
D	baz istasyonu gözlemlenemezliği probleminde birim zamanda bir düğümde üretilen veri miktarı
e_i	i düğümünün enerjisi
r	imzalama oranı
o_1	bir dijital imzalama algoritmasının imza boyu
o_2	bir dijital imzalama algoritmasının imzalama enerjisinin maliyeti

1. GİRİŞ

Bu tez çalışmamızda, kablosuz algılayıcı ağlarda (KAA) ortaya çıkan iki farklı problem üzerinde çalıştık. İlk kısımda inkâr-edememe mekanizmalarının ağ ömrüne olan etkilerini araştırdık. İkinci kısımda ise baz istasyonu gözlemlenemezliğinin ağ ömrüne olan etkilerini inceledik.

KAA'larda güvenlik araştırmaları, düşük maliyetli fakat karmaşık algoritmalardan [1],[2] daha çok enerji tüketen fakat daha standart açık anahtar algoritmalara yönelmiştir [3],[4]. Bazı bağımsız çalışmalar, şu an kullanılan algılayıcı ağlarda açık anahtar uygulamalarının enerji maliyetini ölçmüş ve bu uygulamalar eğer sık sık kullanılmazlarsa (örneğin sadece SSL tarzı uygulamalarda) ağ ömrüne olan etkilerinin kabul edilebileceğini söylemiştir [3],[4]. Bugün, daha karmaşık olan ID-tabanlı kriptografi dahi uygulanabilir durumdadır [5].

İnkâr-edememe, çok enerji gerektiren bir servis olduğu için kablosuz algılayıcı ağlardaki kullanımında ağ ömrüne olan etkisi önem kazanmaktadır. Kablosuz algılayıcı ağlarda inkâr-edememe mekanizmalarının kullanımının çok gerekli olmadığı görüşleri mevcuttur [1]. Bu görüşlere katılmakla birlikte, bazı uygulama alanlarında inkâr-edememe mekanizmalarının kullanımının önemli olduğunu düşünmekteyiz. Bu uygulamalara örnek olarak hız sınırını aşan araçların plaka numaralarının yakalanması ve rapor edilmesini [7], yetkisiz araç hareketlerini tespit edilmesini ve çalıntı araçların takip edilmesini [8], verebiliriz.

Bu noktada, algılayıcı verinin inkâr-edilememesinin ne demek olduğunu açıklamamız gerekiyor. Geleneksel olarak kaynağın inkâr-edilememesi, bir tarafın veriyi kasten imzalaması ve bu tarafın açık anahtarının bir açık anahtar sisteminde sertifikalanmasıyla sağlanır (dijital imzalama için 5. bölüme bakınız). Bu taraf, kendisinden başka biri bu geçerli imzayı atamayacağı için veriyi imzaladığını inkâr-edemez. Bir KAA uygulamasında inkâr etmeye aday bir kişi bir şey imzalamaz; fakat algılayıcı verinin bozulmadığını ve spesifik bir algılayıcıdan çıktığını inkâr eder. Güvenli zamanlama ve yer belirleme servisleri de kullanılarak, inkâr eden kişiye

karşı dijital bir kanıt olarak sunulan algılayıcı verinin spesifik bir algılayıcıdan çıkabilmesi, algılayıcı verinin inkâr-edilememesi demektir.

Birçok protokol tasarımcısı en önemli iki tasarım hedefi olarak enerji verimliliğinden ve ağ ömrünü maksimize etmekten bahseder. Literatürde ağ ömrünü uzatmak için geliştirilmiş işbirlikçi veri toplama teknikleri vardır (örneğin, [9]). Ama yine de en verimli algoritmayı kullanmanın maksimum ağ ömrünü otomatik olarak elde etmek olmadığının ayrımını da yaparlar [10]. Bu son husus sistem seviyesinde karmaşık bir sorundur ve en iyileme problemi olarak modellenmektedir.

KAA'larda inkâr-edememe problemi birçok yöne sahiptir ve geniş bir çalışma bizim inceleme alanımızın dışındadır. Bu tez çalışmasının ilk kısmında bizim amacımız aşağıdaki sorulara cevap vermektir:

1. Verilen bir ağ büyüklüğünde ve topolojide, bir uygulamanın inkâr-edememe talep etmesi durumunda ağ ömründe ne kadar bir düşüş beklenmektedir?

2. Verilen bir çalıştırma koşulu ve istenilen bir güvenlik seviyesinde, hangi dijital imzalama algoritması ağ ömrü maksimizasyonu için en iyi seçim olacaktır?

3. Verilen bir imzalama algoritmasının güvenlik seviyesinin mi yoksa ağ ömrüne olan etkisinin mi daha önemli olduğuna nasıl karar vereceğiz?

Bu sorulara cevap verebilmek için farklı imzalama algoritmalarının performans sonuçlarını kullanarak yapılan basit hesaplamalar yetmeyecektir. Örneğin, hangi algoritmanın en iyi olduğuna nasıl karar vereceğiz? Büyük boyutlu imza üreten fakat neredeyse enerji gerektirmeyen tek-zamanlı imzalar mı (OTS), yoksa küçük boyutlu fakat görece daha fazla enerji gerektiren ECDSA imzaları mı?

Tez çalışmamızın ikinci kısmında baz istasyonu gözlemlenemezliğinin ağ ömrüne olan etkilerini inceledik.

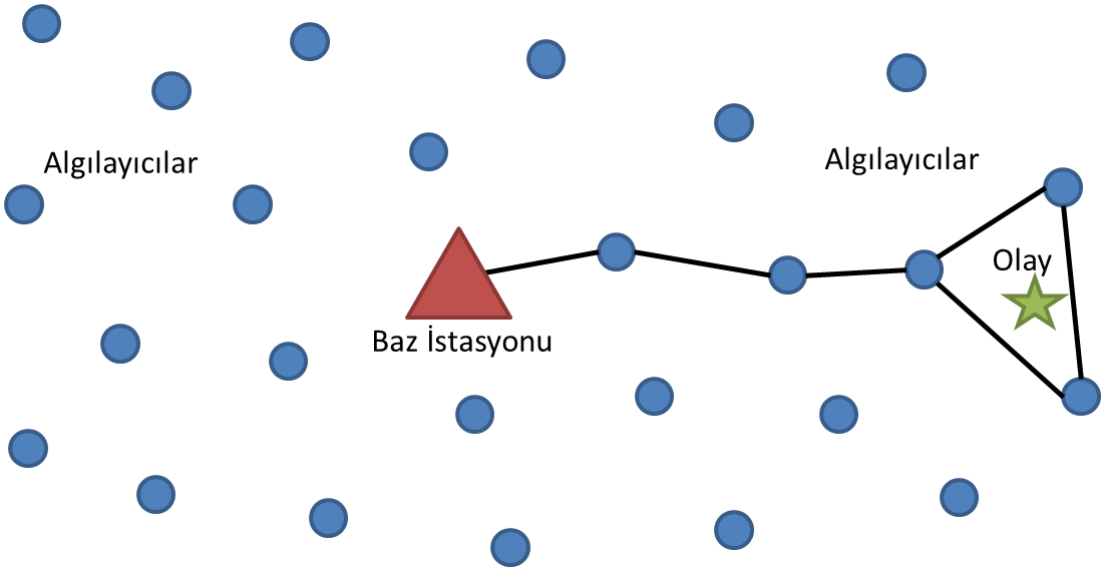
Konum mahremiyetini ihlâl etmeyi amaçlayan bir atağa karşı kriptografik çözümler tek başına yeterli olamazlar. Geleneksel çözümler (örneğin şifreleme), saldırganları şaşırtmak için sahte trafik üreten yaklaşımlarla beraber kullanılmalıdır. KAA'lar için düşünürsek problem iki kategoriye ayrılmaktadır: kaynağın konumunun mahremiyeti ve baz istasyonunun (hedefin) konumunun mahremiyeti.

Mahremiyeti arttırmaya yönelik bir tekniğin verimliliğini ölçmeden önce saldırganın yeteneklerini anlamamız gerekir. Global, pasif ve harici bir saldırganı içeren tehdit modeli gerçekçidir [20] ve önceki çalışmalarda bu bağlamda kaynağın konumunun mahremiyeti problemi araştırılmıştır [20],[18]. Diğer taraftan baz istasyonunun konumunun mahremiyeti problemi bu kuvvetli bağlam altında daha önceden incelenmemiştir. Örneğin, Deng ve arkadaşlarının çalışmasındaki [17] tehdit modelinde, saldırgan bütün bir ağ hakkında global bir bilgiye sahip değildir. Özellikle daha önceki çalışmalarda [20]'de verilen güçlü saldırgan modelindeki gibi bir durumda baz istasyonun konumunun mahremiyetini korumanın ağ ömrüne olan etkisini inceleyen bir çalışma yoktur. Bu tez çalışmasının ikinci kısmında baz istasyonunun mahremiyetini korumak için bir DP sistemimde iki farklı bakış açısı modelledik. Bu sistem ile ideal şartlar altında (başka bir değişle optimal yönlendirme ile) ağ ömrünün limitlerini inceledik ve gelecekteki global saldırgana karşı baz istasyonunu saklama amaçlı protokolleri tasarlayabilmek için temel sağladık.

Bu tez çalışmasında, iki ayrı araştırma konumuz için doğrusal programlama (DP) modelleri kullandık. Bu DP modeller sayesinde her çeşit protokol ve uygulama ayrıntılarından uzak durabileceğimiz bir oyun alanı elde edebiliyor ve en iyilenmiş ama erişilebilir ağ ayarlarında aradığımız sorulara cevap bulabiliyoruz. Bizim geliştirdiğimiz model, ağ ömrünü en iyileme problemlerinin diğer yönlerini analiz etmek için geliştirilmiş bilinen modellerle benzerlik göstermektedir [9],[10],[11].

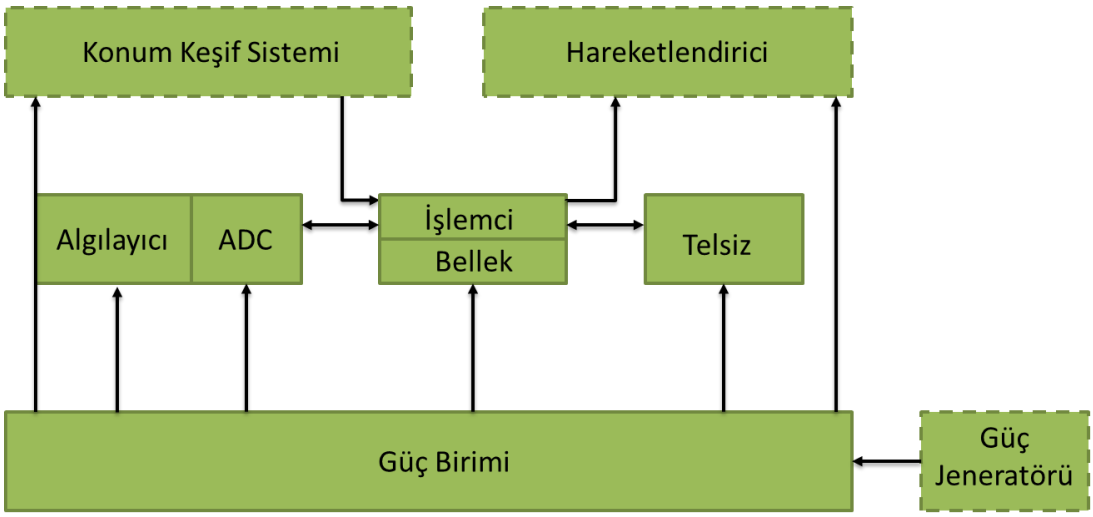
2. KABLOSUZ ALGILAYICI AĞLAR

Bir kablosuz algılayıcı ağ (KAA), bir bölgedeki fiziksel veya çevresel olayları izleyen küçük algılayıcı cihazlardan ve bu cihazların gözlemledikleri bilgileri gönderdiği ana bir merkezden oluşur [6]. Bu algılayıcılar, ortamdan sıcaklık, nem, araç hareketi, yıldırım durumu, basınç, vb. bilgileri algılar ve merkeze gönderir. KAA'lar günümüzde askeri, trafik, sağlık, çevre vb. uygulamalarda kullanılmaktadır. Şekil 1'de örnek bir KAA gösterilmiştir.



Şekil 1 – Örnek bir kablosuz algılayıcı ağ

Burada, algılayıcılar bir olayı gözlemler ve bu gözlemlerini baz istasyonuna iletirler. Baz istasyonu ise bu bilgileri ya kendisinde depolayabilir ya da başka bir yere kablolu ya da kablosuz bir şekilde gönderebilir.



Şekil 2 – Bir algılayıcının bileşenleri.

Bir KAA'da, uygulamaya göre az sayıda ya da çok sayıda algılayıcı bulunabilir. Algılayıcıların standartlaşmış bir büyüklükleri olmadığı gibi fiyatları da değişmektedir. Büyüklük ve fiyatlarındaki kısıtlar, enerji, bellek, hesaplama hızı ve iletişim bant genişliği gibi kaynak kısıtlarına yol açmaktadır.

KAA'larda bir protokol ya da algoritma tasarlamaya yardımcı olacak önemli tasarım faktörleri vardır. Bunları şöyle sıralayabiliriz [27]:

- *Hata Toleransı*: Bazı algılayıcı düğümler, güç eksikliği, fiziksel hasar ya da çevresel parazitlerden dolayı çalışamaz hale gelebilirler. Algılayıcı düğümlerin çalışamaz hale gelmesinin bütün bir algılayıcı ağın görevini sekteye uğratmaması gerekir.

- *Ölçeklenebilirlik*: Bir olayı gözlemlemek için yerleştirilmiş algılayıcı düğümlerinin sayısı yüzlerce veya binlerce olabilir. Uygulamaya göre bu sayı milyonları da bulabilir. Yeni tasarımlar bu kadar sayıdaki düğümlerle beraber çalışabilir olmalıdır.

- *Üretim Maliyeti*: KAA'ların çok sayıda algılayıcı düğümlerden oluşmasından dolayı bir algılayıcı düğümün maliyeti, tüm ağın maliyetini belirlemek için çok önemlidir.

- *Donanım Kısıtları*: Bir algılayıcı ağ, Şekil 2'de de gösterildiği gibi 4 ana bileşenden oluşmaktadır. Bunlar algılayıcı birim, işleme birimi, telsiz birimi ve güç birimidir. Ayrıca uygulamaya göre gerekirse konum keşif sistemi, güç jeneratörü ve hareketlendirici de bulunabilir. Bu birimler küçük bir kutuya sığdırılmak zorundadır.

- *Algılayıcı Ağ Topolojisi*: Yüzlerce veya binlerce algılayıcı düğüm, bir alana yerleştirilmektedir. Bu düğümlerin yoğun bir şekilde yerleştirilmesi, topoloji bakımının dikkatli bir şekilde yapılmasını gerektirir.

- *Ortam*: Algılayıcı düğümler ya olaya çok yakın bir yere ya da olayın direk içine yerleştirilirler. Dolayısıyla genellikle uzak bölgelerde çalışırlar. Bu bölge büyük bir mekanizmanın içi, bir okyanusun dibi, biyolojik ya da kimyasal olarak kirletilmiş bir alan veya bir savaş alanı olabilir.

- *İletim Ortamı*: Bir KAA'da algılayıcı düğümler birbirlerine kablosuz ortam ile bağlıdırlar. Bir ağın global bir şekilde kullanılmasını sağlamak için seçilen iletim ortamının dünya çapında mevcut olması gerekir.

- *Güç Tüketimi*: Mikro elektronik bir cihaz olan algılayıcı düğüm, limitli bir güç kaynağı ile donatılmıştır. Bazı uygulamalarda güç kaynaklarının ikmali mümkün olamamaktadır. Bu yüzden, algılayıcı düğümün ömrü pil ömrüne bağlı olmaktadır. Algılayıcı düğümün güç tüketimi algılama, iletişim ve veri işleme olmak üzere üç ana alana ayrılır.

3. DOĞRUSAL PROGRAMLAMA

Bir doğrusal program, bazı doğrusal kısıtlara bağlı olarak bir doğrusal fonksiyonu maksimize ya da minimize etmektir. Kısıtlar eşitlik veya eşitsizlik olabilir.

Elimizde m uzunluğunda $b=(b_1,...,b_m)^T$ vektörü, n uzunluğunda $c=(c_1,...,c_n)^T$ vektörü ve m x n boyutunda

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

matrisi olsun. O halde *standart maksimizasyon (en büyükleme) problemi*,

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \leq b_1$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \leq b_2$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \leq b_m$$

ve

$$x_1 \geq 0, x_2 \geq 0, \ldots, x_n \geq 0$$

kısıtlarına göre $c^T x = c_1 x_1 + ... + c_n x_n$ denklemini maksimize edecek n uzunluğunda $x=(x_1,...,x_n)^T$ vektörünü bulma şeklinde tanımlanır. Basit bir örneği şöyle verebiliriz:

Elimizde $x_1 + x_2$ toplamını

$$x_1 \geq 0, x_2 \geq 0$$

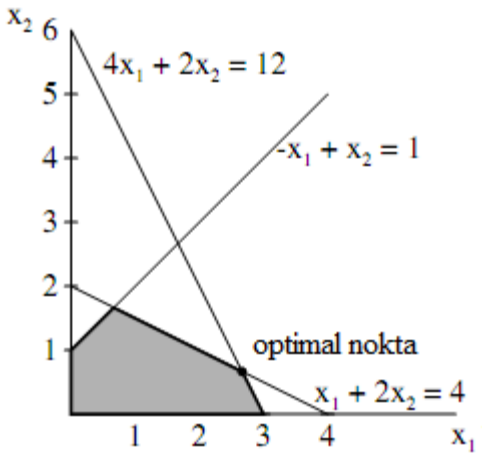
$$x_1 + 2x_2 \leq 4$$

$$4x_1 + 2x_2 \leq 12$$

$$-x_1 + x_2 \leq 1$$

kısıtlarına göre maksimize edecek x_1 ve x_2 sayılarını bulma problemi olsun. Bu problemde iki bilinmeyen (değişken) ve beş kısıt bulunmaktadır. Bütün kısıtlar eşitsizliktir ve her biri değişkenlerin doğrusal bir fonksiyonunu içeren doğrusal eşitsizliklerdir. İlk iki kısıt, $x_1 \geq 0, x_2 \geq 0$, özel kısıtlardır. Bu kısıtlara *işaret kısıtı* denir ve genellikle çoğu doğrusal programlama probleminde bulunur. Diğer kısıtlara *ana kısıtlar* denir. Maksimize (ya da minimize) edilecek fonksiyona *amaç fonksiyonu* denmektedir. Burada amaç fonksiyonu $x_1 + x_2$'dir.

Sadece iki tane değişkenimiz olduğu için bütün kısıtları sağlayan noktalar kümesini (buna kısıt kümesi denmektedir) bir grafikte gösterebiliriz, daha sonra da bu kümenin hangi noktasının amaç fonksiyonumuzu maksimize ettiğini bulabiliriz. Her bir kısıt, noktaların yarı düzlemleri ile sağlanır ve kısıtlar kümesi bütün yarı düzlemlerin kesişimidir. Kısıtlar kümesi Şekil 3'te gösterilmiştir.



Şekil 3 – Doğrusal programlamanın grafiksel gösterimi ve çözümü

Şekil 3'teki grafikte de görüldüğü gibi optimal noktamız, taralı bölgenin içinde (kısıtlar kümesi) kalan ve $x_1 + 2x_2 = 4$ ile $4x_1 + 2x_2 = 12$ eşitliklerinin kesişim noktaları olan $x_1 = 10/3$ ve $x_2 = 2/3$ noktasıdır.

Yukarıda, basit bir DP probleminin çözümünün nasıl elde edileceğini gösterdik. Daha karmaşık problemler için simplex metodu [16] gibi bilinen güçlü metotlar vardır; fakat bu metotlar bizim çalışma alanımız dışındadır. Biz, bu tez çalışmasında DP problemlerini çözmek için GAMS IDE 2.0.31.8 ara yüzü altında CPLEX 9 çözdürücüsünü kullandık [23].

4. SİSTEM MODELİ

Bu kısımda inkâr-edememe ve baz istasyonu gözlemlenemezliği problemleri için geliştirilen DP modelleri anlatılmaktadır.

4.1. İnkâr-edememe Problemi İçin Geliştirilen Sistem Modeli

İnkâr-edememe problemi için geliştirilen modelimizde her bir algılayıcı düğüm, birim zamanda aynı miktarda veri üretmektedir (düğüm-*i*, t zamanına kadar $s_i t$ birim veri üretmektedir). En iyileme problemimizin amacı, aşağıdaki kısıtlarla beraber t'yi (algılayıcı düğümlerin en küçük ömrü, KAA'ların ağ ömrünü inceleyen diğer çalışmalar tarafından kabul edilen bir tanımdır [9-12]) maksimize etmektir.

$$f_{ij} \geq 0 \tag{1.1}$$

$$\sum_j f_{ij} = s_i t + \sum_j f_{ji} \qquad i \in [2, N] \tag{1.2}$$

$$\sum_j f_{ij} = s_i t + s_i t \times r \times o_1 + \sum_j f_{ji} \qquad i \in [2, N] \tag{1.3}$$

$$\left\{ \left[E_{rx} \sum_j f_{ji} \right] + \left[\sum_j E_{tx,ij} f_{ij} \right] \right\} \leq e_i \qquad i \in [2, N] \tag{1.4}$$

$$\left\{\left[E_{rx}\sum_{j} f_{ji}\right]+\left[\sum_{j} E_{tx,ij} f_{ij}\right]+s_i t\times r\times o_2\right\}\le e_i \qquad i\in[2,N] \quad (1.5)$$

Birinci kısıt, bütün veri akışlarının pozitif olması gerektiğini söylemektedir. (f_{ij}, düğüm-*i*'den düğüm-*j*'ye olan akışı göstermektedir). İkinci kısıt, dijital imzalama (Dİ) uygulanmadığı durumlarda veri akış dengesini göstermektedir. Düğüm-*i*'de üretilen verilerinin ve düğüm-*i*'ye gelen verilerin toplamı, düğüm-*i*'den çıkan verilerin toplamına eşit olmak zorundadır. Düğüm indeksimiz 2'den başlamaktadır; çünkü 1. düğümü enerji kısıtı olmayan baz istasyonu olarak seçmekteyiz. Ağımızda baz istasyonu da dahil toplam *N* tane düğüm bulunmaktadır. Üçüncü kısıt, dijital imza uygulandığı durumlarda veri akış dengesini göstermektedir. Düğüm-*i*'den çıkan verilerin miktarı, (*i*) düğüm-*i*'de üretilen verilerin ve (*ii*) düğüm-*i*'ye gelen verilerin miktarıyla (*iii*) imza masrafının toplamına eşit olmak zorundadır. *t* zamanına kadar olan imzalama sayısını $s_i t\times r$ formülü ile buluyoruz. *r* terimi imzalama oranını belirtmektedir. o_1 terimi bir Dİ algoritmasının imza boyutunu, $s_i t\times r\times o_1$ terimi de *t* zamanına kadar düğüm-*i*'deki toplam imza masrafını belirtmektedir. Dördüncü kısıt, Dİ uygulanmadığı durumdaki enerji kısıtını göstermektedir. Kısıtımız, enerji yitiminin, düğüm-*i*'deki alma ve gönderme enerjilerinin, düğüm-*i*'deki enerji stokuyla limitli olduğunu söylemektedir. [12]'de belirtilen *boş alan* ya da *çoklu yol zayıflama kanalı* modelleri kullanılarak düğüm-*i*'deki akış başına düşen alma ve gönderme enerjilerini E_{rx} ve $E_{tx,ij}$ terimleriyle belirtebiliriz. Alma ve gönderme enerjileri şöyle modellenmektedir:

$$E_{rx}=E_{Elec}$$

$$E_{tx,ij}=E_{Elec}+\varepsilon_{amp} d_{ij}^{\alpha}$$

E_{Elec}, elektronik enerjisi, ε_{amp} ise amplifikatör enerjisidir. d_{ij}, düğüm-*i* ile düğüm-*j* arasındaki uzaklıktır. $E_{tx,ij}$, d_{ij}'in α kuvvetine göre artmaktadır, α ise kullanılan kanal modeline bağlıdır (*boş alan* modeli için 2, *çoklu yol zayıflama kanalı* modeli

için 4). Beşinci kısıt, Dİ kullanıldığı durumlardaki enerji kısıtını belirtmektedir. Enerji yitimi, alma enerjisini, gönderme enerjisini ve ek olarak da imzalama enerjisini içermektedir. Modelimizde dijital imzalar, algılayıcı düğümler arasında güvenli iletişim için değil, sadece inkâr-edememe servisinin sağlanabilmesi için kullanılmaktadır. Düğümler arası iletişim güvenliği için düşük maliyetli simetrik ya da melez çözümlerin olduğunu varsaymaktayız ve basitlik için bu çözümlerin enerji maliyetlerini önemsememekteyiz. Bu yüzden, imzalar sadece baz istasyonu tarafından doğrulanmaktadır ve algılayıcı düğümler imzaları doğrulamak için enerji harcamamaktadırlar. İmzalama işlemlerinin sayısını yine $s_i t \times r$ formülü ile bulmaktayız. o_2 terimi bir Dİ algoritmasının imzalama enerjisinin maliyetini, $s_i t \times r \times o_2$ terimi ise t zamanına kadar düğüm-i'deki imzalama işleminin toplam enerji yitimini vermektedir.

4.2. Baz İstasyonu Gözlemlenemezliği Problemi İçin Geliştirilen Sistem Modeli

Baz istasyonu gözlemlenemezliği problemi için geliştirilen modelimizde bir KAA'daki bütün düğümler birim zamanda aynı miktarda veri üretmektedirler ve amacımız üretilen veri miktarını (D) maksimize etmektir. Eğer bütün düğümlerin aynı miktarda veri ürettiklerini düşünürsek bu aynı zamanda ağ ömrünün maksimize edilmesi anlamına da gelmektedir. Bir KAA'nın ağ ömrünü ise bütün düğümlerinin çalışır durumda olduğu zaman şeklinde tanımlayabiliriz [10],[11]. Baz istasyonunun (i=1) konumunun saklanmadığı durumdaki temel şema DP modelimiz (2.1) – (2.3) kısıtları ile formülleştirilmiştir.

$$f_{ij} \geq 0 \tag{2.1}$$

$$\sum_j f_{ij} = D + \sum_j f_{ji} \qquad i \in [2, N] \tag{2.2}$$

$$\left\{ \left[E_{rx} \sum_j f_{ji} \right] + \left[\sum_j E_{tx,ij} f_{ij} \right] \right\} \leq e_i \qquad i \in [2, N] \tag{2.3}$$

Birinci kısıt bütün veri akışlarının pozitif olduğunu göstermektedir (f_{ij} düğüm-*i*'den düğüm-*j*'ye olan veri akışını göstermektedir). İkinci kısıt veri akış dengesini göstermektedir. Birinci düğümün baz istasyonu olduğu *N* düğümlü bir KAA'da, baz istasyonu hariç ($i \neq 1$) bütün düğümlerde üretilen veri miktarı ve düğüme gelen veri miktarı, düğümden gönderilen veri miktarına eşittir. Üçüncü kısıt enerji kısıtıdır. Bir düğümün veri göndermeye ve almaya harcadığı toplam enerji, düğümde depolanan enerji ile kısıtlıdır. $E_{tx,ij}$ ve E_{rx} terimleri inkâr-edememe problemi için geliştirdiğimiz modeldeki terimlerle aynıdır. İnkâr-edememe probleminden farklı olarak α=4 durumları için inceledik.

(2.4) – (2.7) kısıtları bizim *sahte baz istasyonları* (*SBİ*) çözümü diye adlandırdığımız problemi formülleştirir. Bu probleme bu ismi vermemizin sebebi problemimizde baz istasyonu da dahil tüm düğümlerin verileri (baz istasyonu da veri üretir) tek bir yere gönderilmek yerine tüm düğümlere gönderilir. Bu yüzden tüm düğümler baz istasyonu gibi davranır. Gerçek baz istasyonu her zaman olduğu gibi aldığı veriyi işler, diğer düğümler ise kendilerine gelen sahte verileri bırakırlar. Baz istasyonunun iletişiminin izlenemediğini farz ediyoruz (örneğin, kablolu iletişim). Beşinci kısıt, bir düğümden çıkan akışın tekrar kendisine dönmemesini sağlamak için kullanılmaktadır. *k* indisi veri akışının hedefini göstermek için eklenmiştir ve altıncı kısıtta gösterilen veri akış dengesinin tüm hedefler için ayrı ayrı sağlanması gerekir. Enerji harcamalarındaki dengesizlik, bütün akışlar eşit olsa dahi baz istasyonunun konumunu açığa vuracaktır. Bu yüzden yedinci kısıtta (aynı zamanda on ikincide de) düğümlerin enerji harcamalarını da dengeliyoruz.

$$f^{k}_{ij} \geq 0 \tag{2.4}$$

$$f^{k}_{ij} = 0 \qquad i = k \tag{2.5}$$

$$\sum_{j} f^{k}_{ij} = D + \sum_{j} f^{k}_{ji} \qquad \forall i,k \quad i \neq k \tag{2.6}$$

$$\left\{ \left[E_{rx} \sum_{k} \sum_{j} f^{k}_{ji} \right] + \left[\sum_{k} \sum_{j} E_{tx,ij} f^{k}_{ij} \right] \right\} \leq e_i \quad \forall i,k \quad i \neq k \tag{2.7}$$

Baz istasyonunun konumunu saklamak için geliştirdiğimiz ikinci problem (2.8) – (2.12) kısıtları ile formülleştirilmiştir. Buradaki düşüncemiz sahte baz istasyonları oluşturmak yerine ağda daha akıllıca sahte veriler üretmektir. Gerçek ve sahte veri akışları sırasıyla *f* ve *g* akışları ile gösterilmiştir. Dokuzuncu kısıt, *f*-akışları için akış dengesini formülleştirmiştir. Onuncu ve on birinci kısıtlar, ağdaki bütün düğümlerdeki sırasıyla veri çıkışlarının ve girişlerinin dengelenmesi içindir. Bu problemi ise *dengelenmiş akışlar* (*DA*) diye adlandırdık.

$$f_{ij} \geq 0, \quad g_{ij} \geq 0 \tag{2.8}$$

$$\sum_j f_{ij} = D + \sum_j f_{ji} \qquad i \in [2, N] \tag{2.9}$$

$$\sum_j (f_{ij} + g_{ij}) = \sum_j (f_{kj} + g_{kj}) \qquad \forall i,k \tag{2.9}$$

$$\sum_j (f_{ji} + g_{ji}) = \sum_j (f_{jk} + g_{hk}) \qquad \forall i,k \tag{2.9}$$

$$\left\{ \left[E_{rx} \sum_j (f_{ji} + g_{ji}) \right] + \left[\sum_j E_{tx,ij} (f_{ij} + g_{ij}) \right] \right\} \leq e_i \qquad \forall i \tag{2.3}$$

4.2.1. Güvenlik Analizi

Genelde KAA'lar için geliştirilen, verilen kısıtlar altında doğrusal bir amaç fonksiyonunu en iyileyen DP modelleri, düğümler arasındaki akış miktarını elde etmek için kullanılmaktadır. Bu modeller paket planlama üzerinde herhangi bir kısıtlamaya gitmemektedirler. Bu yüzden aşağıda yapılan güvenlik analizinde, sadece akış dağıtımını ve ilgili olguyu ele alacağız.

Bu bölümde *SBİ* ya da *DA* çözümleri uygulandığı zaman, saldırganın tüm ağdaki akışları görse dahi baz istasyonunun konumu hakkında işe yarar bir bilgi elde edemeyeceğini göstereceğiz. [20]'e göre baz istasyonu gözlemlenemezliği üzerine aşağıdaki tanıma sahibiz.

Tanım 1: *N* düğümlü bir KAA ele alalım. Bir A_i düğümünün baz istasyonu olma olasılığı $P(A_i)$ olsun ve *O* da saldırganın yaptığı gözlemi belirtsin. Bir sistem, bütün düğümler ve gözlemler için $\forall_i, \forall O, P(A_i) = P(A_i|O)$ eşitliği sağlanıyorsa baz istasyonu gözlemlenemezliğine sahiptir. Şimdi, iki çözümümüzün de baz istasyonu gözlemlenemezliği sağladığını ispatlayacağız.

Teorem 1: *SBİ* ya da *DA* çözümlerinden biri uygulandığında baz istasyonu gözlemlenemezliği korunabilir.

İspat: Tanım 1'deki $P(A_i) = P(A_i|O)$ eşitliği baz istasyonu olma olasılığının *O*'dan bağımsız olduğu anlamına gelmektedir $((P(A_i \cap O) = P(O).P(A_i|O) = P(O).P(A_i))$. Bu bağımsızlığı ispatlamak için farklı *O* çeşitlerini ele almamız gerekiyor:

- Akış miktarında *O*: *SBİ* ve *DA* çözümlerinin her ikisinde de, her bir düğümdeki toplam gelen ve toplam giden trafiğin miktarı baz istasyonu olmaktan bağımsız olduğu için akış miktarını gözlemlemeyle herhangi bir bilgi elde edilemez. Önerilen çözümlerin, aksine temel şemamızda baz istasyonu, hangi düğüme gelen akış miktarının en fazla olduğuna ve/veya hangi düğümden akış çıkmadığına bakılarak saptanabilir.

- Enerji tüketiminde *O*: Bütün düğümler aynı miktarda enerji harcadıkları için enerji tüketimi ile baz istasyonu olma arasında herhangi bir ilişki yoktur. Bu yüzden baz istasyonu hakkında bir bilgi elde edilemez.

- Mesaj içeriğinde *O*: Saldırgan, mesajların şifrelenmesinden dolayı mesajın içeriğine bakarak baz istasyonu hakkında bir bilgi elde edemez.

Bu nedenle saldırgan tüm bu gözlemleri yapsa dahi, baz istasyonu hakkında bir bilgi elde edemez. Bu yüzden Tanım 1'e göre baz istasyonu gözlemlenemezlik özelliği sağlanır.

5. DİJİTAL İMZA

Dijital imza, dijital bir mesajın ya da dokümanın geçerliliğini göstermek için kullanılan bir matematiksel tekniktir. Geçerli bir imza, kişiye mesajın bilinen bir gönderen tarafından oluşturulduğunun ve mesajın iletilirken değişikliğe uğramadığının garantisini verir.

Bir dijital imza tipik olarak üç tane algoritmadan oluşur:

- Bir kapalı anahtar kümesinden rastgele bir kapalı anahtar seçen bir *anahtar oluşturma* algoritması. Algoritma, bir kapalı anahtar ve bu kapalı anahtara eş bir açık anahtar üretir.

- Verilen bir mesaj ve bir kapalı anahtar ile bir imza üreten *imzalama* algoritması.

- Verilen bir mesaj, bir açık anahtar ve bir imza ile mesajın geçerliliğini kabul eden ya da reddeden bir *imza doğrulama* algoritması.

Bir veriyi imzalamak isteyen kişi, ilk başta bir özet fonksiyonu ile verinin özetini oluşturur. Daha sonra bu özeti kendi kapalı anahtarı ile şifreleyerek imzayı oluşturur. Bu imza veriye eklenerek karşı tarafa gönderilir. Karşı taraftaki kişi ise imzayı imzalayanın açık anahtarı ile çözer ve özeti elde eder. Daha sonra imzalayanın kullandığı özet fonksiyonu ile verinin özetini oluşturur. Son olarak da elindeki iki özeti karşılaştırır ve birbirlerine eşit olup olmamasına göre imzanın geçerliliğine karar verir. Burada önemli olan bir konu imzalayanın açık anahtarının imzalayana ait olduğuna nasıl güveneceğimizdir. Bu "açık anahtar – imzalayanın kimliği" ilişkisi bir açık anahtar sertifikası ile sağlanmaktadır. Bu sertifika ile bir açık anahtarın bir kişiye ait olup olmadığını doğrulayabiliriz.

5.1. Kullanılan İmza Algoritmaları

Simülasyonlarımızda üç farklı dijital imzalama algoritmaları kullandık. Günümüzde çok sık kullanılan bir imzalama algoritması olduğu için RSA'yı ve RSA'ya verimli bir alternatif olduğu için ECDSA'yı seçtik. OTS'i ise büyük imza boyutu ve neredeyse sıfır imzalama maliyeti ile nadir bir ödünleşim sunduğu için seçtik.

Simülasyonlarımızda güvenlik seviyesinin etkilerini görmek için 2^{80} ve 2^{112} olmak üzere iki farklı güvenlik seviyesinde Dİ'ler kullanıldı.

80-bitlik güvenlik seviyesi için OTS-80, RSA-1024 ve ECDSA-160 algoritmalarını kullandık. İmza boyutları (o_1 parametreleri) OTS-80, RSA-1024, ECDSA-160 algoritmaları için sırasıyla 3120, 1024 ve 320'dir [21]. İmza üretimi için gerekli enerji maliyetleri (o_2 parametreleri) OTS-80, RSA-1024, ECDSA-160 algoritmaları için sırasıyla 0 mJ, 304 mJ ve 22.82 mJ'dür [3].

112-bitlik güvenlik seviyesi için OTS-112, RSA-2048 ve ECDSA-224 algoritmalarını kullandık. İmza boyutları (o_1 parametreleri) OTS-112, RSA-2048, ECDSA-224 algoritmaları için sırasıyla 6160, 2048 ve 448'dir [21]. İmza üretimi için gerekli enerji maliyetleri (o_2 parametreleri) OTS-112, RSA-2048, ECDSA-224 algoritmaları için sırasıyla 0 mJ, 2302.7 mJ ve 61.54 mJ'dür [3]. İmza parametreleri ayrıca Çizelge 1'de listelenmiştir.

Çizelge 1 - İmza Parametreleri

	İmza Boyutu (bit) o_1	**Dijital İmzalama Maliyeti (mJ)** o_2
OTS-80	3120	0
RSA-1024	1024	304
ECDSA-160	320	22.82
OTS-112	6160	0
RSA-2048	2048	2302.7
ECDSA-224	448	61.54

6. SİMÜLASYON SONUÇLARI

Bu kısımda inkâr-edememe ve baz istasyonu gözlemlenemezliği problemleri için yaptığımız simülasyon sonuçlarına bakacağız.

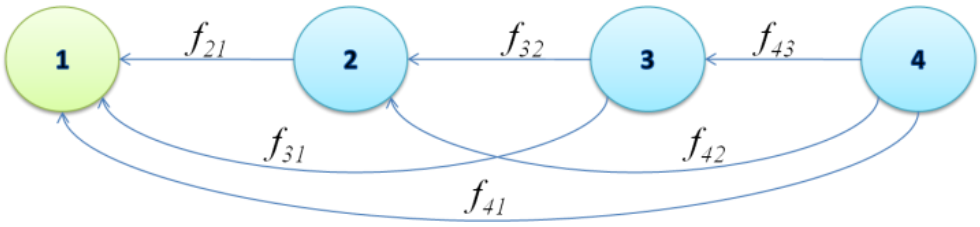
6.1. İnkâr-Edememe Problemi İçin Simülasyon Sonuçları

KAA'larda inkâr-edememenin ağ ömrüne olan etkisini incelemek için kapsamlı bir simülasyon yaptık. Enerji parametreleri için [12]'de verilen parametreleri kullandık, $E_{Elec} = 50\,nJ$, $\varepsilon_{amp} = 100\,pJ$. Her bir düğüm için başlangıç enerjisi $e_i = 243\,J$ olarak seçtik. Bu, 25%'i algılama, sıkıştırma, yön bulma gibi diğer görevlere ayrıldığı farz edilmiş 30 mAh'lik bir pilin %75'ini oluşturmaktadır. Bu parametreler Çizelge 2'de listelenmiştir. Birim zamanda üretilen veri miktarı 1 bittir (si=1). KAA'larda sıkıştırılmış bir resmin boyutu 25344 bit [22] olduğu için simülasyonlarımızda imzalama oranını (r) aksi söylenmedikçe 1/25344 olarak aldık. Matematiksel programlama ve en iyileme için GAMS IDE 2.0.31.8 ara yüzü altında CPLEX 9 çözdürücüsünü kullandık [23].

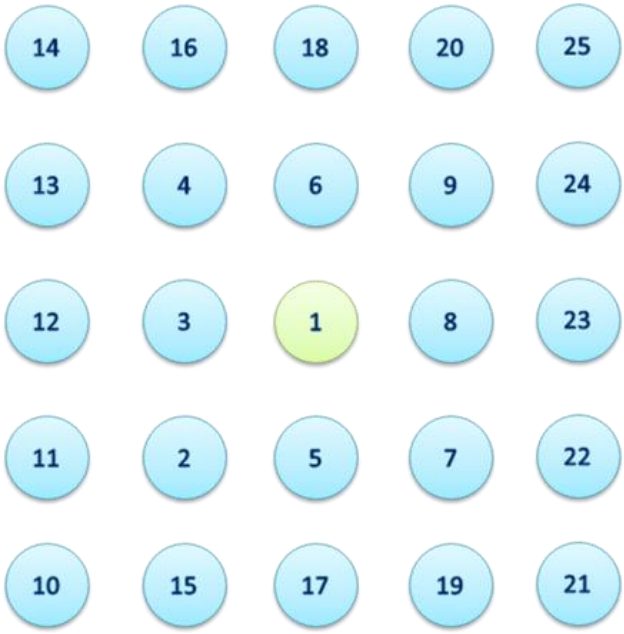
Çizelge 2 – Enerji Parametreleri

	Sembol	**Değer**
Elektronik Enerji	E_{Elec}	50 nJ
Amplifikatör Enerji	ε_{amp}	100 pJ
Algılayıcı Pili	e_i	243 J

Simülasyonlarımızda trafik izleme gibi uygulamalarda da görülebilen [10] doğrusal ağ topolojisini (Şekil 4), ve kare ağ topolojisini (Şekil 5) kullandık.



Şekil 4 - Doğrusal algılayıcı ağ topolojisinin gösterimi. Düğüm-1 baz istasyonudur. Düğüm-*i*'den düğüm-*j*'ye giden veriler f_{ij} ile gösterilmiştir



Şekil 5 - Kare algılayıcı ağ topolojisinin gösterimi. Düğüm-1 baz istasyonudur.

Doğrusal topolojide, N tane düğüm en başta baz istasyonu olacak şekilde eşit aralıklarla bir sıra boyunca dizilmektedir. Komşu düğümler arasındaki uzaklık aynıdır. Şekil 4 aynı zamanda algılayıcı düğümler ve baz istasyonu arasındaki veri akışını da göstermektedir. Şekil 5'de gösterilen kare topolojide ise baz istasyonu ortaya yerleştirilmiştir, dikey ve yatay eksende düğümler arasındaki mesafe aynıdır.

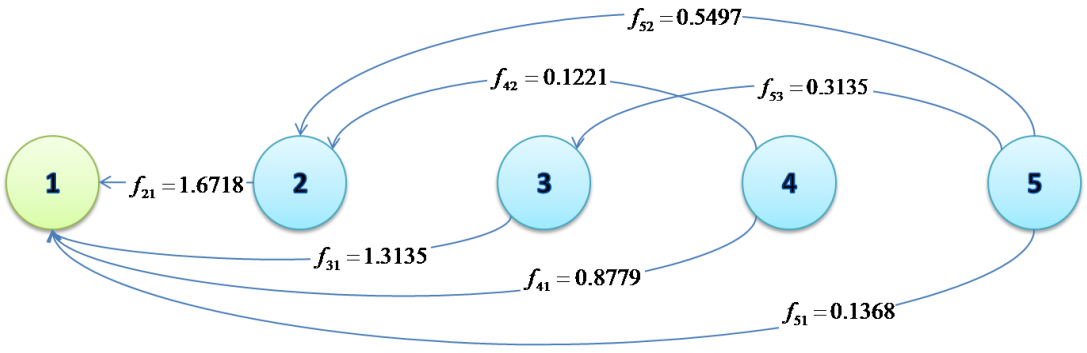
6.1.1. Veri Akışlarını En İyileme

Temel ödünleşimleri ve ağ dinamiklerini kolay bir şekilde gösterebilmek için ilk başta birinci düğümün baz istasyonu olduğu 5 düğümlük doğrusal bir ağ üzerinde çalıştık. Komşu düğümler arası mesafe 10 m'dir ve $E_{tx,ij}$ düğümler arası mesafenin ikinci ve dördüncü kuvvetleriyle artmaktadır (α=2 veya α=4).

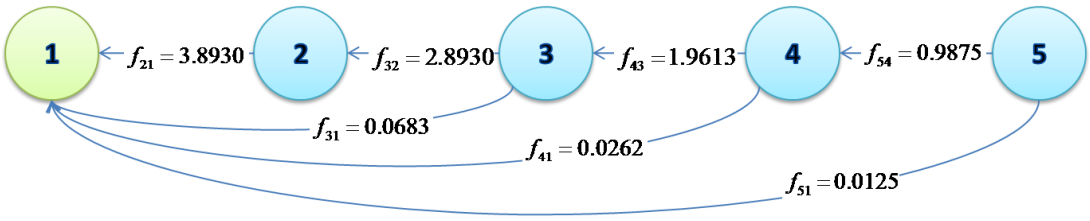
En iyileme problemi Dİ uygulanmadığı durumlarda, yani kısıt (1), (2) ve (4) ile çözülmüştür. Basit ifadelerle söyleyecek olursak, ağ ömrünü maksimize etmek demek düğümler arasındaki veri akışlarının dengelenmesi, herhangi bir düğümün enerjisinin erken bitmemesi ve bütün düğümlerin enerjilerinin aynı anda bitmesi demektir. Şekil 6 ve 7, sırasıyla α=2 ve α=4 olduğu durumlarda en iyilenmiş veri

akışlarını göstermektedir (akışlar her bir düğümün birim miktarda veri ürettikleri düşünülerek normalleştirilmiştir). Örneğin, Şekil 6'da düğüm-5 verilerinin hepsini direk baz istasyonuna göndermek yerine akışını üçe ayırmıştır (% 13.7'sini baz istasyonuna, % 55'ini düğüm-2'ye ve %31.3'ünü düğüm-3'e). Bunun amacı, gönderim enerjisinin uzaklığın karesi ile orantılı bir şekilde arttığı için aşırı enerji tüketiminden kaçınmaktır. Ayrıca, düğüm-5 bütün verilerini hemen yakınında olan düğüm-4'e göndermemektedir, bu şekilde düğüm-4'ün enerjisi düğüm-5'in verilerini taşımak için gereksiz yere kullanılmamış olur. Böylece, veri akışları tek bir düğümün ömrünün en iyilenmesi yerine tüm ağın ömrünün en iyilenmesi amacıyla dengelenmiştir. Değişik yayılma ortamlarında veri dengelemesinin farklılıklar gösterdiğini gözlemledik (mesela, değişik α değerleri için). Daha sert çalışma koşulları, daha uzağa veri gönderimini kısıtlamaktadır. Sonuç olarak α=4 olduğu zaman çoğu iletişim komşu düğümler arasında olmaktadır (düğüm-2, baz istasyonuna diğer düğümlerin verilerinden α=2 olduğu zaman 0.67 birim, α=4 olduğu zaman ise 2.89 birim göndermektedir).

Daha ileri çalışmalara geçmeden önce, bu basit topolojiyi Dİ uygulandığı durumlarda da inceledik. Her üç algoritma için, α=2 ve α=4 için mutlak değerlerin beklendiği gibi düşmesine rağmen akışlar arasındaki oran Şekil 6 ve 7'deki gibi aynı kalmaktadır. Bunun sebebi Dİ'nin ek maliyetinin sadece imzalayanda bulunduğu ve bu ek maliyetin akışların dağıtılmasına bağlı olarak değişmediğidir.



Şekil 6 - α=2 iken 5 düğümlük doğrusal bir algılayıcı ağda akış dengesi.



Şekil 7 - α=4 iken 5 düğümlük doğrusal bir algılayıcı ağda akış dengesi.

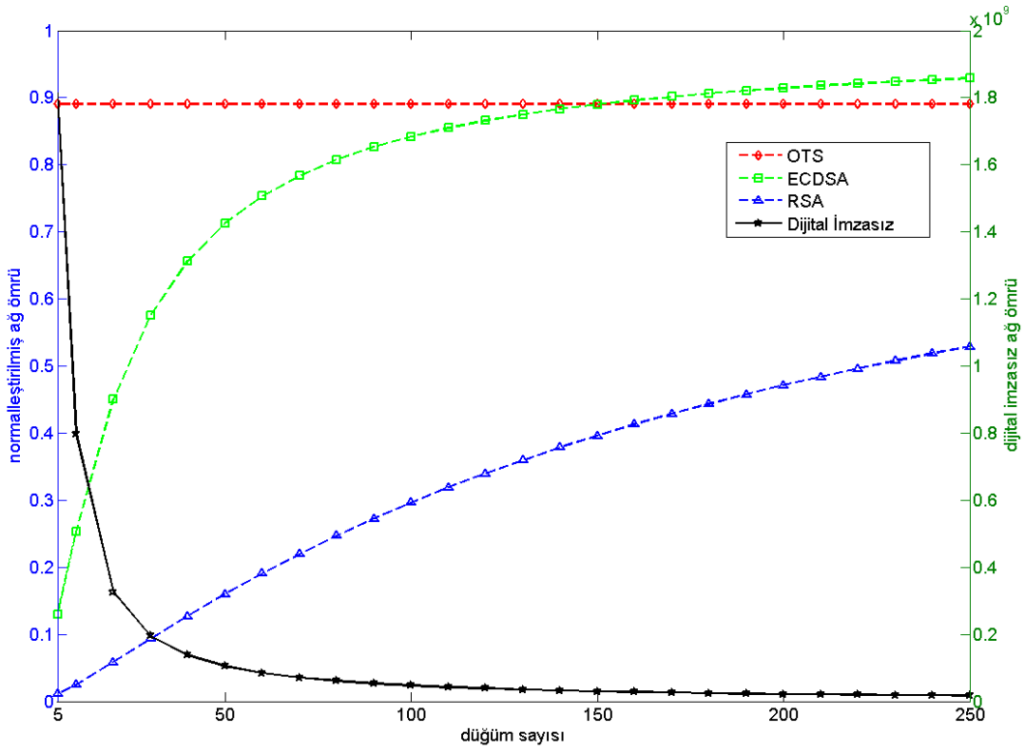
6.1.2. Ağ Topolojisini ve Büyüklüğünü Değiştirme

Bu alt bölümde, Dİ'leri kullanmanın farklı ağ topolojilerinde ve büyüklüklerinde ağ ömrüne olan etkilerini araştırıyoruz. İki farklı yayılma ortamında (α=2 ve α=4) ve 80 bitlik güvenlik seviyesinde (bu yüzden OTS-80, RSA-1024 ve ECDSA-160 algoritmaları kullanıldı) çalıştık.

6.1.2.1. Doğrusal Topoloji

Simülasyonlarda Dİ uygulamak için (2) ve (4) numaralı kısıtları (3) ve (5) numaralı kısıtlar ile değiştirdik. İmza ve enerji parametreleri olarak Çizelge 1 ve 2'de verilen parametreleri kullandık.

Şekil 8 ve 9'da, Dİ uygulanmadığı durumdaki ağ ömrü ile normalleştirilmiş olan OTS-80, ECDSA-160 ve RSA-1024 algoritmalarının kullanıldığı durumdaki ağ ömürleri (y ekseninin sol tarafında), ağ büyüklüğüne karşı çizilmiştir. Dİ uygulanmadığı durumdaki ağ ömrü (y ekseninin sağ tarafında), ağ büyüklüğüne karşı çizilmiştir. Sol eksendeki değerler, sağ eksendeki değerler ile normalleştirilmiştir (örneğin, 0.9 normalleştirilmiş ağ ömrü demek, bu ömrün Dİ uygulanmadığı durumlarda elde edilen ömürden %10 daha az olması demektir). Ağ büyüklüğü 5 düğüm ile başlamakta ve 10'dan 250'ye kadar 10'ar 10'ar artmaktadır. Komşu düğümler arası mesafe 10 m'dir.



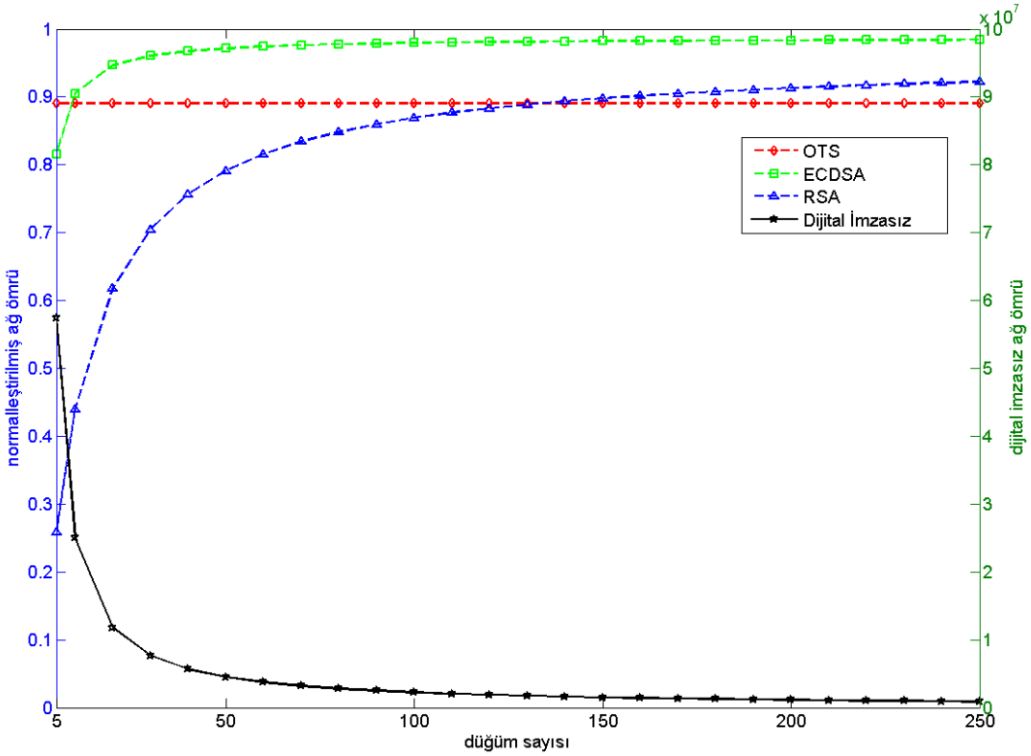
Şekil 8 - Doğrusal topolojide α=2 iken normalleştirilmiş ağ ömürleri

Şekil 8'te $E_{tx,ij}$, düğümler arası mesafenin ikinci kuvveti olarak artmaktadır (α=2, *boş alan* modeli). Ağ ömrü, bütün simülasyonlarımızda da gözlemlediğimiz gibi ağ büyüklüğü arttıkça azalmaktadır. Bunun sebebi, baz istasyonuna yakın düğümlerin ağa yeni düğümler eklendikçe veri göndermek için daha fazla enerji harcamalarıdır. OTS-80 algoritması uygulandığı durumda normalleştirilmiş ağ ömrü 0.9'dur (ağ ömrü %10 azalmıştır) ve bu ağ büyüklüğü arttıkça sabit kalmaktadır. Diğer taraftan RSA-1024 ve ECDSA-160 algoritmaları uygulandığı durumlarda normalleştirilmiş ağ ömürleri, ağ büyüklüğü arttıkça artmaktadır. 150 düğümden az ağlarda OTS-80 algoritması daha iyi sonuç verirken, daha büyük ağlarda ECDSA-160 daha tercih edilebilir durumdadır. Bu topoloji ve ortamda RSA-1024 algoritması zayıf bir adaydır.

Aslında, enerji tüketimi yönünden ele alırsak OTS'nin net etkisi iletilen veri miktarının artmasıdır (örneğin, 10 birim asıl veri ve yaklaşık 1 birim ek maliyet) ve bu yüzdendir ki sistem ömrü bütün ağ büyüklükleri için tam olarak aynı miktarda azalmaktadır. Aynı mekanizma ECDSA ve RSA için de geçerlidir; fakat bu algoritmalara ek olarak imzalama enerjisi iletim maliyetine eklenmektedir. Dİ kullanılmadığı durumda belli bir mesafeye kadar olan iletim maliyetini *x* olarak kabul edersek, ECDSA ve RSA kullanıldığı zaman bu maliyet *x*+*z* olacaktır. Eğer *x*, *z*'den önemli bir derecede büyük değilse, ECDA ve RSA'nın bütün enerji tüketiminde *z* terimi (imzalama enerjisi) ağır basacaktır. Bu yüzden iletim enerjisi nispeten daha az olan küçük ağlarda ECSA ve RSA ile daha küçük ağ ömürleri elde edilir (küçük ağlarda baz istasyona olan uzaklıklar daha azdır). Büyük ağlarda *x*, iletim enerjisine baskın çıkmaktadır. Bundan dolayı, Dİ algoritmaları arasındaki farklılık başlıca imza boyutu tarafından belirlenecektir. Bunun sonucunda da büyük ağlarda OTS'nin ömrü ECDSA'nın ömründen daha azdır.

Şekil 9'da $E_{tx,ij}$, düğümler arası mesafenin dördüncü kuvveti olarak artmaktadır (α=4). Bu yüzden iletim daha maliyetli olmakta ve ağ ömrü önemli bir şekilde düşmektedir. İmzanın iletimi bütün enerji üzerinde daha fazla etkiye sahip olacağından, küçük imza miktarına sahip Dİ algoritmaları daha iyi sonuç

vermektedirler. OTS-80, bu durumda sadece 5 düğümlü ağda en iyi adaydır. İlginçtir ki, yayılma ortamı daha da sertleştikçe inkâr-edememenin ağ ömrüne olan etkisi azalmaktadır. α=4 iken, ECDSA-160 uygulanan ağ büyüklüğünün önemli bir bölümünde ağ ömrü %2.5'ten daha az oranda düşmüştür.

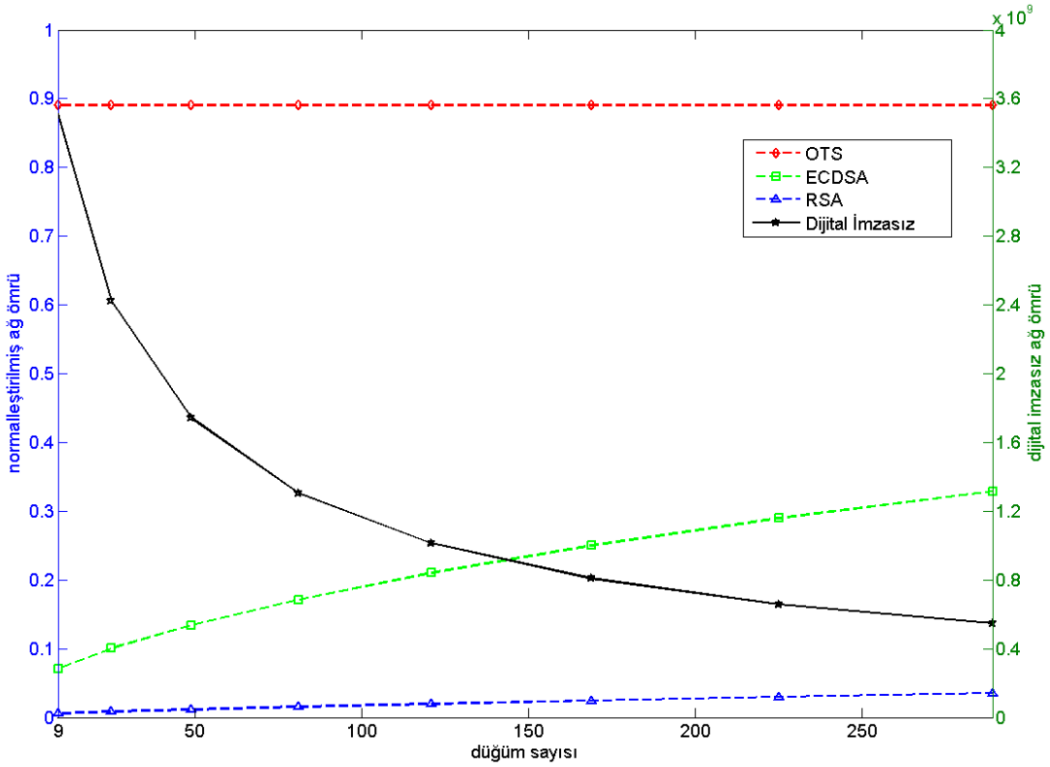


Şekil 9 - Doğrusal topolojide α=4 iken normalleştirilmiş ağ ömürleri

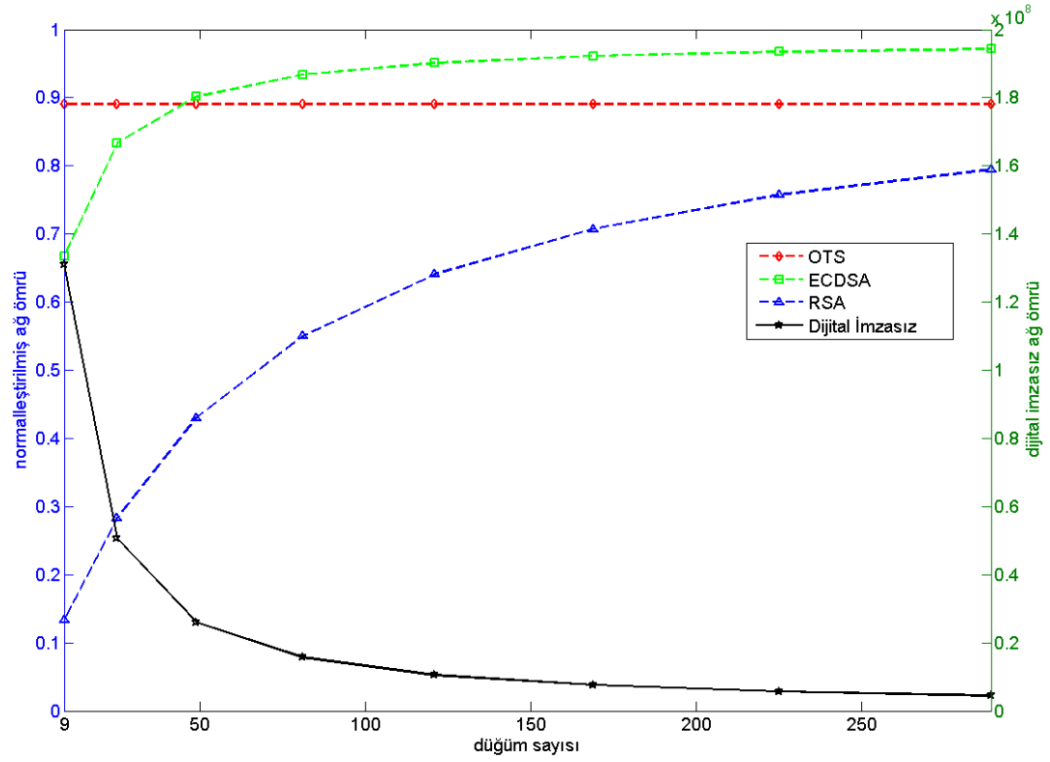
6.1.2.2. Kare Topoloji

Simülasyonlarımızı iki boyutlu (2-D), ortasında baz istasyonu olan kare topolojilerde de çalıştırdık. Dikey ve yatay eksende düğümler arasındaki mesafe aynıdır ve 10 m'dir (Şekil 5).

Şekil 10 ve 11'de, Dİ kullanılmadığı durumdaki ağ ömrü ile normalleştirilmiş olan OTS-80, ECDSA-160 ve RSA-1024 algoritmalarının kullanıldığı ağ ömürleri (y ekseninin sol tarafında), ağ büyüklüğüne karşı çizilmiştir. Dİ uygulanmadığı durumdaki ağ ömrü (y ekseninin sağ tarafında), ağ büyüklüğüne karşı çizilmiştir. Simülasyonlarda ağ büyüklüleri tam bir kare oluşturmak için 9, 25, 49, 81, 121, 169, 225 ve 289 olarak seçilmiştir.



Şekil 10 - Kare topolojide α=2 iken normalleştirilmiş ağ ömürleri



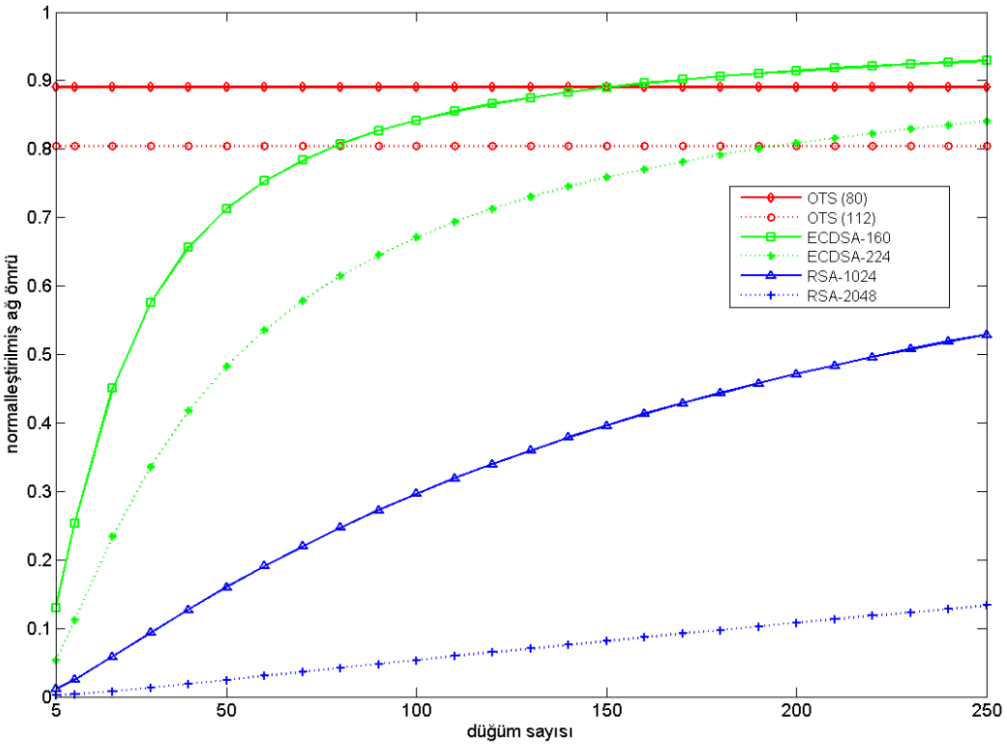
Şekil 11 - Kare topolojide α=4 iken normalleştirilmiş ağ ömürleri

Doğrusal ve kare topolojileri karşılaştırdığımızda, kare topolojide aynı büyüklükteki ağlarda düğümlerin baz istasyonuna olan ortalama uzaklıklarının doğrusal topolojiye göre daha küçük olduğunu görüyoruz. Bu yüzden OTS-80, büyük ağlarda α=2 ve α=4 iken 1-D'ye nazaran 2-D 'de daha iyi sonuçlar vermektedir. Bunun sebebi OTS-80'in normalleştirilmiş ömrünün 0.9 civarında sabitlenmesi değil, diğer algoritmaların normalleştirilmiş ömürlerinin en iyi sonuçlarına daha yavaş yakınsamalarıdır. Ama yine de, ECDSA ve RSA ağ büyüklüğü arttıkça daha iyi sonuçlar vermektedir. Bu yüzden ağın daha büyük bir bölgeye yayıldığı durumlarda OTS, daha zayıf bir aday olacaktır.

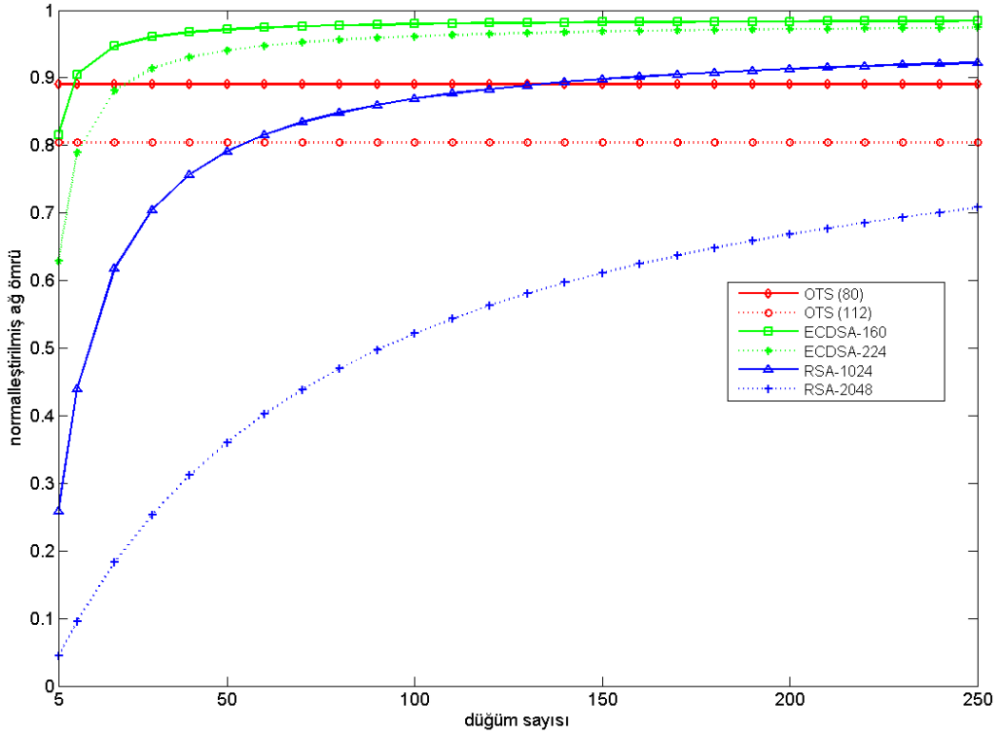
6.1.3. Güvenlik Seviyesini Değiştirme

Güvenlik seviyesinin etkilerini görmek için aynı topolojiler ve ağ büyüklüklerinde simülasyonlarımızı 112-bitlik güvenlik seviyesi için de tekrarladık. Her iki yayılım ortamı için (α=2 ve α=4) OTS-112, RSA-2048 ve ECDSA-224 algoritmalarını kullandık. 80-bitlik güvenlik seviyesinde olduğu gibi yine, Çizelge 1 ve 2'deki parametreleri kullandık.

112-bitlik güvenlik elde etmek için, RSA ve OTS algoritmalarının her ikisinde de imza boyutlarını yaklaşık olarak aynı oranda arttırmak gerekir. Oysa 2048-bit RSA imzası üretmek 1024-bit RSA imzası üretmekten 7.5 kat daha masraflıdır. Bu yüzden Şekil 12, 13, 14 ve 15'te gösterilen simülasyonlarda ortak bir örüntü görmekteyiz. OTS-112'yi OTS-80'e tercih ederken gerekli olan ilave ağ ömrü masrafı her zaman RSA-2048'i RSA-1024'e tercih ederken gerekli olandan daha az olmaktadır. Bunun sonucunda, güvenlik seviyesi düşünüldüğünde OTS, RSA'dan daha tercih edilebilirdir.



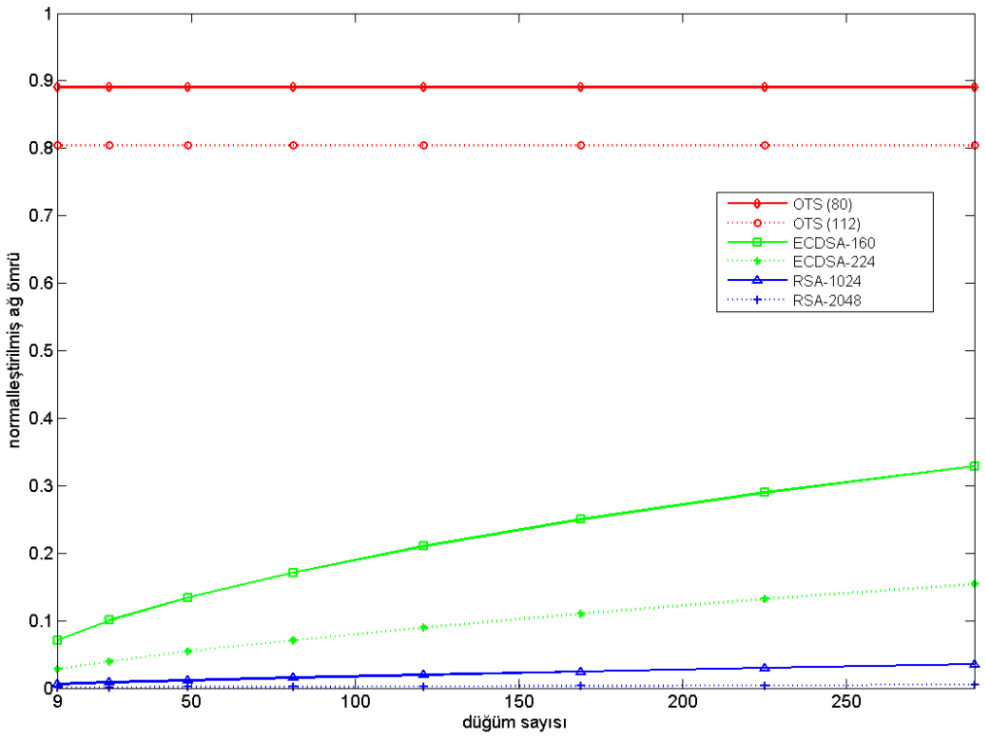
Şekil 12 - Doğrusal topolojide, α=2 iken 80-bitlik ve 112-bitlik güvenlik seviyelerinde normalleştirilmiş ağ ömürleri



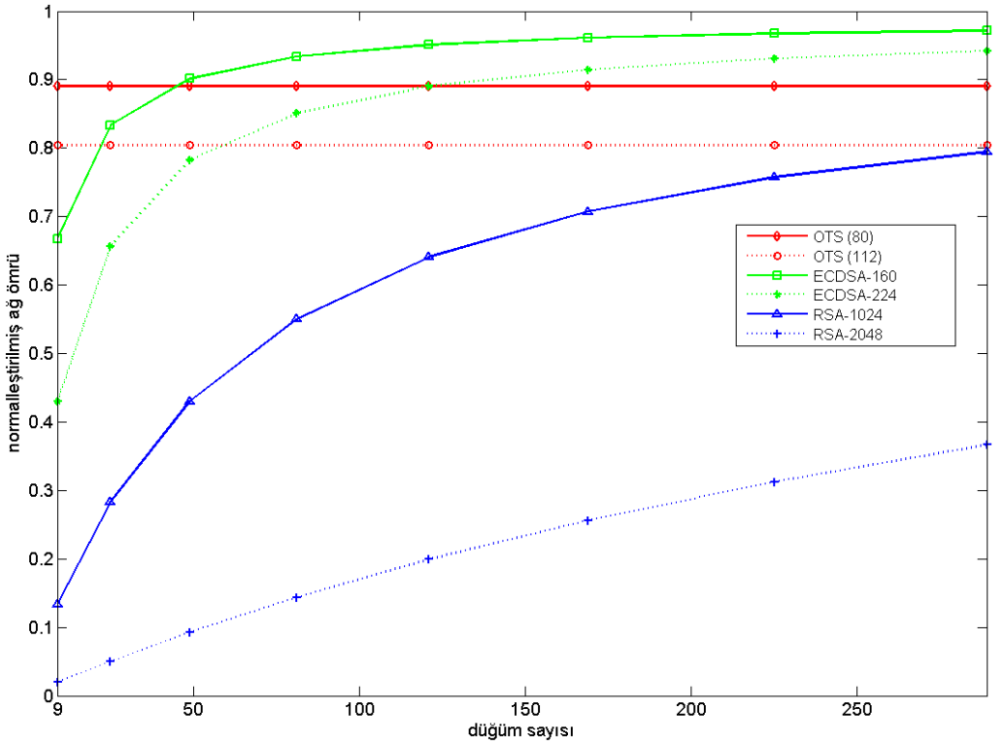
Şekil 13 - Doğrusal topolojide, α=4 iken 80-bitlik ve 112-bitlik güvenlik seviyelerinde normalleştirilmiş ağ ömürleri

OTS ve ECDSA'yı karşılaştırdığımız zaman durum biraz daha kompleks bir hal alıyor. İletim maliyetinin baskın olmadığı durumlarda (α=2), ECDSA'nın imzalama enerjisinin 2.7 kat artması, OTS'in imza boyutunun artmasından daha önemlidir. Bu sebepten dolayı Şekil 12'de, ECDSA'in eğrisinin OTS'in eğrisi ile güvenlik seviyesi 112 iken daha geç kesiştiğini görmekteyiz. Bir başka değişle OTS, 80-bitlik güvenlik seviyesinde ağ büyüklüğü 150 düğümden azken, 112-bitlik güvenlik seviyesinde ise ağ büyüklüğü 190 düğümden azken ECDSA'dan daha iyi sonuç vermektedir.

Daha sert yayılım ortamlarında (α=4), OTS ve ECDSA arasında güvenlik seviyesinin artmasıyla ilgili yaptığımız yorumlar pek değişmemektedir. Küçük ağlarda OTS, ECDSA'dan daha iyi sonuç vermektedir (Şekil 13 ve 15'e bakınız).



Şekil 14 - Kare topolojide, α=2 iken 80-bitlik ve 112-bitlik güvenlik seviyelerinde normalleştirilmiş ağ ömürleri



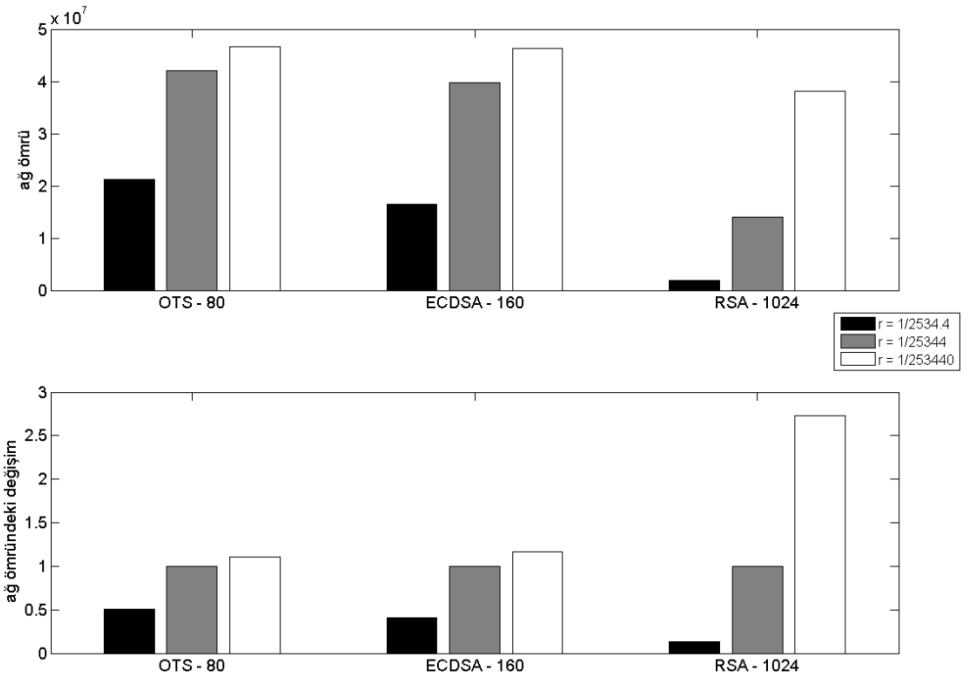
Şekil 15 - Kare topolojide, α=4 iken 80-bitlik ve 112-bitlik güvenlik seviyelerinde normalleştirilmiş ağ ömürleri

6.1.4. İmza Oranını Değiştirme

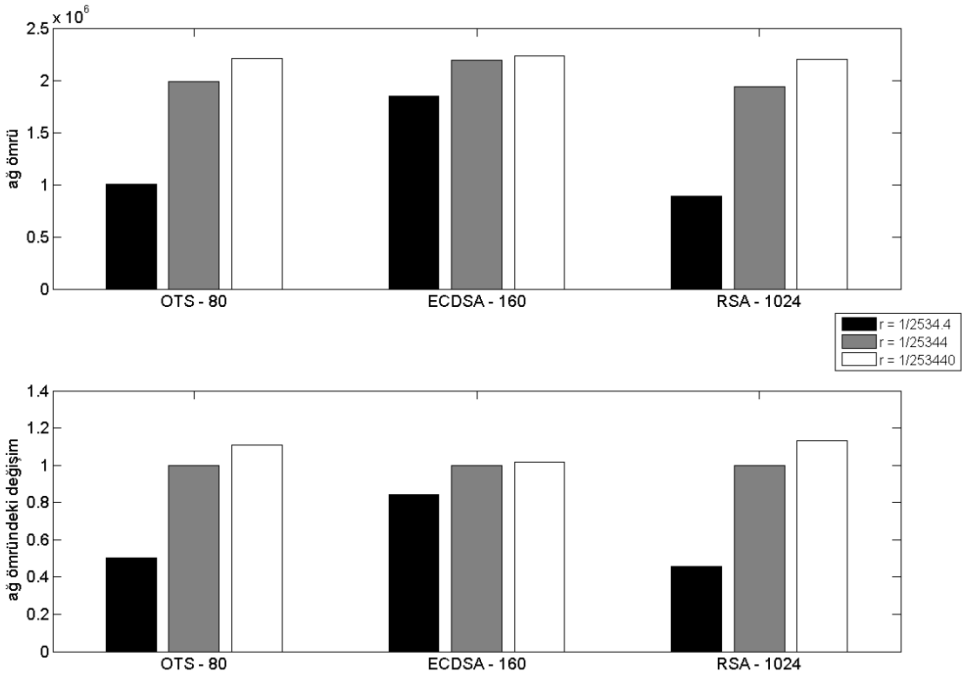
İmza oranının KAA'ların ömürlerine olan etkilerini incelemek için imza oranlarını 10'un katlarıyla arttırarak ve azaltarak simülasyonlarımızı tekrarladık. 100 düğümlü doğrusal topoloji üzerinde çalıştık.

Şekil 16 ve 17'de OTS-80, ECDSA-160 ve RSA-1024 algoritmaları kullanılarak elde edilen ağ ömürleri üç farklı imza oranları ile gösterilmiştir. $E_{tx,ij}$, düğümler arası mesafenin ikinci ve dördüncü kuvveti ile artmaktadır (α=2 ve α=4). Diğer bütün parametreler önceki simülasyonlardaki ile aynıdır. Bu şekillerin üst kısmında ağ ömürlerinin gerçek değerleri, alt kısmında 1/25344 imza oranıyla elde edilen ağ ömrü 1'e eşitlenerek (gri çubuk) diğer ağ ömürlerindeki değişim oranları gösterilmiştir.

İmza oranı, verilen bir topoloji ve ortam için hangi algoritmanın en iyi olduğu sonucunu değiştirmiyor; fakat hangi algoritmanın kullanıldığına bağlı olarak ağ ömrüne olan etkisi önemli bir şekilde değişiyor. Örneğin, RSA kullanıldığında imza oranını 10 kat azaltmak 2.5 kat daha uzun ağ ömürlerine sebep olmakta, fakat ECDSA ve OTS'de bu iyileşme düşük kalmaktadır. Benzer bir şekilde, eğer imza algoritması düzgün seçilmezse imza oranını arttırmak daha kötü sonuçlar doğurmaktadır. Bu şekiller göstermektedir ki daha küçük imza oranı ile inkâr-edememe gerekiyorsa algoritma seçimi daha dikkatli yapılmalıdır.



Şekil 16 - Doğrusal bir topolojide, α=2 iken farklı imza oranları için ağ ömürleri

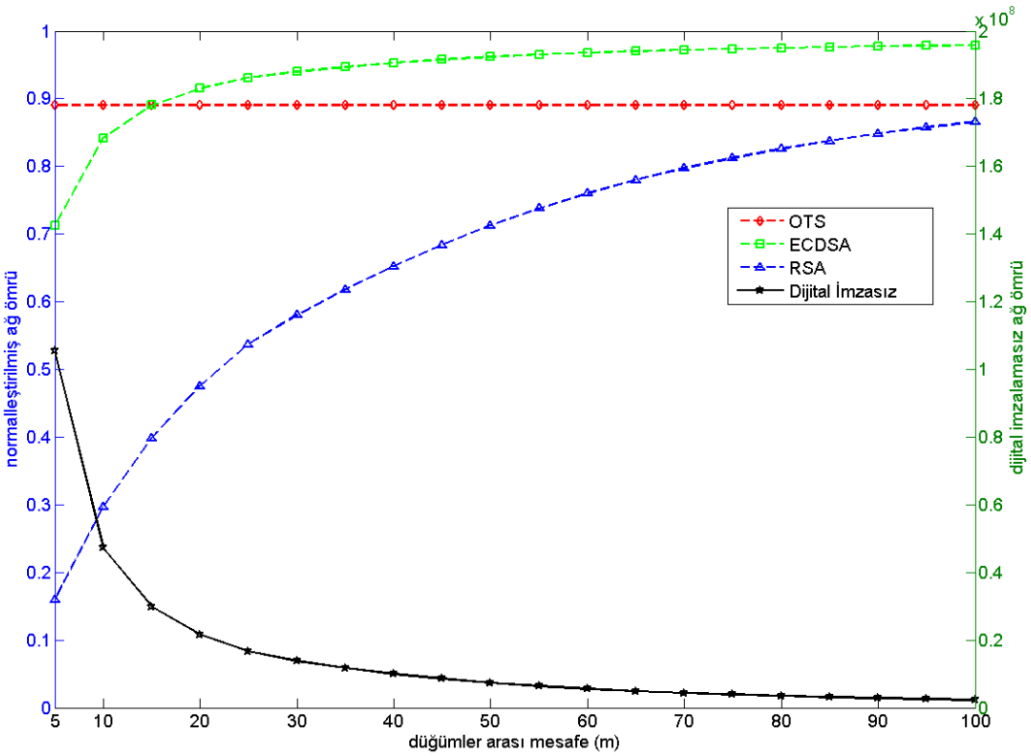


Şekil 17 - Doğrusal bir topolojide, α=4 iken farklı imza oranları için ağ ömürleri

6.1.5. Ağ Yoğunluğunu Değiştirme

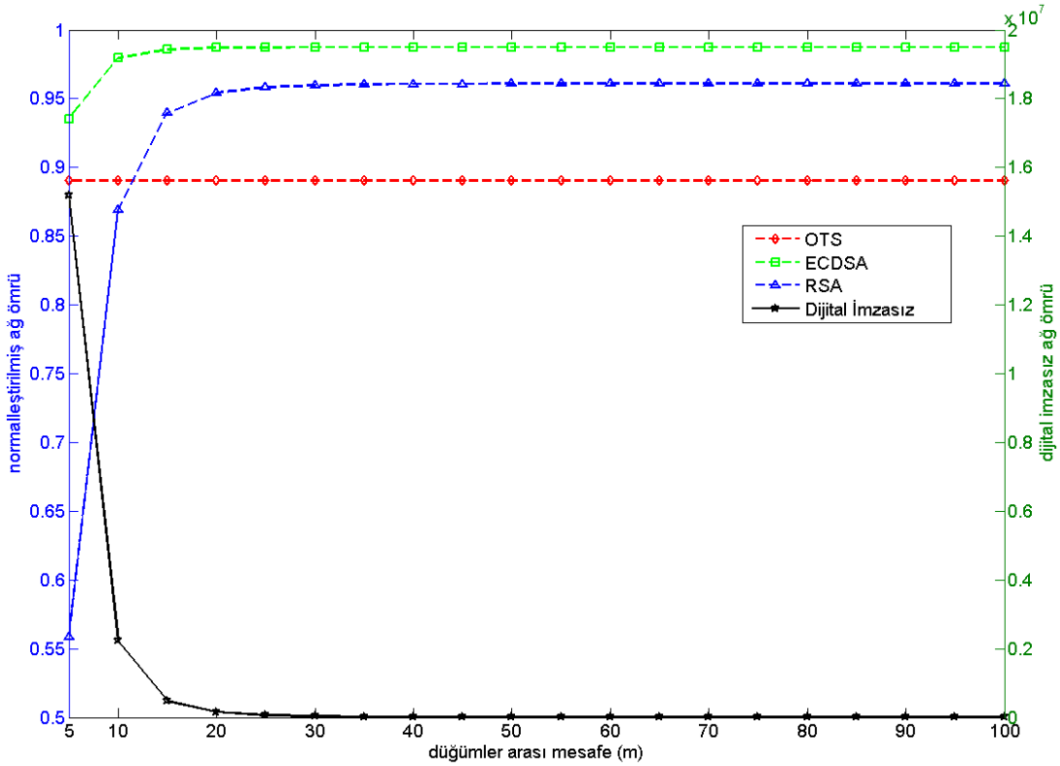
Son olarak, ağ yoğunluğunun (düğümler arası mesafenin) ağ ömrüne olan etkilerini inceledik. Bu kısımda OTS-80, ECDSA-160 ve RSA-1024 algoritmalarını kullandık.

Şekil 18 ve 19'da, OTS-80, ECDSA-160 ve RSA-1024 algoritmaları için Dİ uygulanmadığı durumlardaki ağ ömürleriyle normalleştirilmiş ağ ömürleri α=2 ve α=4 iken sırasıyla gösterilmektedir. 100 düğümlü bir doğrusal ağ kullanılmıştır.



Şekil 18 - Doğrusal topolojide, α=2 iken düğüm dağılımına göre normalleştirilmiş ağ ömürleri

Düğümler arası mesafeyi arttırmanın ağ büyüklüğünü arttırmayla benzer etkiye sahip olduğunu gördük. Uzaklıklar arttıkça iletişim enerjisi daha baskın çıkmakta ve bu yüzden ECDSA ve RSA'nın hesaplama (imzalama) maliyeti daha az öneme sahip olmaktadır. Bu sebepten dolayı düğümler arası mesafe arttıkça ECDSA ve RSA, OTS'den daha çok tercih edilebilir olmaktadır.



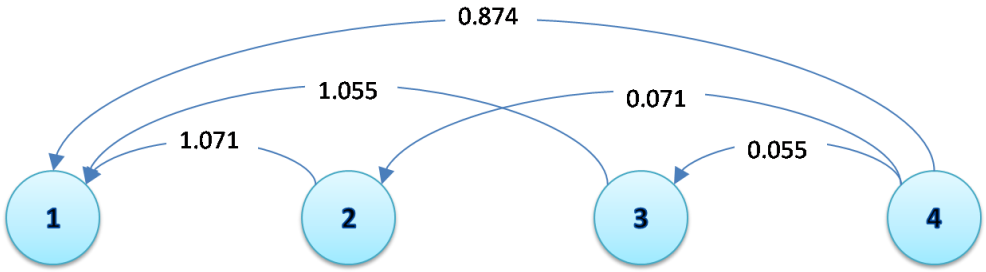
Şekil 19 - Doğrusal topolojide, α=4 iken düğüm dağılımına göre normalleştirilmiş ağ ömürleri

6.2. Baz İstasyonu Gözlemlenemezliği Problemi İçin Simülasyon Sonuçları

4.2'de bahsettiğimiz DP modellerimizdeki temel fikri daha iyi gösterebilmek için bu modellerimizi ilk başta algılayıcı düğümlerin eşit aralıklarla sıralandığı dört düğümlü basit bir doğrusal topolojide çözdük. Düğümler arası mesafe 1m alındı. Enerji parametreleri için [10]'da verilen parametreleri kullandık, $E_{Elec} = 50\,nJ$, $\varepsilon_{amp} = 100\,pJ$. İnkâr-edememe probleminden farklı olarak her bir düğüm için başlangıç enerjisi $e_i = 2\,J$ olarak seçtik. Bu problemlerin çözümü için GAMS IDE 2.0.31.8 ara yüzü altında CPLEX 9 çözdürücüsünü kullandık [23].

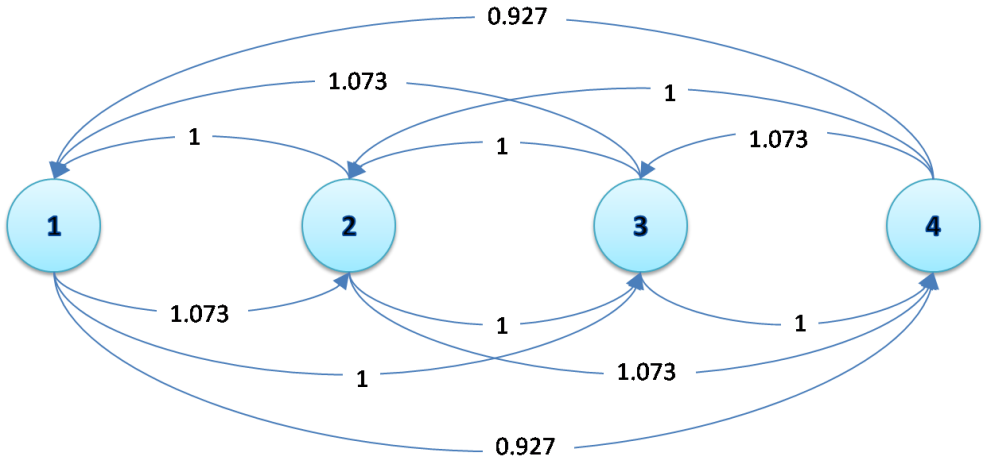
Önce, en iyileme problemi temel şemada çözüldü. Şekil 20 düğümler arasındaki akış miktarının düğüm başına üretilen toplam veri miktarının 1'e normalleştirildiği durumdaki halini göstermektedir. Bu şekilde, her bir düğüme gelen veri miktarı

analiz edilerek ve karşılaştırılarak baz istasyonunun hangi düğüm olduğu kolayca anlaşılabilir.



Şekil 20 – Temel şemada normalleştirilmiş ağ akışları

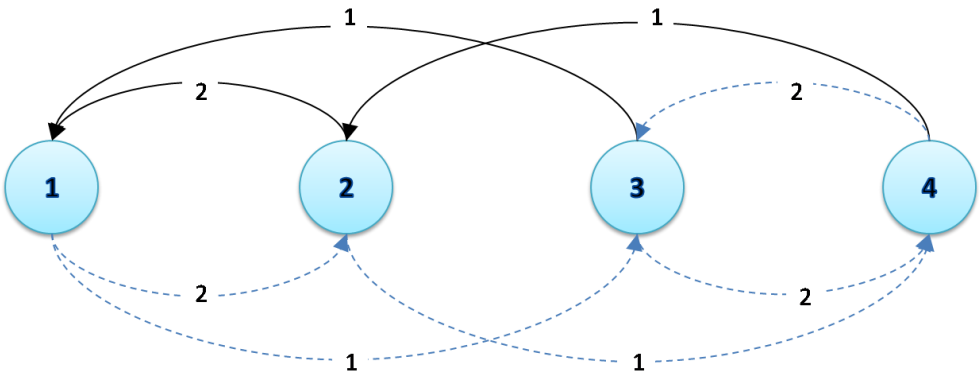
İkinci olarak problemimiz aynı topoloji ve parametrelerle *SBİ* çözümü için çözüldü. Şekil 21, her düğümün baz istasyonu olarak davrandığı durumdaki normalleştirilmiş akışları göstermektedir. Toplam normalleştirilmiş gelen ve giden akış miktarları 3 ila 3.073 arasında değer almaktadır. Bu ufak değişimin sebebi en iyi sonuçta aktarma yapılmasıdır (örneğin, düğüm-1 akışının %7.3'ünü düğüm-2'nin üzerinden aktararak düğüm-4'e göndermektedir). SBİ çözümündeki ağ ömrü, temel şemadaki ağ ömrünün %18'idir.



Şekil 21 – *SBİ* çözümünde normalleştirilmiş ağ akışları

Son olarak problemimiz yine aynı topoloji ve parametrelerle *DA* çözümü için çözüldü. Şekil 22, bu durum için normalleştirilmiş akışları göstermektedir. Düz

çizgiler *f*-akışlarını (gerçek veri), kesikli çizgiler ise *g*-akışlarını (sahte veri) göstermektedir. Toplam normalleştirilmiş gelen ve giden akış miktarları her zaman 3'tür. Bu durumdaki ağ ömrü, *SBİ* çözümünde elde edilen ağ ömründen %5.56 daha fazladır. Ağ ömründeki bu artış, *DA* çözümünün *SBİ* çözümündekine nazaran daha rahatlamış kısıtlara sahip olmasındandır. Burada, pasif bir dış saldırgan şifrelemenin kullanılmasından dolayı gerçek trafiği (*f*-akışları) sahte trafikten (*g*-akışları) ayırt edemez. Bu ayırt edilemezlik, ağdaki bütün düğümlerin aynı akış örüntüsünü kullandığı ve bu yüzden de baz istasyonunun konumunun belli olamayacağı anlamına gelmektedir.

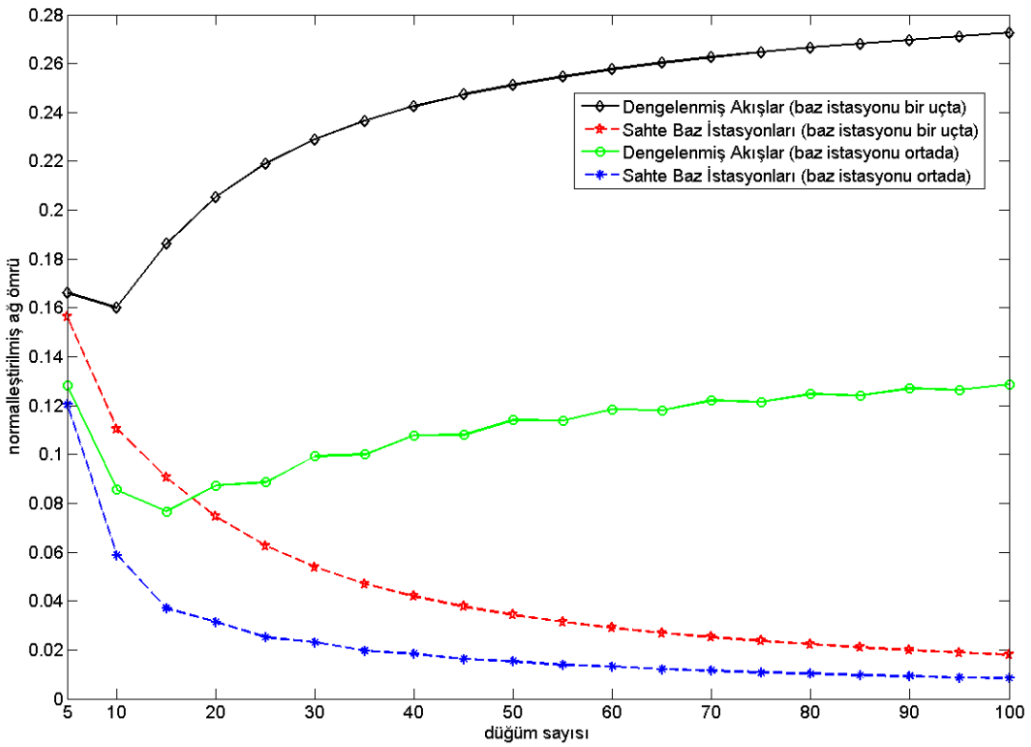


Şekil 22 – *DA* çözümünde normalleştirilmiş ağ akışları

4.2'de bahsettiğimiz üç DP problemini doğrusal bir topolojide farklı ağ büyüklükleri ile çözdük. Bundan sonraki tüm analizlerde ağ ömrü değerleri, temel şemadaki ağ ömrü değerleri ile normalleştirilerek verilecektir. Hangi DP modelinin kullanıldığına bakılmaksızın KAA'nın ağ ömrü, ağ boyutu arttıkça azalmaktadır.

İlk simülasyonumuzda ağdaki düğüm sayısı 5 ile 100 arasında 5'er 5'er artmaktadır ve normalleştirilmiş ağ ömrü değerlerinin dört farklı durum için grafiği verilmiştir. Düğümler arasındaki mesafe 1m alınmıştır. Şekil 23'te gösterilen değerlere göre şu sonuçlara varabiliriz: (1) Baz istasyonunun konumunu gizlemenin ağ ömrüne olan etkisi, gerçek baz istasyonu doğrusal bir topolojinin bir ucunda olduğu durumda daha sadedir. Bunun sebebi, temel şemada elde dilen ağ ömrü değerleri, baz istasyonun merkezde konumlandırılmış olduğu durumlarda daha büyüktür. (2) Normalleştirilmiş ağ ömrü değerlerinin *SBİ* çözümlerinde monotonik bir şekilde

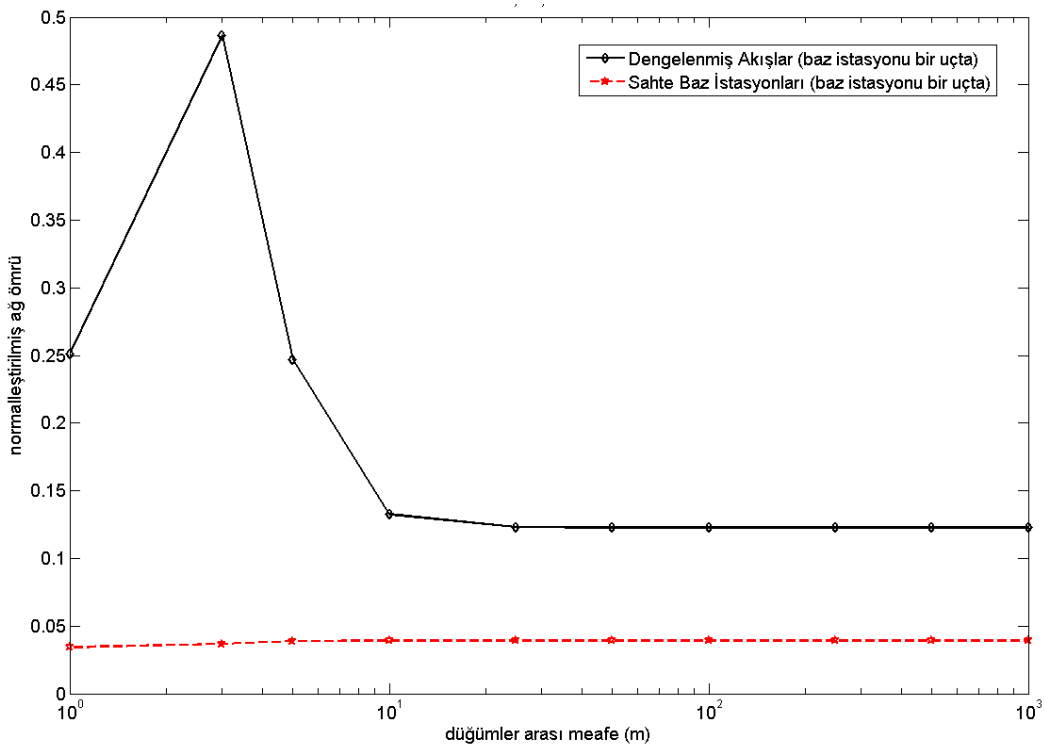
azaldığını görüyoruz. Diğer taraftan *DA* çözümlerinde, ağ büyüklüğünde belirli bir eşik değeri geçildiğinde normalleştirilmiş ağ ömrü değerlerinin ağ büyüklüğü arttıkça arttığını görüyoruz. Sonuç olarak büyük ağlarda *SBİ* çözümü daha az tercih edilen bir önlem olmaktadır. (3) *DA*'yı *SBİ*'ye tercih etmemize sebep olan ağ ömründeki artma miktarı, gerçek baz istasyonunun konumuna bağlı değildir. Örneğin, 25 düğümlük bir topolojide *DA SBİ*'ye göre baz istasyonunun bir uçta ve ortada olduğu durumlarda sırasıyla 3.50 ve 3.53 kat daha iyi sonuç vermektedir.



Şekil 23 – SBİ ve DA çözümleri için düğüm sayılarına göre normalleştirilmiş ağ ömürleri

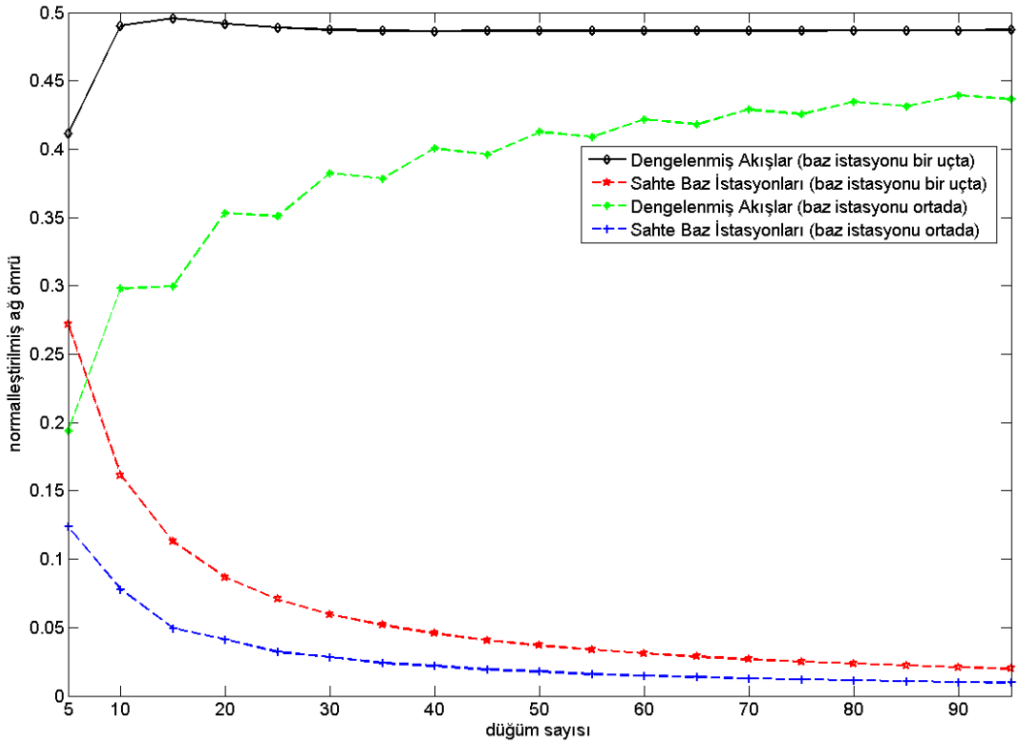
İkinci simülasyonumuzda, *SBİ* veya *DA* çözümlerinden biri uygulandığı durumda düğümler arası mesafenin ağ ömrüne olan etkisini incelemek için düğüm sayısını 50'ye sabitledik. Şekil 24'te normalleştirilmiş ağ ömürlerinin düğümler arası mesafeye göre grafiği verilmiştir. *SBİ* çözümünde normalleştirilmiş ağ ömrü, düğümler arası mesafeye göre kayda değer bir değişme göstermemektedir. Diğer taraftan *DA* çözümünde normalleştirilmiş ağ ömrü ilginç bir karakteristik göstermektedir. Düğümler arası mesafe 3m iken, normalleştirilmiş ağ ömrü tepe noktasına (0.48) ulaşmıştır. Bu davranışın sebebi, temel şemadaki optimal akışların

düğümler arası mesafe 3 m olduğu durumda *DA*'daki dengelenmiş duruma en yakın olduğundandır. Bu yüzden, baz istasyonunu saklamak için gereken en az masraf düğümler arası mesafenin 3m olduğu durumdadır.



Şekil 24 - SBİ ve DA çözümleri için düğümler arası mesafeye göre normalleştirilmiş ağ ömürleri

Üçüncü ve son analizimiz olarak birinci simülasyonumuzu düğümler arası mesafeyi 3m alarak tekrarladık (Şekil 25). Baz istasyonunun bir uçta olduğunda, normalleştirilmiş ağ ömrünün 0.48 civarında olduğu durumun, ağ büyüklüğünün bir eşik değerinden sonra (10 düğüm) elde edildiğini gözlemledik.



Şekil 25 - SBİ ve DA çözümleri için düğümler arası mesafe 3m iken düğüm sayılarına göre normalleştirilmiş ağ ömürleri

7. İLGİLİ ÇALIŞMALAR

KAA'lar üzerinde çalışan araştırmacıların çoğu enerji verimliliği konusu üzerinde durmuştur [15].

Ergen ve Varaiya doğrusal programlama kullanarak iki farklı çoklu-atlama yönlendirme şeması kullanarak algılayıcı ağ ömrünü incelemişlerdir [11]. İlk şema, yönlendirme için toplam enerji tüketimini minimize etmekte, ikinci şema ise ağ ömrünü maksimize etmektedir. Kullandıkları modelde enerji tüketimi devre sisteminde, veri iletimi ve alımında gerçekleşmektedir.

Cheng ve arkadaşları doğrusal programlama kullanarak algılayıcı ağlarda sıcak nokta problemini azaltmak için stratejileri araştırmışlardır [10]. Modellerinde düğümler, kendi iletim menzillerini ayarlayabilirler (sınırlandırılmış iletim menzillerinin etkilerini de incelemişlerdir) ve enerji tüketim modeli [12]'de kullanılan modele

dayanmaktadır. Aynı zamanda ağ yüzölçümünün, ağdaki düğüm sayısının, baz istasyonu sayısının, baz istasyonu hareketliliğinin, kümelemenin, en iyi baz istasyonu konumlandırmanın, en iyi enerjinin ve düğüm dağıtımının ağ ömrüne olan etkilerini de incelemişlerdir.

KAA'larda inkâr-edememe problemimize benzer çalışma olarak Seys ve Preneel'in yaptığı [14] düşük güçlü cihazlarda farklı imzalama şemalarının enerji tüketimlerini karşılaştırmalarını söyleyebiliriz. Çalışmalarında ECDSA'nın daha kolay uygulanabilmesi ve OTS'ye göre sadece 2.5 ila 7 kat daha fazla enerji gerektirmesinden dolayı ECDSA'yı önermişlerdir. Ölçümlerindeki OTS uygulamalarında Merkle ağacı ya da tek-yön zincirleri kullanmışlardır. Dijital imzaları genel amaçlı düşünerek imzaların algılayıcı düğümler tarafından doğrulandığını düşünmüşlerdir. Ayrıca hesaplama ve iletişim maliyetlerini birleştirilmiş bir çatı altında toplamamışlardır. Biz ise aksine, inkâr-edememe problemine özellikle vurgu yaptık ve birleştirilmiş bir DP modeli ile imzalama algoritmalarının kapsamlı ağ ömrü maliyet analizlerini yaptık.

Bazı çalışmalar açık anahtar algoritmalarının kaynak kısıtlı cihazlardaki enerji maliyetlerini ölçmüşlerdir [3-5]. Bu çalışmaların hiçbiri inkâr-edememenin ağ ömrüne olan etkilerini incelememiştir.

Verimli dijital imzalar üzerinde önceki bazı önemli çalışmaların motivasyonu gerçek zaman performansını arttırmaktı [19],[26]. Birçok KAA uygulaması için bu, ağ ömürlerine olan etkileri kadar kritik olmayan ikincil bir sorundur.

Bicakci ve arkadaşları, tek-yönlü enerji maliyetlerinin KAA ömrüne olan etkilerini incelemişlerdir [24]. Örnek tek-yön başlatma işlemleri için açık anahtar şifrelemesi kullanmışlardır. En iyilenmiş ayarlarda açık anahtar şifrelemesinin KAA'ların ömrüne olan etkisinin önemsiz olmadığının sonucuna varmışlardır.

Baz istasyonu gözlemlenemezliği problemimize benzer olarak kaynağın konumunun mahremiyeti problemi araştırılmıştır [20],[18]. Deng ve arkadaşları, saldırganın bütün bir ağ hakkında global bir bilgiye sahip olmadıkları bir tehdit modeli geliştirerek baz istasyonu konumunun mahremiyetini incelemişlerdir [17].

Bizim bu tezde incelediğimiz problemler için geliştirdiğimiz modellerimize benzer modeller KAA'larda başka ömür uzatma problemleri için kullanılmıştır. Bunlar veri sıkıştırmayı [25], tek-yönlü enerji maliyetlerini [24] vb. içermektedir.

8. SONUÇ VE GELECEKTEKİ ÇALIŞMALAR

Bu kısımda, inkâr-edememe ve baz istasyonu gözlemlenemezliği problemleri için çıkarsadığımız sonuçlara değineceğiz. Daha sonra gelecekte planladığımız çalışmalardan bahsedeceğiz.

8.1. İnkâr-edememe Problemi Sonuçları

KAA'larda enerji, az bulunur bir kaynaktır ve ağ ömrünü arttırmak için akıllıca yönetilmelidir. KAA'larda güvenlik, birçok farklı yöne sahiptir ve algılayıcı verinin inkâr-edilememesi genellikle görmemezlikten gelinen fakat bazı gerçek-dünya uygulamalarında kritik hale gelecek bir yönüdür. Önceki çalışmalar göstermiştir ki neredeyse her dijital imzalama algoritması algılayıcı düğümler üzerinde uygulanabilmektedir. Bu yüzden bugünkü KAA'larda inkâr-edememeyi sağlamak için önümüze çıkan gerçek zorluk, ağ ömrüne etkisi en az olan en iyi yöntemi seçmektir.

Bu tez çalışmasında, inkâr-edememenin kablosuz algılayıcı ağların ömrüne olan etkisini inceledik. Bu amaçla bir doğrusal programlama modeli tasarladık ve farklı imza algoritmalarının ağ ömürlerine olan etkilerini ölçmek için geniş simülasyonlar yaptık.

Özetlemek gerekirse, önemli bulgularımızı şöyle sıralayabiliriz:

- 80-bitlik güvenlik seviyesinde uygun algoritma seçimi ve geniş bir ağ parametresi yelpazesinde, inkâr-edememenin sonucu olarak gözlenen ağ ömrü düşüşü %10'dan daha az olabilmektedir. Eğer 112-bitlik bir güvenlik seviyesi isteniyorsa %10'luk ek bir düşüş daha beklenmektedir. Bu değerler 25Kb'lik imza oranı için elde edilmiştir (her 25Kb'lik veri için imzalama yapılmaktadır, bu büyüklük tipik bir resmin büyüklüğüdür).

- Küçük ağlarda, hesaplama olarak düşük maliyetli olan OTS diğer algoritmalara göre daha iyi sonuçlar vermektedir. Ağ büyüdüğünde iletim enerjisi hesaplama enerjisine baskın çıkmaktadır. Bunun sonucunda ECDSA daha tercih edilebilir hale gelmektedir. Bu iki algoritma arasındaki sınırı tam olarak çizebilmek için yayılma ortamı, düğümler arası mesafe ve güvenlik seviyesi gibi diğer parametreleri göz önüne almak gerekir.

- RSA algoritması hiçbir zaman en iyi tercih olmamaktadır; fakat sert ortamlarda ve büyük ağlarda OTS'den daha iyi sonuç verebilmektedir. RSA'nın OTS'ye olan üstünlüğü güvenlik seviyesini arttırdığımız zaman azalmaya başlamaktadır.

- Uygulamaya bağımlı bir parametre olan imza oranının, ağ ömrüne çok önemli bir etkisi vardır; fakat verilen diğer ağ parametreleri için hangi algoritmanın en iyi seçenek olduğunu değiştirmemektedir.

8.2. Baz İstasyonu Gözlemlenemezliği Sonuçları

Bundan önceki KAA'larda baz istasyonunun konumunun mahremiyeti üzerindeki çalışmalar, saldırganın tüm ağı gözlemleyemediğini varsayıyorlardı. Bu varsayım, iyi koordine edilmiş ciddi bir saldırı için geçerli değildir. Tezin bu kısmında, güçlü bir saldırganın var olduğunu farz ederek, *sahte baz istasyonları* ve *dengelenmiş akışlar* adlı iki farklı baz istasyonu saklama metodu için bir DP modeli oluşturduk. Ağ

ömrüne olan etkilerini incelemek için bu çözümleri analiz ettik ve karşılaştırdık. Araştırmamız sonucunda, baz istasyonu gözlemlenemezliğini sağlamanın ağ ömrüne olan etkisinin dikkate değer olduğunu ve en iyi ihtimalle ağ ömründe yarı yarıya bir düşüş beklenildiğini gözlemledik. Ayrıca büyük ağlarda, *dengelenmiş akışlar* çözümü ile elde edilen ağ ömrünün *sahte baz istasyonları* çözümü ile elde edilen ağ ömründen on kat daha uzun olduğunu gözlemledik.

8.3. Gelecekteki Çalışmalar

İleride, inkâr-edememe mekanizmalarının KAA'larda sağlanması problemi için doğrusal programlama modelimizi bütün bir ağda tek bir imzalama algoritma seçiminin gerek olmadığı melez algoritma kullanımının mümkün olabilecek şekilde güncellemeyi planlamaktayız (örneğin, baz istasyonuna yakın olan düğümler OTS, uzak olanlar ise ECDSA algoritmalarını kullanabilirler). Ayrıca inkâr-edememe mekanizması için kimlik tabanlı açık anahtar şifrelemesinin kullanımının ağ ömrüne olan etkilerini incelemeyi planlamaktayız.

Bu tez çalışmasında baz istasyonu gözlemlenemezliği problemi için doğrusal programlama modelimizi ağ ömrünü maksimize edecek şekilde geliştirmiştik. İleride, modelimizi ağdaki toplam enerji tüketimini minimize edecek şekilde değiştirmeyi planlıyoruz.

KAYNAKLAR

[1] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, pp. 521–534, September 2002.

[2] 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*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47.

[3] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 324–328.

[4] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, ser. SASN '06. New York, NY, USA: ACM, 2006, pp. 169–176.

[5] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *Proceedings of 4 the second ACM conference on Wireless network security*, ser. WiSec '09. New York, NY, USA: ACM, 2009, pp. 1–12.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393 – 422, 2002.

[7] S.-e. Yoo, P. K. Chong, and D. Kim, "S3: School zone safety system based on wireless sensor network," *MDPI Sensors*, vol. 9 (No. 8), pp. 5968-5988, 2009.

[8] H. Song, S. Zhu, and G. Cao, "Svats: A sensor-network-based vehicle anti-theft system," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 2128 –2136.

[9] M. Bhardwaj and A. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignments," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2002.

[10] Z. Cheng, M. Perillo, and W. B. Heinzelman, "General network lifetime and cost models for evaluating sensor network deployment strategies," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 484–497, April 2008.

[11] S. Ergen and P. Varaiya, "On multi-hop routing for energy efficiency," *Communications Letters, IEEE*, vol. 9, no. 10, pp. 880 – 881, 2005.

[12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An applicationspecific protocol architecture for wireless microsensor networks," *Wireless Communications, IEEE Transactions on*, vol. 1, no. 4, pp. 660 – 670, Oct. 2002.

[13] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 5, pp. 5:1–5:39, February 2009.

[14] S. Seys and B. Preneel, "Power consumption evaluation of efficient digital signature schemes for low power devices," in *Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on*, vol. 1, 2005, pp. 79 – 86 Vol. 1.

[15] K. Bicakci and B. Tavli, "Prolonging network lifetime with multi-domain cooperation strategies in wireless sensor networks," *Ad Hoc Networks, vol*. 8, no. 6, pp. 582 – 596, 2010.

[16] A. E. Castillo, P. Conejo, R. Pedregal, R. García, N. Alguacil, Building and solving mathematical programming models in engineering and science. Pure and applied mathematics, *in: A Wiley–Interscience Series of Texts, Monographs, and Tracts*, 2001.

[17] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 113–126.

[18] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in *Proceedings of the first ACM conference on Wireless network security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 77–88.

[19] R. Gennaro and P. Rohatgi, "How to sign digital streams," in *Advances in Cryptology CRYPTO '97*, ser. Lecture Notes in Computer Science, B. Kaliski, Ed. Springer Berlin / Heidelberg, 1997, vol. 1294, pp. 180–197, 10.1007/BFb0052235.

[20] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Network Protocols, 2007. ICNP 2007. IEEE International Conference on*, 2007, pp. 314 –323.

[21] NIST report on cryptographic key length and crypto-period (2007), http://www.keylength.com/en/4/.

[22] C.-F. Chiasserini and E. Magli, "Energy consumption and image quality in wireless video-surveillance networks," in *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, vol. 5, 2002, pp. 2357 – 2361 vol.5.

[23] General Algebraic Modeling System (GAMS) home page, http://www.gams.com/

[24] K. Bicakci, H. Gultekin, and B. Tavli, "The impact of one-time energy costs on network lifetime in wireless sensor networks," *Communications Letters, IEEE*, vol. 13, no. 12, pp. 905 –907, 2009.

[25] B. Tavli, M. Kayaalp, O. Ceylan, and I. E. Bagci, "Data processing and communication strategies for lifetime optimization in wireless sensor networks," *AEU - International Journal of Electronics and Communications*, vol. 64, no. 10, pp. 992 – 998, 2010.

[26] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," in *Advances in Cryptology CRYPTO 89 Proceedings*, ser. Lecture Notes in Computer Science, G. Brassard, Ed. Springer Berlin / Heidelberg, 1990, vol. 435, pp. 263–275.

[27] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine*, IEEE, vol. 40, no. 8, pp. 102 – 114, Aug. 2002.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: BAĞCI, İbrahim Ethem
Uyruğu	: T.C.
Doğum Tarihi ve Yeri	: 01.05.1986
Medeni Hali	: Bekâr
Telefon	: 0 (312) 292 4000 - 5045
Faks	: 0 (312) 292 40 91
e-Posta	: iebagci@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Y. Lisans	TOBB ETÜ Bilgisayar Mühendisliği	2011 (bekleniyor)
Lisans	TOBB ETÜ Bilgisayar Mühendisliği	2008

İş Deneyimi

Yıl	Yer	Görev
2008 – 2010	TOBB ETÜ	Araştırma Görevlisi

Yabancı Dil

İngilizce (ileri seviye), İspanyolca (başlangıç seviyesi)

Yayınlar

1. Dergiler

1. K. Bicakci, I. E. Bagci, and B. Tavli, “Lifetime bounds of wireless sensor networks preserving perfect sink unobservability,” *Communications Letters, IEEE*, vol. 15, no. 2, pp. 205 –207, 2011.

2. K. Bicakci, I. E. Bagci, and B. Tavli, “Communication / Computation Tradeoffs for Prolonging Network Lifetime in Wireless Sensor Networks: The Case of Digital Signatures,” (gönderildi) *Information Sciences Journal*, 2010.

3. K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, “Maximizing lifetime of event-unobservable wireless sensor networks,” *Computer Standards & Interfaces*, vol. 33, no. 4, pp. 401 – 410, 2011.

4. B. Tavli, I. Bagci, and O. Ceylan, “Optimal data compression and forwarding in wireless sensor networks,” *Communications Letters, IEEE*, vol. 14, no. 5, pp. 408 –410, May 2010.

5. B. Tavli, M. Kayaalp, O. Ceylan, and I. E. Bagci, “Data processing and communication strategies for lifetime optimization in wireless sensor networks,” *AEU - International Journal of Electronics and Communications*, vol. 64, no. 10, pp. 992 – 998, 2010.

2. Konferanslar

1. M. Kayaalp, O. Ceylan, I. E. Bagci, and B. Tavli, “Data processing and communication strategies for lifetime optimization in wireless sensor networks,” in *Signal Processing and Communications Applications Conference, 2009. SIU 2009. IEEE 17th*, 2009, pp. 769 –771.