KABLOSUZ ALGILAYICI AĞLARDA HABERLEŞME/HESAPLAMA ÖDÜNLEŞMESİ: DÜĞÜM-SEVİYE VE AĞ-SEVİYE STRATEJİLERİNİN KARŞILAŞTIRMASI

HÜSEYİN UĞUR YILDIZ

YÜKSEK LİSANS TEZİ

ELEKTRİK VE ELEKTRONİK MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2013

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Necip CAMUŞCU

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Hamza KURT

Anabilim Dalı Başkanı

HÜSEYİN UĞUR YILDIZ tarafından hazırlanan KABLOSUZ ALGILAYICI AĞLARDA HABERLEŞME/HESAPLAMA ÖDÜNLEŞMESİ: DÜĞÜM-SEVİYE VE AĞ-SEVİYE STRATEJİLERİNİN KARŞILAŞTIRMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Bülent TAVLI	Doç. Dr. Kemal BIÇAKCI
Tez Danışmanı	Tez İkinci Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Hamza KURT _____

Üye : Doç. Dr. Bülent TAVLI _____

Üye : Doç. Dr. Kemal BIÇAKCI _____

Üye : Yrd. Doç. Dr. Hakan GÜLTEKİN _____

Üye : Yrd. Doç. Dr. Harun Taha HAYVACI _____

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.

Hüseyin Uğur YILDIZ

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

Hüseyin Uğur YILDIZ

KABLOSUZ ALGILAYICI AĞLARDA HABERLEŞME/HESAPLAMA ÖDÜNLEŞMESİ: DÜĞÜM-SEVİYE VE AĞ-SEVİYE STRATEJİLERİNİN KARŞILAŞTIRMASI

ÖZET

Tipik bir kablosuz algılayıcı ağdaki (KAA) düğümlerin kısıtlı batarya gücüne sahip olması nedeniyle ağ ömrünün eniyilenmesi için, düğümlerden toplanan verinin baz istasyonuna efektif bir enerji çözümü ile iletilmesi gerekir. Baz istasyonuna iletilen verinin miktarı genellikle düğümler üzerinde gerçekleştirilen yerel işlem miktarına bağlıdır. Bazı durumlarda yerel işlem için harcanan enerji, haberleşme için harcanan enerjiden fazla olurken, bazı durumlarda ise bu durumun tam tersi bir durum söz konusu olabilir. Bu analiz ağ-seviyesinde, yani KAA'daki tüm düğümlerin tek bir algoritma kullanması durumunda, incelenebilirken düğüm-seviyesinde de, yani farklı düğümlerin farklı algoritma kullanması durumunda, incelenebilir. Bu tez çalışmasında, ağ tasarımcıların yukarıda bahsedilen ödünleşmeyi etkili bir şekilde kullanabilmesi adına, düğüm-seviye stratejisini incelemek için özgün bir Karışık Tamsayılı Doğrusal Programlama (KTDP) modeli tasarlanmıştır. Yapılan analizler sonucu düğüm-seviye stratejisi ile ağ ömrünün, ağ-seviye stratejisine göre %22.50 kadar arttırılabileceği gözlenmiştir. Ayrıca, bu çalışmada KTDP modelinin getirdiği hesaplama zorluğunun etkisini azaltmak adına polinom zamanlı sezgisel bir yöntem geliştirilmiştir. Sezgisel yöntem ve KTDP yöntemleri ile elde edilen ağ ömür değerleri arasındaki farkın %1.29'dan daha az olduğu

görülmüştür.

Anahtar Kelimeler: kablosuz algılayıcı ağlar, inkar edememe, sayısal imzalar, ağ ömrü, enerji verimliliği, doğrusal programlama, karışık tamsayılı programlama, altın oran arama, sezgisel yöntemler.

University	:	**TOBB University of Economics and Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Electrical and Electronics Engineering**
Supervisors	:	**Assoc. Prof. Bülent TAVLI**
		Assoc. Prof. Kemal BIÇAKCI
Degree Awarded and Date	:	**M.Sc. – August 2013**

Hüseyin Uğur YILDIZ

COMMUNICATION/COMPUTATION TRADEOFFS IN WIRELESS SENSOR NETWORKS: COMPARING NODE-LEVEL AND NETWORK-LEVEL STRATEGIES

ABSTRACT

In a typical wireless sensor network, data collected from sensors to be conveyed at the base station requires an energy efficient solution due to the scant battery power of nodes in order to extend the network lifetime. The amount of this data usually depends on the amount of local processing performed on nodes. There may be more local processing than communication on a node and vice versa to attain energy efficiency. This analysis can be examined at network-level where a single algorithm is employed by all nodes in a network or at node-level which provides flexibility for different nodes to implement different algorithms. To guide designers in effectively using these tradeoffs to prolong network lifetime at node-level strategy, we develop a novel mixed integer programming (MIP) framework. We show that node-level strategy can extend network lifetime up to 22.50% than the case where a single algorithm is employed at network-level. We also develop a polynomial time heuristic algorithm in order to reduce the computational complexity of the proposed MIP model. Maximum network lifetime could be obtained approximately with an error less than 1.29% with this method in very short times compared with the proposed MIP model.

Keywords: wireless sensor networks, non-repudiation, digital signature, network lifetime, energy efficiency, linear programming, mixed integer programming, golden section search, heuristics.

TEŞEKKÜR

Her şeyden önce, çalışmalarım sırasında bilimsel katkıları ile bana yardımcı olan, yüksek lisans eğitimim süresince benden yardımlarını esirgemeyen, tez danışmanım ve hocam Sayın Doç. Dr. Bülent Tavlı'ya en içten teşekkür ve saygılarımı sunarım. Yüksek lisans çalışmam için kendisinden daha iyi bir danışman ve akıl hocası olamazdı.

Bilgisayar Mühendisliği bölümünden Sayın Doç. Dr. Kemal Bıçakcı'ya da bu tez konusunu bana sağladığı için şükranlarımı sunarım. Ayrıca, bu tez çalışmasında tasarlanan sezgisel yöntem için bana yardımcı olan Endüstri Mühendisliği bölümünden Sayın Yrd. Doç. Dr. Hakan Gültekin'e de minnettarım. Tez sunumumda yorumları, kritikleri ve yorumları için tez komitesi üyeleri Sayın Hocalarım Doç. Dr. Hamza Kurt'a ve Yrd. Doç. Dr. Harun Taha Hayvacı'ya da teşekkürü bir borç bilirim.

Son olarak, Florida Uluslararası Üniversitesi'nde doktora eğitimine başlayan Bekir Sait Çiftler'e, TÜBİTAK'da çalışan Hüseyin Çotuk'a ve Erkam Uzun'a çok teşekkür ederim.

Bu tez beni dünyaya getiren, bana maddi ve manevi her türlü desteği sağlayan ailem Dr. Şükran Yıldız ile Dr. Mustafa Yıldız'a adanmıştır. Ayrıca bu tezdeki düzeltmelerde saatlerce katkıda bulunan ve benden hiçbir yardımlarını esgirmeyen dostlarım; Şafak Enes Yılmazer, Sinan Yıldırım, Arcan Ertürk, Göktuğ Çınar, Çağrı Uysal, Çağrı Uzunoğlu, Serdar Öğüt ve Emrecan Demirörs'e içten teşekkürlerimi ve şükranlarımı sunarım.

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

KISALTMALAR

Kısaltmalar	**Açıklama**
AOA	Altın Oran Arama
DP	Doğrusal Programlama
ECDSA	Eliptik Eğri Sayısal İmza Algoritması (Elliptic Curve Digital Signature Algorithm)
KAA	Kablosuz Algılayıcı Ağ
KTDP	Karışık Tamsayılı Doğrusal Programlama
OTS	Tek-Zamanlı İmza (One Time Signature)
RSA	Rivest-Shamir-Adleman
Sİ	Sayısal İmza

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
a_k^i	Düğüm-i'de hangi sayısal imza algoritmasının kullanıldığı gösteren ikili değişken
d_{ij}	Düğüm-i ile düğüm-j arasındaki uzaklık *(m)*
d_{int}	Komşu iki düğüm arası uzaklık *(m)*
e_i	Her algılayıcıdaki pil enerjisi *(J)*
$E_{c,i}$	Düğüm-i'de sayısal imzadan kaynaklanan ek enerji miktarı *(J)*
E_{Elec}	Elektronik devrede harcanan enerji *(nJ)*
E_{rx}	Bir bit veri alabilmek için gereken enerji miktarı *(J)*
$E_{tx,ij}$	Düğüm-i'den düğüm-j'ye bir bit verinin iletilmesi için gereken enerji miktarı *(J)*
f_{ij}	Düğüm-i'den düğüm-j'ye iletilen veri miktarı *(bit)*
$G = (V, A)$	Ağ topolojisini ifade eden yönlü grafik
k	Sİ algoritma belirleyicisi (k=1 OTS'yi, k=2 RSA'yı, k=3 ECDSA'yı temsil etmektedir.)
M	Ağ ömrünün üst sınırı (Sayısal imza kullanılmadığı durumda elde edilen ağ ömür değeri)
o_1^k	Sayısal imza-k'nın imza boyutu *(bit)*

o_2^k	Sayısal imza-k'yı yaratmak için gereken enerji *(mJ)*
r	İmzalama oranı (bit^{-1})
$S_{c,i}$	Düğüm-i'de sayısal imzadan kaynaklanan ek veri miktarı *(bit)*
s_i	Düğüm-i'de üretilen veri miktarı *(bit)*
t	Ağ ömrü *(s)*
V	Baz istasyonu dahil edilen düğümler kümesi
W	Baz istasyonu hariç düğümler kümesi
w_k^i	$t \times a_k^i$ ifadesini doğrusallaştırmak için kullanılan ara değişken
α	Yol kaybı katsayısı
ε_{amp}	Vericinin verimliliği *(pJ)*

1. GİRİŞ

Kablosuz Algılayıcı Ağlar (KAA) tasarsız ağlar (ad-hoc) sınıfına dahil olup temel olarak algılayıcılar (sensor düğümler) ve bu algılayıcılardan gelen verileri toplayan düğüm istasyonlarından (baz istasyonlarından) oluşmaktadır. Her algılayıcı düğüm düşük kapasiteli işlemciye, kısa menzilli kablosuz alıcı-verici çiftine ve kısıtlı pil enerjisine sahiptir. Bir KAA'da temel amaç, sıcaklık, nem, hareket gibi fiziksel olayları izleyen algılayıcı düğümlerin elde ettikleri verileri bir ana merkeze iletmesidir [1]. Algılayıcı düğümlerdeki kısıtlı batarya gücünden dolayı KAA tasarımı enerji tasarruflu bir şekilde yapılmalıdır.

Tipik bir KAA'da haberleşme ve hesaplama en çok enerji tüketen iki işlemdir. Genellikle haberleşme için gereken enerji hesaplama için gereken enerjiden daha fazladır [2]. Bu yüzden, KAA tasarımı ile uğraşan araştırmacıların temel hedefi düğümler arası haberleşme için gereken enerjiyi eniyileyerek enerji verimli bir ağ tasarlamak ve de böylece ağ ömrünü maksimize etmektir [3].

Enerjiyi verimli kullanacak bir KAA'da karşılaşılan en büyük sorun düğümlerde ne kadar yerel işlem yapılacağıdır. Örnek olarak, algılayıcı düğümlerden elde edilen ham veri hiçbir şekilde işlenmeden doğrudan ana bir merkezde (baz istasyonunda) işlenebilir. Tam zıt durumda ise, algılayıcı düğümlerde ham veri işlenerek ana merkeze daha az veri gönderilebilir. Bunun yanısıra, diğer seçenekler yukarıda bahsedilen iki uç durum arasında yer almaktadır. Örneğin, algılayıcı düğümlerde bir miktar yerel işleme yapılıp daha sonra ana merkeze veri iletimi yapılarak ağ

ömrü de maksimize edilebilir. İşte bu durum haberleşme/hesaplaşma adı altında bir ödünleşme doğrumaktadır.

Bir önceki çalışmada [3] Doğrusal Programlama (DP) modeli kullanılarak yukarıda bahsedilen ödünleşmenin analizi, ağ-seviyesinde yapılmıştır. Ağ-seviye stratejisinde her düğüm sabit bir algoritma (bu algoritma sıkıştırma, veri birleştirme veya sayısal imza vb. algoritma olabilir.) kullanmakta olup buna göre ilgili analizler gerçekleştirilmiştir. Fakat, bu çalışmada hibrit bir yöntem uygulanmak hedeflenmiştir. Yani sadece bazı algılayıcı düğümlerde yerel işleme yapılıp, diğer algılayıcı düğümlerin herhangi bir şekilde yerel işleme yapamayacağı durumun incelenmesi hedeflenmiştir. Bu tip bir strateji bundan böyle "düğüm-seviye stratejisi" olarak anılacaktır. Bu tez çalışmasında, düğüm-seviye strateji ile ağ ömrü uzatımının mümkün olup olamayacağı amaçlanmıştır.

Bu problemi somutlaştırmak adına, bu tez çalışmasında KAA'da güvenlik ile ilgili en yüksek enerji ek yüküne [4,5] sahip inkar-edememe hizmeti [1] incelenmiştir. İnkar-edememe mekanizmasındaki ödünleşmeyi incelemek adına da üç farklı sayısal imza (Sİ) algoritması bu çalışma boyunca kullanılmıştır. Bu algoritmalar, gerçek hayatta sıkça kullanılan Rivest Shamir Adleman (RSA) algoritması [6], RSA'ya alternatif Eliptik Eğri Sayısal İmza (ECDSA - Elliptic Curve Digital Signature Algorithm) algoritması [7] ve de son olarak eşsiz hesaplama/haberleşme ödünleşmesine sahip [2] Tek Zamanlı İmza (OTS - One Time Signature) [3, 8] algoritmasıdır. ECDA algoritması en düşük haberleşme ek enerjisine sahip olduğu için, RSA algoritmasının yukarıda bahsedilen üç algoritma içindeki KAA'ın ağ ömrünü maksimize edebilmek adına en kötü aday olacağı şimdiden rahatlıkla söylenebilir. Tabii ki, bu tip bir yorumu yapabilmek için öncelikli olarak detaylı bir şekilde nümerik analiz yapılmalıdır.

[1] Bu örneği seçmemizin sebebi bir önceki çalışmada [3] elde edilen değerlere göre ek enerji yükünün fazla olmasından kaynaklıdır. Fakat bu çalışmada kullanılan matematiksel model nümerik verinin mevcut olduğu farklı ödünleşme problemleri için de kullanılabilir.

[2] Bu algoritmanın hesaplama enerjisi sıfır olarak kabul edilip en yüksek imza boyutuna sahiptir.

Bu tez çalışmasında aşağıdaki sorulara cevap aranmıştır.

1. Her algılayıcı düğümün farklı opsiyonları uygulamasına müsade eden düğüm-seviye stratejisi [3] ile elde edilecek ağ ömrü değeri, ağ-seviye stratejisi ile elde edilen ağ ömrü değerinden fazla olabilir mi? Olabilirse ne kadar fazla olabilir?

2. Bu çalışmada tasarlanan matematiksel programlama modelinin getireceği hesaplama zorluğunu bir nebze olsun azalatabilecek sezgisel bir algoritma tasarımı yapabilmek mümkün müdür?

Soru 1'e cevap verebilmek adına bu çalışmanın ilerleyen bölümlerinde Karışık Tamsayılı Doğrusal Programlama (KTDP) modeli kurulmuştur. KTDP modelinde kullanılan ikili değişkenler probleme ekstra karmaşıklık kattığı için KTDP problemleri *NP-Tam* problemler olarak sınıflandırılmıştır [9, 10]. Bu hesaplama karmaşıklıkları yüzünden Soru 2'ye cevap vermek için sezgisel bir yöntem tasarlanma ihtiyacı doğmuştur. Sezgisel yöntemler eniyileme problemlerinde sıklıkla kullanılan yöntemlerdir [11, 12]. Pratikte, bu tip yöntemleri büyük ve karmaşık problemlerde kullanmak gerekmektedir. Bu yöntemlerin hedefi en iyi sonuca oldukça yakın sonuçları çok daha kısa sürede bulmaktır.

Bu tez çalışmasının organizasyonu şu şekilde yapılmıştır. Bölüm 2'de literatür taraması bulunmaktadır. Bölüm 3'de KAA ve Bölüm 4'de de matematiksel programlama ile ilgili kısa birer tanıtım yapılmıştır. Bölüm 5'de yukarıda bahsedilen KTDP modeli kurulmuş olup Bölüm 6'de bu modelin detaylı analizi yapılmıştır. Bölüm 7'de sezgisel modelin tasarlanması yapılmış olup bu algoritmanın detaylı analizi gerçekleştirilmiştir. Bölüm 8'de ise bu tez çalışmasında elde edilen önemli sonuçlar listelenmiştir.

[3] Düğüm-seviye stratejisi ekstra hesaplama zorluğu getirmekte olup bu stratejinin her durumda uygulanmayacağını kabul etmekteyiz.

2. LİTERATÜR TARAMASI

Bu bölümde, inkar-edememe ve KAA'da enerji verimliliği üzerinde yapılmış çalışmaların kısa bir özeti bulunmaktadır.

Bıçakcı ve arkadaşlarının bir önceki çalışmasında [3] haberleşme/hesaplaşma ödünleşmesinin detaylı analizi ağ-seviye stratejisi ve de DP yardımı ile gerçekleştirilmiştir. Bu çalışmada da bir güvenlik hizmeti olan inkar-edememe mekanizması bu ödünleşme kapsamında incelenmiştir. Bu çalışmanın sonunda uygun Sİ algoritması seçilmesiyle meydana gelen ağ ömründeki azalmanın %20'den daha az olabileceği gösterilmiştir.

Bu tez çalışmasına oldukça benzer bir çalışma Seys ve Preneel [13] tarafından gerçekleştirilmiştir. O çalışmada, düşük güçlü cihazlarda farklı Sİ algoritmalarına ait farklı enerji tüketim miktarlarının karşılaştırması yapılmıştır. ECDSA'nın kolay yönetilebilmesi ve de OTS'ye göre 2.5 ila 7 kat daha fazla güç gerektirmesi nedeni ile KAA'da rahatlıkla kullanılabileceği sonucuna varılmıştır. Fakat, o çalışmada bu tezden farklı olarak haberleşme ve hesaplama adına herhangi bir birleşik model kurulmamıştır.

Literatürde, enerji kısıtlı cihazlarda açık anahtar algoritmaların getireceği enerji harcamaları ile ilgili birbirinden bağımsız birkaç farklı çalışma mevcuttur [4,5,14]. Ancak bu çalışmaların hiçbirisinde inkar-edememe mekanizmasının ağ ömrüne olan etkisi incelenmemiştir.

DP modelleri kullanılarak KAA'da inceleme yapılan bazı çalışmalar aşağıdaki gibi sıralanmıştır.

Ergen ve Varaiya DP modeli kullanarak iki farklı yönlendirme yönteminin KAA'ın ömrüne olan katkısını incelemiştir [15]. Bu yöntemlerin ilki ağ ömrünü maksimize etmeyi hedeflerken, diğeri ise enerji tüketimini minimize etmeye çalışmıştır. Artan iletim uzaklığının KAA'ın enerji korunumunda (iletim enerjisinin devresel enerjiye oranı) baskın olduğu gözlenmiştir.

Alfieri ve arkadaşları algılayıcıların uzaysal fazlalılığın ağ ömrüne olan etkilerini KTDP modeli yardımı ile incelemiştir [16]. Ağ ömrünü maksimize edebilmek için bazı algılayıcı düğüm kümelerinin belirli zaman periyotlarında aktif olması gerektiği vurgulanmıştır. Ayrıca algılayıcı düğümlerin inaktif olduğu durumlarda ise enerjinin korunması gerektiği önemle belirtilmiştir. Buna ek olarak, merkezi ve dağıtık yaklaşımların (sezgisel yöntem ile) analizi bu çalışma kapsamında yapılmıştır.

Cheng ve arkadaşlarının [17]'deki çalışmalarında DP modeli kullanarak algılayıcı ağlarda sıcak nokta probleminin etkilerini azaltmak adına çalışmışlardır. Kullanılan modelde düğümler, kendi iletim menzillerini ayarlayabilmektedirler. (Ayrıca sınırlandırılmış iletim menzillerinin etkileri de bu çalışmada incelenmiştir.) Aynı zamanda ağ yüz ölçümünün, ağdaki düğüm sayısının, baz istasyonu sayısının, baz istasyonu hareketliliğinin, kümelemenin, en iyi baz istasyonu konumlandırmanın, en iyi enerjinin ve düğüm dağıtımının ağ ömrüne olan etkileri de bu çalışma kapsamında incelenmiştir.

Bıçakcı ve arkadaşları tek-yönlü enerji maliyetlerinin KAA ömrüne olan etkilerini incelemişlerdir [18]. Örnek tek-yön başlatma işlemleri için açık anahtar şifrelemesi kullanmışlardır. KTDP modeli ile yapılan eniyileme ile açık anahtar şifrelemesinin KAA'ların ömrüne olan etkisinin önemsiz olmadığı sonucuna varılmıştır.

Tavlı ve arkadaşları veri boyutunu azaltmak adına, veri sıkıştırmanın uygun bir

şekilde ayarlanması için özgün bir DP modeli geliştirmiştir [19]. Bu çalışmada, üç farklı sıkıştırma ve iletim tekniği tasarlanmıştır. Bu yöntemler ile en uygun veri sıkıştırma ve akım dengelemesi ortaklaşa biçimde gerçekleştirilmiş olup ağ ömrü eniyilenmiştir. Bu durumda elde edilen ağ ömrü değerleri, hiçbir şekilde sıkıştırma yapılmaması veya tamamen sıkıştırma yapılması ile elde edilen ağ ömrü değerinden daha fazladır. Ayrıca daha gelişmiş bir DP modeli yardımı ile çok-seviyeli dinamik sıkıştırmanın ve akım dengelemesinin ortaklaşa eniyilenmesi gerçekleştirilmiştir [20]. Dinamik sıkıştırma tekniği ile elde edilen ağ ömrü değerinin, hiçbir şekilde sıkıştırma yapılmaması veya tamamen sıkıştırma yapılması ile elde edilen ağ ömrü değerinden biraz fazla olduğu gösterilmiştir.

Santos ve arkadaşları KAA topolojisinde düğüm kümelendirmesinin etkilerini incelemiştir. Ayrıca, KAA topolojisi üretmek adına iki tane sezgisel yöntem ve enerji tüketim değerlendirme modelleri tasarlanmışlardır. [21].

Hoang ve arkadaşları bir verinin belirli algılayıcı düğüme ait olması halinde, bu verinin bir kümenin başına gelerek diğer algılayıcı düğümlerin kendi verilerini sıkıştırabilmesi için bu veriyi kullanabilmesini önermiştir [22]. Ağ ömrünü maksimize etmeyi amaçlayan bu eniyileme problemi; iletim, alım ve sıkıştırma işlemlerinin modelde birer kısıt olarak uygulanmasını içermektedir. Ayrıca bu modelde sezgisel bir yöntem tasarlanmış olup en iyi sonuca oldukça yakın sonuçlar elde edilmiştir.

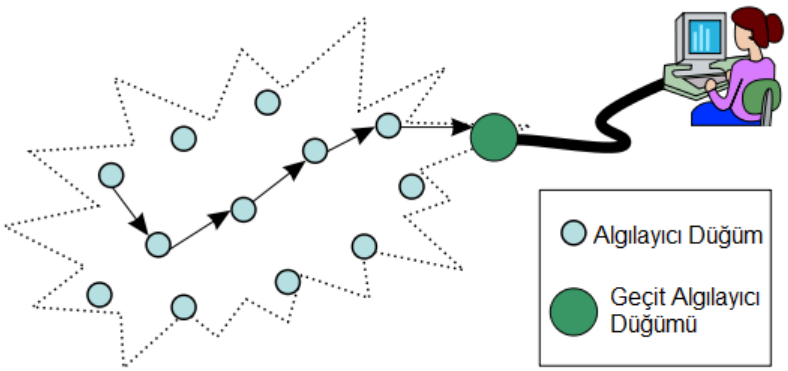
3. KABLOSUZ ALGILAYICI AĞLAR

Bir kablosuz algılayıcı ağ (KAA) kısıtlı bataryaya, kısa mesafeli alıcı-vericiye sahip düşük güç ve maliyetli çok sayıda algılayıcının güvenilir olmayan bir ortama rastgele bırakılmasıyla oluşan tasarsız ağlardır. Her bir algılayıcı düğüm, çevresindeki sıcaklık, nem, basınç gibi fiziksel olayları ölçebilme, basit hesaplama işlemleri yapabilme ve diğer algılayıcı düğümler veya merkez baz istasyonuyla haberleşme yapabilme özelliklerine sahiptir [23, 24]. Algılayıcıların düşük spesifikasyonlarından dolayı, geniş bir alanda oldukça yüksek sayıda algılayıcı kullanımı gerekmektedir.

Bugün gelinen noktada, KAA'lar değişik uygulama alanları için devrimsel algılama özelliği yetenekleri sunmaktadır. KAA'lar askeri uygulamalar başta olmak üzere farklı birçok endüstride kullanılmaktadır. Ayrıca KAA'lar endüstriyel işlem izleme ve kontrolünde, makine sağlık durum kontrolü ve benzeri diğer uygulamalarda sıkıkla kullanılmaktadır [25].

Tipik bir tasarsız ağ ile KAA arasındaki farklar aşağıdaki gibi listelenmiştir [23]:

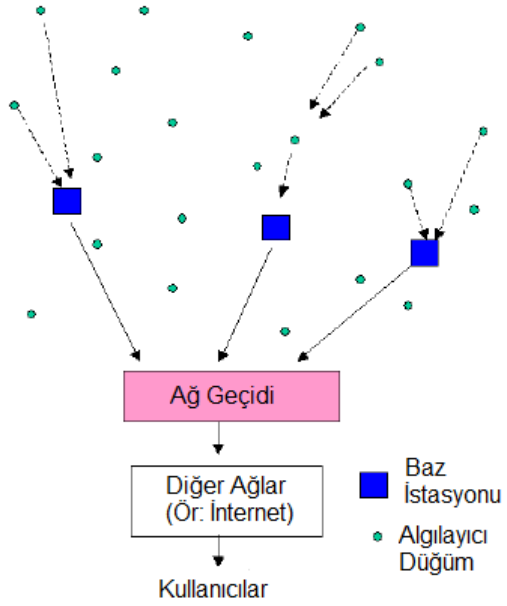
- KAA'daki toplam düğüm sayısı tasarsız ağdaki düğüm sayısından fazla olabilir.



Şekil 3.1: Tek baz istasyonuna sahip tipik çok-atlamalı KAA mimarisi

- KAA'daki düğümler sık bir şekilde konuşlandırılmıştır.
- KAA'daki topoloji değişiklikleri sıktır.
- Algılayıcı düğümlerde hata oluşma riski fazladır.
- Genel olarak, KAA'da düğümler radyo yayını (broadcast) ile haberleşmeyi sağlarken, tasarsız ağlar noktadan noktaya haberleşme teknolojisi kullanırlar.
- Algılayıcı düğümler kısıtlı batarya gücüne, hesaplama kapasitesine ve hafızaya sahiptir.
- Algılayıcı düğümlerin ek yükü fazla olduğu için genel kimlik (ID) değeri olmayabilir.

Şekil 3.1'de tipik bir tek baz istasyonlu KAA mimarisi verilmiştir. Literatürde yapılan hemen hemen bütün çalışmalar, bu geleneksel mimariye sadık kalmıştır. Fakat, bu mimari ölçeklenebilir değildir. Yani, KAA'daki algılayıcı düğüm sayısı arttığı zaman baz istasyonunda toplanan verinin miktarı da artar, böylece baz istasyonu kapasitesine ulaşınca KAA daha fazla genişletilemez [26].



Şekil 3.2: Birden fazla baz istasyonuna sahip tipik çok-atlamalı KAA mimarisi

KAA'da ölçeklenebilirlik problemine çözüm olarak genellikle birden fazla baz istasyonu Şekil 3.2'deki gibi kullanılmaktadır [27–29]. Bu topoloji sayesinde sinyal yayılma koşullarından dolayı verilerini teslim edemeyen düğümlerin birer izole küme oluşturma olasılığı büyük ölçüde azaltılmış olur. Çoklu baz istasyonuna sahip bir KAA'da algılayıcı düğüm sayısı artsa bile ölçeklenebilirlikten dolayı performans kaybı yaşanmamaktadır. Çoklu baz istasyonlu bir KAA, tek baz istasyonlu bir KAA'nın ufak bir gelişimi olarak görülmemelidir. Çoğu durumda düğümler verilerini baz istasyonlarının birisinde toplamaktadır. Bu baz istasyonu ise daha sonra son kullanıcıya veri iletilmesi amacıyla bir ağ geçidi olarak kullanılmaktadır [26].

3.1 KAA'ların Uygulama Alanları

Bilgisayar bilimi ve telekomünikasyon alanlarında, 1990'lı yılların ortasından itibaren KAA üzerine yapılan araştırmalar hızla artmaktadır. Tipik KAA uygulamaları: askeri, çevresel, sağlık ve diğer ticari alanlardaki uygulamalar olarak kategorize edilebilir [23]. Bu sınıflandırma uzay keşfi, kimyasal işleme ve afet yardımı gibi bu tez çalışmasının dışına çıkan konuları da kapsamaktadır. Literatürde üzerinde çalışmalar yapılan popüler KAA uygulamaları aşağıdaki gibi listelenmiştir.

3.1.1 Konum Belirleme

Nesne takibi [30–33] ve çevre izleme [34,35] gibi KAA uygulamalarının temelinde konum belirleme tekniği bulunmaktadır. Ayrıca konum bilgisi topoloji kontrolü, yönlendirme, kümelendirme gibi temel ağ katmanı hizmetleri için de kullanılmaktadır. Bu yüzden, algılayıcı düğümler arasında otonom ilişki kuran konum belirleme teknikleri KAA uygulamalarının içinde önemli bir yere sahiptir [36]. KAA'da konum belirleme ile ilgili yapılan önemli çalışmalar [37–40]'da bulunabilir.

3.1.2 Veri Birleştirme

Algılayıcı düğümlerden toplanan veri, kablosuz ortamda noktadan noktaya transmisyon ile baz istasyonuna iletilmektedir. Maksimum ağ ömrüne ulaşmak için algılanan veri, ara düğümler tarafından uygun bir algoritma ile birleştirilebilir. Veri birleştirme yöntemi ile ağda dolaşan trafik miktarı önemli miktarda azaltılarak algılayıcı düğümlerde haberleşme için gereken enerji miktarı düşmektedir [41–45].

3.1.3 Bağlanırlık

Kapsama (coverage) ve bağlanırlık (connectivity) KAA'daki en temel iki konu olup ağın hizmet kalitesini (Quality of Service) gösteren ölçütler olarak bilinmektedir [46–49]. Bu yöntemler sayesinde bir alan içindeki her düğümün nasıl kapsandığı ve de düğümlerde verilerin nasıl toplandığı öğrenilebilir. Kapsama alanının maksimize edilmesi ve bunun yanısıra ağın bağlanırlığının arttırılması, KAA tasarımında büyük bir önem arz etmektedir [50].

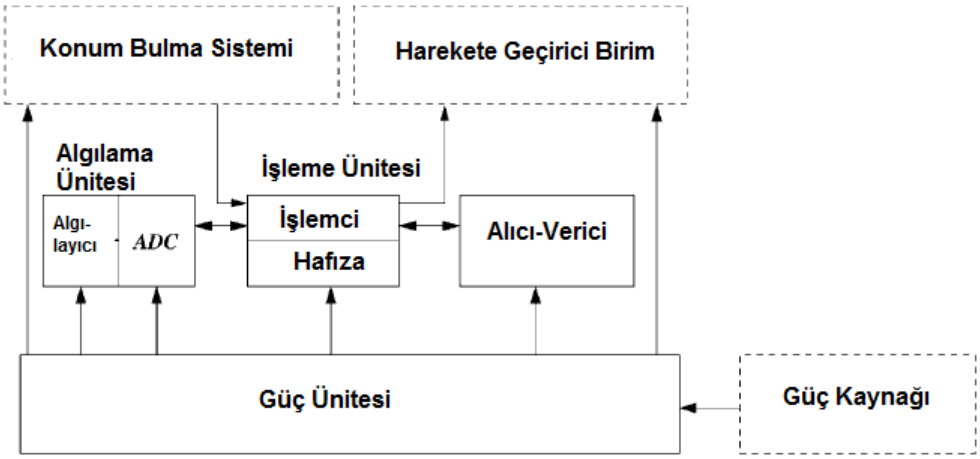
3.1.4 MAC Protokolleri

Ortam Erişim Kontrolü (MAC - Medium Access Control) ağın başarılı bir şekilde çalışmasının garantisini verir [51]. MAC protokollerinin en önemli özelliği enterferans *(girişim)* yapan düğümlerin ağa karışmasını önlemektir. Radyodaki "Boş" dinlemeden dolayı klasik IEEE 802.11 MAC protokolü oldukça fazla miktarda enerji tüketmektedir. Güç bakımından verimli bir MAC protokolü tasarlamak, ağ ömrünü uzatmanın önemli bir yöntemidir. Bu yüzden, ağ tasarımcıları enerjiyi verimli kullanan MAC protokolleri tasarlamak üzerine araştırmalarını yoğunlaştırmaktadır. Literatürdeki en önemli enerji verimli MAC protokolleri: PEGASIS [52], LEACH [53], HEED [54] ve S-MAC [55]'dır.

3.2 Platformlar

3.2.1 Donanım

KAA'daki her algılayıcı düğümün Şekil 3.3'de görüleceği üzere bazı önemli bileşenleri vardır. Bunlar:



Şekil 3.3: Bir algılayıcı düğümdeki bileşenler

1. İletme, Alma, Boş ve Uyku modlarında çalışabilen iç antene sahip kısa menzilli alıcı-verici çifti (radyo) [1] [2].

2. Algılayıcının kontrolünü, hesaplama yapabilmesini ve haberleşme protokollerinin düzgün bir şekilde çalışmasını sağlayan mikroişlemci.

3. Bir grup algılayıcı ve dış dünya ile iletişim kurabilen bir veya birden fazla alıcı istasyon.

4. Her algılayıcı düğüme ait pil enerjisi [3].

Piyasada kabul gören en popüler algılayıcı modeli "Mica" olup 2001 yılında piyasaya sürülmüştür. İlk model Mica, 4 MHz frekanslı Atmel ATmega103L işlemcisini; 4 KB RAM, 128 KB flash hafızası ve 115.2 Kbps'a kadar RF veri iletimine izin verebilen RFM TR1000 radyosunu kullanmaktaydı [56]. Mica'yı takip eden

[1] Düğümlerde sıklıkla kullanılan radyo Chipcon CC1000 olup -20 dBm ile +10 dBm çıkış anten gücüne sahiptir.

[2] Radyonun veri iletilmediği zaman "Boş" konumu yerine tamamen kapatılması enerji tüketimini oldukça azaltmaktadır.

[3] Baz istasyonu pilden bağımsız bir şekilde bir kaynaktan beslenmektedir.

süreçte 2002 yılında Kaliforniya Üniversitesi: Berkeley'de Mica2 ve Mica2Dot düğümleri geliştirilmiştir [57]. Bu aile, Atmel ATmega 128L [58] mikroişlemcisini kullanmakta olup radyo seçiminde FKA (Faz Kaydırmalı Anahtarlama) modülasyonu kullanarak gürültü gücünü azaltan Chipcon CC1000 [59] radyosunu tercih etmiştir. Bundan bir yıl sonra MicaZ, 802.15.4/ZigBee protokolü destekleyen, 250 Kbs üzeri kablosuz veri iletişimi sağlayan Chipcon CC2420 geniş band modülüyle üretildi. Bu modül aynı zamanda kriptografik şifreleme ve kimlik doğrulamayı da desteklemektedir.

3.2.2 Yazılım

KAA için geliştirilmiş farklı uygulamalar ile işletim sistemleri mevcuttur. TinyOS [60] KAA'da sık kullanılan bir işletim sistemi olup RISC mimarisine sahip Atmel ATmega 128L ve TI MSP430 [61] işlemci tabanlı düğümlerde kullanılmaktadır. Ayrıca, ağ ömrünü maksimize edecek, dayanıklılığı sağlayacak, hata toleransını düzenleyecek ve kendinden konfigürasyon yapacak yazılımlar da piyasa da mevcuttur.

4. MATEMATİKSEL PROGRAMLAMA

Matematiksel Programlama (MP) ya da Matematiksel Optimizasyon (eniyileme) matematiksel olarak modellenebilen problemlere ait en iyi sonucu bulma bilimidir. Bu tip problemlerin matematiksel modelleri fiziksel olaylar, yönetimsel konular ya da üretim ile ilgili olabilir [62]. Basit bir örnek olarak, bir gerçel fonksiyonu minimize ya da maksimize etmek amacı ile girdi olarak gerçel ya da tamsayı değerlerini tanımlı bir aralıkta alan değişkenlerin fonksiyona yerleştirilerek sistematik olarak bir problemin incelenmesi ya da çözülmesi, bir eniyileme problemini tanımlar.

4.1 Doğrusal Programlama

Bir fonksiyonun yerel optimum değerlerini bulmak adına cebirsel olarak formülasyonlar geliştiren ilk kişiler Fermat ve Lagrange'dır. Newton ve Gauss ise tekrarlamalı yöntemler ile en iyi sonuca yakınsayan yöntemler geliştirmişlerdir. Tarihsel olarak ilk eniyileme terimi olan "Doğrusal Programlama (DP)", George Dantzig tarafından 1947 yılında yayınlanan makalesinde ortaya çıkmıştır [63]. DP, belli doğrusal eşitsizlikler veya eşitliklerin kısıtlayıcı koşulları altında doğrusal bir amaç fonksiyonunu minimize veya maksimize etmeyi hedefler. Dantzig DP'lerin çözümü

için Simpleks Yöntemini üretmiştir. John von Neumann aynı yıl içinde ikincillik (duality) teorisini çıkarmıştır.

Tipik bir DP'deki zorunlu bileşenler aşağıdaki gibidir:

1. **Karar Değişkenleri:** Çözümü tanımlar.
2. **Amaç Fonksiyonu:** Çözümlerin kalitesinin bir ölçütüdür.
3. **Kısıtlar:** Karar değişkenleri arasındaki ilişkileri belirler.
4. **Sınırlar:** Optimizasyon probleminde kullanılan değişkenlerin değerleri önceden belirlenmiş bir küme içinden verilir.

Bu karar değişkenleri modelin kurulması sürecinde dinamik bir şekilde değişir ve de optimum çözüme/çözümlere ulaşıldığı zaman durur.

Klasik bir DP kanonik formda aşağıdaki gibi ifade edilebilir:

$$\begin{aligned} &\text{maks} \quad c^T x, \\ &\text{kısıtlayıcılar} \quad Ax \leq b, \\ &\text{ve } x \geq 0. \end{aligned}$$

Bu denklemlerde x sürekli değişkenleri içeren vektörü belirtmektedir. Bu değer dinamik bir şekilde değişmektedir. c ve b bilinen katsayıları ifade etmekte, A bilinen bir katsayı matrisini ve c^T matrisin tersi olup $c^T x$ maksimize veya minimize edilmeye çalışılan hedef fonksiyonunu ifade etmektedir. $Ax \leq b$ eşitsizlikleri optimize edilmeye çalışılan hedef fonksiyonu üzerindeki kısıtları göstermektedir. Son olarak, $x \geq 0$ ifadesi x değişkeninin sınırlarını ifade etmektedir.

DP problemlerinin sistematik bir şekilde çözülmesi için birkaç algoritma geliştirilmiştir. Bunlardan en önemlileri Dantzig'in "Simpleks Algoritması", "Karmarkar

Metodu" [64] ve "İç Nokta Algoritması"dır. Fakat, bu tezde bu yöntemlerin detaylarına girilmeyecektir.

4.2 Tamsayılı Programlama

Bir önceki bölümde açıklanan bilinmeyen değişkenlerin sadece tamsayı değerler alması durumunda bu problem "Tamsayılı Programlama (TP)" veya "Tamsayılı Doğrusal Programlama (TDP)" kategorisine girer. DP'ye kıyasla, çoğu TP problemleri pratikte *NP-Zor* [1] sınıfına dahildir.

Bazı durumlarda tamsayı değişkenleri sadece 0 veya 1 değerlerini alabilir. Bu tip programlama modelleri "0-1 Tamsayılı Programlama" veya "İkili Tamsayılı Programlama" olarak bilinir. Bu tip problemler de *NP-Zor* olarak bilinir ve hatta bu model Karp'ın 21 *NP-Tam* problemleri içinde mevcuttur [65].

Bazı değişkenlerin tamsayı, kalan diğer değişkenlerin de sürekli değişken olması gibi bir durum söz konusu olursa, bu tip programlama modelleri ise "Karışık Tamsayılı Doğrusal Programlama (KTDP)" olarak bilinir. Bu tip problemler *NP-Tam* sınıfındadır. *NP* problemlere ait daha detaylı açıklama için Bölüm 7 incelenebilir.

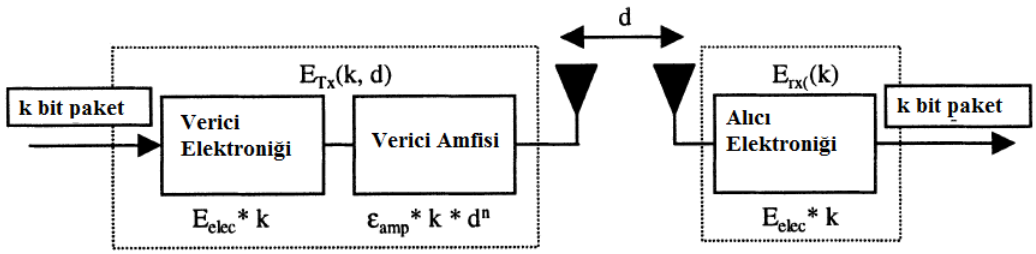
TP'leri çözmek için kullanılan popüler algoritmalar: Dal Sınır Yöntemi *(Branch and Bound)*, Kesme Düzlem Yöntemi *(Cutting-Planes)* ve Dal Kes Yöntemi'dir *(Branch and Cut)*.

CPLEX [66], birkaç programlama dili için API'ye sahip popüler bir çözücüdür. Ayrıca AIMMS, AMPLS, GAMS, MPL, OpenOpt, OPL Development Studio ve TOMLAB ile uyumlu bir şekilde çalışmaktadır. Son olarak CPLEX akademik kullanımlar için de ücretsizdir.

[1] *NP-Zor* problemler kombinatoryal optimizasyon problemler olup detaylı arama yöntemleri ile optimum sonuca ulaşmak uygulanabilir değildir.

5. SİSTEM MODELİ

Bu tez çalışmasında [17, 67]'de belirtilen basit radyo dalga yayılım modeli kullanılmıştır. Şekil 5.1'de bu radyo modelinde kullanılan alıcı ve verici çifti görülebilir.



Şekil 5.1: Radyo Enerji Tüketim Modeli

k bit boyutundaki verinin bu kanal modelinde alınması ve de iletilmesi için gereken enerji miktarları (J) aşağıdaki gibi verilmiştir:

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

$$E_{rx} = E_{Elec} \times k.$$

Doğal olarak, düğüm-i'den düğüm-j'ye gönderilmeye çalışılan bir bit veri için gereken enerji:

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

ve bir bit verinin alınması için gereken sabit enerji:

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

olarak hesaplanabilir. Bu denklemlerde E_{Elec}, elektronik devrede harcanan enerjiyi ifade ederken ε_{amp} vericinin efektifliğini gösterir. α yol kaybını temsil etmekte olup genellikle $\alpha \in [2, 4]$ olarak alınır. Düğüm-i ile düğüm-j arasındaki uzaklık d_{ij} olarak tanımlanmıştır. Literatürde bu enerji/kanal modeli "Çok Yollu Sönümleme Kanalı" olarak bilinir. Her algılayıcı düğüm baz istasyonunda toplanacak şekilde birim zamanda s_i miktarda veri üretmektedir.

Bu çalışmada KAA topolojisi yönlü bir grafik olan $G = (V, A)$ şeklinde kabul edilmiş olup V, tüm düğümlerin (baz istasyonu dahil) kümesini ifade etmektedir. Ayrıca W kümesi, $W = V \setminus \{1\}$, baz istasyonu dışında kalan tüm düğümlerin kümesini gösterir. Ağdaki linklerin kümesi $A = \{(i, j) : i \in W,\ j \in V - i\}$ şeklinde tanımlanmıştır. Dikkat edileceği üzere bu notasyon sayesinde hiçbir algılayıcı düğümün kendisine veri gönderemeyeceği ile baz istasyonunun hiçbir şekilde veri üretemeyeceği garantilenmiş olur. Düğüm-i'den düğüm-j'ye iletilen veri miktarı f_{ij} olarak tanımlanmıştır. Zaman, eşit süreli turlara bölünmüştür. Son olarak, algılayacı düğümlerde üretilen veri, baz istasyonuna ya direkt olarak gidebilir ya da diğer algılayıcı düğümler üzerinden aktarılarak iletilebilir.

Varsayımlarımızda, KAA'nın durağan algılayıcı düğümlerden oluştuğunu ve mobil (hareketli) tasarsız ağlardaki gibi topoloji değişikliklerinin sık gerçekleşmediğini kabul etmekteyiz. Literatürdeki tanımlara sadık kalınarak ağ ömrü [15,17,68], ilk algılayıcı düğümün tüm batarya gücünü tükettiği zaman olarak tanımlanmıştır.

Bu tez çalışmasında kullanılan kısaltmaların açıklamalı listesi Çizelge 0.1'de sunulmuş olup simgeler ise Çizelge 0.2'de verilmiştir.

Ağ ömrünü (amaç fonksiyonu t'yi) maksimize etmeyi amaçlayan eniyileme probleminin en genel hali, aşağıdaki kısıtlara göre verilmiştir:

$$\sum_{j \in V} f_{ij} - \sum_{j \in W} f_{ji} = s_i t + S_{c,i} \ \forall i \in W, \tag{5.1}$$

$$E_{rx} \sum_{j \in W} f_{ji} + \sum_{j \in V} f_{ij} \ E_{tx,ij} + E_{c,i} \leq e_i \ \forall i \in W, \tag{5.2}$$

$$S_{c,i} = s_i \times r \times t \times \{\sum_{k=1}^{n} o_1^k \times a_k^i\} \ \forall i \in W, \tag{5.3}$$

$$E_{c,i} = s_i \times r \times t \times \{\sum_{k=1}^{n} o_2^k \times a_k^i\} \ \forall i \in W, \tag{5.4}$$

$$\sum_{k=1}^{n} a_k^i = 1 \ \forall i \in W, \tag{5.5}$$

$$f_{ij} \geq 0 \ \forall (i,j) \in A, \tag{5.6}$$

$$a_k^i \in \{0,1\} \ \forall i \in W, \forall k \in [1,n]. \tag{5.7}$$

Denklem (5.1), akım dengeleme kısıtı olup baz istasyonu dışında kalan düğümler için, düğüm-i'den çıkan akımlar ile düğüm-i'ye gelen akımlar arasındaki farkın düğüm-i'de üretilen toplam veri miktarına eşit olduğunu belirtmektedir. Düğüm-i'de üretilen toplam veri miktarı, ağ ömrü boyunca düğüm-i'nin ürettiği veri miktarı ($s_i t$) ile Sİ'den kaynaklanan ek yük miktarının ($S_{c,i}$) toplamı kadardır.

Denklem (5.2), enerji kısıtını ifade etmektedir. Bir algılayıcı düğümdeki toplam enerji tüketimi; alma enerjisi, iletim enerjisi ve de düğümlerde Sİ üretiminden kaynaklanan ek enerji yükünü ($E_{c,i}$) içermektedir. Ayrıca, tanım gereği hiçbir algılayıcı düğüm batarya enerjisinden (e_i) daha fazla enerji tüketememektedir.

Denklem (5.3) ve Denklem (5.4), düğüm-i'de Sİ'den kaynaklanan ek imza boyutunu ve ek hesaplama enerjisini göstermektedir. Diğer haberleşme/hesaplama ödünleşmesi problemleri için sadece bu iki denklemin değişmesi yeterlidir.

Ağ ömrü boyunca imzalama işlemlerinin sayısı $s_i \times t \times r$ olarak verilmiştir. Burada r imzalama oranını ifade etmektedir. Ayrıca çeşitli Sİ algoritmalarının imza boyutları o_1^k, imza yaratmak için gereken ek enerji miktarı o_2^k olarak tanımlanmıştır.

Denklem (5.5)'de tanımlanan ve de kısıtları verilen a_k^i'nın sadece tek bir değer almasından dolayı Denklem (5.3)'deki $-\{\sum_{k=1}^{n} o_1^k \times a_k^i\}-$ ve Denklem (5.4'deki $-\{\sum_{k=1}^{n} o_2^k \times a_k^i\}-$ terimlerinde kullanılan o_1^k ile o_2^k değişkenleri de tek bir değer almaktadır. Daha açık olmak gerekirse, eğer $a_1^3 = 1$ ise Denklem (5.5)'e göre $a_2^3 = a_3^3 = 0$ olur. Bu da Denklem (5.3) ve Denklem (5.4)'deki o_1^1 ve o_2^1 değişkenlerini ortaya çıkararak düğüm-3'ün OTS algoritmasını kullanacağını gösterir. Böylelikle, her düğüm kendisi için en uygun olan Sİ algoritmasını seçerek (farklı düğümlerin farklı algoritma kullanması durumu: düğüm-seviye stratejisi) ağ ömrü maksimize edilir.

Denklem (5.6), ağdaki tüm akımların negatif olamayacağını belirten kısıtıdır. Denklem (5.7) ile a_k^i değişkeninin sadece ikili değerler alabileceği belirtilmektedir. Bu denklemde n, farklı Sİ algoritma sayısını ifade etmektedir.

Denklem (5.3) ve (5.4)'deki sürekli değişken t ile ikili değişken a_k^i'nın çarpımı eniyileme problemini doğrusallıktan çıkarır. Fakat bu model, doğrusal KTP modeline dönüştürülebilir. Eniyileme problemi için ilk önce doğrusal olmayan modeli açıklamayı tercih edilmesinin sebebi anlaşılmasının kolay olmasındandır.

Çizelge 5.1: $w_k^i = t \times a_k^i$ için olası tüm çarpımlar

a_k^i	t	$t \times a_k^i$	Kısıtlar	Sonuç
0	$t : 0 \leq t \leq M$	0	$w \leq t$ $w \leq 0$ $w \geq 0$ $w \geq t - M$	$w = 0$
1	$t : 0 \leq t \leq M$	t	$w \leq t$ $w \leq M$ $w \geq t$ $t \geq 0$	$w = t$

Doğrusallaştırma için, doğrusal olmayan $t \times a_k^i$ terimi yerine Denklem (5.8) ve (5.9)'de w_k^i kullanılmıştır.

$$S_{c,i} = s_i \times r \times \{\sum_{k=1}^{n} o_1^k \times \underbrace{w_k^i}_{t \times a_k^i}\} \; \forall i \in W. \tag{5.8}$$

$$E_{c,i} = s_i \times r \times \{\sum_{k=1}^{n} o_2^k \times \underbrace{w_k^i}_{t \times a_k^i}\} \; \forall i \in W. \tag{5.9}$$

Denklem 5.10'deki kısıt eklenerek sürekli değişkenin yerini aldığı terimin özelliklerini koruduğu garantilenmiştir. Yani, $w_k^i = t$ eşitliği sadece bir k değeri için sağlanırken, diğer k değerleri için 0 olmalıdır. Ayrıca a_k^i değerlerinden bağımsız olarak, w_k^i, Denklem (5.10)'de de görüleceği üzere ağ ömründen fazla olmamalıdır.

$$w_k^i \leq t \; \forall i \in W, \forall k \in [1, n]. \tag{5.10}$$

Denklem (5.11)'de ağ ömrünün (t) herhangi bir Sİ algoritması kullanılmadığı durumda elde edilen ağ ömrü değerinden (M) küçük olacağı belirtilmektedir.

$$w_k^i \leq M \times a_k^i \ \forall i \in W, \forall k \in [1, n]. \tag{5.11}$$

$a_k^i = 0$ olduğu durumda $w_k^i = 0$ şartını sağlamak için Denklem (5.12)'deki gibi pozitiflik kısıtı eklenmiştir.

$$w_k^i \geq 0 \ \forall i \in W, \forall k \in [1, n]. \tag{5.12}$$

$a_k^i = 1$ olduğu zaman, $w_k^i = t$ eşitliğini sağlanması için Denklem (5.10) ile birlikte çalışan Denklem (5.13) eklenmiştir.

$$w_k^i \geq t - M \times (1 - a_k^i) \ \forall i \in W, \forall k \in [1, n]. \tag{5.13}$$

$a_k^i = 0$ olursa Denklem (5.13)'ün sağ tarafı pozitif olamayacağı için ve de Denklem (5.12)'deki pozitiflik kısıtından ötürü, w_k^i doğru değeri olan 0 değerini alır. $w_k^i = t \times a_k^i$'a ait tüm olası çarpımlar Çizelge 5.1'de verilmiştir.

Sonuç olarak, doğrusallaştırılmış KTP modeli (5.1), (5.2) ve (5.5)'den (5.13)'e kadar olan denklemlerdeki kısıtlar ile kurulmuştur.

6. DENEYSEL ÇALIŞMA

Tez çalışmasının bu kısmında, Bölüm 1'de tartışılan haberleşme/hesaplama ödünleşmesi ile ilgili detaylı analizler çeşitli kurgular ve parametre kümeleri için incelenmiştir. Bahse konu bu ödünleşmenin somut bir şekilde incelenmesi için bir güvenlik mekanizması olan inkar-edememe hizmeti kullanılmıştır. Bu hizmet üç farklı Sİ algoritmasını desteklemektedir. Her Sİ algoritması 80-bit (2^{80}) ve 112-bit (2^{112}) olmak üzere iki güvenlik seviyesinde incelenmiştir.

Güvenlik seviyesinin 80 bit olduğu durumda kullanılan Sİ algoritmaları OTS-80, RSA-1024 ve ECDSA-160'dır. Bu imzaların boyutları (o_1^k) sırasıyla 3120 bit, 1024 bit ve 320 bittir [69]. Bu algoritmaların imza yaratma enerjileri (o_2^k) ise yine sırasıyla 0 mJ, 304 mJ ve 22.82 mJ'dir [5]. 112-bit güvenlik seviyesi incelendiği zaman kullanılan Sİ algoritmaları OTS-112, RSA-2048 ve ECDSA-224'dır [69]. Bu durumda, imzaların boyutları sırasıyla 6160 bit, 2048 bit ve 448 bittir. İmza yaratma enerjileri ise yine sırasıyla 0 mJ, 2302.7 mJ ve 61.54 mJ'dür [5]. Bu tez çalışmasında kullanılan Sİ'lere ait parametrelerin listesi Çizelge 6.1'de verilmiştir.

Alıcı-verici çifti için kullanılan enerji parametreleri, $E_{Elec} = 50\ nJ$ ve $\varepsilon_{amp} = 100\ pJ$'dir [67]. Her algılayıcı düğümün batarya enerjisi $e_i = 243\ J$'dür. Bu değer, %25'i algılama, sıkıştırma, yön bulma gibi diğer görevlere ayrıldığı farz edilmiş 30 mAh'lik bir pilin %75'ini oluşturmaktadır [3]. Bu parametreler Çizelge 6.2'de listelenmiştir.

Çizelge 6.1: Sayısal imzalara ait parametreler

k	Sİ	Sİ boyutu *(bit)* o_1^k	Sİ maliyeti *(mJ)* o_2^k
1	OTS-80	3120	0
2	RSA-1024	1024	304
3	ECDSA-160	320	22.82
1	OTS-112	6160	0
2	RSA-2048	2048	2302.7
3	ECDSA-224	448	61.54

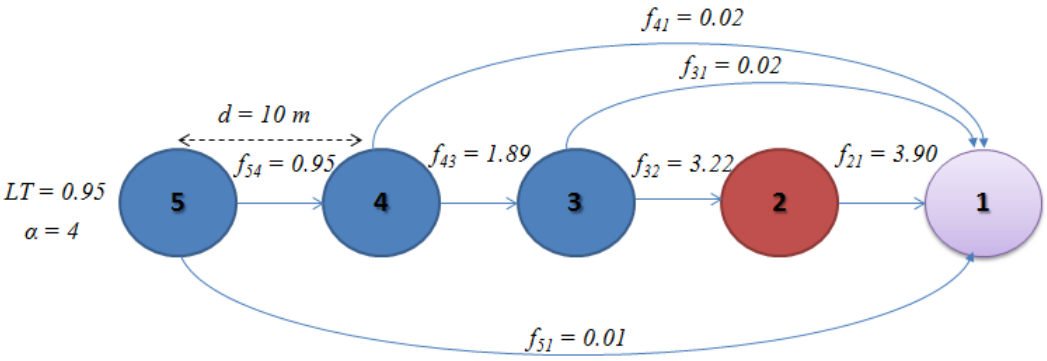
Çizelge 6.2: Enerji Parametreleri

Açıklama	**Sembol**	**Değer**
Elektronik Enerji	E_{Elec}	50 nJ
Amfi Enerjisi	ε_{amp}	100 pJ
Batarya Enerjisi	e_i	243 J

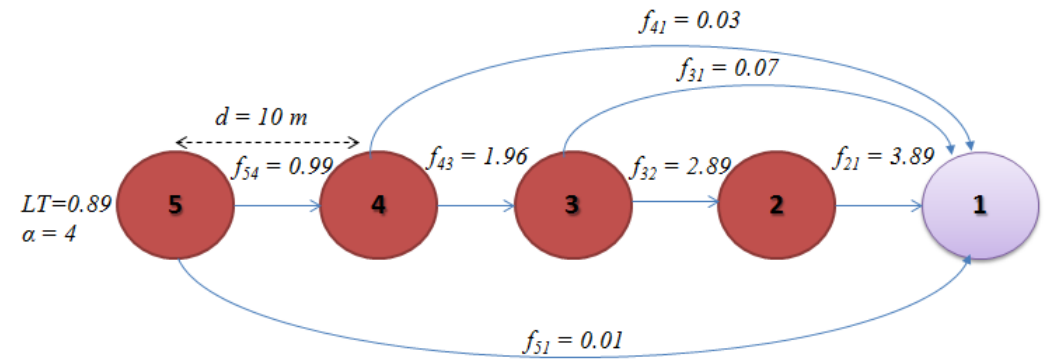
Her algılayıcı düğümde birim zamanda üretilen veri miktarı (s_i) 1 bittir. KAA'larda sıkıştırılmış tipik bir resmin boyutu 25344 bit (25 KB) [70] olduğu için simülasyonlarda imzalama oranı (r) aksi söylenmedikçe 1/25344 olarak alınmıştır. Matematiksel programlama ve eniyileme için GAMS IDE 23.9.1 [71] ara yüzü altında CPLEX 12.4 [66] çözdürücüsü kullanılmıştır.

6.1 Basit Örnek

Detaylı analizlere başlamadan önce bu bölümde Şekil 6.1a'deki basit bir doğrusal topoloji üzerinde haberleşme/hesaplama ödünleşmesi incelenmiştir. Bu doğrusal topoloji beş düğüm içermekte olup düğümler 10 metre aralıklar ile dizilmiştir ($d_{int} = 10\ m$). Yol kayıp katsayısı $\alpha = 4$ alınıp 80-bit güvenlik seviyesi için basit

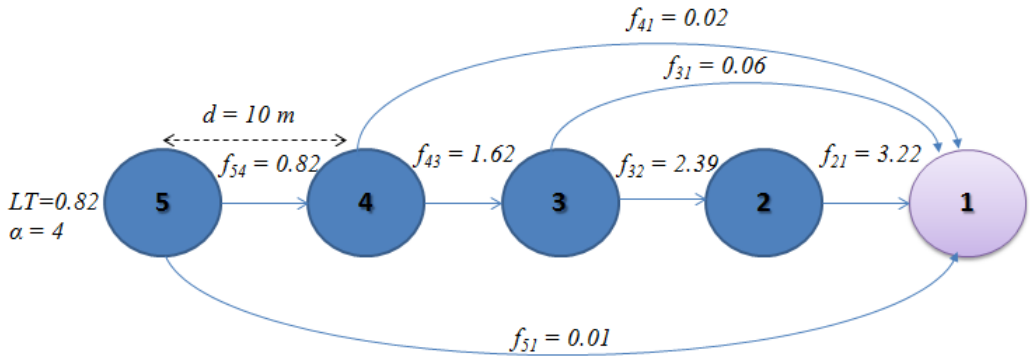


(a) Düğüm-Seviye stratejisi

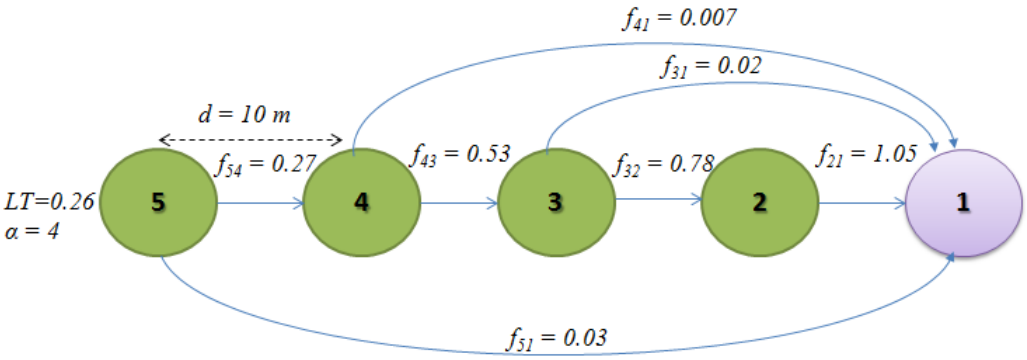


(b) Ağ-Seviye stratejisi: OTS-80

Şekil 6.1: Sİ algoritmalarının düğüm-seviyesinde (a), OTS-80'nin ağ-seviyesinde (b), ECDSA-160'ın ağ-seviyesinde (c), RSA-1024'ün ağ-seviyesinde (d) uygulandığı durumdaki akım dengeleri ile buna karşılık gelen ağ ömür değerleri *(Kırmızı ile renklendirilen düğümler OTS-80 kullanırken, ECDSA-160 kullananlar mavi, RSA-1024 kullananlar yeşil renk ile gösterilmiştir.)*



(c) Ağ-Seviye stratejisi: ECDSA-160



(d) Ağ-Seviye stratejisi: RSA-1024

analizler yapılmıştır.

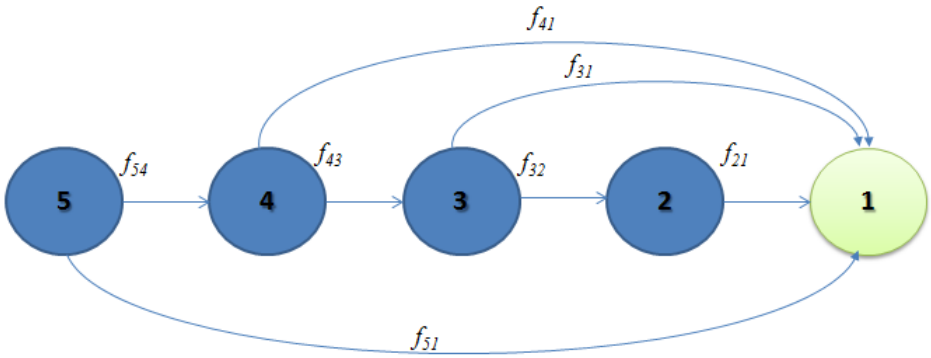
Şekil 6.1a'dan Şekil 6.1d'ye kadar olan topolojide baz istasyonu düğüm-1 olarak kabul edilmiş olup koordinatları $(0, 0)$'dır. Kalan düğümlerin koordinatları ise $(-10, 0)$, $(-20, 0)$, $(-30, 0)$ ve $(-40, 0)$'dır. Ağ ömrünün maksimize edilmesi için yani herhangi bir düğümün enerjisi erkenden bitmemesi ve bütün düğümlerin enerjilerini aynı anda bitirebilmesi için düğümler arasındaki veri akışlarının akıllı bir şekilde dengelenmesi gerekir.

Bölüm 5'de geliştirilen KTDP modeli (Şekil 6.1a) ile [3]'de geliştirilen DP modelleri (Şekil 6.1b'den 6.1d'e kadar) GAMS yardımı ile çözdürülmüştür. Bu grafiklerde gösterilen mutlak ağ ömrü değerleri (LT), Sİ algoritmaları kullanılmadığı durumda elde edilen ağ ömrü değerlerine göre normalleştirilmiştir. Şekil 6.1b'deki düğüm-5 incelenecek olursa akımınını iki parçaya böldüğü (%99'unu düğüm-4'e, %1'ini de baz istasyonuna) görülebilir. Eğer düğüm-5 tüm akımını baz istasyonuna göndermeye çalışsaydı, optimum durumdan daha fazla enerji tüketimi gerçekleşecekti böylece ağ ömrü maksimize edilemeyecekti.

Düğüm-seviye stratejisi ile elde edilen normalleştirilmiş ağ ömrü $LT = 0.95$ olarak hesaplanmıştır. OTS-80'in ağ-seviyesinde uygulanmasıyla elde edilen ağ ömrü değeri $LT = 0.89$, ECDSA-160 için $LT = 0.82$ ve de RSA-1024 için $LT = 0.26$ olarak hesaplanmıştır. Böylece ilk baştaki tezimizi destekleyecek şekilde düğüm-seviye stratejisi ile ağ ömrü, OTS-80'in ağ-seviye strateji ile uygulandığı durumda elde edilen ağ ömrüne göre %6.74 arttırılmıştır. Bu durumda, Şekil 6.1a'de, maksimum ağ ömrü, düğüm-2'nin OTS-80 (kırmızı ile renklendirilen düğüm), kalan diğer algılayıcı düğümlerin ECDSA-160 algoritması kullanması (mavi ile renklendirilmiş) ile elde edilir. RSA-1024'ün bu senaryoda kullanılmamasının sebebi, verilen Sİ algoritmaları içinde imza yaratma enerjisinin en yüksek olmasından kaynaklanmaktadır.

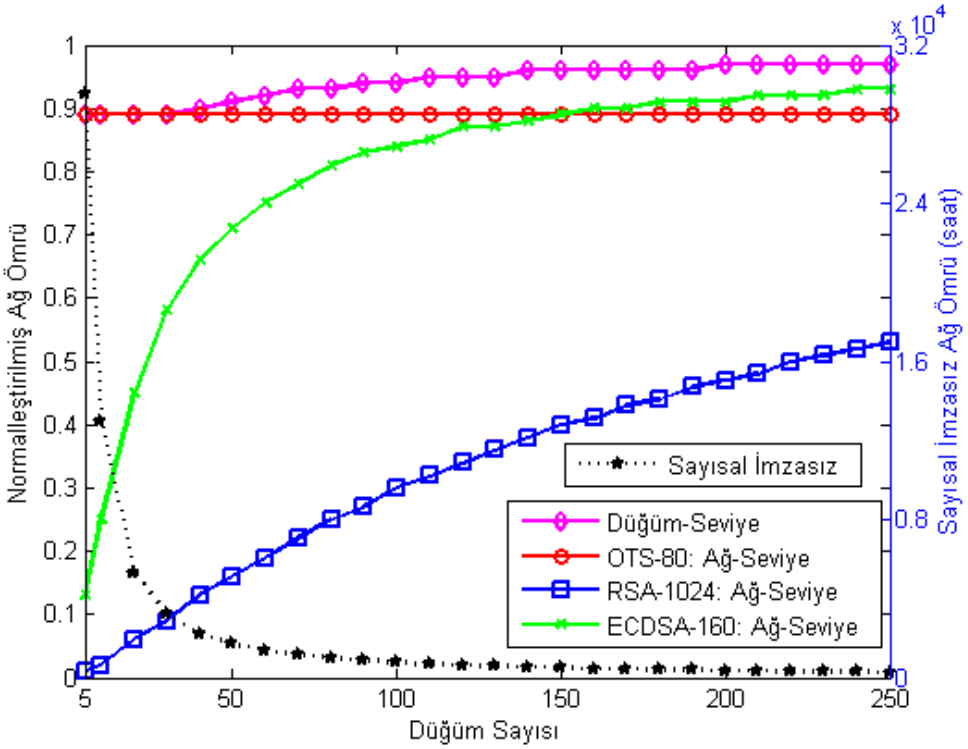
6.2 Doğrusal Topoloji

Bu noktaya kadar, haberleşme/hesaplama ödünleşmesinin basit bir analizi beş düğümlük doğrusal bir topoloji üzerinde incelenmiştir. Bu kısımda, Bölüm 6.1'de uygulanan yöntemler baz alınarak daha büyük bir doğrusal topoloji için analizler yapılmıştır. Otoyolu ve trafik izleme [17] gibi uygulamalar doğrusal ağ topolojileri esas alınarak tasarlandığı için, böyle bir analizin bu tez çalışması kapsamında gerekli olduğu aşikardır.



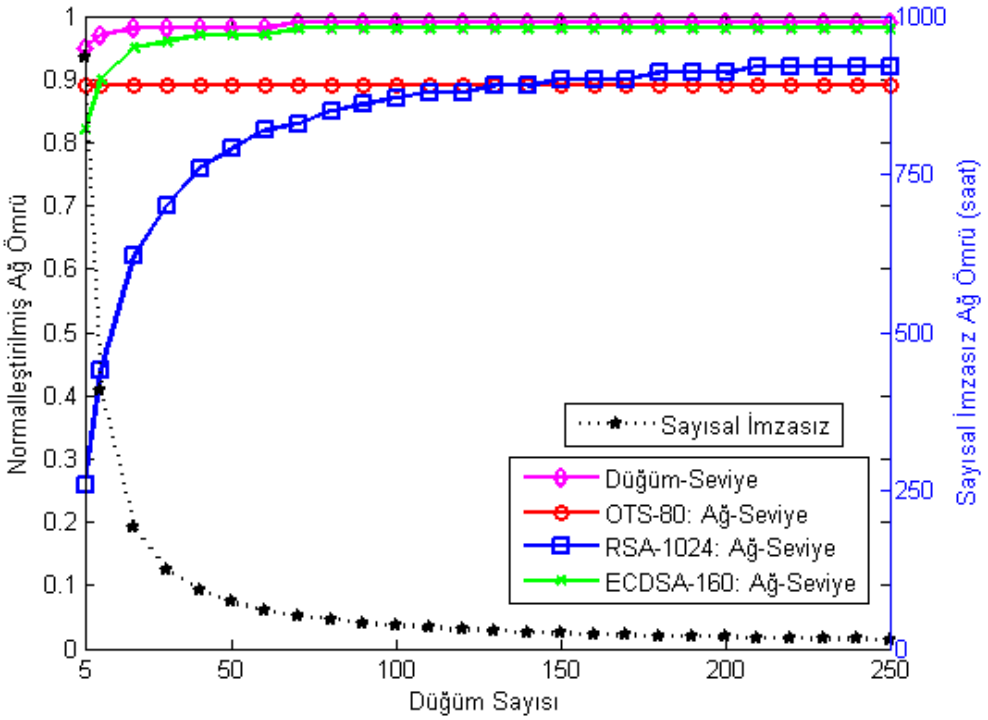
Şekil 6.2: Doğrusal ağ topolojisi. Düğüm-1 baz istasyonunu temsil etmektedir. Düğüm-i'den düğüm-j'ye akan veri f_{ij} ile gösterilmiştir.

Bu bölümde kullanılan doğrusal ağ topolojisinde N tane düğüm eşit aralıklarla bir doğru üzerine sıralanmış olup baz istasyonu Şekil 6.2'de görüleceği üzere bu doğrunun en sağ ucunda yer almaktadır (düğüm-1). Komşu iki düğüm arası uzaklık sabit tutulup $d_{int} = 10\ m$ olarak alınmıştır. Ağ-seviye ve düğüm-seviye stratejileri ile elde edilen normalize edilmiş ağ ömrü değerleri, farklı yol kayıp katsayıları ve iki farklı güvenlik seviyesi için incelenmiştir. İlk olarak güvenlik seviyesi 80-bit alınmış olup OTS-80, RSA-1024 ve ECDSA-160 Sİ algoritmaları kullanılmıştır. Düğüm-seviye stratejisi ile elde edilen ağ ömrünün ağ-seviye stratejisi ile elde edilen ağ ömrüne göre daha fazla olması beklenmiştir.



Şekil 6.3: 80-bit güvenlik seviyesi, $\alpha = 2$ ve doğrusal topoloji için normalleştirilmiş ağ ömür değerleri

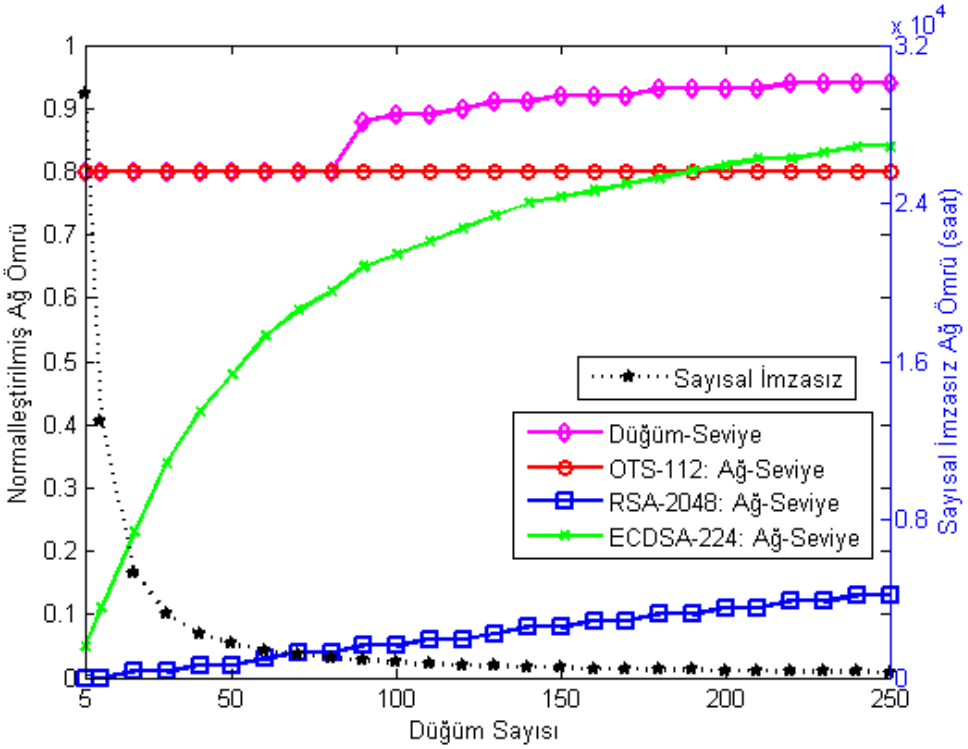
Şekil 6.3 ve 6.4'de düğüm-seviye ve ağ-seviye stratejileri ile elde edilen ağ ömür değerleri herhangi bir Sİ algoritması kullanılmadığı durumda elde edilen ağ ömrüne göre normalleştirilmiştir (y-ekseninin sol tarafında). Ayrıca Sİ kullanılmadığı zaman elde edilen mutlak ağ ömrü değerleri ise (saat cinsinden) y-ekseninin sağında çizdirilmiştir. Yani kısacası, y-eksenin solunda kalan değerler, y-ekseninin sağında kalan değerlere göre normalleştirilmiştir. Örneğin, normalleştirilen ağ ömrünün 0.9 çıkması demek, Sİ kullanılmadığı zaman elde edilen ağ ömrü değerine göre %10 daha düşük bir ağ ömrüne sahip olduğu anlamında gelir. Bu bölümde ağ boyutları önce 5, daha sonra 10 düğüm ile devam edip, 10'ar düğüm artarak 250 düğüme kadar çıkmaktadır.



Şekil 6.4: 80-bit güvenlik seviyesi, $\alpha = 4$ ve doğrusal topoloji için normalleştirilmiş ağ ömür değerleri

Şekil 6.3'de yol kaybı katsayısı serbest uzay modelindeki gibi ($\alpha = 2$) alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-160'ın veya OTS-80'in ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömürlerine göre %8.99 daha fazla olabileceği görülmüştür. Bu durumda, baz istasyonuna yakın olan ilk 30 düğüm OTS-80 kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-160 kullandığı tespit edilmiştir. Böylece, 30 düğümden fazla düğüm içeren ağların ömürlerinin düğüm-seviye stratejisi ile arttırılabileceği açıktır. Önceden de belirtildiği gibi yüksek enerji maliyetinden ötürü ağdaki hiçbir algılayıcı RSA-1024 algoritmasını seçmemektedir.

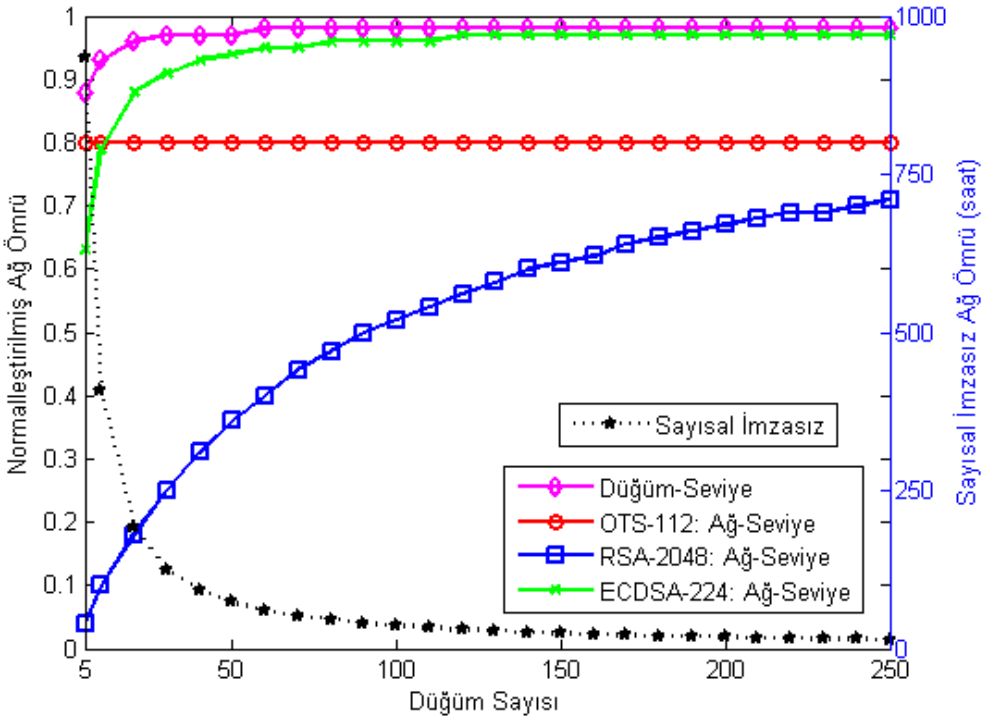
Şekil 6.4'de yol kaybı katsayısı arttırılmıştır ($\alpha = 4$). Bu durumda düğüm-seviye



Şekil 6.5: 112-bit güvenlik seviyesi, $\alpha = 2$ ve doğrusal topoloji için normalleştirilmiş ağ ömür değerleri

stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-160'ın veya OTS-80'in ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömürlerine göre %11.24 daha fazla olabileceği görülmüştür. Haberleşmeden kaynaklı artan enerji maliyetinden ötürü baz istasyonuna yakın olan ilk 5 düğüm OTS-80 kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-160 kullandığı tespit edilmiştir. Böylece, 5 düğümden fazla düğüm içeren ağların ağ ömrünün düğüm-seviye stratejisi ile arttırılabileceği açıktır. Yine, beklenildiği gibi hiç bir algılayıcı RSA-1024 algoritmasını seçmemektedir.

Güvenlik seviyesinin 80 bitten 112 bite çıkarılmasıyla ağ ömründe meydana gelecek değişimi izlemek için, aynı doğrusal topoloji ve yol kayıp katsayıları ile deneyler tekrarlanmıştır. 112 bit güvenlik seviyesi için OTS-112, RSA-2048 ve



Şekil 6.6: 112-bit güvenlik seviyesi, $\alpha = 4$ ve doğrusal topoloji için normalleştirilmiş ağ ömür değerleri

ECDSA-224 algoritmaları Çizelge 6.1'deki o_1^k ve o_2^k değerleri ile kullanılmıştır.

Şekil 6.5'de $\alpha = 2$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-224'ün veya OTS-112'nin ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömürlerine göre %17.50 daha fazla olabileceği görülmüştür. Bu durumda, baz istasyonuna yakın olan ilk 80 düğüm OTS-112 kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-224 kullandığı tespit edilmiştir. Böylece, 80 düğümden fazla düğüm içeren ağların ağ ömrünün düğüm-seviye stratejisi ile arttırılabileceği açıktır.

Şekil 6.6'de $\alpha = 4$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-224'ün veya OTS-112'nin ağ-seviye stratejisi

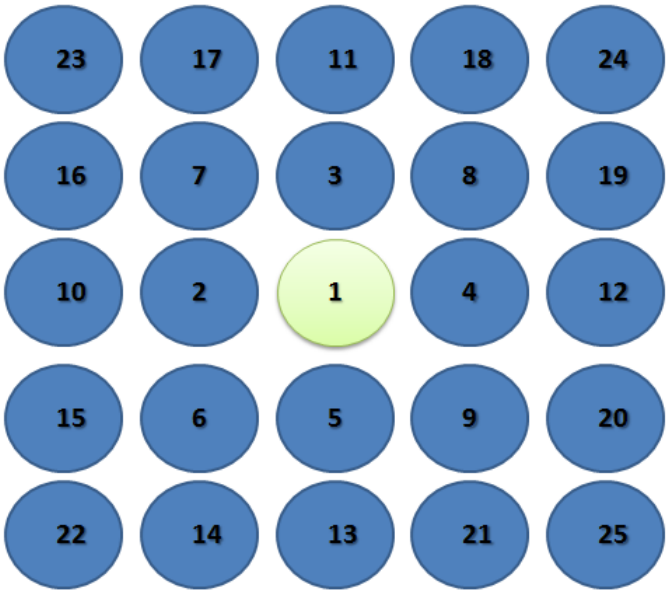
ile uygulanması ile elde edilen ağ ömürlerine göre %22.50 daha fazla olabileceği görülmüştür. Bu durumda, baz istasyonuna yakın olan ilk 5 düğüm OTS-112 kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-224 kullandığı tespit edilmiştir. Böylece, 5 düğümden fazla düğüm içeren ağların ağ ömrünün düğüm-seviye stratejisi ile arttırılabileceği açıktır.

Demek ki, yol kayıp kat sayısı düşük tutulduğunda düşük ek enerjiye sahip OTS Sİ algoritmasını kullanan düğümlerin sayısı 112 bit güvenlik seviyesi için 80-bit güvenlik seviyesine göre daha fazla çıkmaktadır. Fakat, haberleşme enerjisinin baskın enerji tüketimi olduğu durumda (yani yol kayıp katsayının arttırıldığı durumda) az sayıda düğümün OTS algoritmasını seçtiği görülmüştür. Bunun en önemli sebebi, ECDSA algoritmasının en düşük ek enerji yüküne sahip olmasındandır. Böylece düğümlerde haberleşmeden kaynaklı ek enerji yükü büyük ölçüde azaltılmıştır.

6.3 Kare Topoloji

İnkar-edememe hizmeti, KAA'da en iyi doğrusal topolojide gözlenmesine rağmen çoğu pratik ağ topolojileri iki boyutlu (2D) olarak tasarlanmıştır. Bu yüzden tezin bu kısmında, Bölüm 6.2'de yapılan analizlerin kare topoloji için tekrarı yapılmıştır. Literatürde KAA'lar için iki boyutlu topoloji olarak kare topolojinin kullanıldığı çalışmalar [16, 72–74]'de görüleceği üzere sıklıkla kullanılmıştır.

Şekil 6.7'deki kare topolojisi bu bölümdeki analizlerde kullanılmıştır. Bu topolojide baz istasyonu karenin ortasına yerleşmiş olup dikey ve yatay eksenlerdeki komşu düğümlerin uzaklıkları yine 10 metre olarak alınmıştır. Ayrıca kare topolojilerin boyutları 9, 25, 49, 81, 121, 169, 225 ve 289 düğümlü olup bu durum bir kare yaratmak için yeterlidir.

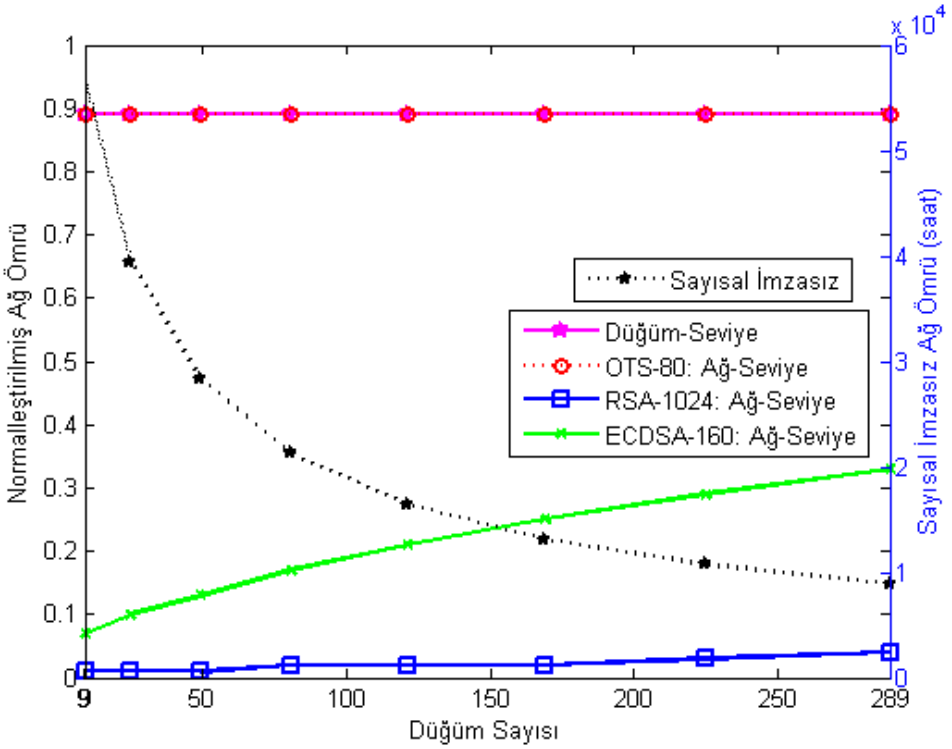


Şekil 6.7: Kare ağ topolojisi. Düğüm-1 baz istasyonunu temsil etmektedir.

Şekil 6.8'de $\alpha = 2$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrü; OTS-80'in ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömrüne eşittir. Ayrıca, RSA-1024 ile ECDSA-160 hiçbir düğüm tarafından kullanılmamıştır.

Şekil 6.9'de $\alpha = 4$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-160'ın veya OTS-80'in ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömürlerine göre %10.11 daha fazla olabileceği görülmüştür. Ayrıca, baz istasyonuna en yakın olan 9 düğüm OTS-80 kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-160 kullandığı tespit edilmiştir. Böylece, 9 düğümden fazla düğüm içeren ağların ömrünün düğüm-seviye stratejisi ile arttırılabileceği açıktır.

Güvenlik seviyesinin 80 bitten 112 bite çıkarılmasıyla ağ ömründe meydana gelecek değişimi izlemek için, aynı kare topoloji ve yol kayıp katsayıları ile deneyler tekrarlanmıştır. 112 bit güvenlik seviyesi için OTS-112, RSA-2048 ve ECDSA-224

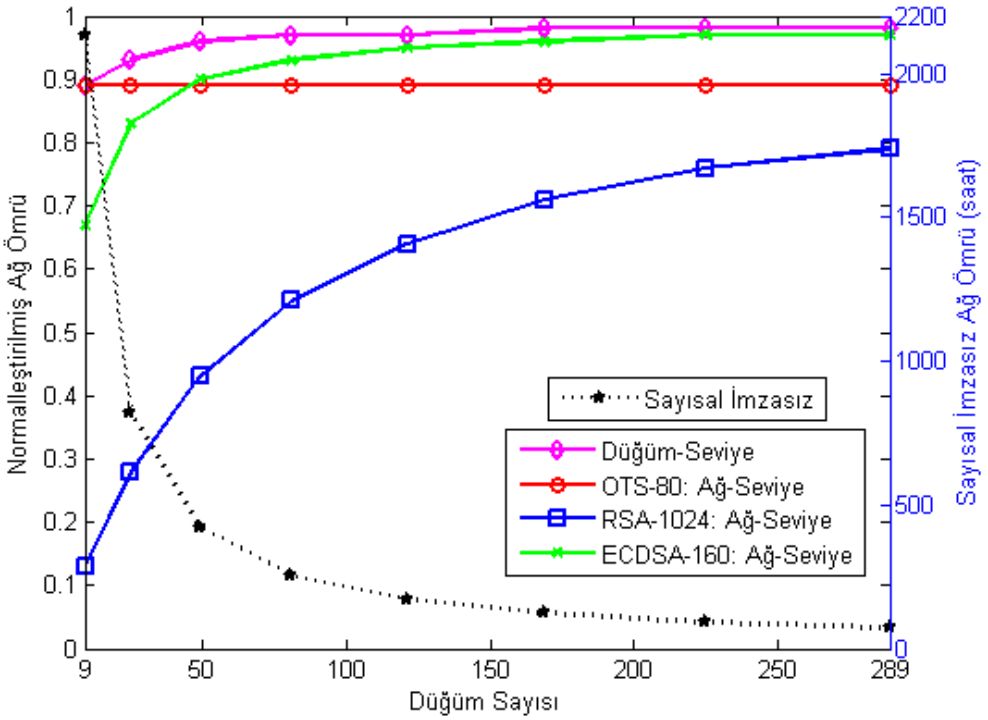


Şekil 6.8: 80-bit güvenlik seviyesi, $\alpha = 2$ ve kare topoloji için normalleştirilmiş ağ ömür değerleri

algoritmaları Çizelge 6.1'deki o_1^k ve o_2^k değerleri ile kullanılmıştır.

Şekil 6.10'de $\alpha = 2$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrü; OTS-112'nin ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömrüne eşittir. Ayrıca, RSA-2048 ile ECDSA-224 hiçbir düğüm tarafından kullanılmamıştır.

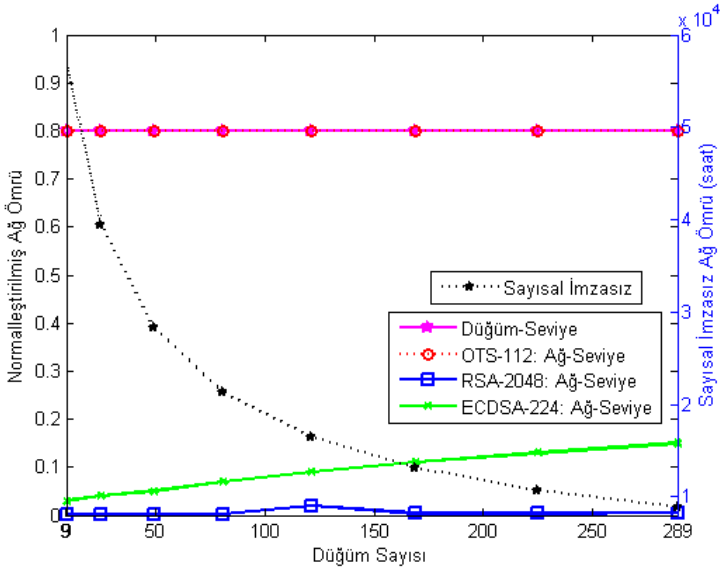
Şekil 6.11'de $\alpha = 4$ alınmıştır. Bu durumda düğüm-seviye stratejisi uygulanarak elde edilen ağ ömrünün, ECDSA-224'ün veya OTS-112'nin ağ-seviye stratejisi ile uygulanması ile elde edilen ağ ömürlerine göre %21.25 daha fazla olabileceği görülmüştür. Bu durumda, baz istasyonuna en yakın olan 9 düğüm OTS-112



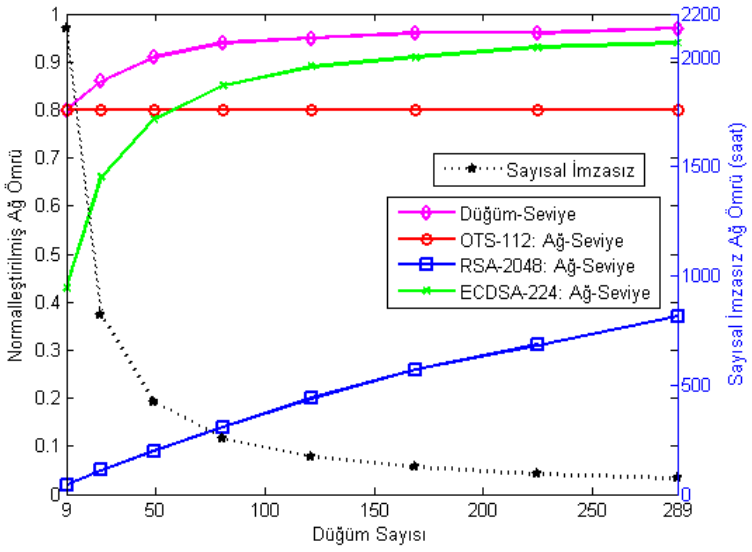
Şekil 6.9: 80-bit güvenlik seviyesi, $\alpha = 4$ ve kare topoloji için normalleştirilmiş ağ ömür değerleri

kullanırken, kalan diğer algılayıcı düğümlerin ECDSA-224 kullandığı tespit edilmiştir. Böylece, 9 düğümden fazla düğüm içeren ağların ömrünün düğüm-seviye stratejisi ile arttırılabileceği açıktır.

Demek ki, yol kayıp kat sayısı düşük tutulduğunda tüm düğümler güvenlik seviyelerinden bağımsız olarak en düşük ek enerjiye sahip OTS Sİ algoritmasını kullanmaktadır. Fakat, haberleşme enerjisinin baskın enerji tüketimi olduğu durumda (yani yol kayıp katsayının arttırıldığı durumda) az sayıda düğümün OTS algoritmasını seçtiği görülmüştür. Bunun en önemli sebebi, ECDSA algoritmasının en düşük ek enerji yüküne sahip olmasındandır.



Şekil 6.10: 112-bit güvenlik seviyesi, $\alpha = 2$ ve kare topoloji için normalleştirilmiş ağ ömür değerleri



Şekil 6.11: 112-bit güvenlik seviyesi, $\alpha = 4$ ve kare topoloji için normalleştirilmiş ağ ömür değerleri

6.4 Ağ Yoğunluğu Değişimi

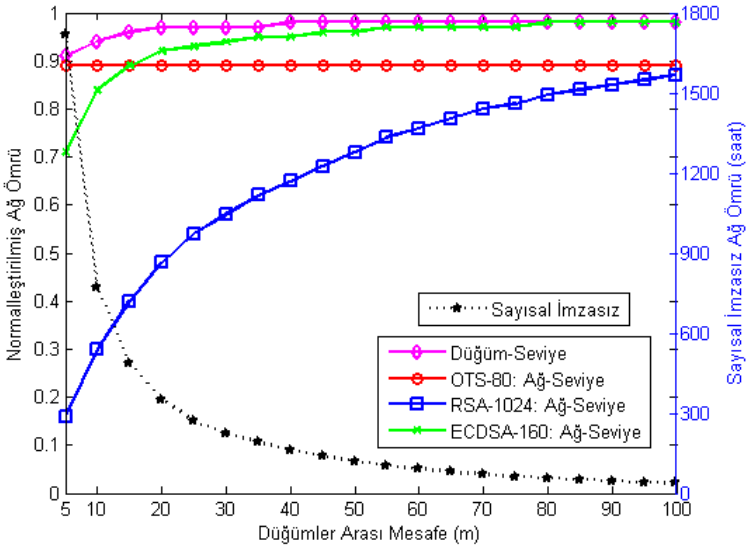
Bu bölümde 100 düğümlük doğrusal topoloji üzerinde düğümler arası mesafenin (d_{int}) değişiminin ağ ömrüne olan etkileri incelenmiş olup 80-bit güvenlik seviyesindeki Sİ algoritmaları ele alınmıştır.

Şekil 6.12 ve 6.13'de düğüm-seviye ve ağ-seviye stratejileri ile hesaplanan normalleştirilmiş ağ ömür değerlerinin düğümler arası mesafeye göre değişimi verilmiştir. Bu grafiklerden görüleceği üzere düğümler arası mesafenin arttırılması, ağ boyutunun arttırılması ile paralel bir etkiye sahiptir. Beklenildiği gibi, KAA'nın seyrekleştiği durumda, haberleşme için gereken enerji baskın olmaya başlayacağı için ECDA-160'ın hesaplamadan kaynaklı ek yükünün etkisi azalacaktır. Ortam koşulların hafif olması durumunda ($\alpha = 2$), $d_{int} \geq 80\ m$ için ağdaki tüm düğümler ECDSA-160 kullanarak ağ ömrünü maksimize ederken ortam koşulları ağırlaştığı zaman ($\alpha = 4$), $d_{int} \geq 15\ m$ için ağdaki tüm düğümlerin ECDSA-160 kullanmasıyla ağ ömrü maksimize edilmektedir.

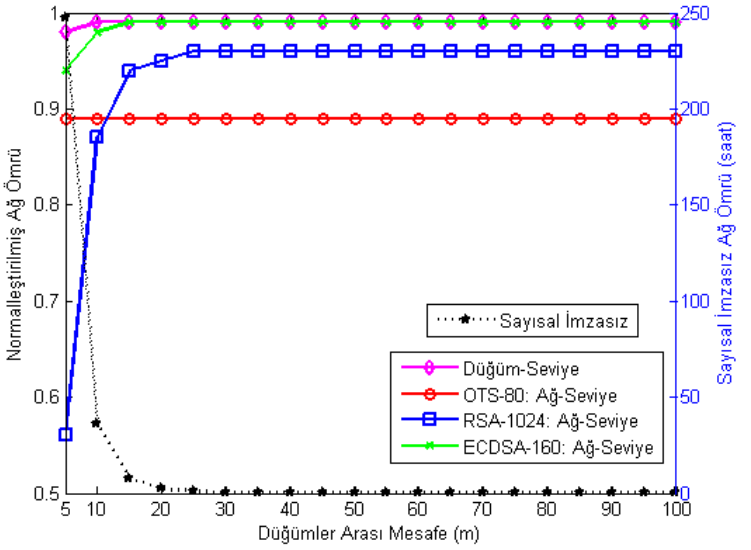
6.5 İmzalama Oranının Değişimi

İmzalama oranının (r) değişiminin KAA'ın ömrüne olan etkilerinin incelenmesi bu bölümün temel amacıdır. Bu kapsamda, 100 düğümlük doğrusal topoloji üzerinde 80-bit güvenlik seviyesinin incelendiği durumda, imzalama oranı 10'ar kat azalıp artacak şekilde değiştirilmiştir. Şekil 6.14 ve 6.15'de normalleştirilmiş ağ ömür değerleri üç farklı imzalama oranı ve iki farklı ortam koşulu ile gösterilmiştir. Tutarlılık açısından, kalan diğer tüm parametreler önceki çalışmalarda baz alınan değerler kadardır.

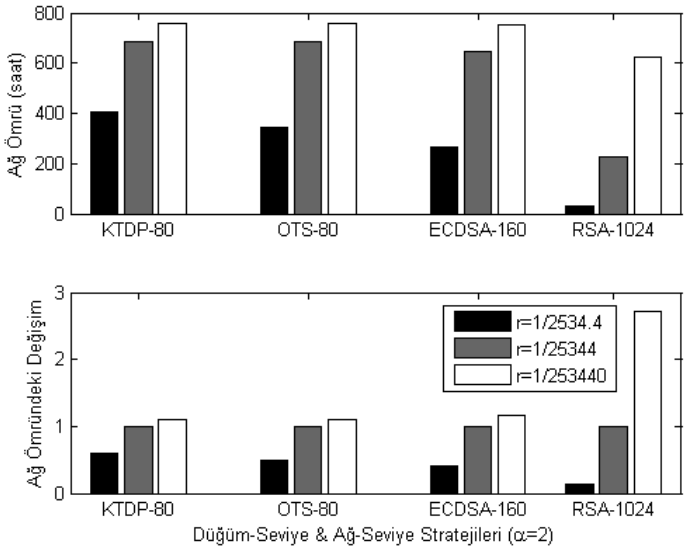
Üstteki figürlerde düğüm-seviye ve ağ-seviye stratejilerinin farklı imza oranları



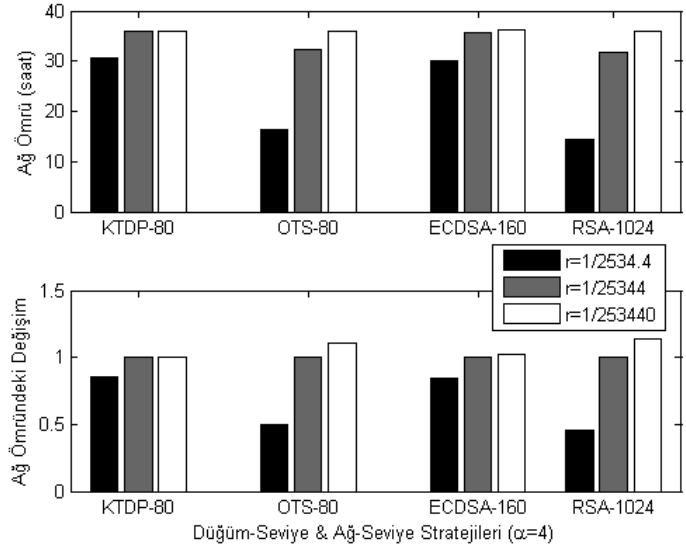
Şekil 6.12: 80-bit güvenlik seviyesi, $\alpha = 2$ ve doğrusal topoloji için düğümler arası mesafeye bağlı normalleştirilmiş ağ ömür değerleri



Şekil 6.13: 80-bit güvenlik seviyesi, $\alpha = 4$ ve doğrusal topoloji için düğümler arası mesafeye bağlı normalleştirilmiş ağ ömür değerleri



Şekil 6.14: 80-bit güvenlik seviyesinde, $\alpha = 2$ ve doğrusal topolojide farklı imzalama oranları için ağ ömrü ve ağ ömrü değişim değerleri



Şekil 6.15: 80-bit güvenlik seviyesinde, $\alpha = 4$ ve doğrusal topolojide farklı imzalama oranları için ağ ömrü ve ağ ömrü değişim değerleri

kullanıldığı takdirde elde edilen saat cinsinden ağ ömür değerleri sunulurken, alttaki figürlerde $r = 1/25344\ bit^{-1}$'nin 1'e eşitlenmesi ile (gri barlar) ağ ömründe meydana gelen değişimler gösterilmiştir. Beklenildiği gibi, düğüm-seviye stratejisinde imza boyutunun azalması ile ağ ömrü artmaktadır. Yani, imzalama oranı 100 kat azalınca ağ ömrü $\alpha = 2$ için 1.86 kat artarken, $\alpha = 4$ için 1.17 kat artmıştır. Bununla birlikte, düğüm-seviye stratejisinde imzalama oranının artması ile düğümlerdeki ECDSA-160 kullanımı da artmakadır. Bu durum ortam koşullarının ağırlaşması ile daha net bir biçimde Şekil 6.15'de görülebilir.

6.6 Trafik Yükünün Değişimi

Bu bölümde günlük iletilen görüntü dosya miktarının (günlük toplamda 10×25 KB, 50×25 KB ve 100×25 KB boyutlarındaki görüntü dosyalarının iletildiği varsayılmıştır.) KAA'ın ömrüne olan etkileri üç farklı durum için incelenmiştir. Bu durumlar herhangi bir Sİ algoritması kullanılmadığı zamanki strateji (Sİ Yok), düğüm-seviye stratejisi (KTDP) ve ağ-seviye stratejileridir (OTS, ECDSA, RSA). Çizelge 6.3, farklı ortam koşulları, topolojiler ve güvenlik seviyeleri için günlük iletilen görüntü dosyası sayısına bağlı olarak hesaplanan ağ ömür değerlerini (gün cinsinden) içermektedir.

İlk olarak, doğrusal topoloji için yapılan analizlerde düğüm sayısı 50 olarak alınmış olup komşu düğümler arası mesafe (d_{int}) 10 metredir. Beklenildiği üzere, günlük iletilen görüntü miktarı arttığı zaman ağ ömrü azalmaktadır. Doğal olarak, herhangi bir Sİ algoritması uygulanmadığı durumda elde edilen ağ ömrü, ağ-seviye ve düğüm-seviye stratejileriyle elde edilen ağ ömründen fazladır. Fakat bu durum haricinde, görüntü iletimi yapılırken en yüksek ağ ömrünü düğüm-seviye stratejisi sağlamaktadır. Güvenlik seviyesi 80-bitten 112-bit'e çıkarıldığı zaman, halen düğüm-seviye stratejisi, ağ-seviye stratejisinden daha uzun ağ ömrünü garantiler.

İkinci olarak, kare topoloji için yapılan analizlerde düğüm sayısı 49 olarak alınmış olup dikey ve yatay eksenlerde komşu düğümler arası mesafe (d_{int}) 10 metredir. Yine herhangi bir Sİ algoritması uygulanmadığı durumda elde edilen ağ ömrü, ağ-seviye ve düğüm-seviye stratejileri ile elde edilen ağ ömründen fazladır. $\alpha = 2$ için düğüm-seviye stratejisi ile OTS'nin ağ-seviyesinde uygulanmasıyla elde edilen ağ ömür değerleri, güvenlik seviyelerinden bağımsız olarak en iyi performansı vermektedir. Fakat, ortam koşulları ağırlaştıkça düğüm-seviye stratejisinin performansı, ağ-seviye stratejisinden daha iyidir.

Son olarak, bu bölümde görüleceği üzere 80-bit güvenlik seviyesi ile elde edilen ağ ömür değerleri (stratejilerden bağımsız olarak) 112-bit güvenlik seviyesi ile elde edilen ağ ömründen daha yüksektir.

Çizelge 6.3: Doğrusal ve kare topolojilerde görüntü iletimine bağlı olarak değişen mutlak ağ ömür değerleri (gün cinsinden).

		Doğrusal Topoloji			**Kare Topoloji**		
		Bir günde iletilen toplam görüntü sayısı					
Algoritma	α	10	50	100	10	50	100
Sİ Yok	2	416.03	83.21	41.6	6870.3	1374.06	687.03
	4	17.85	3.57	1.79	102.5	20.5	10.25
KTDP-80	2	379.96	75.78	37.89	6117.23	1223.45	611.72
	4	17.57	3.51	1.76	98.07	19.61	9.81
OTS-80	2	370.42	74.08	37.04	6117.23	1223.45	611.72
	4	15.9	3.18	1.59	91.27	18.25	9.13
ECDSA-160	2	296.46	59.29	29.65	920.4	184.08	92.04
	4	17.34	3.49	1.73	92.44	18.49	9.24
RSA-1024	2	66.62	13.32	6.66	78.98	15.8	7.9
	4	14.13	2.83	1.41	44.13	8.83	4.41
KTDP-112	2	342.96	68.59	34.3	5526.95	1105.39	552.7
	4	17.38	3.48	1.74	93.21	18.64	9.32
OTS-112	2	334.68	66.94	33.47	5526.95	1105.39	552.7
	4	14.36	2.87	1.43	82.46	16.49	8.25
ECDSA-224	2	200.86	40.17	20.09	373.05	74.61	37.3
	4	16.8	3.36	1.68	80.25	16.05	8.03
RSA-2048	2	10.27	2.05	1.03	10.54	2.11	1.05
	4	12.88	2.58	1.29	9.5	1.9	0.95
		Ağ Ömür Değerleri (gün)					

7. SEZGİSEL YÖNTEM

Bu tez çalışmasında, KAA'da sıklıkla karşılaşılan haberleşme/hesaplama ödünleşmesinin KTDP çatısı altında incelenmesi hedeflenmiştir. KTDP modelleri içinde barındırdığı ikili değişkenlerden ötürü *NP-Tam* olarak sınıflandırılmaktadır [65]. *NP* problemler, belirsiz Turing Makinesi ile polinomsal zamanda çözülebilen karar problemlerini içeren karmaşıklık sınıfıdır [9]. Fakat, belirsiz Turing makinesinin varlığı tamamen teorik olduğu için günümüzde bilinen bilgisayar mimarisi ile örtüşmemektedir. Bu yüzden, bu problemlerin günümüz bilgisayarlarında polinom zamanda çözülmesi mümkün değildir. Buna ek olarak, *NP-Tam* problemler hem *NP* olup hem *NP-Zor* olan problemlerin sınıfıdır. *NP-Zor* problemler ise en az her bir *NP* problem kadar zor olan problemlerdir.

KTDP problemlerinin karmaşıklığı arttırıldığında günümüz hesaplama metotları optimum çözüme ulaşmak adına yetersiz kalmaktadır. Bu yüzden, *NP-Tam* problemleri *NP* sınıfının en zor problemleri olarak bilinmektedir [9]. KTDP modellerini çözmek için kullanılan popüler "Dal Sınır" ya da "Kesme Düzlem" yöntemleri, küçük çaplı modellerde bile aşırı hesaplama zamanı gerektirmektedir. İşte, bu yüzden tasarımcılar tarafından eniyileme problemlerinin hızlı bir şekilde çözülmesi için sezgisel yöntemler geliştirilmiştir [9,10]. Bilgisayar bilimlerinde sıklıkla kullanılan sezgisel yöntemler ile sonucun doğruluğunun kanıtlanabilir olup olmadığının önemi yoktur, fakat genellikle optimum sonuca yakın iyi sonuçlar elde etmek temel amaçtır. Ayrıca, bu yöntemler optimum çözümü aramaktan vazgeçerek çözüm

zamanını önemli ölçüde azaltan yöntemlerdir.

7.1 Model

Bölüm 5'de tasarlanan KTDP modelinin hesaplama zorluğunu önemli ölçüde azaltmak üzere bu bölümde bir sezgisel algoritma tasarlanmıştır. Bu sezgisel yöntem, polinom zamanlı bir algoritma olan Altın Oran Arama (AOA) algoritmasını baz almaktadır. AOA yöntemi *unimodal*[1] bir fonksiyonun maksimum veya minimum noktasını (ekstremum) bulabilmek adına ekstremum noktanın bilindiği aralığın her iterasyonda belli bir oran kadar daraltılması ile sonuca ulaşmayı hedefler [75, 76]. AOA hakkında daha detaylı bilgi için Ek A incelenebilir.

Detaylara inmeden önce Bölüm 6'de elde edilen sonuçlardan yola çıkarak aşağıda sezgisel yöntem için bazı varsayımlar yapılacaktır. Bu tez çalışmasında kullanılan sezgisel yöntemin sözde kodu *(pseudo-code)* Algoritma 1'de verilmiştir. Kodlama ve analizler yine GAMS ve CPLEX ile yapılmıştır.

İlk olarak Bölüm 5'de tasarlanan KTDP modelinde Denklem (5.8)'den (5.13)'e kadar kullanılan denklemler çıkartılmıştır. w_k^i yerine tekrardan $t \times a_k^i$ terimi kullanılmış olup bu noktadan sonra ikili değişken a_k^i'nin değerleri eniyileme problemi tarafından değil; sezgisel yöntem tarafından değerleri önceden tayin edilen parametreye dönüşmüştür. Yani, her iterasyon öncesi sezgisel yöntem tarafından a_k^i değerleri sıfır veya bir olarak atanır.

Bölüm 6'da elde edilen sonuçlara göre RSA algoritması düğüm-seviye stratejisinde hiçbir düğüm tarafından kullanılmamıştır. Bu durum sezgisel algoritmanın ilk varsayımı olan hiçbir düğümün RSA kullanmamasını ($a_2^i = 0 \; \forall i \in W$) oluşturmaktadır (Satır 1). Satır 2 ve 3'de 2 tane gerçel sayı, n ve m, tanımlanmış olup bu değerler AOA algoritmasında kullanılacak olan ekstremum noktanın içinde

[1] Bir aralıkta sadece bir tane tepe noktası bulunan fonksiyonlara *unimodal* fonksiyon denir.

Do: $a_2^i = 0 \; \forall i \in W$;
$n \leftarrow 0$;
$m \leftarrow$ (Ağdaki düğüm sayısı) $- 1$;
$k \leftarrow$ Ağdaki düğüm sayısı;
$\phi \leftarrow (-1 + \sqrt{5})/2$;
$\lambda_1 \leftarrow n + \phi \times (m - n)$;
$\lambda_2 \leftarrow m - \phi \times (m - n)$;
while $|m - n| \geq 0.1$ $(Tol.)$ **do**
    for $i \leftarrow 2$ **to** k **do**
        if $i \in [2, \lfloor \lambda_1 \rfloor + 1]$ **then**
            $a_1^i \leftarrow 1$;
            $a_3^i \leftarrow 0$;
        else
            $a_1^i \leftarrow 0$;
            $a_3^i \leftarrow 1$;
        end
    end
    $\alpha \leftarrow \lambda_1$ ile elde edilen ağ ömrü;
    for $i \leftarrow 2$ **to** k **do**
        if $i \in [2, \lfloor \lambda_2 \rfloor + 1]$ **then**
            $a_1^i \leftarrow 1$;
            $a_3^i \leftarrow 0$;
        else
            $a_1^i \leftarrow 0$;
            $a_3^i \leftarrow 1$;
        end
    end
    $\beta \leftarrow \lambda_2$ ile elde edilen ağ ömrü;
    if $\alpha < \beta$ **then**
        $m \leftarrow \lambda_1$; $\lambda_1 \leftarrow \lambda_2$;
        $\lambda_2 \leftarrow m - \phi \times (m - n)$;
    else
        $n \leftarrow \lambda_2$; $\lambda_2 \leftarrow \lambda_1$;
        $\lambda_1 \leftarrow n + \phi \times (m - n)$;
    end
end
Result: $OTS \leftarrow 2 \leq i \leq \left\lfloor (\frac{n+m}{2}) \right\rfloor + 1$;
Result: $ECDSA \leftarrow \left\lfloor (\frac{n+m}{2}) \right\rfloor + 1 < i \leq k$;

Algoritma 1: Sezgisel Yöntemin Sözde Kodu

yer aldığı aralığın sınırlarını ifade etmektedir. Ayrıca n ve m değerleri λ_1 ve λ_2 değerlerini hesaplamak için de kullanılmaktadır. İlk iterasyonda, $n = 0$ ifadesini kullanmak, hiçbir algılayıcı düğümün OTS kullanmadığını gösterirken, $m = k-1$ ifadesi ile tüm algılayıcı düğümlerin ECDSA algoritmasını kullandığını göstermektedir. Satır 4'de kullanılan k değişkeni KAA'daki toplam düğüm sayısını ifade etmektedir. AOA algoritmasının anahtar parametresi olan altın oran (ϕ) değeri Satır 5'deki gibi tanımlanmıştır [75, 76].

Satır 6 ve 7'de tanımlanan λ_1 ve λ_2 değişkenleri ($n < \{\lambda_1,\ \lambda_2\} < m$) KAA'da kaç tane düğümün OTS, kalan diğer kaç tane düğümün ECDSA algoritması kullanacağını gösterir. Daha açık olmak gerekirse, örneğin, $\lambda_1 = 5.34$ değeri için tutarlılık sağlamak adına bu değer $\lfloor \lambda_1 \rfloor = 5$ olarak yuvarlanır. Bu da baz istasyonuna yakın olan kaç tane düğümün OTS kullanacağını gösterir. Bu durum fiziksel olarak, düğüm-2'den düğüm-7'ye kadar olan 5 tane algılayıcının OTS kullanacağını göstermektedir (yani düğüm-$2, 3, 4, 5$ ve 6 OTS algoritmasını kullanmaktadır). Matematiksel olarak bu kural Satır 10 ve 20'de belirtilmiştir. Satır 13 ve Satır 23 ile $\lfloor \lambda_1 \rfloor + 1$. düğümden (veya $\lfloor \lambda_2 \rfloor + 1$. düğümden) baz istasyonuna en uzak olan düğüme kadar olan kalan tüm algılayıcı düğümlerin ECDSA algoritmasını kullanması gerektiği gösterilmektedir.

α ve β değerleri, λ_1 ve λ_2 değerleri sayesinde elde edilen ağ ömrü değerleridir. Ağ ömrü değeri elde edebilmek için eniyileme problemi Denklem 5.1'den Denklem 5.7'e kadar olan denklemler ile DP çatısı altında tasarlanmıştır. Eniyileme problemi sonucunda $\alpha \geq \beta$ olduğu zaman, AOA yöntemi $[n, m]$ arasında tanımlanan fonksiyonu $[n = \lambda_2, m]$ aralığına çeker ve optimum sonuca ulaşmak için iterasyonlara bu yeni aralıkta devam eder (Satır 29'den Satır 31'a kadar). Fakat, $\alpha < \beta$ olduğu durumda AOA yöntemi $[n, m]$ arasında tanımlanan fonksiyonu bu kez $[n, m = \lambda_1]$ aralığına çekerek (Satır 32'den Satır 34'a kadar) iterasyonlara bu aralıktan devam eder. Kısıtlanan bu yeni aralıklarda yeni λ_1, λ_2, n ve m değerleri hesaplanır ve bu işlemler $|m-n|$'nin önceden tanımlı bir tolerans değerine erişene kadar devam eder. $\left\lfloor (\frac{n+m}{2}) \right\rfloor + 1$ değeri, KAA'ın ağ ömrünü maksimize etmek adına

hangi düğümlerin OTS, hangilerinin ECDSA kullanacağını gösteren eşik değerini temsil etmektedir. Böylece optimuma oldukça yakın geçerli bir sonuç çok kısa sürede elde edilebilmektedir.

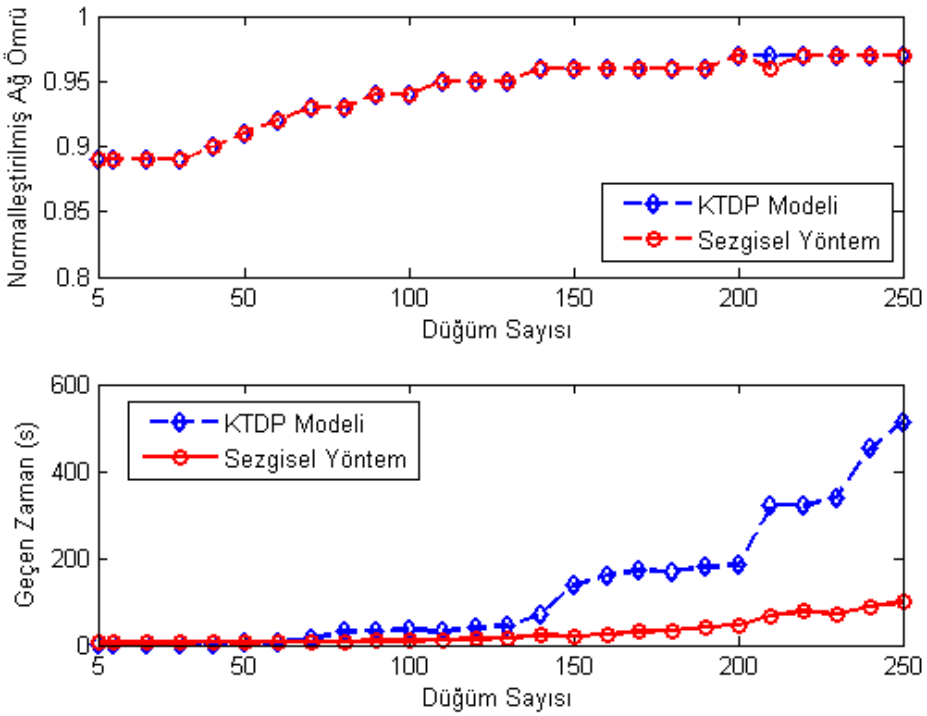
Sezgisel yöntemin ilk iterasyonu $n = 0$ ve $m = k - 1$ aralığında başlar. Bu aralığın iki ucu için 2 farklı eniyileme problemi çözülür. Bunlar, tüm düğümlerin OTS kullandığını varsayan problem (α) ile tüm düğümlerin ECDSA algoritması kullandığı problemdir (β). İkinci ve sonraki iterasyonlarda bazı düğümlerin OTS, kalan diğer düğümlerin ECDSA algoritması kullandığı varsayılır. Her iterasyonda yine 2 tane eniyileme problemleri çözdürülür, α ve β değerlerinin karşılaştırması yapılarak aralık daraltılır. Yukarıda da bahsedildiği gibi bu işlemler $|m - n|$'nin önceden tanımlı tolerans değerine (0.1) erişene kadar devam eder.

7.2 Analiz

Bu kısımda, Bölüm 7.1'da geliştirilen sezgisel algoritmanın performansı (burada performanstan kasıt, sezgisel algoritmanın optimuma yakın bir sonuca tahminen ne kadar sürede ulaşabileceğidir.) Şekil 6.2'deki doğrusal ve Şekil 6.7'deki kare topolojiler üzerinde incelenmiştir.

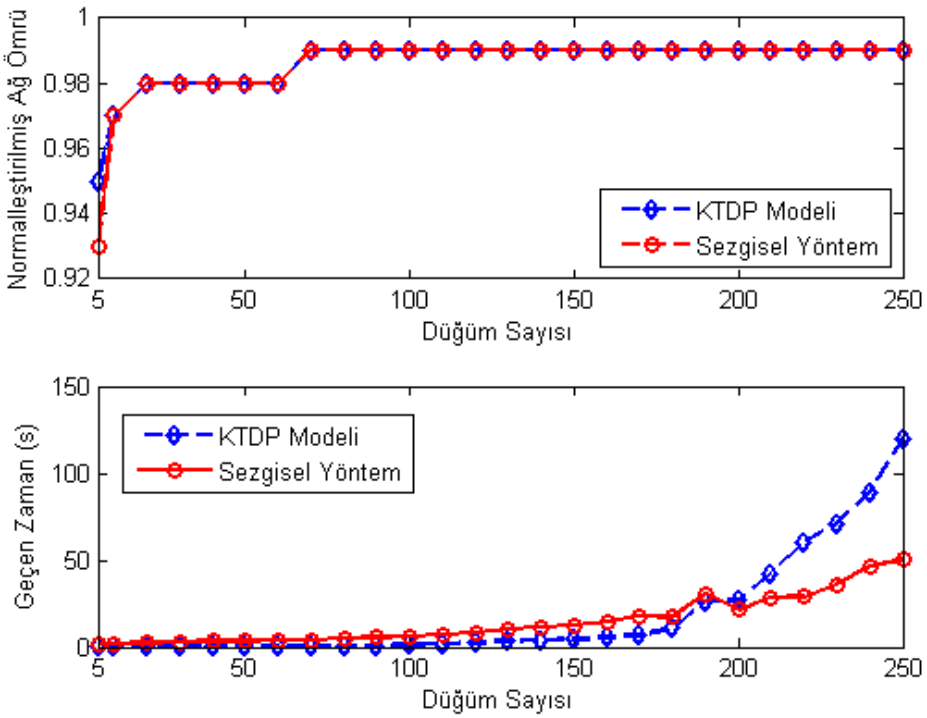
Şekil 7.1'den 7.8'ye kadar olan grafiklerin üstündeki grafiklerde, KTDP modeli ve sezgisel yöntem ile elde edilen normalleştirilmiş ağ ömür değerleri ağ boyutuna bağlı olarak gösterilmiştir. Aşağıdaki grafiklerde ise KTDP modeli ve sezgisel yöntemin performans karşılaştırması yine ağ boyutuna bağlı olarak verilmiştir.

Şekil 7.1 ve 7.2'de doğrusal topoloji, 80-bit güvenlik seviyesi ile kullanılmıştır. KTDP modeli ve sezgisel yöntem ile elde edilen normalleştirilmiş ağ ömür değerleri arasındaki fark $\alpha = 2$ için %0.99'dan, $\alpha = 4$ için %1.29'dan azdır. 250 veya daha fazla düğüme sahip bir topolojinin KTDP modeli ile çözülebilmesi aşırı



Şekil 7.1: 80-bit güvenlik seviyesi, $\alpha = 2$ ve doğrusal topoloji için KTDP modeli ile sezgisel yöntemin ağ ömrü & performans karşılaştırması

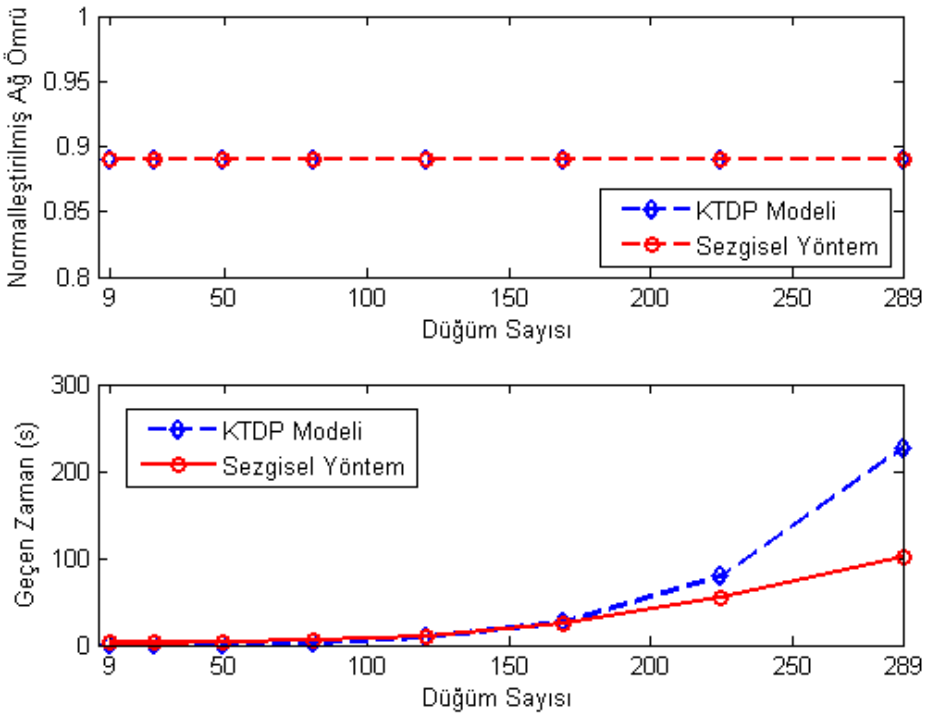
hesaplama zamanı gerektirdiği için problemin optimum sonuca ulaşmasını beklemek efektif değildir. Fakat, kübik spline ekstrapolasyon [77] yöntemi ile KTDP'nin optimum sonuca tahminen ne kadar sürede ulaşabileceği bulunabilir. Ekstrapolasyonlar neticesinde $\alpha = 2$ iken, KTDP modelinin 750 düğümlük bir topolojide optimum sonuca ulaşması için gerekecek süre yaklaşık olarak 4.13×10^6 saniye olarak hesaplanmış olup 1000 düğümlük ağda bu değer 13.61×10^6 saniye; $\alpha = 4$ iken 350 düğümlük topoloji için 63.32×10^3 saniye ve 500 düğümlük topoloji için 44.28×10^4 saniye olarak tahmin edilmiştir. Fakat, sezgisel yöntemin $\alpha = 2$ iken 750 ve 1000 düğümlük topolojilerde optimuma yakın bir sonuç elde etmesi en fazla 1761 ve 3626 saniye sürerken $\alpha = 4$ için 350 ve 500 düğümlük topolojilerde en fazla 108 ve 1028 saniye sürmektedir. Bu tip geniş ağlarda, sezgisel yöntem



Şekil 7.2: 80-bit güvenlik seviyesi, $\alpha = 4$ ve doğrusal topoloji için KTDP modeli ile sezgisel yöntemin ağ ömrü & performans karşılaştırması

ile normalleştirilmiş ağ ömür değerleri 0.98'e ($\alpha = 2$ için) ve 0.99'a ($\alpha = 4$ için) kadar arttırılabilmektedir.

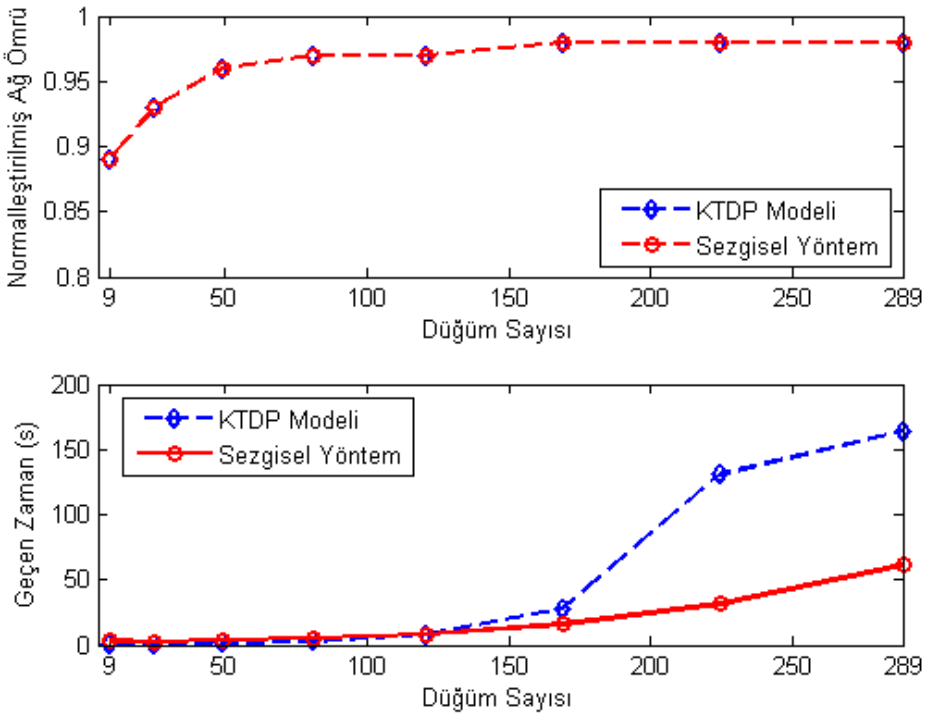
Şekil 7.3 ve 7.4'de kare topoloji 80-bit güvenlik seviyesi ile kullanılmıştır. $\alpha = 2$ ve $\alpha = 4$ için sezgisel algoritma, KTDP modeliyle elde edilen optimum sonuç ile aynı sonucu elde etmiştir. Performans açısından, sezgisel yöntem 169 ve daha fazla düğüme sahip topolojilerde, yayılım ortamından bağımsız olarak, KTDP'ye oranla daha iyi performans vermektedir. Ekstrapolasyonlar neticesinde, KTDP modelinin $\alpha = 2$ iken, 729 ve 1089 düğümlük topolojilerde optimum ağ ömrüne ulaşabilmesi için gereken tahmini süreler 80.84×10^3 ve 32.02×10^4 saniye; $\alpha = 4$ iken 26.57×10^3 ve 13.25×10^4 saniye olarak hesaplanmıştır. Sezgisel yöntemin $\alpha = 2$ iken 729 ve 1089 düğümlük topolojilerde optimuma yakın bir sonuç elde



Şekil 7.3: 80-bit güvenlik seviyesi, $\alpha = 2$ ve kare topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması

etmesi en fazla 1356 ve 2707 saniye sürmekte olup $\alpha = 4$ için bu değerler en fazla 1356 ve 2707 saniye olarak ölçülmüştür. Bu tip geniş ağlarda, sezgisel yöntem ile normalleştirilmiş ağ ömrü 0.99'a ($\alpha = 4$ için) kadar çıkarılabilir. $\alpha = 2$ için ağ ömrü, beklenildiği gibi, sabit kalmaktadır.

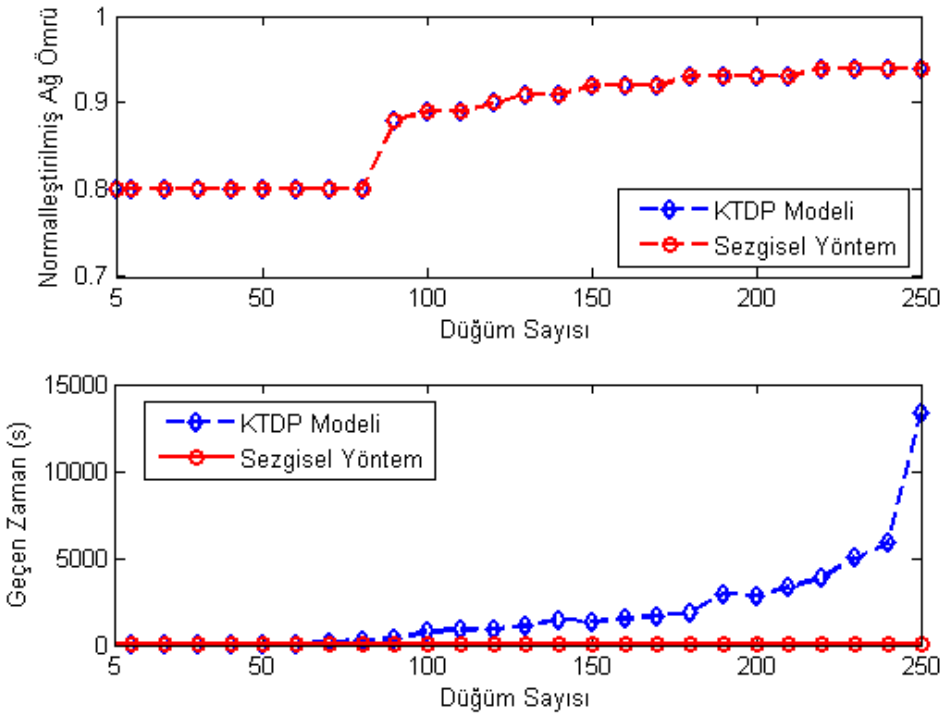
Şekil 7.5 ve 7.6'de doğrusal topoloji 112-bit güvenlik seviyesi ile kullanılmıştır. KTDP modeli ve sezgisel yöntem ile elde edilen ağ ömürleri arasındaki fark $\alpha = 2$ için %0.05'dan, $\alpha = 4$ için %0.95'dan düşük olarak gözlenmiştir. 70 ($\alpha = 2$ için) ve 140 ($\alpha = 4$ için) düğümden daha fazla düğüme sahip bir topolojinin KTDP modeli ile çözülebilmesi aşırı hesaplama zamanı gerektirdiği için problemin optimum sonuca ulaşmasını beklemek efektif değildir. Ekstrapolasyonlar neticesinde,



Şekil 7.4: 80-bit güvenlik seviyesi, $\alpha = 4$ ve kare topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması

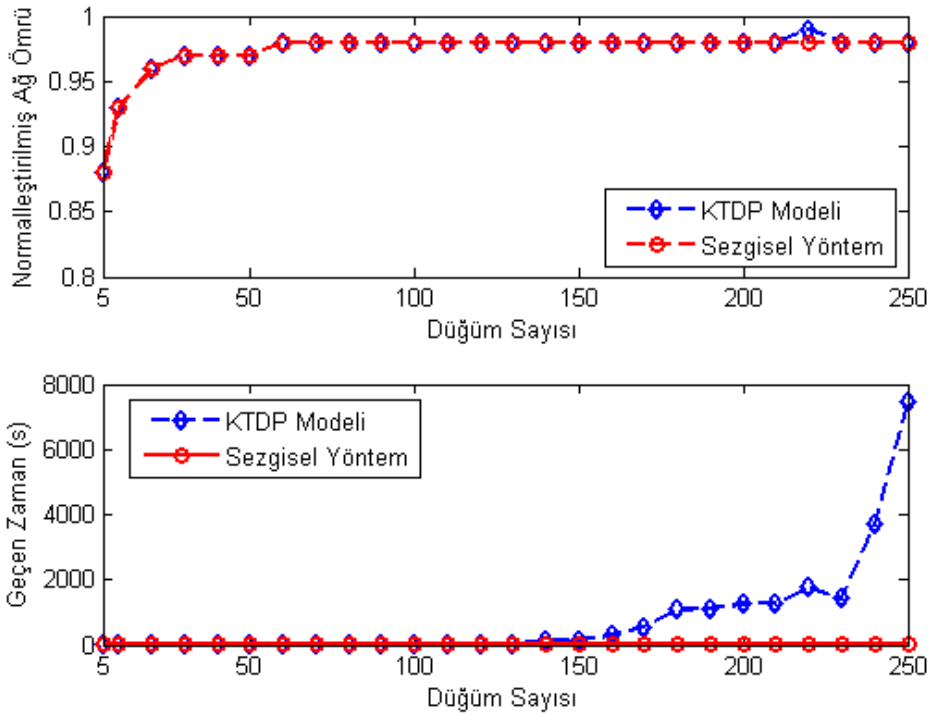
$\alpha = 2$ iken, KTDP modelinin 750 düğümlük bir topolojide optimum sonuca ulaşmabilmesi için gerekecek süre yaklaşık olarak 2.13×10^8 saniye ve 1000 düğümlük ağda 6.96×10^8 saniye olarak hesaplanmış olup $\alpha = 4$ iken bu değerler 350 düğümlük topoloji için 0.48×10^6 saniye ve 500 düğümlük topoloji için 7.48×10^6 saniye olarak hesaplanmıştır. Sezgisel yöntemin $\alpha = 2$ iken 750 ve 1000 düğümlük topolojilerde optimuma yakın bir sonuç elde etmesi en fazla 1602 ve 2160 saniye sürmekte olup $\alpha = 4$ için 350 ve 500 düğümlük topolojilerde bu değerler en fazla 402 ve 772 saniye olarak ölçülmüştür. Bu tip geniş ağlarda, sezgisel yöntem ile normalleştirilmiş ağ ömrü 0.97'a ($\alpha = 2$ için) kadar çıkarılabilir. $\alpha = 4$ için ağ ömrü, beklenildiği gibi, sabit kalmaktadır.

Şekil 7.7 ve 7.8'de kare topoloji 112-bit güvenlik seviyesi ile kullanılmıştır. $\alpha = 2$



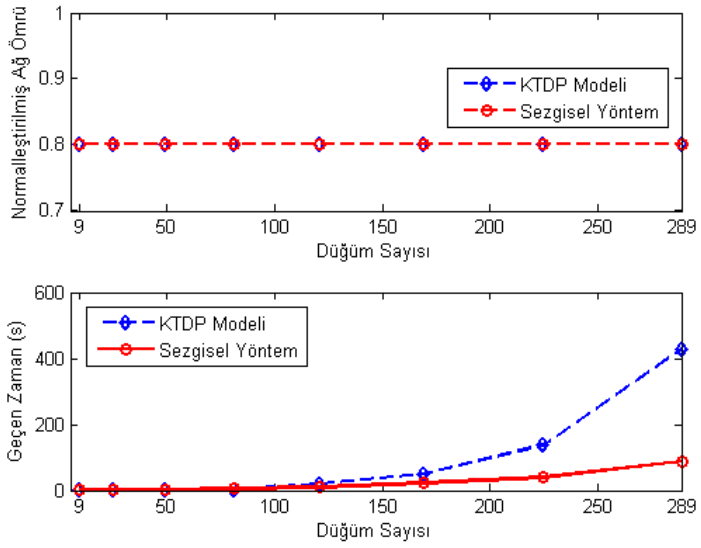
Şekil 7.5: 112-bit güvenlik seviyesi, $\alpha = 2$ ve doğrusal topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması

ve $\alpha = 4$ için sezgisel algoritma, KTDP modeli ile elde edilen optimum sonuç ile aynı sonucu elde etmiştir. Performans açısından, sezgisel yöntem 121 ve daha fazla düğüme sahip topolojilerde, yayılım ortamından bağımsız olarak, KTDP'ye oranla daha iyi performans vermektedir. Ekstrapolasyonlar neticesinde KTDP modelinin $\alpha = 2$ iken, 729 ve 1089 düğümlük topolojilerde optimum ağ ömrüne ulaşabilmesi için gereken tahmini süreler 20.45×10^3 ve 85.16×10^3 saniye; $\alpha = 4$ iken 38.58×10^3 ve 17.39×10^4 saniye olarak hesaplanmıştır. Sezgisel yöntemin $\alpha = 2$ iken 729 ve 1089 düğümlük topolojilerde optimuma yakın bir sonuç elde etmesi en fazla 1356 ve 2707 saniye sürmekte olup $\alpha = 4$ için bu değerler en fazla 1913 ve 6150 saniye olarak ölçülmüştür. Bu tip geniş ağlarda, normalleştirilmiş ağ ömrü 0.98'a ($\alpha = 4$ için) kadar çıkarılabilir. $\alpha = 2$ için ağ ömrü, beklenildiği

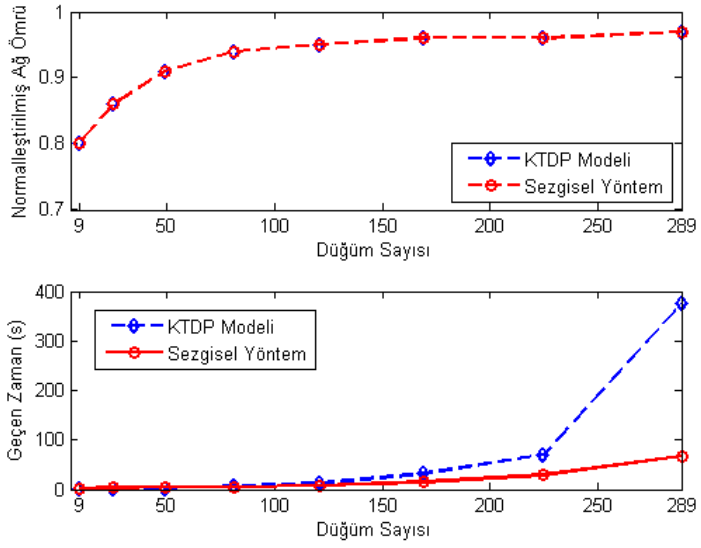


Şekil 7.6: 112-bit güvenlik seviyesi, $\alpha = 4$ ve doğrusal topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması

gibi, sabit kalmaktadır.



Şekil 7.7: 112-bit güvenlik seviyesi, $\alpha = 2$ ve kare topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması



Şekil 7.8: 112-bit güvenlik seviyesi, $\alpha = 4$ ve kare topoloji için KTDP modeli ile sezgisel algoritmanın ağ ömrü & performans karşılaştırması

8. SONUÇ

Tipik bir KAA'da farklı iki tip enerji harcaması mevcuttur. Bunlar düğümler arası haberleşme için harcanan enerji ile her algılayıcı düğümde gerçekleştirilebilen yerel işlemler için harcanan hesaplama enerjisidir. Genellikle KAA'larda, haberleşme için harcanacak enerji, baskın olan enerji tüketimidir. Algılayıcı düğümlerdeki kısıtlı batarya gücü nedeniyle bir KAA'da haberleşme ve hesaplama için harcanacak enerjilerin dikkatli bir şekilde ayarlanması gerekir. Dengeli şekilde enerjilerini tüketen düğümlerin optimum ağ ömrüne ulaşılmasında önemi oldukça büyüktür.

Bu tez çalışmasında yukarıda bahsedilen ödünleşmenin daha detaylı bir analizinin gerçekleştirilebilmesi adına bir önceki çalışmada [3] tasarlanan ağ-seviye statejisi için kullanılan DP modeli geliştirilerek özgün bir KTDP modeline dönüştürülmüştür. Böylece bu çalışmada ağ-seviyesi stratejine göre daha detaylı bir analiz yapabilme imkanı doğarak ağ ömrünün ağ-seviye stratejisine göre daha da artabileceği gözlenmiştir.

Bu çalışmanın ikinci bölümünde, KTDP'nin *NP-Tam* problemler sınıfına dahil olmasından ötürü getirdiği hesaplama zorluklarını hafifletebilmek adına sezgisel bir algoritma tasarımı yapılmıştır. Bu sezgisel algoritma, polinom zamanlı bir algoritma olan AOA tekniğini kullanmakta olup KTDP modeli ile elde edilen optimum sonuca oldukça yakın sonuçları kısa çözüm zamanında sağlamaktadır.

KTDP modeli ve sezgisel algoritma ile yapılan kapsamlı analizler sayesinde, bu tez çalışmasında elde edilen önemli sonuçlar aşağıdaki gibi listelenmiştir:

1. Algılayıcı düğümlerin kendine en uygun Sİ algoritması seçmebilmesine imkan tanıyan düğüm-seviye stratejisi sayesinde ağ-seviye stratejine göre ağ ömrü %22.50 oranında arttırılabilir.

2. Küçük ölçekli ağlarda, yani hesaplama için gereken enerjinin haberleşme için gereken enerjiden fazla (baskın) olduğu durumda, sıfır ek hesaplama enerjisine sahip olan OTS algoritması diğer Sİ algoritmalarına göre algılayıcı düğümler tarafından tercih edilmektedir. Fakat, ağ büyüdüğü zaman, yani haberleşme enerjisi hesaplama enerjisini bastırdığı zaman, düşük imza boyutuna sahip ECDSA algoritması, algılayıcı düğümler tarafından tercih edilmektedir.

3. Ağ seyrekleştiği zaman haberleşme enerjisi hesaplama enerjisini bastırmaktadır. Bu da algılayıcı düğümlerde ECDSA algoritmasının kullanımını arttırmaktadır.

4. İmza oranının ağ ömrü üzerinde oldukça büyük bir etkisi vardır. İmza oranı arttırıldığı zaman algılayıcı düğümlerde OTS'den ziyade ECDSA algoritması kullanıldığı gözlenmiştir. Bu durum haberleşme ortamının güçleştiği durumda açıkça görülmektedir. Fakat, düşük imza oranlarında düğümlerin OTS algoritmasını tercih etme olasılığı oldukça yüksektir.

5. Sezgisel algoritma yardımıyla %1.29'dan daha düşük bir hata ile optimum sonuç (KTDP model ile elde edilen) çok kısa sürelerde (KTDP modeline nazaran) elde edilebilir.

6. Büyük ağlarda KTDP'nin hesaplama zorluğu baskın olmaktadır. Böyle bir durumda, geliştirilen sezgisel algoritma yardımı ile optimuma yakın iyi sonuçlar çok kısa sürelerde elde edilebilmektedir.

KAYNAKLAR

[1] S. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 1, pp. 377 – 381 Vol.1, dec. 2003.

[2] D. Incebacak, K. Bicakci, and B. Tavli, "Energy cost of mitigating physical attacks in wireless sensor networks," in *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, pp. 1 –5, may 2012.

[3] K. Bicakci, I. E. Bagci, and B. Tavli, "Communication/computation tradeoffs for prolonging network lifetime in wireless sensor networks: The case of digital signatures," *Inf. Sci.*, vol. 188, pp. 44–63, Apr. 2012.

[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*, SASN '06, (New York, NY, USA), pp. 169–176, ACM, 2006.

[5] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pp. 324 – 328, march 2005.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[7] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[8] L. Lamport, "Constructing digital signatures from a one-way function," *SRI International Computer Science Laboratory*, Oct. 1979.

[9] M. R. Garey and D. S. Johnson, *Computers and Intractability; A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1990.

[10] C. H. Papadimitriou and K. Steiglitz, *Combinatorial optimization: algorithms and complexity*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1982.

[11] R. Bixby and E. Rothberg, "Progress in computational mixed integer programming—A look back from the other side of the tipping point," *Annals of Operations Research*, vol. 149, pp. 37–41, Jan. 2007.

[12] E. A. Silver and E. A. Silver, "An overview of heuristic solution methods," in *In Proceedings of the 7th Annual International Conference on Industrial Engineering Theory, Applications and Practice*, 2002.

[13] 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, pp. 79 – 86 Vol. 1, aug. 2005.

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

[15] S. Ergen and P. Varaiya, "On multi-hop routing for energy efficiency," *Communications Letters, IEEE*, vol. 9, pp. 880 – 881, oct. 2005.

[16] A. Alfieri, A. Bianco, P. Brandimarte, and C.-F. Chiasserini, "Maximizing system lifetime in wireless sensor networks," *European Journal of Operational Research*, vol. 181, no. 1, pp. 390–402, 2007.

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

[18] 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, pp. 905 –907, december 2009.

[19] M. Kayaalp, O. Ceylan, I. 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*, pp. 769 –771, april 2009.

[20] B. Tavli, I. Bagci, and O. Ceylan, "Optimal data compression and forwarding in wireless sensor networks," *Communications Letters, IEEE*, vol. 14, pp. 408 –410, may 2010.

[21] A. C. Santos, F. Bendali, J. Mailfert, C. Duhamel, and K. M. Hou, "Heuristics for designing energy-efficient wireless sensor network topologies," *JNW*, vol. 4, no. 6, pp. 436–444, 2009.

[22] A. Hoang and M. Motani, "Collaborative broadcasting and compression in cluster-based wireless sensor networks," in *Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on*, pp. 197 – 206, jan.-2 feb. 2005.

[23] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.

[24] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," in *Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on*, pp. 636–641, 2009.

[25] Wikipedia, "Wireless sensor network — Wikipedia, the free encyclopedia." `http://en.wikipedia.org/wiki/Wireless_sensor_network`. [Online; accessed 17-June-2013].

[26] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[27] C.-Y. Lin, Y.-C. Tseng, and T. Lai, "Message-efficient in-network location management in a multi-sink wireless sensor network," in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, vol. 1, pp. 8 pp.–, 2006.

[28] D. De, A. Sen, and M. Gupta, "Cluster based energy efficient lifetime improvement mechanism for wsn with multiple mobile sink and single static sink," in *Computer and Communication Technology (ICCCT), 2012 Third International Conference on*, pp. 197–199, 2012.

[29] A. Forstert and A. Murphy, "Froms: Feedback routing for optimizing multiple sinks in wsn with reinforcement learning," in *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pp. 371–376, 2007.

[30] T. Gulrez and M. Kavakli, "Precision position tracking in virtual reality environments using sensor networks," in *Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on*, pp. 1997–2003, 2007.

[31] D.-S. Wu and C.-L. Wang, "Decentralized cooperative positioning and tracking based on a weighted sign algorithm for wireless sensor networks," in

Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp. 1–6, 2009.

[32] D.-S. Wu and C.-L. Wang, "A reduced-complexity decentralized positioning and tracking algorithm for wireless sensor networks," in *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, pp. 1–5, 2010.

[33] W. Ming, L. Zhengqiu, J. Shan, S. Beng, and C. Qingzhang, "Design of an indoor positioning and tracking algorithm for wireless sensor networks," in *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on*, pp. 3081–3084, 2011.

[34] I. Khemapech, I. Duncan, and A. Miller, "Energy preservation in environmental monitoring wsn," in *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, pp. 312–319, 2010.

[35] J. Ong, Z. You, J. Mills-Beale, E. L. Tan, B. Pereles, and K. G. Ong, "A wireless, passive embedded sensor for real-time monitoring of water content in civil engineering materials," *Sensors Journal, IEEE*, vol. 8, no. 12, pp. 2053–2058, 2008.

[36] Z. Yang, "A survey on localization in wireless sensor networks."

[37] J. Park and H. Y. Song, "Multilevel localization for mobile sensor network platforms," in *Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on*, pp. 711–718, 2008.

[38] B.-S. Choi and J.-J. Lee, "Sensor network based localization algorithm using fusion sensor-agent for indoor service robot," *Consumer Electronics, IEEE Transactions on*, vol. 56, no. 3, pp. 1457–1465, 2010.

[39] B. Zhang and F. Yu, "An event-triggered localization algorithm for mobile wireless sensor networks," in *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, vol. 1, pp. V1–250–V1–253, 2010.

[40] T. Srinath, "Localization in resource constrained sensor networks using a mobile beacon with in-ranging," in *Wireless and Optical Communications Networks, 2006 IFIP International Conference on*, pp. 5 pp.–5, 2006.

[41] P. Sethi, N. Chauhan, and D. Juneja, "A multi-agent hybrid protocol for data fusion and data aggregation in non-deterministic wireless sensor networks," in *Information Systems and Computer Networks (ISCON), 2013 International Conference on*, pp. 211–214, 2013.

[42] T. Pham, E. J. Kim, and M. Moh, "On data aggregation quality and energy efficiency of wireless sensor network protocols - extended summary," in *Broadband Networks, 2004. BroadNets 2004. Proceedings. First International Conference on*, pp. 730–732, 2004.

[43] H. Chen and S. Megerian, "Cluster sizing and head selection for efficient data aggregation and routing in sensor networks," in *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, vol. 4, pp. 2318–2323, 2006.

[44] B. Liang and Q. Liu, "A data fusion approach for power saving in wireless sensor networks," in *Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on*, vol. 2, pp. 582–586, 2006.

[45] H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, "Espda: Energy-efficient and secure pattern-based data aggregation for wireless sensor networks," in *Sensors, 2003. Proceedings of IEEE*, vol. 2, pp. 732–736 Vol.2, 2003.

[46] H. Ammari and S. Das, "A study of k-coverage and measures of connectivity in 3d wireless sensor networks," *Computers, IEEE Transactions on*, vol. 59, no. 2, pp. 243–257, 2010.

[47] X. Xing, G. Wang, J. Wu, and J. Li, "Square region-based coverage and connectivity probability model in wireless sensor networks," in *Collaborative*

Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on, pp. 1–8, 2009.

[48] X. Liu, "Coverage with connectivity in wireless sensor networks," in *Broadband Communications, Networks and Systems, 2006. BROADNETS 2006. 3rd International Conference on*, pp. 1–8, 2006.

[49] L. Liu, B. Hu, and L. Li, "Energy conservation algorithms for maintaining coverage and connectivity in wireless sensor networks," *Communications, IET*, vol. 4, no. 7, pp. 786–800, 2010.

[50] A. Ghosh and S. Das, "Review: Coverage and connectivity issues in wireless sensor networks: A survey," *Pervasive Mob. Comput.*, vol. 4, pp. 303–334, June 2008.

[51] H. Gong, X. Zhang, L. Yu, X. Wang, and F. Yi, "A study on mac protocols for wireless sensor networks," in *Frontier of Computer Science and Technology, 2009. FCST '09. Fourth International Conference on*, pp. 728–732, 2009.

[52] S. Lindsey and C. Raghavendra, "Pegasis: Power-efficient gathering in sensor information systems," in *Aerospace Conference Proceedings, 2002. IEEE*, vol. 3, pp. 3–1125–3–1130 vol.3, 2002.

[53] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pp. 10 pp. vol.2–, 2000.

[54] O. Younis and S. Fahmy, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 3, no. 4, pp. 366–379, 2004.

[55] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient mac protocol for wireless sensor networks," in *INFOCOM 2002. Twenty-First Annual Joint*

Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3, pp. 1567–1576 vol.3, 2002.

[56] RFM1000, "916.50 mhz hybrid transceiver." `http://www.rfm.com/products/data/tr1000.pdf`. [Online; accessed 17-June-2013].

[57] G. Anastasi, M. Conti, A. Falchi, E. Gregori, and A. Passarella, "Performance measurements of motes sensor networks," in *In MSWiM '04: Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pp. 174–181, ACM Press, 2004.

[58] Atmel, "Atmega128/l datasheet." `http://www.atmel.com/Images/doc2467.pdf`. [Online; accessed 17-June-2013].

[59] T. Instruments, "Cc1000 single chip very low power rf transceiver." `http://www.ti.com/lit/ds/symlink/cc1000.pdf`. [Online; accessed 17-June-2013].

[60] TinyOS, "Tinyos home page." `http://www.tinyos.net/`. [Online; accessed 17-June-2013].

[61] Texas.Instruments, "Msp430 ultra-low-power microcontrollers brochure 2012 (rev. v) - slab034v.pdf." `http://www.ti.com/lit/sg/slab034v/slab034v.pdf`. [Online; accessed 17-June-2013].

[62] R. Horst and P. M. Pardalos, *Handbook of Global Optimization*. Kluwer Academic Publishers, 1994.

[63] G. B. Dantzig, *Maximization of a Linear Function of Variables Subject to Linear Inequalities, in Activity Analysis of Production and Allocation*, ch. XXI. New York: Wiley, 1951.

[64] N. Karmarkar, "A new polynomial-time algorithm for linear programming," in *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, STOC '84, (New York, NY, USA), pp. 302–311, ACM, 1984.

[65] R. M. Karp, "Reducibility Among Combinatorial Problems," in *Complexity of Computer Computations* (R. E. Miller and J. W. Thatcher, eds.), pp. 85–103, Plenum Press, 1972.

[66] "Gams/cplex 12." `http://www.ibm.com/software/commerce/optimization/cplex-optimizer`.

[67] 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.

[68] Q. Dong, "Maximizing system lifetime in wireless sensor networks," in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pp. 13–19, april 2005.

[69] "Nist report on cryptographic key length and crypto-period.."

[70] 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, pp. 2357 – 2361 vol.5, sept. 2002.

[71] "General algebraic modeling system (gams) home page." `http://www.gams.com/`.

[72] 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*, vol. 3, pp. 1587 – 1596 vol.3, 2002.

[73] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *Networking, IEEE/ACM Transactions on*, vol. 12, pp. 609 – 619, aug. 2004.

[74] S. Jiang and Y. Xue, "Optimal wireless network restoration under jamming attack," in *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, pp. 1 –6, aug. 2009.

[75] J. Kiefer, "Sequential minimax search for a maximum," *Proceedings of the American Mathematical Society*, vol. 4, no. 3, pp. 502–506, 1953.

[76] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes 3rd Edition: The Art of Scientific Computing*, vol. 1. Cambridge University Press, 2007.

[77] J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*. New York: Springer, 3 ed., Aug. 2002.

EKLER

A. Altın Oran Arama Algoritması

Altın Oran Arama (AOA) algoritması kesinlikle *unimodal*[1] olan bir fonksiyonun ekstremum (uç - minimum veya maksimum) noktasını bulmaya yarayan bir algoritmadır. Algoritmanın temel mantığı ekstremum noktanın bulunduğu yerin belirlenen bir aralığın daraltılması ile bulunmasıdır. Bu algoritmaya ismini veren altın oran sayesinde, bu aralığın başlangıç ve bitiş noktaları özyinelemeli olarak tayin edilir. Bu algoritma Fibonacci aramasının değiştirilmiş bir biçimidir.

Bu bölümde AOA algoritması ile bir fonksiyonun maksimum değerinin nasıl hesaplanacağı kısaca açıklanmıştır[2].

Şekil A.1'deki gibi $[a, b]$ aralığında tanımlı *unimodal* bir f fonksiyon verilsin. Algoritma, $[a, b]$ aralığında aşağıdaki (x_1, x_2) değerlerinin hesaplanması ile başlar.

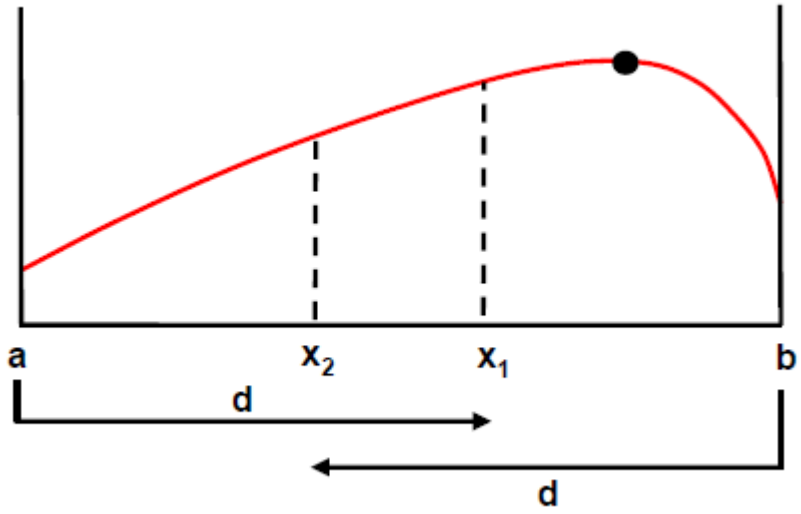
$$x_1 = a + d = a + \phi(b - a).$$

$$x_2 = b - d = b - \phi(b - a).$$

Yukarıdaki denklemlerde ϕ altın oran değerini $(0.618\ldots)$ temsil etmekdir. Dikkat

[1] $f(x)$ fonksiyonu $[a, b]$ aralığında tanımlanmış olsun ve de belirli bir x noktası için $[a, x]$ aralığında $f(x)$ kesinlikle artıyor, $[x, b]$ aralığında azalıyorsa $f(x)$ fonksiyonu *unimodal*dır. (tam tersi durum için de geçerlidir.)

[2] Eğer burada açıklanan mantık tersten yürütülürse bir fonksiyonun minimum noktası bulunabilmektedir.



Şekil A.1: $[a, b]$ aralığında tanımlanan sürekli *unimodal* $f(x)$ fonksiyonu

edileceği üzere, x_1 ve x_2 değerleri rastgele seçilmemiştir. ϕ değeri sayesinde x_1 ve x_2 bilinmeyen aralığı aşağıdaki gibi iki parçaya ayırır:

$$\frac{\text{Tüm parçanın uzuluğu}}{\text{Büyük parçanın uzunluğu}} = \frac{\text{Büyük parçanın uzunluğu}}{\text{Küçük parçanın uzunluğu}}$$

Doğru parçasının $[0, 1]$ aralığında ve 1 birim uzuluğunda tanımlandığı varsayılsın. Büyük parçanın uzunluğu da r olarak kabul edilsin. Böylece:

$$\frac{1}{r} = \frac{r}{1-r}$$

$$r = \frac{-1+\sqrt{5}}{2} = 0.618\ldots$$

Daha sonra, x_1 ve x_2 noktalarında $f(x_1)$ ve $f(x_2)$ değerleri hesaplanır.

Eğer $f(x_1) < f(x_2)$ şartı sağlanırsa f fonksiyonunun $[x_1, x_2]$ aralığında arttığı söylenebilir. Böylece, en kötü durumda, fonksiyonun o anki değerinin $f(x_1)$'den büyük olacağı açıktır. f fonksiyonu zaten *unimodal* oluduğu için bu fonksiyonun maksimum değeri x_1'den küçük olamaz. Böylece, f fonksiyonunun maksimum değeri $[a, x_1]$ aralığındadır.

Eğer $f(x_1) \geq f(x_2)$ şartı sağlanırsa, f fonksiyonun alt sınırı $f(x_2)$'dir. Ayrıca, f fonksiyonu *unimodal* olduğu için, fonksiyonun maksimum değeri x_2'den daha düşük olamaz. Böylece, f fonksiyonun maksimum değerinin $[x_2, b]$ aralığında bulunur.

Daraltılan bu yeni aralıklara göre yeni x_1 ve x_2 değerleri hesaplanır. Her iterasyonda aralıklar ϕ faktörü kadar düşürülür. İterasyonlar $|m - n|$ değerinin belirli bir değere düşmesi ile sonlanarak ekstremum noktanın tespiti yapılır.

Bu algoritmanın en büyük avantajı, her doğru parçasının ϕ ile bölünmesiyle iki test noktasından birisinin tanımlanan aralığın güncellendiği sırada tekrardan kullanılmasına imkan tanımasıdır.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: YILDIZ, Hüseyin Uğur
Uyruğu	: T.C.
Doğum Tarihi ve Yeri	: 05.01.1988, Diyarbakır
Medeni Hali	: Bekar
Telefon	: 0533 383 48 77
E-mail	: huyildiz@.etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Y. Lisans	TOBB ETÜ, Elektrik-Elektronik Müh.	2013
Lisans	Bilkent Üniversitesi, Elektrik-Elektronik Müh.	2009

İş Deneyimi

Yıl	Yer	Görev
2010-Halen	Türk Telekom	Ağ Mühendisi
06.2008-07.2008	Nortel Netaş	Stajyer
06.2007-07.2007	Vodafone	Stajyer

Yabancı Dil

İngilizce (Çok iyi)

Yayınlar

Bicakci, K., Yildiz, H.U., Tavli, B., "Communication/Computation Tradeoffs in Wireless Sensor Networks: Comparing Node-Level and Network-Level Strategies", IEEE Topical Conference on Wireless Sensor and Sensor Networks (WiSNet), [Submitted], 2013.

Yildiz, H.U., Bicakci, K., Tavli, B., "Maximizing Wireless Sensor Network Lifetime by Communication/Computation Energy Optimization: Node Level versus Network Level Strategies", IEEE Transaction on Secure and Dependable Computing, [Submitted], 2013.