KABLOSUZ ALGILAYICI AĞLARDA AĞ YAŞAM SÜRESİ VE AĞ GÜVENLİĞİ ENİYİLEMESİ

UĞUR YILDIZ

YÜKSEK LİSANS TEZİ

ENDÜSTRİ MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2014

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof. Dr. Tahir HANALİOĞLU
Anabilim Dalı Başkanı

UĞUR YILDIZ tarafından hazırlanan KABLOSUZ ALGILAYICI AĞLARDA AĞ YAŞAM SÜRESİ VE AĞ GÜVENLİĞİ ENİYİLEMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Salih TEKİN Tez Danışmanı	Doç. Dr. Hakan GÜLTEKİN Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Bülent TAVLI _____

Üye : Yrd. Doç. Dr. Salih TEKİN _____

Üye : Yrd. Doç. Dr. Gültekin KUYZU _____

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.

Uğur YILDIZ

Üniversitesi	:	**TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü	:	**Fen Bilimleri**
Anabilim Dalı	:	**Endüstri Mühendisliği**
Birinci Tez Danışmanı	:	**Yrd. Doç. Dr. Salih TEKİN**
İkinci Tez Danışmanı	:	**Doç. Dr. Hakan GÜLTEKİN**
Tez Türü ve Tarihi	:	**Yüksek Lisans – Ağustos 2014**

Uğur YILDIZ

KABLOSUZ ALGILAYICI AĞLARDA AĞ YAŞAM SÜRESİ VE AĞ GÜVENLİĞİ ENİYİLEMESİ

ÖZET

Bu çalışmada kablosuz algılayıcı ağlarda ağ yaşam süresi ve ağ güvenliği eniyilemeye çalışılmaktadır. Düşmanların ellerinde bulunan anahtar bilgileri ile ağda toplanmış olan verileri ele geçirmeye çalıştıkları varsayılmaktadır. Bu çalışmada, uygulama alanına göre algılayıcı konumlandırma ve anahtar ataması kararlarının deterministik veya rassal olarak verilebileceği göz önünde bulundurularak olası tüm konumladırma ve anahtar ataması yöntemleri kombinasyonları için çeşitli matemakiksel modeller geliştirilmiştir. Önerilen çözüm yöntemleri, hazırlanan test problemleri üzerinde test edilerek hem çözüm yöntemlerinin hem de farklı algılayıcı konumlandırma ve anahtar ataması yöntemlerinin birbirlerine karşı üstünlükleri incelenmiştir. Matematiksel modellerin yani sıra büyük boyutlu problemlerde kısa sürelerde olurlu çözümler elde edebilmek için matematiksel model tabanlı bir sezgisel algoritma geliştirilmiştir. Geliştirilen sezgisel algoritmanın performansı hazırlanan test problemleri ile test edilerek sezgisel algoritmanın kısa sürelerde iyi sonuçlar verdiği gösterilmiştir.

Anahtar Kelimeler: Kablosuz algılayıcı ağlar, yaşam süresi, güvenlik, anahtar yönetimi .

University	:	**TOBB University of Economics and Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Industrial Engineering**
Supervisor	:	**Asst. Prof. Salih TEKİN**
Co-Supervisor	:	**Assoc. Prof. Hakan GÜLTEKİN**
Degree Awarded and Date	:	**M.Sc. – August 2014**

Uğur YILDIZ

LIFETIME AND SECURITY OPTIMIZATION IN WIRELESS SENSOR NETWORKS

ABSTRACT

In this study, both lifetime and security in wireless sensor networks are jointly optimized. It is assumed that enemies try to steal gathered data with the key informations they have. In this study, mathematical models are developed for all possible sensor deployment and key assignment strategy combinations considering that both deployment and key assignment strategies can be applied deterministically and randomly depending on application area. Performance of the proposed solution methods and advantages of deployment and key assignment strategies are investigated on test problems. In addition to mathematical models, a mathematical programming based heuristic algorithm is developed to obtain feasible solutions for large instances. Computational experiments conducted on a set of test instances indicate that both the solution time and the efficiency of the proposed heuristic is quite promising.

Keywords: Wireless sensor networks, lifetime, security, key management .

TEŞEKKÜR

Tezimi okuyarak değerlendiren ve tavsiyelerde bulunarak katkı sağlayan değerli hocalarım Doç. Dr. Bülent TAVLI ve Yrd. Doç. Dr. Gültekin KUYZU'ya, tez çalışmasına başladığımız ilk günden beri desteklerini hiç esirgemeyen değerli tez danışmanlarım ve hocalarım Yrd. Doç. Dr. Salih TEKİN ve Doç. Dr. Hakan GÜLTEKİN'e, tüm hayatım boyunca maddi manevi olarak hep yanımda olan sevgili aileme teşekkürü bir borç bilirim.

İçindekiler

Şekil Listesi

Tablo Listesi

1. GİRİŞ

Kablosuz Algılayıcı Ağlar (KAA), kapasite kısıtlı çok sayıda algılayıcıdan ve algılayıcıların topladıkları verileri ilettikleri baz istasyonu olarak adlandırılan çıkış noktalarından oluşan ağlardır. KAA'da algılayıcılar ortaklaşa çalışarak topladıkları verileri baz istasyonuna iletmeye çalışırlar. KAA bir ortamdaki ısı, ışık, hareket, nem ve basıncın durumsal değişikliklerini belirleyebilmek için çeşitli uygulamalarda kullanılabilmektedir. Bu ağların uygulama alanları askeri, çevre, sağlık, ev ve diğer ticari alanlar olmak üzere sınıflandırılabilir. Askeri alanda, özellikle savaş alanlarında mevcut donanım bilgisine ulaşmak, düşman askerinin hareketlerini izlemek ve savaş hasarı ile ilgili bilgi toplamak için, çevresel uygulamalarda hayvanların hareketlerini izlemek, kimyasal ve biyolojik tespitlerde bulunmak, orman yangınlarını ve sel felaketlerini tespit etmek için, sağlık uygulamalarında ise hasta takibi için kullanılabilir [1].

Uygulama alanlarının geniş olması nedeniyle son yıllarda KAA ile ilgili yapılan çalışmaların sayısında artış olduğu görülmektedir. Algılayıcılar tüm işlemlerini sahip oldukları enerji kaynakları ile gerçekleştirmektedirler. Bu enerji kaynakları sınırlıdır ve bir algılayıcı konumlandırıldıktan sonra eğer enerji kaynağı tükenirse enerji kaynağının değiştirilmesi mümkün olmamaktadır. Enerji kaynaklarının sınırlı olması ve veri alma, veri gönderme ile veri işleme işlemlerinin enerji gereksinimlerinden dolayı enerji sarfiyatının en uygun şekilde gerçekleştirilerek ağların tasarlanması gerekmektedir.

Literatürde algılayıcı konum kararlarının rassal olarak verildiği çalışmalara yoğunlaşılmaktadır. Bu çalışmalarda algılayıcıların helikopter aracılığıya gözetlenmek istenilen alana rassal olarak konumlandırıldığı varsayılmaktadır [20]. Algılayıcıların rassal konumlandırması ağın kurulum maliyetlerini azaltırken diğer

taraftan ağın enerji verimliliğinin kötü olması nedeniyle ağı verimsiz yapmaktadır. Algılayıcı konumları verilen olarak ele alınarak mevcut ağların ağ yaşam süreleri veri alış veriş miktarları belirlenerek uzatılmaya çalışılmaktadır. Çeşitli çalışmalarda, algılayıcıların önceden belirlenen aday noktalara konumlandırılmasının ağ yaşam süresi üzerinde olumlu etkileri olduğu gösterilmiştir [17], [18].

KAA'da bir diğer önemli konu ağın güvenliğidir. Bazı uygulamalarda toplanan verilerin 3'üncü şahıslar tarafından ele geçirilmesinin önlenmesi gerekmektedir. Algılayıcılar radyo dalgaları ile haberleşmektedirler. Aynı frekansta alıcısı olan 3'üncü şahıslar toplanılan verileri ele geçirebilmektedirler. Okyanusta balinaların göç yollarının incelendiği bir uygulama için veri güvenliği fazla önemli değildir fakat; yurt güvenliği veya sağlık alanlarında gerçekleştirilen uygulamalarda verilerin güvenli bir şekilde baz istasyonlarına ulaştırılması önemli olmaktadır. Literatürde KAA için en uygun güvenlik yöntemi ikili anahtar değişim yöntemi olarak ele alınmaktadır [9]. Anahtarlar verilerin şifrelenmesi için kullanılan gizli bilgilerdir. Bir algılayıcı tarafından veri gönderilmeden önce şifrelenir ve eğer verinin şifrelenmesi için kullanılan anahtar bilgisi alıcıda mevcut değilse alınan veri algılayıcı için anlamsız olmaktadır. Bu yöntem sayesinde veriler şifrelenerek güvenli veri alışverişi sağlanmaktadır. Bu yöntem kolay uygulanabilir bir yöntemdir fakat algılayıcıların hafıza limitli olması nedeniyle anahtarların algılayıcıları nasıl atanması gerektiği araştırmacılar tarafından fazlaca ilgi görmüştür. Algılayıcıların rassal olarak konumlandırıldığı bir uygulama için ağın bağlı olmasını garanti etmek pek kolay olmamaktadır. Bir algılayıcının ağda bulunan tüm algılayıcılar ile veri alış verişi gerçekleştirebileceği varsayılarak anahtar ataması gerçekleştirilirse v algılayıcılı bir ağda herbir algılayıcıya $v-1$ adet anahtar yüklenmesi gerekmektedir. Ağın büyüklüğü arttıkça algılayıcıların hafızaları kısıt olarak ortaya çıkmaktadır. Sonuç olarak ikili anahtar değişimi, kullanım açısından basit, verimli bir anahtar yönetemini gerçekleştirme açısından oldukça zor bir yöntemdir.

Bu çalışmada, ağ yaşam süresi enbüyüklenmesi ve veri alış verişlerinin mümkün olduğunca güvenli bir şekilde gerçekleştirilmesi amaçlanmaktadır. Çeşitli algılayıcı konumlandırma ve anahtar ataması yöntemleri için tanımlanmış olan senaryolara çözüm yöntemleri önerilmektedir. Veri alış verişleri, algılayıcı konumları ve anahtar ataması kararlarının birlikte verildiği bu tez çalışması altı bölümde

incelenecektir. Bir sonraki bölümde ağ yaşam süresi, algılayıcı konumlandırma yöntemleri ve güvenlik ile ilgili yapılmış çalışmaların derlendiği literatür taraması yer almaktadır. Üçüncü bölümde detaylı problem tanımı anlatılmaktadır. Dördüncü bölümde tanımlanmış olan problem için önerilen çözüm yöntemleri sunulmaktadır. Beşinci bölümde önerilen çözüm yöntemleri için gerçekleştirilen deneysel çalışmalar yer almaktadır. Son bölüm çalışmayla ilgili genel sonuçlar ve yorumların yanında gelecekte yapılabilecek çalışmalara ayrılmıştır.

2. LİTERATÜR ARAŞTIRMASI

Bu bölümde KAA ile ilgili yapılmış olan çalışmalar 3 başlık altında incelenmiştir. Bölüm 2.1 KAA'da yaşam süresi enbüyüklemesi çalışmalarına, Bölüm 2.2 KAA'da algılayıcıların konumlandırılması çalışmalarına ve Bölüm 2.3 KAA'da güvenli veri alışverişinin ele alındığı çalışmalara ayrılmıştır.

2.1 Yaşam Süresi

Chang ve Tassiulas üç ayrı çalışmada [5], [6], [7] KAA'ın yaşam sürelerini enbüyüklemeyi amaçlayan matematiksel modeller sunmuşlardır. İlk çalışmalarında ağın yaşam süresini, ağda güç kaynağı en çabuk tükenen algılayıcının yaşam süresi olarak tanımlamışlardır. Sunulan matematiksel model ile algılayıcılar arası veri akış miktarını bu amaç doğrultusunda belirlemişlerdir [5]. Bir doğrusal programlama modeli yardımıyla algılayıcıların enerji tüketimlerini dengeleyen sezgisel algortima geliştirmişlerdir. Daha sonraki çalışmalarında ise modellerini ve algoritmalarını çok ürünlü durum için genişletmişlerdir [6]. Çok ürünlü durumda, algılayıcıların ürettikleri verileri hangi algılayıcılara göndericeği bilgisi bulunmaktadır ve gidiş noktası belli olan bu verilerin üretim hızları bilinen olarak tanımlanmaktadır. Son çalışmalarında ise sabit ve değişken veri üretim oranları durumlarını incelemişlerdir [7]. İlk iki çalışmalarında algılayıcıların veri üretim hızlarının sabit olduğu varsayılmaktadır. Son çalışmalarında [7] ise gözetlenmekte olan alanda bir hareket olduğunda algılayıcılar veri üretmektedirler. Sonuç olarak problemin değişken veri üretim hızı altında incelenmesi gerekmektedir. Bu çalışmada veri göndermenin enerji sarfiyatının yanı sıra veri almanın enerji sarfiyatı da göz önünde bulundurulmuştur. Problemlerin çözümü için alıcı ve

gönderici algılyacıların enerji tüketimlerinin ve enerji seviyelerinin kullanıldığı en düşük maliyetli yol algoritması geliştirmişlerdir. Yapmış oldukları simülasyon çalışmasında algoritmanın çoğu zaman matematiksel modellerle elde edilen optimal sonuçlara ulaştığını göstermişlerdir. Kalpakis vd. [14] algılayıcıların veri algılama işlemini periyodik olarak gerçekleştirdiği varsayımı altında ağ yaşam süresini enbüyüklemeye çalışmışlardır. Ağ yaşam süresini, veri algılanması ve algılanan verinin baz istasyonuna ulaştırılması işlemlerinin tüm algılayıcılar tarafından yapıldığı süre olarak tanımlamışlar ve probleme En Çok Veri Toplama Problemi (Maximum Data Gathering Problem) adını vermişlerdir. Çözüm yöntemi olarak veri birleştirmenin olduğu ve olmadığı durumlar için polinom zamanlı sezgisel algoritmalar sunmuşlarıdır.

Alfieri vd. [2] algılayıcıların aktif ve pasif olabildiği durumu incelemişlerdir. Çalışmada hedef noktaların olduğu ve bu hedef noktaların hangi algılayıcılar tarafından gözetlenebildiğinin bilindiği varsayımı bulunmaktadır. Bu çalışmada hizmet kalitesi tanımlanmaktadır. Hizmet kalitesi ağdaki hedef noktaların verilmiş olan bir değerde gözetlenebilmesi anlamına gelmektedir. Yaşam süresini ağın kullanıma başlandığı andan itibaren tüm hedef noktaların verilmiş olan hizmet kalitesinde gözetlendiği toplam süre olarak tanımlamışlardır. Algılayıcılar verilmiş olan hizmet kalitesini sağlayacak şekilde gruplanmakta ve her an sadece bir grubun aktif çalışmasına müsade edilmektedir. Böylelikle algılayıcıların her an aktif çalışması önlenerek ağ yaşam süresinin uzatılması amaçlanmaktadır. Ağın yaşam süresi tüm grupların yaşam sürelerinin toplamı şeklinde elde edilmekte ve grupların yaşam süreleri de grup içinde güç kaynağı en çabuk tükenen algılayıcının çalışır durumda olduğu süre olarak tanımlanmaktadır. Merkezi karar vermenin mümkün olduğu durumlar için sütün türetme yöntemi geliştirilmiştir. Bu çalışmada ayrıca merkezi karar vermenin olmadığı dağıtılmış uygulamalar için sezgisel algoritma önerilmektedir. Zhao ve Gurusamy [22] aktif algılayıcı tanımında ufak bir değişiklik ile problemi ele almışlardır. Problemde röle algılayıcılar tanımlanmaktadır. Röle algılayıcılar, veri algılama işlemi yapmadan sadece veri alış veriş işlemini gerçekleştirebilmektedirler. Algılayıcılar kaynak, röle ve uyku olmak üzere üç farklı durumda bulunabilmektedir. Kaynak ve röle algılayıcılar aktif, uyku durumunda olan algılayıcılar ise pasif algılayıcılar olarak tanımlanmaktadır. Kaynak algılayıcılar, röle algılayıcılardan farklı olarak

veri algılama işlemini de gerçekleştirebilmektedirler. Zhao ve Grusamy [22] algılayıcıların aktif zamanlarını çizelgelemek için ağı Maksimum Kapsar Ağaç Problemi (Maximum Cover Tree Problem) olarak modellemişler ve problemin NP-Tam olduğunu göstermişlerdir. Ağın yaşam süresi için üst sınır değeri hesaplayabilmek amacıyla bir doğrusal programlama modeli geliştirmişlerdir. Çözüm yöntemi olarak etkili bir kestirim algoritması ve hızlı bir aç gözlü sezgisel algoritma sunmuşlardır.

Hong ve Prasanna [13] ve Sadagopan ve Krishnamachari [16] heterojen yapılı KAA üzerinde çalışmışlardır. Algılayıcıların her işlemi aynı anda yapmak zorunda olmadığı ağlar heterojen yapılı olarak adlandırılmaktadır. İki çalışmada da algılayıcılar öncelikle veri toplama işlemini gerçekleştirmekte ve bu işlem tamamlandıktan sonra verilerin baz istasyonuna gönderilmesi işlemini gerçekleştirilmektedir. Her iki çalışmada da problem en büyük akış problemi olarak ele alınmış ve matematiksel modeller geliştirilmiştir. Hong ve Prasna [13] çalışmalarında kısa menzilli problemleri ele almışlar ve veri gönderme ile veri alma enerji sarfiyatları çok yakın olduğu için eşit kabul etmişlerdir. Sadagopan ve Krishnamachari [16] geliştirdikleri modelin dual formunu kullanan bir sezgisel algoritma sunmuşlardır. Yapılan deneysel çalışmada sunulan yöntemin optimal değerlere yakın sonuçlar verdiğini göstermişlerdir.

Basagni vd. [3] çalışmalarında baz istasyonu konumunun kontrol edilebilmesinin ağ yaşam süresi üzerine etkilerini incelemişlerdir. Tanımlamış oldukları problemde algılayıcılar sabit konuma sahiptir fakat; baz istasyonu önceden belirlenmiş veri toplama noktalarına hareket edebilmektedir.Poblemde baz istasyonunun hangi noktalara hangi rota üzerinden gideceğine ve ne kadar süre bu noktalarda kalacağının cevabı aranmaktadır. Problemin çözümü için karma tamsayılı bir matematiksel programlama modeli geliştirilmiştir. Kararların merkezi olarak verilemediği, baz istasyonunun kararlarını kendisinin vermesinin gerektiği senaryolar için de aç gözlü bir sezgisel algoritma sunmuşlardır. Yapılan simülasyon çalışmaları sonucunda hareketli baz istasyonunun ağ yaşam süresini iki katına kadar arttırdığını göstermişlerdir. Yun ve Xia [21] hareketli baz istasyonuna ek olarak problemde toplanan verilerin belirli bir gecikme toleransı altında toplanmasının ağ yaşam süresine etkilerini incelemişlerdir. Bazı uygulamalarda toplanan verinin işlenmek üzere anında iletilmesi gerekliliğinin olmadığını öne

sürerek problemi gecikme toleransı kısıtları altında ele almışlardır. Algılayıcılların, veri transferini gerçekleştirmek için baz istasyonunun ağ yaşam süresine en çok fayda sağlayacak konuma gelmesini bekleyerek toplanmış veriyi belirli bir süre depolamasına müsade edilmektedir. Çalışma ile gecikme toleransının daha önce ele alınmış olan hareketli baz istasyonu problemlerine göre yaşam süresi açısından daha iyi sonuçlar verdiğini göstermişlerdir.

Matematiksel programlama modelleri, protokol ve algoritma çalışmalarına ek olarak KAA'ın performans sınırlarının belirlenmesini amaçlayan bir çok çalışmada yer almıştır. Krishnamachari ve Ordóñez [15] bu amaç doğrultusunda doğrusal olmayan programlama modelleri geliştirmişlerdir. Bu modeller ile algılyıcı sayısı, enerji seviyesi, adil kullanım gibi tasarım parametrelerinin ağ performansına etkilerini incelemişlerdir. Bhardwaj vd [4] ağ yaşam süresine teorik üst sınır elde edebilecekleri bir aktivite çizelgeleme modeli geliştirmişlerdir. Matematiksel model yardımı ile algılayıcıların veri alma, gönderme ve birleştirme işlemlerinin optimal olarak çizelgelenmesi ile teorik en büyük ağ yaşam süresi tespit edilmektedir. Cheng vd. [8] ise algılayıcılar arasında dengeli enerji kullanımının ağın kullanılabilirliği açısından önemini vurgulamış ve özellikle baz istasyonuna yakın algılayıcıların yoğun kullanımının ağ ömrüne olumsuz etkilerine yönelik tek/çoklu, sabit/hareketli baz istasyonu kullanımı, homojen/heterojen enerji dağılımı; eşit/eşit olmayan veri üretme hızı gibi çeşitli kurulum stratejilerini incelemişlerdir. Çalışmada bu stratejilerin analizi ve değerlendirmelerinde kullanılmak üzere temel bir doğrusal programlama modeli geliştirilmiştir. Modelde başlangıçta verilen başlangıç enerji seviyeleri ve menzil değerleri kullanılarak algılayıcılar arasıdaki akış miktarlarına karar verilmektedir. Yapılan analizler sonucunda iyi bir kurulum stratejisinin enerji verimliliği ve dengeli kullanımı birlikte sağlaması gerektiği sonucuna varılmıştır.

2.2 Konumlandırma

Algılayıcıların konumlandırılması yöntemi algılayıcı tipi, uygulama alanı ve algılayıcıların kullanılmasının planlanıldığı çevrenin özelliklerine göre değişmektedir.

Savaş alanı veya felaket bölgesinin gözetlenmesi gibi uygulamalarda rassal konumlandırma olurlu tek yöntem olarak öne çıkmaktadır. Diğer taraftan bir alandan görüntü almak, okyanusta canlıların yaşamları hakkında bilgi toplamak veya bir binanın kolonlarındaki gerilimin ölüçülmesi gibi uygulamalarda deterministik konumlandırma yönteminin kullanılması gerekmektedir [20].

Literatürde rassal konumlandırma yöntemi uygulanırken algılayıcıların düzgün dağılım ile alana konumlandırıldığı varsayılmaktadır [20]. Uygulama geliştiriciler çeşitli tasarım hedeflerini göz önünde bulundurmaktadırlar. Bunlar; kapsamanın arttırılması, güçlü bağlı ağın elde edilmesi, ağ yaşam süresinin arttırılması veya toplanmış olan verinin doğruluğunun sağlanması olarak sıralanabilmektedir. Bunların yanında, algılayıcı bozulmalarına toleransın arttırılması, yük dengeleme gibi ikincil hedefler de bulunabilmektedir. Deterministik konumlandırma ile yukarıda verilmiş olan tasarım hedeflerinin tamamını gerçekleştirebilmek mümkün iken rassal konumlandırma ile zor olabilmektedir [20].

Turkogulları vd. [17], [18], deterministik konumlandırma yönteminin uygulandığı problemleri incelemiş ve çeşitli matematiksel modeller ile çözüm yöntemleri sunmuşlardır. İki çalışmada da algılayıcıların konumlandırıldıkları alanın ardışık noktalar arasında eşit uzaklığa sahip gözetlenmesi gereken hedef noktalardan oluştuğu varsayılmaktadır. Bu hedef noktaların aynı zamanda algılayıcıların konumlandırılabileceği aday noktalar olduğu da varsayılmaktadır. Ayrıca iki çalışmada da farklı tipte algılayıcıların kullanıldığı varsayılmıştır. Her tip algılayıcı kendi içinde özdeş olmakla birlikte, algılayıcıların veri toplama, veri alma, veri gönderme enerji sarfiyat gereksinimleri farklılık göstermektedir. Son olarak algılayıcıların maliyetleri, başlangıç enerji seviyeleri, algılama ve gönderme menzilleri de tipine göre farklılık göstermektedir. İki çalışmada da zaman, periyotlardan oluşmaktadır ve ağın kısıtları sağladığı toplam zaman periyodu sayısı ağ yaşam süresi olarak tanımlanmaktadır.

İlk çalışmada [17], ağda kullanılabilecek algılayıcı sayısı bütçe ile sınırlandırılmaktadır. Bu çalışmada amaç kapsama yaşam süresinin enbüyüklenmesi olarak ele alınmaktadır. Algılayıcılar aktif ve uyku durumunda bulunabilmektedirler. Problemde hangi tip algılayıcının hangi noktaya yerleştirildiğine ve hangi periyotlarda aktif veya uyku modunda olduğuna karar verilmektedir. Çalışmada,

agılayıcıları, aktif oldukları periyotlarda algılayıcı tipine göre belirli bir miktarda enerji sarfettiği varsayılmaktadır. Problem için karma tamsayılı programlama modeli ve çözüm yöntemi olarak da Lagrange gevşetmesi tabanlı bir sezgisel algortima önerilmektedir.

İkinci çalışmada [18], yeni bir maliyet tanımlaması bulunmaktadır. Her tip algılayıcının aday noktalara konumlandırılması farklı maliyetlere neden olmaktadır. Bu çalışmada bütçe, algılayıcıların konumlandırılması için kullanılmaktadır. Tanımlanmış olan problemde, ağda kullanılacak baz istasyonu sayısı bilinmektedir fakat konumları bilinmemektedir. Problemde, algılayıcı ve baz istasyonlarının konumları ile algılayıcıların kendi arasındaki veri akışları ve baz isatasyonları ile geçekleşen veri akış miktarları belirlenmektedir. Genel olarak çalışmada, algılayıcı ve baz istasyon konumları, veri akış miktarları ve algılayıcıların aktif ve pasif durumda bulundukları periyotlar belirlenmektedir. Problemde amaç fonksiyonu ağ yaşam süresinin enbüyüklenmesi olarak ele alınmaktadır. Çözüm yöntemi olarak sütün türetme tabanlı bir sezgisel algoritma önerilmektedir.

Güney vd. [12], algılayıcıların kapsama olasılığı tanımlaması altında problemi ele almışlardır. Bu tanımlamaya göre bir algılayıcının bir hedef noktasını gözetleyebilmesi olasılığı hedef noktasından uzaklaştıkça azalmaktadır. Her bir hedef noktasının verilmiş olan bir değer ile gözetlenebilmesi gerekmektedir. Bu problemde amaç toplam kapsama enerjisini enküçüklemek olarak ele alınmaktadır. Bu amaç fonksiyonu ile ağ yaşam süresinin mümkün olduğunca enbüyükleneceği varsayılmaktadır. Problemde bir önceki çalışmada [18] olduğu gibi bütçe algılayıcıların konumlandırılması için kullanılmaktadır. Problem için tek ürünlü ağ akış problemi ve atama problemi olmak üzere iki tane matematiksel model önerilmektedir. Önerilen modellerin çözümlerinin zor olması nedeni ile büyük boyutlu problemlerin çözümü için tabu araması algoritması önerilmektedir.

2.3 Güvenlik

Algılayıcı ağları görev odaklı olduğu için güvenlik KAA'da ele alınması gereken bir diğer problem olarak değerlendirilmektedir. Radyo frekanslarının kısıtlı limitlerle kullanılması KAA'ın saldırılara karşı duyarlılığının fazla olmasına neden

olmaktadır. Literatürde güvenlik gereksinimleri uygunluk (availability), yetki (authorization), gizlilik (confidentiality), bütünlük (integrity) ve tazelik (freshness) olarak tanımlanmaktadır. Uygunluk; saldırıların varlığına rağmen istenilen servis kalitesinin mümkün olması, yetki; sadece yetkili algılayıcıların veri alış verişi yapabilmesi, gizlilik; mesajların sadece ilgili algılayıcılar tarafından anlaşılabilir olması, bütünlük; algılayıcılar arası veri alış verişi sırasında mesajların kötü amaçlı algılayıcılar tarafından değiştirilmemesi ve tazelik ise verilerin yakın zamana ait olarak düşmanlar tarafından tekrar ettirilmesinin engellenmesi olarak tanımlanmaktadır [9].

Literatürde saldırılar iç ve dış olmak üzere iki ana kategori altında incelenmektedir. İç saldırı ağa ait olan bir algılayıcının istenmeyen şekilde hareket etmesi, dış saldırı ise ağa ait olmayan algılayıcılar aracılığı ile gerçekleştirilen saldırılar olarak tanımlanmaktadır. Saldırılar ayrıca pasif ve aktif olarak da değerlendirilmektedir. Pasif saldırılar ağın dinlenilmesi veya veri alış verişinin izlenilmesi, aktif saldırılar ise veri yayınına yanlış verilerin eklenmesi olarak ele alınmaktadır [9].

Djenouri vd. [9] çalışmalarında bir güvenlik düzeninin KAA için uygun olup olmadığını belirlemek için bazı kriterler sunmuşlardır. Bu kriterler; güvenlik (security), dayanıklılık (resiliency), enerji verimliliği (energy efficiency), esneklik (flexibility), ölçeklendirilebilirlik (scalability), hata toleransı (fault-tolerance) olarak sıralanmaktadır. Güvenlik; bir güvenlik düzenin yukarıda belirtilmiş olan güvenlik gereksinimlerini karşılaması gerektiğini, dayanıklılık; ağda bulunan algılayıcılardan bazılarının açığa cıkmasına rağmen güvenlik düzeninin ağı saldırılara karşı koruyabilir olmasını, enerji verimliliği; güvenlik düzeninin enerji kullanımının verimli olmasını, esneklik; güvenlik düzeninin ağa yeni algılayıcıların eklenebilmesine olanak sağlamasını, ölçeklendirilebilirlik; güvenlik düzeninin güvenlik gereksinimlerini açığa çıkarmadan ölçeklendirilebilir olmasını ve hata toleransı ise güvenlik düzeninin hataların ortaya çıkması durumunda çalışmaya devam edebilmesini belirtmektedir. Bu çalışmada, KAA için en uygun güvenlik düzeninin ikili anahtar değişim yöntemi olduğu belirtilmektedir.

Du vd. [10] çalışmalarında veri alış verişinin şifrelenerek gizli bir şekilde gerçekleştirilmesi gerektiğini öne sürmüşlerdir. Çalışmada anahtarların algılayıcılara dağıtılması problemi için çeşitli güvenlik düzenleri incelenmiş ve anahtarların

algılayıcılara atanmasının, algılayıcıların dağıtımından önce yapılmasının KAA için en uygun güvenlik düzeni olduğunu öne sürmüşlerdir.

Du vd. [11] çalışmalarında anahtar atamasında algılayıcıların konumlarının kısmen bilindiğini varsaymışlardır. Çalışmada algılayıcıların helikopter aracılığı ile belirli alanlara atıldığı fakat bu alanlar içerisine eşit olasılıkla düştüğü varsayılıp anahtar atamasının yapıldığı bir güvenlik düzeni önermişlerdir.

Younis vd. [19] çalışmalarında, ağ gruplardan oluşmakta ve her bir grubun, grubu yöneten algılayıcı düğümü bulunmaktadır. Çalışmalarında, düşmanın ele geçirdiği algılayıcıların hafızalarını okuyarak anahtar bilgilerini elde edebildiği durumlar için güvenlik düzeni önerilmektedir. Çalışmada tüm ağın düşman tarafından ele geçirilmesi olasılığının enküçüklenmesi amaçlanmaktadır.

3. PROBLEM TANIMI

Bu çalışmada KAA'da ağ yaşam süresini enbüyüklemek birincil amaç, ağ yaşam süresi en büyük olacak şekilde ikili anahtar paylaşım yöntemi ile ağın güvenliğini enbüyüklemek ise ikincil amaç olarak ele alınmaktadır. Bir KAA tasarlanmadan önce bazı kararların verilmesi gerekmektedir. Bu kararların en önemlilerinden bir tanesi algılayıcıların konumlandırılmasıdır. Bazı uygulamalarda algılayıcıların önceden belirlenmiş olan yerlere konumlandırılması mümkün iken bazı uygulamalarda ise bu işlem çok maliyetli olmakta veya hiç mümkün olmamaktadır. Algılayıcıların önceden belirlenmiş konumlara yerleştirilmesinin mümkün olmadığı uygulamalarda algılayıcılar gözetlenmesi gereken alana helikopter yardımı ile rassal şekilde konumlandırılabilmektedir. Algılayıcıların rassal olarak konulandırılması kolay ve maliyetsiz olurken diğer taraftan verimsiz olabilmektedir.

KAA tasarlanırken ağın kullanım amacı ve çeşitli tasarım kısıtları bulunmaktadır. Ağın kurulmasının öncelikli amacı agılama alanının gözetlenebilmesi ve bu işlemin mümkün olan en uzun süre gerçekleştirilebilmesidir. Algılayıcılar veri alışverişilerini sahip oldukları sınırlı enerji kaynakları ile gerçekleştirmektedirler. İki algılayıcı arasında veri alışverişi gerçekleştiği zaman gönderici ve alıcı algılayıcıların ikisi de veri miktarına bağlı olarak enerji sarfetmektedir. Alıcı düğümün sarfettiği enerji miktarı mesafeden bağımsız iken gönderici algılayıcının sarfettiği enerji miktarı gönderici ve alıcı algılayıcılar arasındaki mesafe ile ters orantılı olarak hesaplanmaktadır. Prx bir birim veri almak için alıcı algılayıcının sarfetmesi gereken enerji miktarını belirtmektedir. Ptx_{ij} ise i ve j noktalarındaki algılayıcılar arasında gerçekleşen birim miktardaki verinin alışverişi için i noktasındaki gönderici algılayıcının sarfetmesi gereken enerji miktarını ifade

etmektedir. Algılayıcıların enerji kaynakları limitli olduğu için ağın yaşam süresini enbüyükleyecek veri akış rotalarının belirlenmesi gerekmektedir. Rotalar belirlenirken algılayıcıların veri gönderme menzillerini dikkate alması gerekmektedir. İki algılayıcı arasında veri alış verişi gerçekleşebilmesi için aralarındaki mesafenin veri gönderme menzili olarak tanımlanmış olan t_{men} değerinden daha az olması gerekmektedir. Ağın kurulum amacı, verilmiş olan noktaların gözetlenmesi olarak ele alınmaktadır. Bu noktalar hedef noktalar olarak adlandırılmakta ve her bir hedef noktanın ağın yaşam süresi boyunca en az bir algılayıcı tarafından gözetlenmesi gerekmektedir. Bir hedef noktanın gözetlenebilmesi için hedef noktaya, algılayıcıların algılama menzili olarak verilmiş olan r_{men} değerinden, daha yakın mesafede en az bir algılayıcının bulunması gerekmektedir.

Bu çalışmada, ağda kullanılması gereken algılayıcı sayısının bilindiği varsayılmıştır ve v değeri ağda kullanılması gereken algılayıcı sayısını belirtmektedir. v adet algılayıcı ile bir ağ tasarlanması ve menzil kısıtları göz önünde bulundurularak veri akış rotalarının ağ yaşam süresini enbüyükleyecek şekilde belirlenmesi amaçlanmaktadır.

Problem, algılayıcı konumlandırma stratejisinin uygulamadan uygulamaya farklılık gösterebileceği göz önünde bulundurularak, algılayıcı konumlarının deterministik olarak belirlendiği ve algılayıcı konumlandırmanın rassal olarak yapılması sonucunda algılayıcı konumlarının verilen olarak kabul edildiği iki ana problem olarak ele alınmaktadır. Algılayıcı konum kararlarının önceden verildiği uygulamalarda yukarıda bahsedilen tasarım kısıtlarının tamamı göz önünde bulundurulurken rassal konumlandırmanın mümkün olduğu uygulamalarda bu kısıtlar göz ardı edilmektedir. Rassal konumlandırmanın olduğu uygulamalarda her hedef noktasının en az bir algılayıcı tarafından gözetlenebilmesi kısıtı gevşetilmektedir çünkü bu kısıtın kesinlikle sağlanmasını garanti etmek rassallıktan dolayı zor olmaktadır.

Bu çalışmada, ağ yaşam süresini enbüyüklemenin yanında veri akışlarının en güvenli şekilde gerçekleştirilmesi amaçlanmaktadır. Güvenlik yöntemi olarak literatürde KAA için en uygun güvenlik yöntemi olduğu belirtilen ikili anahtar değişim yöntemi kullanıldığı varsayılmıştır. Güvenliğin artırılmasından söz edebilmek için öncelikle hangi tür saldırılara karşı ağın savunulması gerektiğinin

belirtilmesi gerekmektedir. Düşman saldırılarının, toplanmış olan verinin ele geçirilmesine yönelik olduğu varsayılmaktadır. Düşmanın elinde m adet anahtar bilgisi bulunduğu ve bu anahtarlar aracılığı ile tüm ağı dinleyebileceği varsayılmaktadır. Düşmanın hangi anahtarlara sahip olduğu bilinmemektedir fakat amacımız düşmanın ele geçirebilieceği veri miktarını enküçüklemek olduğu için düşmanın her zaman için kendisine en çok faydayı sağlayacak m adet anahtara sahip olduğu varsayılmaktadır. Düşmanın sahip olduğu anahtar sayısı sabit olduğu için öncelikle ağda mümkün olan en çok sayıda anahtar kullanmak güvenliği artıracaktır fakat; algılayıcıların limitli hafızaya sahip olmaları bir algılayıcının hafızasında depolayabileceği anahtar bilgisi sayısını sınırlandırmaktadır. $smax$ değeri algılayıcıların hafızasında bulundurabileceği anahtar sayısını belirtmektedir.

İkili anahtar değişim yöntemine göre iki algılayıcı arasında veri alış verişinin gerçekleşebilmesi için algılayıcıların ortak anahtar bilgilerine sahip olması gerekmektedir. Arasında veri alış verişi bulunan algılayacılar veri akışını birden fazla anahtar ile geçekleştirebilir. Eğer algılayıcılar arasında, birden fazla sayıda ortak anahtar bulunuyorsa veri, her anahtardan eşit miktarda gönderilecek şekilde iletilmektedir. Algılayıcılara dağıtılması gereken anahtar bilgilerinin yeterince fazla olduğu varsayılmaktadır. Böylelikle ağda kullanılan anahtar bilgilerinin ilgili alıcı ve gönderici düğümlerde bulunmak üzere 2 algılayıcıda bulunmasına müsade edilmektedir. Bu şekilde güvenlik önlemleri arttırılmaktadır.

Rassal konumlandırımanın gerekli olduğu uygulamalarda anahtar atamalarının yapılış şekli de farklılık gösterebilmektedir. Bazı uygulamalarda, algılayıcıların konumlandırılması işleminden sonra algılayıcılara anahtar bilgilerinin yüklenebilmesi mümkün iken, bazı uygulamalarda ise algılayıcıların konumlandırılması işleminden önce hafızalarına anahtar bilgilerinin yüklenmesi gerekmektedir. Algılayıcı konumlarının ve veri akış rotaların bilinmemesi anahtar ataması işleminin rassal olarak yapılmasını gerektirmektedir. Anahatar atamalarının önceden rassal olarak gerçekleştirilmesi veri akış rotaları için kısıt olarak ortaya çıkmaktadır. Konum ve anahtar ataması kararlarının rassal olarak verilmesi gereken uygulamalarda algılayıcıların hafızalarındaki anahtar bilgileri veri akışlarını sınırlandırmaktadır.

Bu problemde, v adet algılayıcı ile ağ yaşam süresi en uzun ve güvenlik seviyesi mümkün oldukça yüksek olan bir KAA tasarlanmaya çalışılmaktadır. N kümesi algılayıcıların konumlandırılabileceği aday noktalar ve aynı zamanda en az bir algılayıcı tarafından gözetlenmesi gereken hedef noktalar kümesi olarak tanımlanmış olsun. İki algılayıcı arasında veri alış verişi gerçekleşebilmesi için algılayıcılar arasıdaki mesafe, veri gönderme menzili parametresinden küçük olmalıdır ve algılayıcıların en az bir tane ortak anahtara sahip olmaları gerekmektedir. Düşmanın sahip olduğu anahtar bilgisi sayısı m paremetresi ile ifade edilmektedir ve bu değerin bilindiği varsayılmaktadır. Düşmanın hangi anahtarlara sahip olduğu bilinmemektedir; fakat en kötü senaryoya göre güvenlik önlemleri alınmaktadır. Buna göre düşmanın bildiği anahtarların ağda en yüksek miktarda veri alış verişi gerçekleştirmek için kullanılan anahtarlar olduğu varsayılmaktadır.

Problemde iki tane amaç fonksiyonu bulunmaktadır. İlk ve öncelikli amaç fonksiyonu ağ yaşam süresini enbüyüklemektir. Bu çalışmada, yaşam süresi ağda enerji kaynağı ilk tükenen algılayıcının yaşam süresi olarak tanımlanmıştır. Diğer bir ifadeyle, ağ yaşam süresi, enerjisi ilk tükenen algılayıcının enerjisi tükenene kadar geçen süredir ve amaç bu süreyi enbüyüklemektir. Ağdaki algılayıcıların özdeş olduğu, yani, birim zamanda eşit miktarda veri ürettikleri varsayılmaktadır. Bu varsayım altında, ağ yaşam süresinin enbüyüklenmesi, en çok enerji harcayan algılayıcının harcadığı enerji miktarının en küçüklenmesine eşdeğerdir. Bu tanımlamaya göre ağda birim zamanda üretilen verilerin baz istasyonuna ulaştırılması için en çok enerji sarfeden algılayıcının sarfettiği enerji miktarının enküçüklenmesi ağ yaşam süresinin enbüyüklenmesini sağlamaktadır. İkincil amaç fonksiyonu düşmanın sahip olduğu anahtar bilgileri ile ele geçirebileceği veri miktarının enküçüklenmesidir. Amaç fonksiyonları arasında öncelik ilişkisi bulunması, problemin iki aşamalı çözülmesine olanak sağlamaktadır. İlk aşamada problem sadece birincil amaç fonksiyonu kullanılarak çözüldükten sonra elde edilen değer, güvenliğin enbüyüklenmeye çalışıldığı ikinci aşamada kısıt olarak ele alınmaktadır.

Bu çalışmada, veri akış rotaları kararlarının, tasarım kısıtları göz önünde bulundurularak, ağ yaşam süresini en büyükleyecek şekilde belirlenmesi öncelikli amaç olarak ele alınmaktadır. Ağ yaşam süresinden kayıp yaşamayacak şekilde ikili anahtar değişimi yöntemi ile en güvenli ağın tasarlanması ise ikinci amaç

olarak ele alınmıştır.

Sonraki bölümde herbir algılayıcı konumlandırma ve anahtar ataması yöntemi kombinasyonu için önerilen çözüm yöntemleri ele alınacaktır.

4. ÇÖZÜM YÖNTEMİ

Problem tanımında verildiği üzere problemde 2 tane amaç fonksiyonu bulunmaktadır ve bu amaç fonksiyonları arasında öncelik ilişkisi bulunmaktadır. Amaçlar arasında öncelik ilişkisi bulunması problemin aşamalı olarak ele alınmasına olanak sağlamaktadır. İlk aşamada ağ yaşam süresi enbüyüklenmekte ve ikinci aşamada ise güvenli veri akışları belirlenmeye çalışılmaktadır. İlk aşama için karma tamsayılı doğrulsal programlama modeli önerilmektedir. Düşmanın ele geçirebileceği veri miktarının en küçüklendiği ikinci aşama için ise alternatif çözüm yöntemleri önerilmektedir.

Algılayıcı konum kararlarının deterministik olarak verilebildiği uygulamalarda anahtar ataması kararları da deterministik olarak verilebilmektedir. Dolayısıyla bu tip uygulmalarda anahtar atamasının rassal şekilde yapılmasının hiçbir faydası bulunmayacaktır. Diğer taraftan rassal algılayıcı konumlandırmanın gerekli olduğu uygulamalarda anahtar ataması hem rassal olarak hem de deterministik olarak gerçekleştirilebilir. Sonuç olarak toplamda 3 farklı senaryo ortaya çıkmaktadır. Önerilen çözüm yöntemlerinin yukarıda belirtilmiş olan senaryolar için uyarlanışları sonraki alt bölümlerde detaylıca açıklanmaktadır. Bölüm (4.1)'de algılayıcı konumlandırma ve anahatar ataması kararlarının ağ kurulumundan önce verildiği senaryo için, Bölüm (4.2)'de algılayıcı konumlandırmanın rassal yapılmasının zorunlu olduğu fakat anahtar bilgilerinin algılayıcılara sonradan yüklenebildiği senaryo için ve son olarak Bölüm (4.3)'de ise algılayıcı konum kararları ile anahtar ataması kararlarının rassal olarak veriliği senaryo için geliştirilmiş olan çözüm yöntemleri verilmektedir. Çalışmanın bundan sonraki bölümlerinde, sırasıyla deterministik konumlandırma-deterministik anahtar atama,

rassal konumlandırma-deterministik anahtar atama ve rassal konumlandırma-rassal anahtar atama senaryoları, senaryo-1, senaryo-2 ve senaryo-3 olarak ifade edilecektir.

4.1 Deterministik Konumlandırma, Deterministik Anahtar Ataması

Problem tanımında verildiği üzere ağ yaşam süresi, enerjisi ilk tükenen algılayıcının yaşam süresi olarak tanımlanmıştır ve ağ yaşam süresinin en büyüklenmesi, en çok enerji harcayan algılayıcının harcadığı enerjinin enküçüklenmesine eşdeğerdir. Ağ yaşam süresinin büyüklendiği yani, birim zamanda üretilen verilerin baz istasyonuna iletilmesi için en çok enerji harcayan algılayıcının harcadığı enerjinin enküçüklenmesi problemi için geliştirilen karma tamsayılı doğrusal programlama modelinin (P_1) parametre ve karar değişkenleri Tablo 4.1'de verilmektedir ve geliştirilen matematiksel model aşağıda sunulmaktadır..

Tablo 4.1: P_1 Modeli Parametre ve Karar Değişkenleri.

Kümeler	
N	Aday ve hedef noktalar kümesi.
Parametreler	
v	Konumlandırılacak algılayıcı sayısı.
s	Veri üretme hızı (byte/sn).
λ	Baz istasyonunun konumunu belirten indis.
d_{ij}	Nokta-i ile nokta-j arasındaki mesafe.
c_{ij}	1; eğer $d_{ij} \leq r_{men}$, 0 diğer durumda
a_{ij}	1; eğer $d_{ij} \leq t_{men}$, 0 diğer durumda
Ptx_{ij}	Nokta-i' den nokta-j' ye 1 paket veri göndermenin enerji sarfiyat miktarı.
Prx	1 paket veri almanın enerji sarfiyat miktarı.
Karar Değişkenleri	
L	En çok enerji tüketen algılayıcının enerji sarfiyat miktarı.
x_i	1; eğer Nokta-i' ye algılayıcı konumlandırılırsa, 0 diğer durumda
f_{ij}	Nokta-i' den nokta-j' ye iletilen veri miktarı.

$$
\begin{aligned}
(P_1) \qquad Min \quad & L && (4.1)\\
s.t. \quad & \sum_{j\in N} Ptx_{ij}f_{ij} + Prx \sum_{j\in N\setminus\{\lambda\}} f_{ji} \leq L \quad \forall i \in N \setminus \{\lambda\} && (4.2)\\
& \sum_{j\in N} f_{ij} = \sum_{j\in N\setminus\{\lambda\}} f_{ji} + sx_i \quad \forall i \in N \setminus \{\lambda\} && (4.3)\\
& \sum_{j\in N} f_{ij} \leq Mx_i \quad \forall i \in N \setminus \{\lambda\} && (4.4)\\
& \sum_{j\in N\setminus\{\lambda\}} f_{ji} \leq Mx_i \quad \forall i \in N && (4.5)\\
& \sum_{i\in N} x_i = v && (4.6)\\
& \sum_{j\in N\setminus\{\lambda\}} c_{ji}x_j \geq 1 \quad \forall i \in N && (4.7)\\
& f_{ij} \leq Ma_{ij} \qquad \forall i \in N \setminus \{\lambda\}, \forall j \in N && (4.8)\\
& f_{ij} \geq 0 \quad \forall i,j \in N && (4.9)\\
& x_i \in \{0,1\} \quad \forall i \in N && (4.10)\\
& L \geq 0 && (4.11)
\end{aligned}
$$

Ağ yaşam süresi problemi amaç fonksiyonu (4.1) en çok enerji sarfeden algılayıcının enerji sarfiyat miktarını ifade etmektedir. Amaç fonksiyon değerinin hangi algılayıcı tarafından belirleneceği bilinmediği için problem *minmax* problemi olarak ele alınmıştır. Eşitsizlik (4.2) *minmax* amaç fonksiyonunun doğrusallaştırılması için modele eklenmiştir ve her bir algılayıcının enerji sarfiyatınının amaç fonksiyon değerinden küçük veya eşit olması gerektiğini ifade etmektedir.

Eşitsizlik (4.3) akış dengeleme kısıtları olarak adlandırılmakta ve her bir algılayıcının diğer algılayıcılara ve baz istasyonuna gönderdiği toplam veri miktarının diğer algılayıcılardan aldığı ve kendisinin ürettiği veri miktarına eşit olmasını sağlamaktadır. Ayrıca bu eşitsizlik ile algılayıcı yerleştirilmemiş noktaların veri üretmesi engellenmektedir. Eşitsizlik (4.4) ve (4.5) ile veri alış verişinin sadece algılayıcı yerleştirilmiş olan noktalar arasında gerçekleştirilmesi, eşitlik (4.6) ile de v adet algılayıcının konumlandırılması sağlanmaktadır.

Eşitsizlik (4.7), N kümesindeki herbir noktanın en az bir algılayıcı tarafından

gözetlenmesini sağlamaktadır. Eşitsizlik (4.8) iki algılayıcı arasında veri akışının gerçekleşebilmesi için algılayıcıların arasındaki mesafenin gönderme menzilinden küçük olması gerektiğini ifade etmektedir. Son olarak (4.9)-(4.11) işaret ve tamsayı kısıtlarıdır.

Düşmanın hangi anahtarlara sahip olduğu bilinmediğinden olası veri kaybını enküçüklemek için düşmanın her zaman en çok veriyi elde edebileceği anahtarları bildiği varsayılmaktadır. Diğer taraftan iki algılayıcı arasındaki anahtar sayısı ilgili algılayıcılar arasındaki anahtarların ne kadarlık veriyi iletmek için kullanıldığını etkilemektedir. Arasında veri akışı bulunan iki algılayıcının ortak anahtarlarının hepsi eşit miktarda veriyi iletmek için kullanılmaktadır. Algılayıcı-i ile algılayıcı-j arasındaki anahtarların ilettiği veri miktarı f_{ij}/y_{ij} şeklinde hesaplanmaktadır. y_{ij}, (i,j) ayrıtına atanmış olan yani; algılayıcı-i ile algılyıcı-j'nin veri iletimi için kullabilecekleri, toplam ortak anahtar sayısını ifade eden karar değişkeni olarak tanımlanmıştır. Düşmanın her zaman en çok veriyi elde edeceği anahtarları bildiği varsayıldığı için sahip olduğu anahtarlar f_{ij}/y_{ij} oranı en yüksek olan (i,j) ayrıtlarından olacaktır. Düşmanın anahtarlarını m adet olana kadar oranı yüksek olan ayrıtlardan başlayarak seçtiği varsayılabilir. Sonuç olarak düşmanın anahtarlarını bildiği ayrıtlardan bir tanesi hariç hepsinin tüm anahtarlarını kesinlikle bildiği varsayılabilir. Düşman anahtarlarını bildiği ayrıtlar içerisinde kendisine en az fayda sağladığı anahtarlara sahip ayrıtın anahtarlarının tamamını veya bir kısmını bilmektedir ve bu ayrıtın iki tane özelliği bulunmaktadır. İlk özellik düşmanın anahtarlarının tamamını kesinlikle bildiği ayrıtlardan daha küçük f/y oranına sahip olmasıdır çünkü düşman her zaman için en çok faydayı sağladığı anahtarlara sahip ayrıtları öncelikle bilmektedir. İkinci özellik ise düşmanın anahtarlarından hiçbirisini bilmediği diğer ayrıtlardan daha yüksek f/y oranına sahip olmasıdır çünkü düşman f/y oranı en yüksek olan ayrıtların anahtarlarını bilmesidir.

P_1 modeli ile ağ yaşam süresini enbüyükleyecek enerji sarfiyatı değeri (L^*) belirlenmektedir. Bu değerin kısıt olarak ele alınması ile güvenlik enbüyüklemesi amaç fonksiyonu için problem tekrardan çözülebilir. Anahtar atamalarının gerçekleştirilebilmesi için yeni parametre, karar değişkenleri ve kısıtların tanımlanması gerekmektedir. Algılayıcıların limitli hafızaya sahip olmaları algılayıcılara atanabilecek anahtar sayısını sınırlamaktadır ve bu değer $smax$ parametresi ile ifade

edilmektedir. Elimizde çok sayıda anahtar bilgisi olduğu varsayımı altında bir anahtarın sadece iki tane algılayıcıda bulunmasına müsade edilmektedir. Eğer iki algılayıcı arasında birden fazla anahtar kullanılmış ise veri akışlarının bu anahtarlara eşit olarak dağıtılarak gerçekleştirildiği varsayılmaktadır. Aşağıda güvenlik enbüyüklemesi (düşmanın ele geçirebileceği veri miktarının enküçüklenmesi) problemi için tanımlanan parametre, karar değişkenleri Tablo 4.2'de ve geliştirilen matematiksel model (P_1^1) aşağıda sunulmaktadır.

Tablo 4.2: P_1^1 Modeli Parametre ve Karar Değişkenleri.

Kümeler	
N	Aday Noktalar Kümesi
Parametreler	
m	Düşmanın sahip olduğu anahtar sayısı.
$smax$	Algılayıcıların anahtar taşıyabilme kapasitesi.
L^*	Ağ yaşam süresini enbüyükleyecek enerji sarfiyatı miktarı.
Karar Değişkenleri	
f_{ij}	Algılayıcı-i'den algılayıcı-j'ye gönderilen veri miktarı.
y_{ij}	Algılayıcı-i ile algılayıcı-j'nin sahip olduğu ortak anahtar sayısı.
u_{ij}	1; eğer düşman i ve j algılayıcılarının ortak anahtarlarından tamamını veya bir kısmını biliyorsa
o_{ij}	1; eğer (i,j) ayrıtı u değişkeni 1 değerini alan ayrıtlar içerisinde en küçük f/y oranına sahip olan ayrıt ise, 0 diğer durumda.
g_{ij}	Düşmanın elindeki anahtarlardan (i,j) ayrıtında bulunanların sayısı.

$$(P_1^1) \qquad Min \quad \sum_{i \in N-\lambda} \sum_{j \in N} f_{ij} g_{ij} / y_{ij} \tag{4.12}$$

$$s.t. \quad \text{Kısıt (4.3)-(4.10)} \tag{4.13}$$

$$\sum_{j \in N} Ptx_{ij} f_{ij} + Prx \sum_{j \in N \setminus \{\lambda\}} f_{ji} \leq L^* \quad \forall i \in N \setminus \{\lambda\} \tag{4.14}$$

$$\sum_{j \in N} (y_{ij} + y_{ji}) \leq smax \quad \forall i \in N \tag{4.15}$$

$$g_{ij} \leq y_{ij} + M(1 - u_{ij} + o_{ij}) \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.16}$$

$$y_{ij} \leq g_{ij} + M(1 - u_{ij} + o_{ij}) \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.17}$$

$$f_{ij}/y_{ij} \leq f_{kl}/y_{kl} + M(1 + u_{ij} - u_{kl}) \quad \forall i, j \in N \setminus \{\lambda\} \forall k, l \in N \tag{4.18}$$

$$f_{ij}/y_{ij} \leq f_{kl}/y_{kl} + M(2 - o_{ij} - u_{kl}) \quad \forall i, j \in N \setminus \{\lambda\} \forall k, l \in N \tag{4.19}$$

$$o_{ij} \leq u_{ij} \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.20}$$

$$\sum_{i \in N \setminus \{\lambda\}} \sum_{j \in N} o_{ij} = 1 \tag{4.21}$$

$$g_{ij} \leq y_{ij} \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.22}$$

$$g_{ij} \leq M u_{ij} \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.23}$$

$$f_{ij} \leq M y_{ij} \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.24}$$

$$y_{ij} \leq M f_{ij} \quad \forall i \in N \setminus \{\lambda\}, \forall j \in N \tag{4.25}$$

$$\sum_{i \in N \setminus \{\lambda\}} \sum_{j \in N} g_{ij} = m \tag{4.26}$$

$$y_{ij}, g_{ij} \geq 0, \text{tamsayı} \quad \forall i, j \in N \tag{4.27}$$

$$u_{ij}, o_{ij} \in \{0, 1\} \quad \forall i, j \in N \tag{4.28}$$

Doğrusal olmayan anahtar ataması problemi modeli P_1^1'in amaç fonksiyonunda (4.12) düşmanın elde edebileceği veri miktarı enküçüklenmektedir. Düşmanın ayrıtlardan ne kadar veriyi ele geçirdiğinin hesaplanması gerekmektedir. Düşman ayrıtlardan verileri ayrıtlarda kullanılan ve aynı zamanda kendisinde olan anahtar bilgileri ile ele geçirmektedir. Ayrıtlarda iletilen veri miktarı, ayrıta atanmış olan anahtar sayısı ve düşmanın bu anahtarlardan kaç tanesini bildiği, karar değişkenleri ile ifade edilmektedir. Sonuç olarak amaç fonksiyonu doğrusal olmayan bir ifadedir. Eşitsizlik (4.14) ile problemin ilk aşaması olan ağ yaşam süresini enbüyükleme aşamasında elde edilen L^* değeri kısıt olarak ele alınmaktadır. Algılayıcı konum kararları, veri akış miktarları ağ yaşam süresini enbüyükleyecek olan enerji sarfiyatı değeri göz önünde bulundurularak tekrar belirlenmelidir. (4.3)-(4.10) numaralı kısıtlar problemin ilk aşamasının kısıtlarıdır ve bu aşamada da sağlanmaları gerekmektedir. Eşitsizlik (4.15) algılayıcılara $smax$ adetten fazla anahtar atanmasını engellemektedir. Eşitsizlik (4.16) ve (4.17) düşmanın ayrıtlardan bildiği anahtar sayılarının belirlenmesi için yazılmıştır. Eğer düşman bir ayrıttaki tüm anahtarları biliyorsa ilgili u değişkeni 1 ve ilgili

o değişkeni 0 değerini almalıdır. Bu durumda düşmanın bir ayrıttan bildiği toplam anahtar sayısı olarak tanımlanmış olan g karar değişkeni, ilgili ayrıttaki atanmış olan anahtar sayısını belirten y karar değişkenine eşit olmaktadır. Diğer durumlarda, eşitsizlikler gereksiz duruma gelmektedir. Eşitsizlik (4.18), u karar değişkenleri 1 değerini alan ayrıtların, 1 değerini almamış olan diğer ayrıtlardan daha yüksek f/y oranına sahip olmasını sağlamaktadır ve bu kısıt ile düşmanın anahtarlarını bildiği ayrıtlar belirlenmektedir. Eşitsizlik (4.19) ise o karar değişkeni 1 değerini alan ayrıtın, yani u değişkeni 1 değerini alan ayrıtlar içerisinde f/y oranı en düşük olan ayrıtın belirlenmesini sağlamaktadır. Eşitsizlik (4.20), o değişkeninin sadece u karar değişkeni 1 değerini alan ayrıtlar için 1 değerini alabileceğini belirtmektedir. Eşitsizlik (4.21), o değişkenlerinden sadece bir tanesinin 1 değerini almasına müsade etmektedir. Eşitsizlik (4.22) düşmanın bir ayrıttan en fazla o ayrıtta kullanılan anahtar sayısı kadar anahtarı bilebileceğini ve eşitsizlik (4.23) ise düşmanın herhangi bir ayrıtın anahtarını bilebilmesi için öncelikle ilgili ayrıtı bilmesi gerektiğini ifade etmektedir. Eşitsizlik (4.24) eğer bir ayrıtta veri alış verişi gerçekleşmiş ise o ayrıtta anahtar kullanılması gerektiğini belirtmektedir. Eşitsizlik (4.25) veri alış verişi gerçeklememiş ayrıtlara anahtar ataması yapılmasını engellemektedir. Eşitlik (4.26) düşmanın bildiği toplam anahtar sayısının m adet olmasını sağlamaktadır. Son olarak (4.27) ve (4.28) işaret ve tamsayı kısıtlarıdır.

Güvenlik önlemlerinin en kötü durum senaryosuna göre alınması nedeni ile düşmanın sahip olduğu anahtarların ağda en çok verinin iletilmesi için kullanılan anahtarlar olması gerekmektedir. Eşitsizlik (4.19) ve (4.20) ile düşmanın, anahtar başına düşen veri iletim oranı yüksek olan ayrıtlardan, daha yüksek orana sahip olanları bilmesini sağlatmaktadır. Bir ayrıttaki anahtarların ne kadar veriyi iletmek için kullanıldığının hesaplaması, ayrıtta iletilen veri miktarının (f), ayrıta atanmış olan anahtar sayısına (y) bölünmesi ile elde edilmektedir çünkü ayrıtta bulunan anahtarların hepsi aynı miktarda verinin iletilmesi için kullanılmaktadır. Karar değişkenlerinin bölünmesi şeklinde ifadelerin bulunması ilgili kısıtların doğrusal olmayan bir şekilde ifade edilmesine neden olmaktadır.

Problem iki aşamalı olarak ele alınmasına rağmen P_1 ve P_1^1 modellerinin ikisinde de algılayıcı konumları ve veri akış miktarları belirlenmektedir. P_1^1 modelinde algılayıcı konumlarının ve veri akış miktarlarının tekar belirlenmesinin nedeni P_1

modelinde alternatif optimal çözümlerin olması ihtimalidir. Eğer P_1 modelinde alternatif optimal çözümler varsa ağ güvenliği açısından en uygun olan ilk aşamanın optimal çözümünnün ele alınması gerekmektedir. Eğer P_1 modelinde alternatif optimal çözümler yoksa, P_1 modelinde elde edilen karar değişkenlerinin değerleri P_1^1 modelinde de aynı şekilde elde edilecektir çünkü P_1 modeli amaç fonksyion değeri P_1^1 modelinde kısıt olarak ele alınmaktadır. P_1^1 modelinde çok fazla sayıda doğrusal olmayan ifadenin bulunmasının nedeni P_1 modelinde alternatif optimal çözümlerin olabilmesi ihtimalidir. Eğer P_1 modelinde alternatif optimal çözümlerin olmadığı varsayılarak problem sınırlandırılırsa P_1^1 modelinde algılayıcı konum kararlarının ve veri akış miktarlarının tekrar belirlenmesine gerek kalmayacaktır. Bu sınırlandırma ile P_1^1 modelinde bazı değişiklikler yapılarak doğrusal olmayan ifadeler azaltılabilmektedir fakat, eğer P_1 modelinde alternatif optimal çözümler varsa P_1^1 modeli ile en uzun ağ yaşam süresi için en güvenli ağın tasarlandığını söylemek mümkün olmayacaktır. Sınırılandırmanın diğer bir faydası da P_1^1 modelinin daha sade bir şekilde ele alınabilmesine olanak sağlamasıdır. Öncelikle eşitsizlik (4.24) ve (4.25) gereksiz duruma gelmektedir. Bu kısıtların asıl var oluş nedenleri hangi ayrıtlarda veri alışverişinin olduğunun bilinmemesidir. Problemin sınırılandırılması ile algılayıcı konumları ve algılayıcılar arsındaki veri akış miktarları verilmiş olarak kabul edilmektedir ve modelde eğer ayrıtlarda veri iletimi varsa anahtar atanmalıdır şeklinde kısıtların gerekliliği ortadan kalkmaktadır. P_1^1 modelinde amaç fonksiyonu ile ayrıtlarda kullanılan anahtarların veri iletim oranlarının belirlendiği kısıtlar doğrusal değildir. Eşitsizlik (4.19) ve (4.20)'de bulunan f_{ij} karar değişkenleri artık parametre olarak ele alınmaktadır. Problemin sınırlandırılması, doğrusal olmayan kısıtların doğrusallaştırılmasına ve modelin daha sade bir şekilde ifade edilebilmesine olanak sağlamaktadır. Ek olarak problemin ilk aşamasını ifade eden P_1 modelinin (4.3)-(4.10) kısıtları da gereksiz duruma gelmektedir. Son olarak problemde kullanılan N kümesinin kullanım zorunluluğu ortadan kalkmaktadır çünkü sınırılandırma ile algılayıcıların konumları problemin ilk aşamasında belirlenen konumlar olarak değerlendirilmektedir. Problemin sınırlandırılması ile elde edilen çözüm yöntemlerinde N kümesi yerine W kümesi kullanılmaktadır ve bu küme algılayıcılar kümesini ifade etmektedir.

P_1^2 modeli P_1^1 modelinde f karar değişkenlerinin parametre olarak ele alınması

sonucu elde edilen modeli ifade etmektedir. f karar değişkenlerinin parametre olarak ele alınması ayrıtlardaki anahtarların veri taşıma oranlarının belirlenebilmesini kolaylaştırmaktadır. P_1^1 ve P_1^2 modellerinde amaç fonksiyonları düşmanın ele geçirebileceği veri miktarlarını enküçüklemektir. Düşmanın bir ayrıttan elde edeceği veri miktarı iki karar değişkeni tarafından etkilenmektedir. Öncelikle düşman verileri elinde bulunan m adet anahtar bilgisi ile ele geçirmektedir. Düşmanın bir ayrıttan ele geçireceği veri miktarı, ilgili ayrıttaki anahtarların veri iletme oranları ile ilgili ayrıttan düşmanın bildiği anahtar sayısının çarpımı olarak hesaplamaktadır. Düşmanın ayrıtlardan ne kadar anahtar bilgisine sahip olduğu g karar değişkeni ile belirlenmektedir. Ayrıtlarda anahtarların veri taşıma oranları ise f^*/y oranı ile hesaplanmaktadır. Düşmanın ele geçireceği toplam veri miktarı hesaplanırken g/y ifadesi kullanılmaktadır. İki karar değişkeninin bölüm şekilinde bulunması, problemin sınırlandırılması ile ortadan kaldırılamamaktadır. Sonuç olarak P_1^2 modeli amaç fonksiyonunun doğrusallaştırılamaması nedeniyle doğrusal değildir.

P_1^2 modeli doğrusallaştırılamamaktadır fakat ayrıtlara atanan anahtar sayıları, tanımlanan yeni parametreler ve karar değişkenleri ile problemin karma tamsayılı doğrusal programlama modeli P_1^3 geliştirilmiştir. Tablo 4.3'te P_1^3 modelinin parametre ve karar değişkenleri verilmektedir ve aşağıda P_1^3 modeli sunulmaktadır.

Tablo 4.3: P_1^3 Modeli Parametre ve Karar Değişkenleri.

Kümeler	
W	Algılayıcılar Kümesi
R	Anahtar Sayıları Kümesi
Parametreler	
f_{ij}^*	Algılayıcı-i'den algılayıcı-j'ye gönderilen veri miktarı.
m	Düşmanın sahip olduğu anahtar sayısı.
$smax$	Algılayıcıların anahtar taşıyabilme kapasitesi.
Karar Değişkenleri	
z_{ijrh}	1, eğer (i,j) ayrıtına r adet anahtar atanmış ve düşman bunlardan h tanesini biliyorsa, 0 diğer durumda
t_{ijr}	1, eğer (i,j) ayrıtına r adet anahtar atanmışsa, 0 diğer durumda
q_{ijr}	1, eğer düşman (i,j) ayrıtından r adet anahtar biliyorsa, 0 diğer durumda
u_{ij}	1, eğer düşman i ve j algılayıcılarının ortak anahtarlarından tamamını veya bir kısmını biliyorsa
o_{ij}	1, eğer u değişkeni 1 olanlar içerisinde en küçük anahtar başına veri taşıma oranına sahip olan ayrıt ise, 0 diğer durumda

$$(P_1^3) \qquad Min \quad \sum_{i\in W}\sum_{j\in W}\sum_{r\in R}\sum_{h\in W} f_{ij}^* z_{ijrh} r/h \tag{4.29}$$

$$s.t. \quad \sum_{j\in W}\sum_{r\in R} r(t_{ijr}+t_{jir}) \le smax \quad \forall i \in W \tag{4.30}$$

$$\sum_{r\in R} rq_{ijr} \le \sum_{r\in R} rt_{ijr} + M(1-u_{ij}+o_{ij}) \quad \forall i,j \in W \tag{4.31}$$

$$\sum_{r\in R} rt_{ijr} \le \sum_{r\in R} rq_{ijr} + M(1-u_{ij}+o_{ij}) \quad \forall i,j \in W \tag{4.32}$$

$$\sum_{r\in R} f_{kl}^* t_{klr}/r \le \sum_{r\in R} f_{ij}^* t_{ijr}/r + M(1-u_{ij}+u_{kl}) \quad \forall i,j,k,l \in W \tag{4.33}$$

$$\sum_{r\in R} f_{ij}^* t_{ijr}/r \le \sum_{r\in R} f_{kl}^* t_{klr}/rM(2-o_{ij}-u_{kl}) \quad \forall i,j,k,l \in W \tag{4.34}$$

$$o_{ij} \le u_{ij} \quad \forall i,j \in W \tag{4.35}$$

$$\sum_{i\in N}\sum_{j\in W} o_{ij} = 1 \tag{4.36}$$

$$\sum_{i\in N}\sum_{j\in W}\sum_{r\in R} rq_{ijr} = m \tag{4.37}$$

$$\sum_{r\in R} rq_{ijr} \leq Mu_{ij} \quad \forall i,j \in W \tag{4.38}$$

$$z_{ijrh} \geq t_{ijr} + q_{ijh} - 1 \quad \forall i,j \in W \quad \forall r,h \in R \tag{4.39}$$

$$z_{ijrh} \leq t_{ijr} \quad \forall i,j \in W \quad \forall r,h \in R \tag{4.40}$$

$$z_{ijrh} \leq q_{ijh} \quad \forall i,j \in W \quad \forall r,h \in R \tag{4.41}$$

$$\sum_{r\in R} rq_{ijr} \leq \sum_{r\in R} rt_{ijr} \quad \forall i,j \in W \tag{4.42}$$

$$t_{ijr}, q_{ijr} \in \{0,1\} \quad \forall i,j \in W \quad \forall r \in R \tag{4.43}$$

$$u_{ij}, o_{ij} \in \{0,1\} \quad \forall i,j \in W \tag{4.44}$$

$$z_{ijrh} \in \{0,1\} \quad \forall i,j \in W \quad \forall r,h \in R \tag{4.45}$$

P_1^3 modelinin amaç fonksiyonu (4.29) düşmanın ele geçirebileceği veri miktarını enküçüklemektedir. z karar değişkeni ait olduğu ayrıt için kaç tane anahtar atandığını ve bu anahtarlardan kaç tanesinin düşman tarafından bilindiğini belirtmektedir. z_{ijrh} değişkeni (i,j) ayrıtı hakkında yukarıdaki bilgileri barındırsa da o bilgiler doğrultusunda düşmanın ne kadar veriyi ele geçireceğini söyleyememektedir. Sonuç olarak z değişkeni hangi r ve h indisleri için 1 değerini almış ise düşmanın ele geçireceği veri miktarının hesaplanması gerekmektedir. Problemin sınırlandırılması sonucunda algılayıcılar arasındaki veri akış miktarları verilen olarak kabul edildiğinden z değişkeninin 1 değerini aldığı r ve h indisleri için düşmanın elde edeceği veri miktarı f^*h/r şeklinde hesaplanabilmektedir. f^*/r ifadesi ile ilgili ayrıttaki anahtarların veri iletim oranları hesaplanmaktadır. f^*/r ifadesinin h indisi ile çarpılması ile düşmanın elde edeceği toplam veri hesaplanmış olmaktadır. Eşitsizlik (4.30) hafıza kısıtlarıdır. Eşitsizlik (4.31) ve (4.32) kısıtları düşmanın ayrıtlardan bildiği anahtar sayılarının belirlenmesini sağlamaktadır. Eşitsizlik (4.33) ve (4.34) ile düşmanın anahtarlarını bildiği ayrıtlar belirlenmektedir. Eşitsizlik (4.35) düşmanın bir ayrıtın anahtarlarının bir kısmını bilebilmesi için önce ayrıtı bilmesi gerektiğini belirtmektedir. Eşitsizlik (4.36) ise düşmanın anahtarlarının tamamı yerine bir kısmını bildiği ayrıtın sadece bir tane olabileceğini belirtmektedir. Eşitsizlik (4.37) düşmanın bildiği toplam anahtar sayısının m adet olmasını sağlamaktadır. Eşitsizlik (4.38) düşmanın

bir ayrıtın anahtar bilgilerine sahip olabilmesi için öncelikle ayrıttan anahtar bilebilmesi gerektiğini ifade etmektedir. (4.39)-(4.41) numaralı eşitsizlikler z karar değişkeninin t ve q karar değişkenleri ile olan ilişkisini göstermektedir. z_{ijrh} değişkeninin 1 değerini alması için t_{ijr} ve q_{ijh} değişkenlerinin de 1 değeri alması gerekmektedir. Düşmanın r anahtar atanmış olan bir ayrıttan h adet anahtarı bilebilmesi için ayrıta r anahtar atandığını gösteren karar değişkenini ve düşmanın ayrıttan h adet anahtarı bildiğini gösteren karar değişkenlerinin 1 değerlerini alması gerekmektedir. Diğer olası durumların tamamında z değişkeni 0 değerini almalıdır. Eşitsizlik (4.42) ile düşmanın bir ayrıttan bilebileceği anahtar sayısının ayrıta atanmış olan anahtar sayısından küçük olması sağlanmaktadır. (4.43)-(4.45) numaralı kısıtlar tamsayı kısıtlarıdır.

Problem sınırlandırılması; P_1^1 modelinin daha sade ve doğrusal kısıtlı versiyonu olan P_1^2 modelinin geliştirilmesine olanak sağlamıştır. Sınırılandırılmış probleme faklı bir yaklaşımla problem, yukarıda verilmiş olan P_1^3 karma tamsayılı doğrusal programlama modeli olarak formule edilmiştir. Problemin sınırlandırılması ile P_1^1 modelinden çözümü daha kolay modeller elde edilmiş olsa da problemin boyutu büyüdükçe P_1^2) ve P_1^3 modelleri ile sonuç bulmak zorlaşmaktadır. Büyük boyutlu problemlere çözüm üretebilmek amacıyla problemin ikinci aşamasının sınırılandırılmış versiyonu için bir sezgisel algoritma geliştirilmiştir.

Sezgisel algoritma probleme m parametresinden bağımsız olarak çözüm üretmektedir. Eğer m parametresi 1 değerine eşit ise problem ağda en yüksek f/y oranına sahip ayrıtın oranının en küçüklenmesi şeklinde ele alınabilir. Bu durumda matematiksel modelin $minmax$ modeli olarak formüle edilmesi gerekmektedir. Tablo 4.4'te $m = 1$ için geliştirilen P_1^4 modelinin parametre ve karar değişkenleri ve aşağıda P_1^4 modeli verilmektedir.

Tablo 4.4: P_1^4 Modeli Parametre ve Karar Değişkenleri.

Kümeler	
W	Algılayıcılar Kümesi
Parametreler	
m	Düşmanın sahip olduğu anahtar sayısı.
$smax$	Algılayıcıların anahtar taşıyabilme kapasitesi.
f_{ij}^*	Algılayıcı-i' den algılayıcı-j' ye gönderilen veri miktarı.
Karar Değişkenleri	
y_{ij}	Algılayıcı-i ile algılayıcı-j' nin sahip olduğu ortak anahtar sayısı.
L_2	Doğrusallaştırmak için tanımlanan yapay değişken.

$$(P_1^4) \qquad Min \quad L_2 \tag{4.46}$$

$$s.t. \quad \sum_{j \in W} (y_{ij} + y_{ji}) = smax \quad \forall i \in W \tag{4.47}$$

$$f_{ij}^* / y_{ij} \leq L_2 \quad \forall i, j \in W \tag{4.48}$$

$$y_{ij} \geq 0, \text{tamsayı} \quad \forall i, j \in W \tag{4.49}$$

$$L_2 \geq 0 \tag{4.50}$$

P_1^4 modeli, eşitsizlik (4.48)'ün doğrusal olmaması nedeniyle doğrusal değildir. Doğrusallaştırmak için min olan amaç fonksiyonunun max ile ve eşitsizlik (4.48)'ün ise aşağıdaki gibi değiştirilmesi gerekmektedir.

$$y_{ij} / f_{ij}^* \geq L_2 \quad \forall i, j \in W \tag{4.51}$$

Yapılan değişiklik ile matematiksel modelin amaç fonksiyon değeri $m = 1$ için düşmanın elde edeceği veri miktarını vermeyecektir; fakat $m = 1$ için optimal çözümü verecektir. $m = 1$ için problemin optimal çözümünü veren P_1^4 modelinin

değiştirilmiş hali olan P_1^5 modeli aşağıda sunulmaktadır.

$$(P_1^5) \qquad Max \quad L_2 \tag{4.52}$$

$$s.t. \quad \sum_{j \in W} (y_{ij} + y_{ji}) = smax \quad \forall i \in W \tag{4.53}$$

$$y_{ij}/f_{ij}^* \geq L_2 \quad \forall i, j \in W \tag{4.54}$$

$$y_{ij} \geq 0, \text{tamsayı} \quad \forall i, j \in W \tag{4.55}$$

$$L_2 \geq 0 \tag{4.56}$$

Geliştirilen sezgisel çözüm yöntemi P_1^5 matematiksel modelini baz alarak çözüm bulmaktadır. Algoritma çözüme P_1^5 matematiksel modelinin çözümüyle başlamaktadır. Algoritma, P_1^5 modelinin çözümünde amaç fonksiyon değerini veren ayrıt ve bu ayrıta atanmış anahtar sayısı bilgilerini alarak P_1^5 matematiksel modeline aşağıda verilen kısıtların eklenmiş ve (4.54) kısıtının $((y_{ij}/f_{ij}^*) + M(\alpha_{ij}) \geq L_2)$ şeklinde güncellenmiş hali olan P_1^6 modelini tekrar çözmektedir.

$$y_{ij} \leq \gamma_{ij} + M(1 - \alpha_{ij}) \quad \forall i, j \in W \tag{4.57}$$

$$\gamma_{ij} \leq y_{ij} + M(1 - \alpha_{ij}) \quad \forall i, j \in W \tag{4.58}$$

γ_{ij} parametresi (i,j) ayrıtının anahtar atamalarının algoritmanın daha önceki adımlarında belirlenip belirlenmediğini ifade etmektedir. γ_{ij} parametresi eğer (i,j) ayrıtına atanan anahtar sayısı kesinleşmiş ise 1 değerini kesinleşmemiş ise 0 değerini almaktadır. γ_{ij} prametresi ise eğer (i,j) ayrıtına anahtar ataması kesinleşmiş ise atanan anahtar sayısını belirten parametre olarak tanımlanmıştır.

Sezgisel algoritma her bir adımda düşmanın sahip olduğu anahtarların hangi ayrıtlara ait olduğunu belirlemeye çalışmaktadır. Her adımda bulunan optimal çözüm değerleri sonraki adımlara taşınarak düşmanın bildiği anahtar sayısı olan m değeri elde edilene kadar P_1^6 matematiksel modeli çözdürülmektedir. Sezgiel çözüm yöntemi algoritmik olarak aşağıda verilmektedir.

Algoritma 1 Sezgisel Çözüm Yöntemi

Girdi: f^*, m, α_{ij}, γ_{ij}, k, t.
Çıktı: y_{ij}.
P_1^5 **modelini** $m = 1$ **için çöz**
t: P_1^5 **modelinde amaç fonksiyon değerini veren ayrıtı belirle**
k: **Düşmanın ele geçirdiği anahtar sayısını güncelle** $k \leftarrow k + y_t$
α_{ij} **ve** γ_{ij} **parametrelerini güncelle**
  $k < m$ **İken tekrarla**
    P_1^6 modelini çöz
    α_{ij},γ_{ij}, t, k **parametrelerini güncelle**
  Döngüyü bitir
Algoritmayı bitir

Sezgisel algoritmanın girdileri, m parametresi ve ağ yaşam süresinin enbüyüklendiği ilk aşamada elde edilen veri akış miktarlarıdır (f^*). Algoritma çözüme P_1^5 ile başlamaktadır. P_1^5 modelinde $m = 1$ değeri için problem çözdürülerek anahtar başına en çok veri iletim oranına (f/y) sahip ayrıt ve bu ayrıta atanan anahtar sayısı belirlenmektedir. Eğer ayrıta atanan anahtar sayısı m değerinden küçük ise algoirtma ilk adımda elde ettiği bilgileri kullanarak P_1^6 modelini $m = 1$ değeri için çözerek işleme devam etmektedir. Her çözümden sonra düşmanın elde ettiği anahtar sayısının m değerinden küçük olup olmadığı kontrolu yapılarak işleme devam edilmektedir. Düşmanın ele geçirdiği anahtar sayısı m değerini geçtiği noktada algoritma sonlandırıllmakta ve düşmanın ele geçirdiği toplam veri miktarı hesaplanmaktadır.

Sonraki bölümlerde bu bölümde sunulmuş olan çözüm yöntemlernin senaryo-2 ve senaryo-3 için uyarlanışları verilecektir.

4.2 Rassal Konumlandırma, Deterministik Anahtar Ataması

Senaryo-2 ile senaryo-1 arasındaki tek fark algılayıcıların konumlandırma stratejisidir. 4.1'de önerilen tüm çözüm yöntemleri ufak değişiklikler ile senaryo-2 için de uygun duruma gelmektedir. Senaryo-1'de deterministik konumlandırma yapıldığı için algılayıcıların konum kararları verilmektedir fakat; senaryo-2'de algılayıcı

konumları verilen olarak ele alınmaktadır. Senaryo-2' de problem; konum bilgileri verilmiş olan algılayıcılar için en uzun ağ yaşam süresininin sağlandığı düşmanın ele geçirebileceği veri miktarının enküçüklenmesi problemi olarak ele alınmaktadır. Senaryo-1' de v adet algılayıcı N kümesinin elemanları olan aday noktalara konumlandırılmaktadır. Senaryo-2' de konumlandırma işlemi yapılmadığı için algılayıcılar kümesini belirten W kümesinin kullanılması gerekmektedir. Senaryo-2' de rassal konumlandırma gerçekleştiği için N kümesinde bulunan herbir hedef noktasının ağ yaşam süresi boyunca gözetlenmesi kısıdı göz ardı edilmektedir. Rassal konumlandırmanın gerçekleştirildiği ugyulamalarda kapsama kısıdı gibi tasarım kısıtları ikinci planda tutularak performans değerlendirmesi olarak ele alınmaktadır [20]. Aşağıda ağ yaşam süresinin enbüyüklendiği birinci aşamanın 4.1' de tanıtılmış olan P_1 modelinin senaryo-2 için uyarlanmış hâli olan P_2 modeli sunulmaktadır.

$$
\begin{aligned}
(P_2) \qquad Min \quad & L && (4.59)\\
s.t. \quad & \sum_{j \in W} Ptx_{ij} f_{ij} + Prx \sum_{j \in W} f_{ji} \leq L \quad \forall i \in W - \backslash \{\lambda\} && (4.60)\\
& \sum_{j \in W} f_{ij} = \sum_{j \in N} f_{ji} + s \quad \forall i \in W \setminus \{\lambda\} && (4.61)\\
& f_{ij} \leq M a_{ij} \qquad \forall i, j \in W && (4.62)\\
& f_{ij} \geq 0 \quad \forall i, j \in W && (4.63)\\
& L \geq 0 && (4.64)
\end{aligned}
$$

P_2'de ikili değişken bulunmadığı için problem doğrusal programlama modeli olarak ifade edilmiştir. W kümesindeki herbir eleman bir algılayıcı temsil etmektedir dolayısıyla W kümesindeki elemanlar eğer aralarındaki mesafe t_{men} parametresinden küçük ise veri akışı gerçekleştirebileceklerdir. (4.61)' te eşitsizliğin sağ tarafında bulunan sx_i ifadesi yerine s ifadesinin yazılması gerekmektedir çünkü P_1 modelindekinin aksine her bir indis bir algılayıcı temsil etmektedir.

P_2^1 modeli ile P_1^1 modeli arasındaki iki fark bulunmaktadır. Bunlardan ilki; ilk aşamadan gelen kısıtların farklı olmasıdır. İkinci fark ise P_1^1 modelinde noktalar kümesi (N) kullanılması gerekmektedir fakat; P_2^1 modelinde algılayıcılar kümesi

(W) kullanılması gerekmektedir. Bu iki değişikliğin dışında P_2^1 ve P_2^2 modelleri arasında başka hiçbir faklılık bulunmamaktadır.

Problemin sınırılandırılması ile elde edilen P_3^1, P_4^1, P_5^1 ve P_6^1 matematiksel modelleri hiçbir değişikliğe gerek duyulmadan senaryo-2 için de kuulanılabilir durumdadır çünkü bu modellerde problemin sınırılandırılması ile (N) kümesi yerine (W) kümesi kullanılmaktadır. Önerilen sezgisel yöntemde algılayıcı konumlarından bağımsız olarak veri akış miktarlarının verilen olarak varsayılması sonucu çözüm üretebilmektedir dolayısıyla sezgisel algortima da hiçbir değişkliğe ihtiyaç duymadan senaryo-2 için kullanılabilir durumdadır.

4.3 Rassal Konumlandırma, Rassal Anahtar Ataması

Senaryo-3'te algılayıcıların hafızalarına anahtar atamaları rassal bir şekilde gerçekleştirilmektedir. Anahtar atamalarının gerçekleştirilmesinden sonra algılayıcılar alana rassal bir şekilde konumlandırılmakta ve algılayıcı konumları ile anahtar bilgileri verilmiş kabul edilmektedir. Ağ kurulduktan sonra önceki bölümlerde verilmiş olan amaçlar doğrultusunda çözüm üretilmektedir.

Senaryo-3'te de amaçlar arasındaki öncelik ilişkisi bulunmaktadır. Anahtar atamaları verilen olduğu için ikinci amaç olan düşmanın elde edebileceği veri miktarının enküçüklenmesi senaryo-1 ve senaryo-2'de olduğundan biraz farklıdır. Öncelikle ağ yaşam süresinin en büyüklendiği enküçük enerji sarfiyatı değerinin belirlenmesi gerekmektedir. Sonra ilk aşamada elde edilen değerin kısıt olarak ele alınması ile anahtar ataması bilgileri göz önünde bulundurularak veri akış miktarlarının düşmanın ele geçirebileceği veri miktarını enküçükleyecek şekilde güncellenmesi gerekmektedir.

4.2'de sunulmuş olan ağ yaşam süresini enbüyükleyen P_2 matematiksel modeline yeni kısıtlar eklenerek senaryo-3 için ağ yaşam süresini enbüyüklemek mümkün olmaktadır. Kısıt eklenmesinini nedeni P_1 ve P_2 modellerinden farklı olarak yeni modelde algılayıcılar arasında veri verişlerinin gerçekleşebilmesi için algılayıcıların ortak anahatarlara sahip olmaları gerekmesidir.P_2^1 modeli

senaryo-2 için geliştirilmiş, veri akış karaları ile anahtar ataması kararlarının ortak verildiği doğrusal olmayan modeldir. Modelin doğrusal olmamasının nedeni içinde bulunan fy ifadesinin iki karar değişkenini çarpım şeklinde içermesidir. Senaryo-3'te y karar değişkeni parametre olarak ele alınmaktadır dolayısıyla P_2^1 modelinin kısıtlarındaki doğrusal olmayan ifadeler doğrusallaşmış olmaktadır. P_2^1 modelinin aynı zamanda amaç fonksiyonu da doğrusal değildir çünkü amaç fonksiyonu fg ifadesini içermektedir ve bu ifadede de iki karar değişkenin çarpımı bulunmaktadır.

Senaryo-1 ve senaryo-2 için problemlerin sınırılandırılması ile elde edilen diğer matematiksel modeller ile sezgisel çözüm yönteminin senaryo-3 için uygulanması mümkün değildir. Problemlerin sınırılandırılması sonucunda önerilen çözüm yöntemlerinde, ilk aşamada veri akış miktarı kararları ikinci aşamada verilen olarak kabul edilmektedir. Eğer senaryo-3 için aynı işlem gerçekleştirilecek olursa problemin ilk aşamasının çözülmesinden sonra diğer yöntemlerinin uygulanması anlamsız olacaktır çünkü düşmanın her zaman için veri akış oranı (f/y) en yüksek anahtarları bildiği varsayılmaktadır. Eğer problem sınırlandırılarak çözüm bulunmaya çalışılırsa sonuçta ortaya çıkacak çözüm düşmanın f/y oranı en yüksek olan ayrıtlardan başlayarak m adet anahtarı seçmesi şeklinde olacaktır ve sınırılandırma sonucu önerilen çözüm yöntemlerinin kullanılmasna gerek kalmayacaktır.

Senaryo-3 için önerilen matematiksel modeller tanıtılmadan önce e_{ij} parametresinin tanıtılması gerekmektedir. e_{ij} (i,j) ayrıtlarında (algılayıcılar arasında) bulunanan ortak anahtar sayısını belirtmektedir. e parametresi algılayıcılara anahtarların rassal bir şekilde atanması sonucu elde edilmektedir. Aşağıda senaryo-3'ün ilk aşaması olan ağ yaşam süresinin enbüyüklenmesi için önerilen doğrusal matematiksel programlama modeli sunulmaktadır.

$$(P_3) \qquad Min \quad L \tag{4.65}$$

$$s.t. \quad \sum_{j \in W} Ptx_{ij} f_{ij} + Prx \sum_{j \in W} f_{ji} \leq L \quad \forall i \in W - \backslash\{\lambda\} \tag{4.66}$$

$$\sum_{j \in W} f_{ij} = \sum_{j \in N} f_{ji} + s \quad \forall i \in W \tag{4.67}$$

$$f_{ij} \leq Ma_{ij} \qquad \forall i, j \in W \tag{4.68}$$

$$f_{ij} \leq Me_{ij} \quad \forall i, j \in W \tag{4.69}$$

$$f_{ij} \geq 0 \quad \forall i, j \in W \tag{4.70}$$

$$L \geq 0 \tag{4.71}$$

P_3 modelinde P_2 modeline ek olarak (4.69) kısıtı bulunmaktadır. Eşitsizlik (4.69) ile arasında ortak anahtar bulunmayan algılayıcıların veri akışı gerçekleştirmeleri engellenmektedir. Problemin ikinci aşaması olan düşmanın ele geçirebileceği veri miktarının enküçüklendiği doğrusal olmayan matematiksel programlama modeli P_3^1 aşağıda sunulmaktadır.

$$(P_3^1) \qquad Min \quad \sum_{i\in W}\sum_{j\in W} f_{ij}g_{ij}/e_{ij} \tag{4.72}$$

$$s.t. \quad \text{Kısıt (4.67)-(4.69)} \tag{4.73}$$

$$\sum_{j\in W} Ptx_{ij}f_{ij} + Prx\sum_{j\in N} f_{ji} \leq L^* \quad \forall i \in N \tag{4.74}$$

$$g_{ij} \leq e_{ij} + M(1 - u_{ij} + o_{ij}) \quad \forall i,j \in W \tag{4.75}$$

$$e_{ij} \leq g_{ij} + M(1 - u_{ij} + o_{ij}) \quad \forall i,j \in W \tag{4.76}$$

$$f_{ij}e_{kl} \leq f_{kl}e_{ij} + M(1 + u_{ij} - u_{kl}) \quad \forall i,j,k,l \in W \tag{4.77}$$

$$f_{ij}e_{kl} \leq f_{kl}e_{ij} + M(2 - o_{ij} - u_{kl}) \quad \forall i,j,k,l \in W \tag{4.78}$$

$$o_{ij} \leq u_{ij} \quad \forall i,j \in W \tag{4.79}$$

$$\sum_{i\in N}\sum_{j\in N} o_{ij} = 1 \tag{4.80}$$

$$g_{ij} \leq e_{ij} \quad \forall i,j \in W \tag{4.81}$$

$$g_{ij} \leq Mu_{ij} \quad \forall i,j \in W \tag{4.82}$$

$$\sum_{i\in W}\sum_{j\in W} g_{ij} = m \tag{4.83}$$

$$g_{ij} \geq 0, \text{tamsayı} \quad \forall i,j \in W \tag{4.84}$$

$$u_{ij}, o_{ij} \in \{0,1\} \quad \forall i,j \in W \tag{4.85}$$

P_3^1 modelinde P_2^1 modelinde olduğu gibi hafıza kısıtlarına gerek duyulmamaktadır çünkü anahtar atamaları hafıza kısıtına uyularak gerçekleştirilmiştir. P_2^1 modelinde anahtar atamaları algılayıcılar arasında veri akışı gerçekleşmiş ise gerçekleştirilmektedir ve eğer veri akışı yoksa anahtar atamasının gerçekleştirilmesi engellenmektedir. P_3^1 modelinde anahtar atamaları verilmiş kabul edildiği için bu kısıtlar gereksiz duruma gelmektedir. Gereksiz kısıtların çıkarılması ve y karar değişkeni yerine e parametresinin kullanılması ile P_2^1 modeli senaryo-3 için kullanılabilir duruma gelmektedir.

Sonraki bölümde, ele alınan senaryolar için önerilen çözüm yöntemlerinin test problemleri üzerinde analiz edildiği deneysel çalışma ve sonuçlar yer almaktadır.

5. DENEYSEL ÇALIŞMA VE SONUÇLAR

Bu bölümde, çözüm yöntemi olarak önerilen yöntemler hazırlanan test problemleri ile test edilmektedir. Test problemleri üç amaç için hazırlanmıştır. Bunlardan ilki problemleri sınırılandırmanın etkilerinin incelenebilmesidir. İlk testte önerilen tüm çözüm yöntemleri ile sonuçlar elde edilmektedir. Çözüm yöntemleri arasında doğrusal olmayan matematiksel programlama modelleri olduğu için ilk test küçük boyutlu problemler üzerinde gerçekleştirilmiştir. Problemin sınırlandırılması, senaryo-1 ve senaryo-2 için önerildiğinden, ilk testte sadece senaryo-1 ve senaryo-2 için önerilen çözüm yöntemleri test edilmiştir. İkinci testte Bölüm 4'te tanıtılmış olan sezgisel çözüm yönteminin performansının ölçülmesi amaçlanmıştır. Önerilen sezgisel yönteme göre problemin ağ yaşam süresinin enbüyüklendiği ilk aşamada belirlenen veri akış miktarları parametre olarak ele alınmaktadır. Sezgisel çözüm yöntemi, problemlerin sınırılandırıldığı varsayımı altında algılayıcıların konum ve veri akış kararlarından bağımsız olarak çözüm üretmektedir. Bu yüzden sezgisel algoritmanın performansının ölçülmesi için hazırlanan test problemleri senaryo-2 için test edilmiştir. Üçüncü test problemleri ise verilmiş olan problemlerin üç senaryo için ağ yaşam süreleri ve güvenlik seviyelerinin karşılaştırılabilmesi için gerçekleştirilmiştir.

Problemi sınırılandırmanın etkileri senaryo-1 ve senaryo-2 için incelenmektedir. Hazırlanan test problemlerinde deterministik konumlandırmanın yapıldığı senaryo-1'de aday noktaların belirlenmesi için çeşitli yöntemler uygulanabilmektedir. Algılayıcıların konumlandırılabileceği aday noktalar ile en az bir algılayıcı

tarafından gözetlenmesi gereken hedef noktaları ifade eden N kümesinin elemanları [12],[17] ve [18]'de olduğu gibi belirlenmiştir. Algılayıcıların konumlandırıldığı alanın x ve y eksenlerinde birbirine eşit uzaklıktaki çizgiler ile çizildiği ve çizgilerin kesişim noktalarının N kümesinin elemanları olduğu varsayılmaktadır. Rassal konumlandırmanın uygulandığı senaryo-2 için ise algılayıcılar N kümesinin elemanlarının bulunduğu alana rassal olarak konumlandırılmaktadır. Konumlandırılmanın rassal olarak gerçekleştirildiği her bir problem için 15 farklı problem üretilerek ortalama değerler göz önünde bulundurulmuştur. Tablo 5.1'de bu test için hazırlanan problemlere ait parametreler özetlenmektedir.

Tablo 5.1: Sınırılandırma Testi Problemleri Parametre Değerleri.

Tanım	**Parametre**	**Değer**	**Senaryo**
Aday nokta sayısı	$\|N\|$	10, 15, 20	1
Düşmanın sahip olduğu anahtar sayısı	m	20, 50	1, 2
Algılayıcıların hafıza limiti	$smax$	50	1, 2
Ağda kullanılacak algılayıcı sayısı	v	10	1, 2

Ele alınan problemlerin büyüklüğünü etkileyen en önemli parametreler N kümesinin boyutu, v ve $smax$ parametreleridir. N kümesi sadece senaryo-1 için tanımlanmış bir kümedir. Deterministik konumlandırmada algılayıcılar için en uygun konumlar belirlenemebilmektedir fakat; algılayıcılar sadece verilmiş olan aday noktalara konumlandırılabilmektedir. Sonuç olarak aynı alan içerisinde aday nokta sayısının arttırılması ile daha iyi çözümler elde edilebilmektedir. Bu nedenle üretilen her bir problemin aday nokta sayısı için 3 farklı değer ele alınmıştır. Rassal konumlandırmanın uygulandığı senaryo-2 için ise aday nokta sayısı önemsiz olmaktadır çünkü algılayıcı konum kararları rassal olarak verilmektedir. Problem boyutunu direk olarak etkileyen bir diğer parametre ağda kullanılan algılayıcı sayısını ifade eden v parametresidir. Bu test küçük boyutlu problemler üzerinde uygulandığı için v parametresi 10 olarak ele alınmıştır. m parametresi ile $smax$ parametresinin etkileri birlikte ele alınmaktadır. Senaryo-1 ve senaryo-2 için Bölüm 4'te problemin sınırlandırılması sonucu önerilen karma tamsayılı programlama modellerinde $smax$ parametresi aynı zamanda küme boyutunu belirtmektedir. Problem boyutunun küçük olabilmesi için $smax$ değeri 50 olarak ele alınmış ve m parametresi için de $smax$ parametresinin değerinden birisi küçük

diğeri büyük olmak üzere iki tane değer ele alınmıştır. Senaryo-1 için toplamda 6 adet test problemi ele alınmıştır. Senaryo-2 için ise m parametresinin belirlenmiş olan 20 ve 50 değerlerinin ele alındığı iki test problemi ele alınmaktadır çünkü N parametresinin farklı değerleri senaryo-2 için problemi etkilememektedir. Her iki test probleminde de algılayıcıların 15 farklı şekillde rassal olarak konumlandırıldığı problemler üretilerek senaryo-2 için sınırılandırmanın etkileri incelenmiştir.

Yukarıda tanıtılmış olan test problemlerinin sonuçları düşmanın ele geçirebileceği veri miktarları göz önünde bulundurularak değerlendirilmektedir. 2 senaryo için de ağ yaşam süreleri herbir çözüm yönteminde senaryo-1 için (P_1) modelinin çözülmesi ve senaryo-2 için ise (P_2) modelinin çözülmesi ile elde edilmektedir. Çözüm yöntemleri ağ yaşam süresi açısından biribirlerine karşı bir avantaj veya dezavantaja sahip değillerdir. Hazırlanmış olan test problemlerinin senaryo-1 için 1 saatlik zaman limiti altında elde edilen sonuçları Tablo 5.2'de sunulmaktadır.

Tablo 5.2: Senaryo-1 İçin Sınırlandırma Testi Sonuçları.

Problem no	**m**	**|N|**	**Amaç Fonksiyon Değeri (% Hata)**			
			P_1^1	P_1^2	P_1^3	**Sezgisel**
1		10	1.3(0)	1.3(0)	1.71(32)	1.3(0)
2	20	15	-	2.9(0)	3.26(12)	2.9(0)
3		20	-	3.83(0)	3.83(0)	3.92(2.4)
4		10	3,81(17)	3.26(0.3)	3.41(5)	3.25(0)
5	50	15	-	7.1(0.5)	7.06(0)	7.06(0)
6		20	-	9.2(0)	10.16(10)	9.21(0.57)
Ortalama Hata	-	-	**8.5**	**0.14**	**9.84**	**0.5**

Tablo 5.2' nin ilk sütununda görüldüğü üzere problemi sınırılandırmanın etkileri 6 problem üzerinde test edilmiştir. İkinci ve üçüncü sütunlar test edilen problemin parametreleri hakkında bilgi vermektedir. Bunlar sırasıyla ilgili problemde düşmanın elindeki anahtar sayısı ve algılayıcıların konumlandırılabileceği aday noktalar kümesinin boyutunu belirten parametrelerdir. Test edilen çözüm yöntemlerinin 1 saat zaman limiti altında çözülmesinden elde edilen amaç fonksiyon değerleri son dört sütunda sunulmaktadır. Amaç fonksiyon değerlerinin yanında parantez içinde yüzde hata değerleri sunulmaktadır. Yüzde hata, ilgili problemde çözüm yöntemleri tarafından elde edilmiş olan en iyi çözüm ile aradaki yüzde farkı ifade etmektedir. Senaryo-1 için problemin orjinal modeli olan P_1^1 matematiksel modeli

ile 6 problemin 4 tanesinde 1 saatlik sürede çözüm elde edilememiştir. 1 ve 4 numaralı problemlerde P_1^1 ile çözüm elde edilebilmiş fakat 4 nolu problemde elde edilen çözüm diğer çözüm yöntemleri ile elde edilen çözümdelerden daha kötü amaç fonksiyon değerine sahiptir. 1 numaralı problemde P_1^1 ile elde edile sonuç diğer çözüm yöntemleri ile elde edilen sonuçlardan daha kötü değildir. P_1^1 modeli ile daha iyi sonuçlar elde edilememesinin nedeni modelin zaman limiti altında çözdürülüyor olmasıdır. Eğer modeller ile optimal sonuçlar elde edilebilirse P_1^1 modeli ile kesinlikle daha kötü sonuçlar elde edilemeyecektir çünkü diğer çözüm yöntemleri ile elde edilen tüm sonuçlar P_1^1 modeli için olurlu çözümdür. P_1^3 ve P_1^2 modelleri sınırlandırılmış olan problemin farklı modelleridir. P_1^3 modeli doğrusal olmasına rağmen algılayıcılara atanabilecek anahtar sayısı küme olarak tanımlandığı için P_1^2 modelinden daha kötü performans göstermektedir. Tablo 5.2' ye göre sezgisel algoritmanın test problemleri üzerinde iyi sonuçlar verdiği söylenebilir. 6 test problemin 4' ünde sezgisel algoritma ile en iyi sonuçlar elde edilmiştir. Çözüm yöntemlerinin performansları hakkında daha sağlıklı analizler yapabilmek için çözüm sürelerinin de göz önünde bulundurulması gerekmektedir. Senaryo-1 için çözdürülen problemlerin çözüm süreleri Tablo 5.3'de sunulmaktadır.

Tablo 5.3: Senaryo-1 İçin Sınırlandırma Testi Problemleri Çözüm Süreleri.

Problem no	**m**	**|N|**	**Çözüm Süresi**			
			P_1^1	P_1^2	P_1^3	**Sezgisel**
1	20	10	3600	3600	3600	0.03
2		15	3600	1260	3600	0.2
3		20	3600	57	3600	0.05
4	50	10	3600	3600	3600	0.05
5		15	3600	3600	3600	0.28
6		20	3600	520	3600	0.39
Ortalama Süre	-	-	**3600**	**2166**	**3600**	**0.166**

Tablo 5.3' de görüldüğü üzere (P_1^1) modeli tüm test problemlerinde zaman limitine takılmıştır. (P_1^2) modeli ise 3 problemde zaman limitine takılmadan optimal çözüme ulaşabilmiştir. (P_1^3) modeli ile tüm test problemlerinde olurlu çözüm elde edilmiş olmasına rağmen tüm test problemlerinde zaman limitine ulaşılmıştır. Sezgisel çözüm yönteminin ise çözüm süresinin diğer çözüm yöntemlerine oranla

çok daha iyi olduğunu söylemek mümkündür.

Tablo 5.4: Senaryo-2 İçin Sınırlandırma Testi Sonuçları.

Problem no	**m**	**Amaç Fonksiyon Değeri (% hata)**			
		P_2^1	P_2^2	P_2^3	**Sezgisel**
7	20	2.6(11)	2.34(0)	2.96(26)	2.35(0.4)
8	50	5.475(0)	5.64(3)	6.568(20)	5.643(3)
Ortalama Hata		**5.5**	**1.5**	**23**	**1.7**

Tablo 5.4' te aynı testlerin senaryo-2 için uygulanması sonucunda elde edilen sonuçlar sunulmaktadır. Senaryo-2 için problemi sınırlandırmanın etkileri senaryo-1'de olduğundan daha net ortaya çıkmaktadır. 8 numaralı test problemi için üretilen 15 problemde ortalama değer olarak (P_2^1) modeli ile daha iyi sonuçlar elde edilmektedir. 8 numaralı problemin ortalama değerleri incelendiğinde problemin sınırlandırılmasının amaç fonksiyonunu kötüleştirdiği görülmektedir. Diğer taraftan 7 numralı problemde 8 numaralı problemin aksine (P_2^1) modeli ile ortalamada daha iyi sonuçlar elde edilememiştir. Çözüm sürelerinin verildiği Tablo 5.5'te 7 numaralı problemde 15 test problemi için ortalama sürenin verilmiş olan zaman limitinden daha az olduğu görülmektedir. Ortalamada çözüm süresinin zaman limtinin altında olmasına rağmen bazı problemlerde zaman limtine ulaşılması sonucu amaç fonksiyon değerlerinin ortalama değeri diğer çözüm yöntemleri ile elde edilen amaç fonksiyon değerlerininin ortalamalarından daha kötüdür.

Bu teste dayanarak problemin sınırlandırılmasının amaç fonksiyonunu kötüleştirebileceği fakat sınırlandırma sonu önerilen çözüm yöntemleri ile kısa sürelerde iyi sonuçlar elde edilebileceği söylenebilir. Gerçekleştirilen ilk test sonucunda hem senaryo-1 hem de senaryo-2 için elde edilen sonuçlara göre sınırlandırılmış olan problemin karma tamsayılı programlama modelleri olan (P_1^3) ve (P_2^3) modellerinin diğer çözüm yöntemlerinden her konuda kötü olduğu söylenebilir.

Gerçekleştirilen ikinci test çalışması Bölüm 4'te önerilen sezgisel çözüm yöntemlerinin performanslarının ölçülebilmesi için gerçekleştirilmiştir. Yukarıda bahsedildiği üzere sezgisel algoritma senaryo-1 ve senaryo-2 için önerilmektedir. Sezgisel algoritma algılayıcıların konumlarından bağımsız olarak sınırlandırılmış problemler için çözüm üretebilmektedir. Sezgisel algoritma ağ yaşam süresini enbüyükleyen veri akışlarını parametre olarak ele almakta ve bu değerlere göre

Tablo 5.5: Senaryo-2 İçin Sınırlandırma Testi Çözüm Süreleri.

Problem no	**m**	**Çözüm Süresi**			
		P_2^1	P_2^2	P_2^3	**Sezgisel**
7	20	1913	721	3433	0.1
8	50	2516	2239	3600	0.14
Ortalama Süre		**2214.5**	**1480**	**3516.5**	**0.12**

çözüm üretmektedir. Sonuç olarak sezgisel algoritma problemin ilk aşamasından bağımsız olarak hareket etmektedir. Sezgisel algoritma hiçbir değişikliğe ihtiyaç duymadan senaryo-1 ve senaryo-2 için kullanılabilir durumdadır. Bu nedenle sezgisel algoritmanın performansının ölçülmesi için üretilen test problemleri senaryo-2 için üretilmiştir. Test problemlerine ait parametre değerleri Tablo 5.6'da sunulmaktadır.

Tablo 5.6: Sezgisel Algoritma İçin Performans Testi Problemleri Parameterleri.

Tanım	**Parametre**	**Değer**
Ağda kullanılacak algılayıcı sayısı	v	10, 20, 30, 40
Düşmanın sahip olduğu anahtar sayısı	m	20, 150
Algılayıcıların hafıza limiti	$smax$	100

Sezgisel algoritmanın performansının değerlendirildiği bu testte ağda kullanılacak algılayıcı sayısı için 10, 20, 30 ve 40 olmak üzere 4 farklı değer ele alınmıştır. m parametresi için $smax$ parametresinden bir tanesi küçük ve diğeri büyük olmak üzere iki değer göz önünde bulundurulmuştur. Sezgisel algoritmanın performansı 8 problem üzerinde test edilmiştir. Algılayıcı konumlandırılması rassal olarak gerçekleştirildiği için her bir problemde 20 adet farklı problem üretilmiştir. Bu testte sezgisel algoritmanın sonuçları (P_2^2) modeli ile karşılaştırılmaktadır. Problemin karma tamsayılı programalama modeli olan (P_2^3) modeli bu testte göz önünde bulundurulmamıştır. (P_2^3) modelinin göz önünde bulundurulmamasının nedeni önceki test sonuçlarına göre (P_2^3) modelenin (P_2^2) modelinden performans olarak daha kötü olmasıdır. Test problemlerinin (P_2^2) ve sezgisel algoritma ile 1 saatlik zaman limiti altında çözdürülmesi sonucunda elde edilen sonuçlar Tablo 5.7'de sunulmaktadır.

Sezgisel algoritma hazırlanan 8 test probleminin 6 tanesinde daha iyi sonuç

Tablo 5.7: Sezgisel Algoritma İçin Performans Testi Sonuçları.

Problem no	**m**	**v**	**Amaç Fonksiyon Değeri (%Hata)**	
			P_2^2	**Sezgisel**
9	20	10	1.378(0)	1.379(0.07)
10		20	20.475(0.04)	20.466(0)
11		30	64.378(22)	52.508(0)
12		40	9.251(150)	3.692(0)
13	150	10	7.501(0)	7.734(3)
14		20	15.283(8)	14.062(0)
15		30	23.533(34)	17.478(0)
16		40	26.369(19)	21.976(0)
Ortalama Hata	**-**	**-**	**29.13**	**0.38**

vermektedir. 9 ve 13 numaralı problemlerde ortalamada daha kötü sonuç vermektedir fakat; (P_2^2) modeli ile elde edilen sonuçlardan en fazla yüzde 3 kötüdür. Ortalamada (P_2^2) modeli ile yüzde 29'luk bir hata oranı elde edilirken sezgisel algoritma ile yüzde 0.38'lik bir hata oranı ile sonuçlar elde edilmiştir. Tablo 5.7'de ortalama sonuçları verilmiş olan test problemlerinin, ortalama çözüm süreleri incelendiğinde sezgisel algoritmanın kısa sürelerde iyi sonuçlara ulaştığı görülmektedir. Gerçekleştirilen ilk test ve bu testin sonuçlarına bakarak sezgisel algoritma ile sınırlandırılmış problem için iyi sonuçlara ulaşıldığı söylenebilir.

Tablo 5.8: Sezgisel Algoritma İçin Performans Testi Çözüm Süreleri.

Problem no	m	v	**Çözüm Süresi**	
			P_2^2	**Sezgisel**
9	20	10	3600	0.074
10		20	3600	0.131
11		30	3600	1.191
12		40	3600	2.254
13	150	10	3600	0.253
14		20	3600	0.247
15		30	3600	0.373
16		40	3600	0.362
Ortalama Süre	**-**	**-**	**3600**	**0.61**

Senaryo-1 ve senaryo-2 için önerilen sezgisel algoritmanın performansının iyi olduğu önceki test çalışmalarında gözükmektedir. 3 senaryo için de ağ yaşam

süresi önerilen çözüm yöntemleri ile optimal olarak belirlenebilmektedir. Senaryo-1 ve senaryo-2 için düşmanın ele geçirebileceği veri miktarının enküçüklendiği aşamada problemin sınırlandırılarak sezgisel algoritmanın çözüm yöntemi olarak kullanılması önerilmektedir. Senaryo-3 için problemin sınırlandırılmada doğrusal olmayan programlama modeli ile çözülmesi çözüm yöntemi olarak sunulmaktadır. Önerilen çözüm yöntemlerinin kullanılması ile 3 senaryo için de ağ yaşam süresi ve veri kaybı miktarlarının incelendiği karşılaştırma testi gerçekleştirilmiştir. Bu testte belirli bir alana önceden belirlenmiş olan miktarda algılayıcı ile bir ağ tasarlanması hedeflenmektedir. Problemler 2 alan için hazılanmıştır. İlk alanın boyutları 250x500 olarak ele alınırken ikinci alanın boyutları 500x500 olarak ele alınmıştır. Tablo 5.9'da karşılaştırma testi için hazırlanan problemlerin parametre değerleri özetlenmektedir.

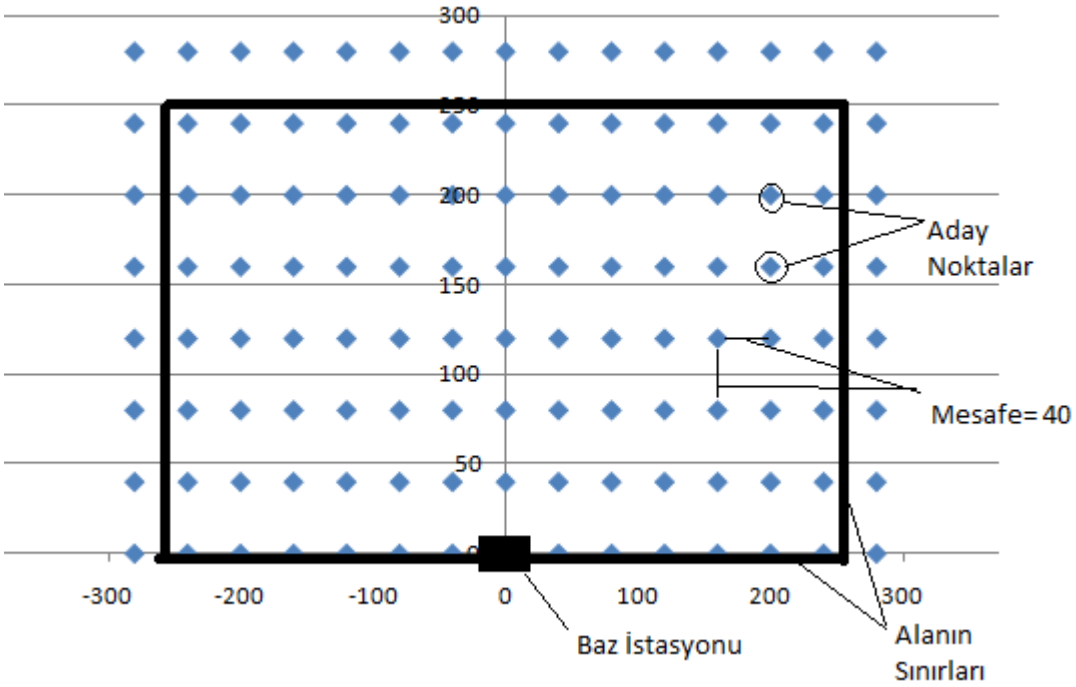
Tablo 5.9: Karşılaştırma Testi Parametreleri ve Değerleri.

Tanım	**Parametre**	**Değer**
Ağda kullanılacak algılayıcı sayısı	v	20, 40, 60
Düşmanın sahip olduğu anahtar sayısı	m	50, 100, 150, 200, 250
Algılayıcıların hafıza limiti	$smax$	100

Bu test problemlerinde baz istasyonun, alanın kenarı üzerinde tam ortada bulunduğu varsayılmaktadır. Senaryo-1 için hazırlanan problemlerde algılayıcıların konumlandırılabileceği aday noktalar 3 farklı şekilde belirlenmiştir. Aday noktalar daha önce ifade edildiği üzere, aynı eksen üzerinde birbirine komşu noktaların arasındaki uzaklık eşit olacak şekilde belirlenmektedir. Noktalar arasındaki mesafe için 40, 45 ve 50 olmak üzere 3 farklı değer göz önüne alınmıştır. Aday noktalar arası mesafenin 40 algılayıcıların yerleştirildiği alanın boyutlarının 500x250 olduğu durum için aday noktaların konumları Şekil 5.1'de gösterilmektedir.

Şekilde görüldüğü üzere aday noktalar alanı kapsayacak şekilde üretilmektedir. Alanda bulunan aday nokta sayısı, alanın boyutları ve aday noktalar arasındaki mesafe ile ilişkilidir. Tablo 5.10'da senaryo-1 için alanın boyutları ve aday noktalar arası mesafenin farklı değerlerinden elde edilen aday nokta sayıları verilmektedir.

Tablo 5.10, karşılaştırma testi için üretilen ve parametre değerleri Tablo 5.9'da



Şekil 5.1: Aday Noktaların Konumları.

sunulmuş olan karşılaştırma testi problemlerinin senaryo-1 için 3'er farklı durumda çözdürülmesi gerektiğini göstermektedir. Senaryo-1 için hazırlanan test problemleri 3 farklı durumda çözdürülürken rassal konumlandırmanın uygulandığı senaryo-2 ve senaryo-3 için ise algılayıcıların rassal konumlandırıldığı 30' ar farklı problem ele alınmıştır. Tablo 5.11'de karşılaştırma testi için hazırlanmış olan problemlerin tüm senaryolar altında ağ yaşam süresi ve veri kaybı miktarlarının senaryo-1 için Tablo 5.10'da sunulmuş olan durumlar ve senaryo-2 ile senaryo-3 için rassal üretilen 30'ar problemin ortalama değerleri sunulmaktadır.

Tablo 5.10: Karşılaştırma Testi Problemleri Senaryo-1 İçin Aday Noktalar Sayısı.

Durum	**Alan**	**Aday noktalar Arası Mesafe**	**Aday Nokta Sayısı**
1	500x250	40	120
2	500x250	45	91
3	500x250	50	66
4	500x500	40	210
5	500x500	45	169
6	500x500	50	121

Tablo 5.11: Karşılaştırma Testi Problemleri Ortalama Amaç Fonksiyon Değerleri.

Problem no	**Alan**	**v**	**m**	**Ortalama Değerler**					
				Senaryo-1		**Senaryo-2**		**Senaryo-3**	
				L_1	L_2	L_1	L_2	L_1	L_2
17	(500x250)	20	50	1	3.07	0.32	7.22	0.227	9.15
18			100		6.11		14.06		16.57
19			150		9.15		17.75		22.65
20			200		12.17		21.26		28.43
21			250		15.17		24.15		30.31
22		40	50	0.643	4.87	0.386	12.99	0.283	15.43
23			100		9.74		24.92		26.88
24			150		14.59		32.34		35.21
25			200		19.44		38.68		40.1
26			250		24.28		43.64		44.8
27		60	50	0.511	4.81	0.601	13.15	0.315	16.12
28			100		9.6		25.17		28.49
29			150		14.37		33.76		37.55
30			200		19.08		41.74		44.5
31			250		23.79		48.39		50.99
32	(500x500)	20	50	0.374	8.11	0.116	11.24	0.081	13.33
33			100		16.15		22.07		24.4
34			150		22.33		28.41		31.39
35			200		27.87		33.98		36.5
36			250		32.81		38.14		40.62
37		40	50	0.511	6.32	0.155	15.29	0.159	18.66
38			100		12.63		29.78		31.93
39			150		18.92		38.98		44.01
40			200		25.15		47.41		51.79
41			250		31.38		54.57		59.48
42		60	50	0.427	7.7	0.176	22.64	0.102	25.83
43			100		15.29		43.84		42.66
44			150		22.85		57.21		58.6
45			200		30.41		69.17		70.12
46			250		37.94		78.53		81.31

L_1: Ölçeklenmiş ağ yaşam süresi değeri
L_2: Toplam veri kaybı miktarı

Tablo 5.11'de ilk sütun problem numaralarını ifade etmektedir. İkinci sütun algılayıcıların yerleştirildiği alanın boyutlarını ve üçüncü sütünda alana konumlandırılan algılayıcı sayılarını belirtmektedir. Dörüncü sütun düşmanın sahip olduğu anahtar bilgisi sayısını ifade etmektedir. L_1 ile gösterilen sütunlar ele alınan problem için elde edilen ortalama ağ yaşam sürelerini göstermektedir. Problemde ağ yaşam süresi öncelikli olarak belirlendiğinden m parametresinin farklı değerleri için ağ yaşam süresi değişmeyecektir. Ağ yaşam süreleri, algılayıcı sayısı değişmedikçe hep aynı kalacaktır sonuç olarak L_1 ile gösterilen sütunlarda da algılayıcıların konumlandırıldıkları alan ve algılayıcı sayıları aynı olan problemlerin ağ yaşam süreleri birbirine eşit olarak elde edilmiştir. Daha önce bahsedildiği üzere ağ yaşam süreleri matematiksel modeller aracılığı ile direk olarak hesaplanmamaktadır. Matematiksel modeller ile ağın ömrünü enbüyükleyecek enerji sarfiyat değerleri belirlenmektedir. Bu işlem, algılayıcıların ellerindeki birim miktar veriyi en çok enerji sarfeden algılayıcının en az enerji sarfedeceği şekilde baz isatasyonuna ulaştırlması ile gerçekleştirilmektedir. L_1 ile gösterilen sütunlarda, elde edilen ağ yaşam süreleri 1'e ölçeklendirilmiş olarak sunulmaktadır. L_2 ile gösterilen sütunlarda düşmanın ele geçirebileceği en çok veri miktarı değerleri göstermektedir. Ağ yaşam süreleri tüm senaryolar göz önünde bulundurularak incelenirse ağ yaşam süresinin konumlandırılan algılayıcı sayısından bağımsız olduğu söylenebilir. Küçük alanda senaryo-1 için algılayıcı sayısı arttıkça ağ yaşam süresi azalmaktadır fakat; büyük alanda ağ yaşam süresi ile algılayıcı sayısı arasında böyle bir ilişki bulunmamaktadır. Senaryo-2 ve senaryo-3'de ise ağ yaşam sürelerinin genellikle algılayıcı sayılarındaki artışla arttığı söylenebilir fakat; senaryo-3'de büyük alana da algılayıcı sayısındaki artış her zaman için ağ yaşam süresinde azalış veya artışa neden olmamaktadır.

Tablo 5.11'e göre senaryo-1 diğer senaryolardan iki amaç açısından da daha iyi sonuçlar vermektedir. Aynı şekilde senaryo-2 de senaryo-3'e göre daha iyi sonuçlar vermektedir. Problemde modeller aracılığı ile verilen kararların artması ile amaç fonksiyonları açısından daha iyi sonuçlara ulaşıldığı görülmektedir. Senaryo-1 ve senaryo-2'de problemin ikinci aşamasında aynı sezgisel algoritma kullanılmasına rağmen kayıp veri miktarları arasında ciddi fark bulunmaktadır. Bu farkın ortaya çıkmasının nedeni senaryo-2'de algılayıcı konumlarının rassal olarak belirlenmesidir. Senaryo-1 ile her zaman için daha iyi sonuçlara ulaşılmasına

rağmen uygulama odaklı düşünüldüğünde senaryo-2 ve senaryo-3 kurulumları açısından senaryo-1'e göre çok daha kolay uygulanabilir senaryolardır.

Yapılan testler sonucunda senaryo-1 ve senaryo-2 için problemin sınırlandırılmasının amaç fonksiyon değeri açısından büyük farklılıklara neden olmadığı gözlemlenmiştir. Problemin sınırlandırılması sonucunda önerilen karma tamsayılı doğrusal programlama modellerinin karma tamsayılı doğrusal olmayan programlama modellerinden daha kötü performans gösterdiği gerçekleştirilen testler ile gösterilmiştir. Önerilen sezgisel algoritmanın hem çözüm süresi hem de amaç fonksiyon değeri açısından gayet iyi sonuçlar vermesi sonucunda anahtar ataması yöntemi olarak önerilebileceği gözükmektedir. Herbir senaryo için önerilen çözüm yöntemleri ile senaryoların karşılaşıtılması yapılmış ve problemlerde karar verilen sayısının artışının hem ağ yaşam süresi açısından hem de kayıp veri miktarı açısından olumlu sonuçlar verdiği gözlemlenmiştir.

6. SONUÇLAR VE DEĞERLENDİRME

Bu çalışmada KAA'da ağ yaşam süresi ve ağ güvenliği eniyilenmesi birlikte ele alınmıştır. Çalışmada güvenlik yöntemi olarak literatürde Djenouri vd. [9] tarafından KAA için en uygun güvenlik yöntemi olduğu belirtilen ikili anahtar değişim yönteminin kullanıldığı varsayılmıştır. Uygulama alanına göre farklı senaryolar ortaya çıkabileceği düşünülerek problem için farklı senaryolar altında uygulanabilir çözüm yöntemleri önerilmiştir.

Problemde ağ yaşam süresi eniyilemesi amacı ile günvenlik eniyilemesi amacı arasında öncelik ilişkisi bulunduğu varsayımı altında problem tanımlanmış olan senaryolar için iki aşamalı olarak ele alınmıştır. Ağ yaşam süresinin eniyilendiği aşama olan ilk aşama senaryo-1 için karma tamsayılı doğrusal programlama modeli olarak senaryo-2 ve senaryo-3 için ise doğrusal programlama modelleri olarak formüle edimiştir. Problemin ilk aşamasında ele edilen ağ yaşam süresini eniyileyen değer problemin ikinci aşamasında sağlanması gereken kısıt olarak ele alınmıştır. Problemin ikinci aşamasında karar verilmesi gereken çok fazla değişkenin olması ve bu değişkenlerin birbiri ile çok fazla bağımlı olması nedeniyle problemler karma tamsayılı doğrusal olmayan programlama modelleri olarak formüle edilmiştir.

Senaryo-1 ve senaryo-2 için problemin sınırlandırılması ile çözümü daha kolay olan modeller geliştirilmiştir. Önerilen sınırlandırma ile problemin ilk aşamasında ağ yaşamını enbüyükleyen veri akışları problemin ikinci aşamasında verilmiş olarak ele alınmıştır. Bu sınırlandırma ile problemlerin ikinci aşamasında veri

akış miktarlarına karar verilmesine gerek kalmamaktadır. Problemin sınırlandırılması amaç fonksiyonu hariç modelde bulunan doğrusal olmayan ifadelerin ortadan kalkmasına neden olmuştur. Problemin sınırlandırılması problemin farklı şekillerde ele alınarak modellenmesine de olanak sağlamaktadır. Sınırlandırma sonucu senaryo-1 ve senaryo-2 için karma tamsayılı matematiksel modeller geliştirilmiştir. Matematiksel modellere ek olarak büyük boyutlu problemlerde hızlı ve etkili sonuçlar alabilmek için matematiksel model tabanlı bir sezgisel algoritma geliştirilmiştir.

Algılayıcı konumlandırmanın ve anahtar atamasının rassal olarak gerçekleştirildiği senaryo-3 için problemin ikinci aşamasının sınırlandırılması önerilmemektedir. Algılayıcı konumları ve anahtar ataması kararları verilen olarak kabul edildiği için problemin sınırlandırılması ikinci aşamada problemin ortadan kalkması anlamına gelmektedir. Sonuç olarak senaryo-3 için problem sınırlandırılmamış ve geliştirilen matematiksel modeller ile analizler gerçekleştirilmiştir.

Problemin tanımlanan senaryolar için önerilen çözüm yöntemleri çeşitli amaçlar doğrultusunda test edilmiştir. Öncelikle senaryo-1 ve senaryo-2 için problemin sınırlandırılmasının avantaj ve dezavantajları belirlenmeye çalışılmıştır. Problemin sınırılandırılmasının etkileri senaryo-1 için 6 senaryo-2 için herbir durumda 15 rassal problem olmak üzere 2 ana problem üzerinde test edilmiştir. Matematiksel modeller çözdürülmesi kolay olmayan modeller olduğu için testler küçük boyutlu problemler ile zaman limiti altında gerçekleştirilmiştir. Senaryo-1 için elde edilen sonuçlar problemin sınırlandırılmasının çözüm üretme açısından çok avantajlı olduğunu göstermektedir. Senaryo-1 için gerçekleştirilen testler sonucunda problemin sınırlandırılması ile amaç fonksiyonun kötüleştiğini gösteren bir sonuca ulaşılamamıştır. Diğer taraftan senaryo-2 için gerçekleştirilen testler, problemin sınırlandırılmasının bazı durumlarda amaç fonksiyonunda kötüleşmeye neden olduğunu göstermiştir. Bazı durumlarda amaç fonksiyonunda kötüleşme olmasına rağmen zaman limitine ulaşılmadan optimal olarak çözülebilen durumların çoğunluğunda sınırlandırmanın amaç fonksiyonunu kötü etkilemediği görülmüştür. İki senaryo için de gerçekleştirilen testlerde önerilen sezgisel algoritmanın kısa sürelerde iyi sonuçlar verdiği gözlemlenmiştir. Gerçekleştirilen testler ile sınırlandırma sonucu geliştirilen karma tamsayılı matematiksel programlama modellerinin performanslarının diğer yöntemlere göre çok kötü olduğu görülmüştür. Sezgisel

algoritmanın amaç fonksiyonu açısından iyi çözümlere kısa sürelerde ulaşması nedeni ile sezgisel algoritma orta büyüklükteki problemler üzerinde test edilmiştir.

Problemin sınırılandırılması ile uygulanabilir olan sezgisel algoritmanın performansı senaryo-2 için hazırlanan test problemleri üzerinde test edilmiştir. Sezgisel algoritmanın performansı senaryo-2 için sınırılandırma sonucu önerilen doğrusal olmayan programlama modeli ile karşılaştırılmıştır. Hazırlanan test problemlerinin sonuçları, sezgisel algoritmanın oldukça iyi sonuçlar verdiğini göstemiştir. Sonuçlar sezgisel algoritmanın senaryo-1 ve senaryo-2 için makul çözüm yöntemleri olduğunu göstermektedir. 3 senaryoda da problemlerin ilk aşamaları optimal olarak çözülebilmektedir. Senaryo-3 için problemin matematiksel modellerinden başka çözüm yöntemi önerilmemiştir. Sonuç olarak büyük boyutlu problemlerde ilk 2 senaryo ve senaryo-3 için sırasıyla, sezgisel algoritma ve doğrusal olmayan programlama modelleri önerilmiştir. Önerilen çözüm yöntemleri hazırlanan test problemleri ile ağ yaşam süresi ve ağ güvenliği açısından karşılaştırılmıştır.

Ağ yaşam süresi ve düşmanın ele geçirebileceği veri miktarlarının senaryolara göre nasıl değiştiğini gözlemleyebilmek için gerçekleştirilen test, KAA tasarlanırken karar verilen sayısındaki artışın ağın hem yaşam süresini hem de güveliğini arttırdığını ortaya koymaktadır.

Bu çalışmada, güvenlik önlemlerinin pasif saldırılara karşı alındığı varsayılmıştır. Gelecek çalışmalarda, aktif saldırıların da olabileceği ve bu saldırılar ile düşmanın algılayıcıların hafızalarında bulunan anahtar bilgilerini ele geçirerek ağı dinleyebileceği veya ağa hatalı veri enjekte edebileceği varsayılarak problem genişletilebilir. Saldrılara ek olarak algılayıcıların çeşitli sebepler nedeniyle bozulabilieceği ve fonksiyonunu yitirebileceği göz önünde bulundurularak güvenli veri alış verişine ek olarak ağın güvenli olması da çalışmaya eklenebilir.

Kaynakça

[1] Alaybeyoğlu, A., Kantarcı, A. ve Erciyes,K., Telsiz Duyarga Ağlarında Hedef İzleme Senaryoları, *Akademik Bilişim 2009 konferansı*, Şanlıurfa, 2009.

[2] Alfieri, A., Bianco, A., Brandimarte, P. ve Chiasserini, C.F., Maximizing system lifetime in wireless sensor networks,*European Journal of Operational Research*, **181**(1), 390-402, 2007.

[3] Basagni, S., Carosi, A., Melachrinoudis, E., Controlled sink mobility for prolonging wireless sensor networks lifetime, *Wireless Networks* , **14**(6), 831-858, 2008.

[4] Bhardwaj, M., Chandrakasan, A.P., Bounding the lifetime of sensor networks via optimal role assignments, *Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, **3**, 1587-1596, 2002.

[5] Chang, J.H. ve Tassiulas, L., Routing for maximum system lifetime in wireless ad-hoc networks, 37th Annu. Allerton Conf. Communication, Control, and Computing, Monticello, IL, Eylül 1999.

[6] Chang, J.H. ve Tassiulas, L., Energy conserving routing in wireless adhoc networks, Proceedings of IEEE INFOCOM 2000, 22-31 Mart 2000.

[7] Chang, J.H. ve Tassiulas, L., Maximum lifetime routing in wireless sensor networks, *IEEE/ACM Transactions on Networking (TON)*, **12**(4): 609-619, 2004.

[8] Cheng, M.Z., Prillo, M., ve Heinzelman, W.B., General network lifetime and cost models for evaluating sensor network deployment strategies, *IEEE Transactions on Mobile Computing* , **7**(4), 484-497, 2008.

[9] Djenouri, D., Khelladi, Y. ve Badajche, N., A survey of security issues in mobile ad hoc and wireless Networks, *IEEE Communications Surveys and Tutorials*, **7**(4), 2-28, 2005.

[10] Du, W., Deng, J., Badajche, N., Han, Y.S., Varshney, P.K., Katz, J. ve Khalili, A., A pairwise Key Predistribution Scheme , *ACM Transaction on Information and System Security* , **8**(2), 228-258, 2005.

[11] Du, W., Deng, J., Badajche, N., Han, Y.S. ve Varshney, P.K., A key Predistribution Scheme for Sensor Networks Using Deployment Knowledge , *IEEE Transaction on Dependable and Secure Computing* , **3**(1), 62-77, 2006.

[12] Güney, E., Aras, N., Altınel, İ.K. ve Ersoy, C., Efficient solution techniques for the integrated coverage, sink location and routing problem in wireless sensor networks, *Computers and Operations Research*, **39**(7) 1530-1539, 2012.

[13] Hong, B. ve Prasanna, V.K., Constrained flow optimization with applications to data gathering in sensor networks,*Algorithmic Aspects of Wireless Sensor Networks*, Springer Berlin Heidelberg, Germany, 187-200, 2004.

[14] Kalpakis, K., Dasgupta, K. ve Namjoshi, P., Maximum lifetime data gathering and aggregation in wireless sensor networks, *Proceedings of IEEE Networks*, **2**, 685-696, 2002.

[15] Krishnamachari, B., Ordonez, F., Analysis of energy-efficient, fair routing in wireless sensor networks through non-linear optimization,*Vehicular Technology Conference*, **5**, 2844-2848, 2003.

[16] Sadagopan, N. ve Krishnamachari, B., Maximizing data extraction in energy energy limited sensor networks, *International Journal of Distributed Sensor Networks*, bf 1(1), 123-147, 2005.

[17] Türkoğulları, Y.B., Aras, N., Altınel, İ.K. ve Ersoy, C., Optimal placement and activity scheduling to maximize coverage lifetime in wireless sensor networks, *22nd International Symposium on Computer and Information Science*, 275-280, 2007.

[18] Türkoğulları, Y.B., Aras, N., Altınel, İ.K. ve Ersoy, C., A column generation based heuristic for sensor placement, activity scheduling and data routing in wireless sensor networks, *European Journal of Operational Research*, **207**(2) 1014-1026, 2010.

[19] Younis, M.F, Deng, J., Ghumman, K. ve Eltoweissy, M., Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks , *IEEE Transaction on Parallel and Distributed Systems* , **17**(8), 865-882, 2006.

[20] Younis, M. ve Akkaya, K., Strategies and techniques for node placement in wireless sensor networks: A survey, *Ad Hoc Networks* , **6**(4), 621-655, 2008.

[21] Yun, Y., Xia, Y., Maximizing the Lifetime of Wireless Sensor Networks with Mobile Sink in Delay-Tolerant Applications, *IEEE Transactions on Mobile Computing* , **9**(9), 1308-1318, 2010.

[22] Zhao, Q. ve Gurusamy, M.,Lifetime maximization for connected target coverage in wireless sensor networks, *IEEE/ACM TRANSACTIONS ON NETWORKING*, **16** (6), 1378-1391, 2008.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: YILDIZ, Uğur
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 01.04.1987 Antalya
Medeni hali	: Bekar
Telefon	: +905052686145
e-mail	: uyildiz@.etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Y. Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2014
Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2012

İş Deneyimi

Yıl	Yer	Görev
2012-2014	TOBB Ekonomi ve Teknoloji Üniversitesi	Burslu Yüksek Lisans Öğrencisi

Yabancı Dil

İngilizce (Çok iyi)

Yayınlar

Yıldız, U., Batur, İ., Gültekin, H., Alev, S.A., A bi-criteria machine location problem with pick-up and drop-of points. 20th European Working Group on Locational Analysis Meeting (EWGLA 2013), Ankara, Türkiye, 17-19 Nisan, 2013.

Yıldız, U., Gültekin, H., Tavlı, B., Maximizing lifetime with minimum required bandwidth in wireless sensor networks. 26th European Conference on Operational Research (EURO-INFORMS Joint International Meeting 2013), Roma, İtalya, 1-4 Temmuz, 2103.