TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SUALTI AKUSTİK ALGILAYICI AĞLARDA GİZLİ DİNLEME ENKÜÇÜKLEMESİ VE AĞ YAŞAM SÜRESİ ENBÜYÜKLEMESİ ÖDÜNLEŞMESİNİN KARIŞIK TAMSAYI PROGRAMLAMA YAKLAŞIMIYLA MODELLENMESİ VE İRDELENMESİ

YÜKSEK LİSANS TEZİ

Alper ÖZMEN

Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Bülent TAVLI

MART 2021

ÖZET

Yüksek Lisans Tezi

SUALTI AKUSTİK ALGILAYICI AĞLARDA GİZLİ DİNLEME ENKÜÇÜKLEMESİ VE AĞ YAŞAM SÜRESİ ENBÜYÜKLEMESİ ÖDÜNLEŞMESİNİN KARIŞIK TAMSAYI PROGRAMLAMA YAKLAŞIMIYLA MODELLENMESİ VE İRDELENMESİ

Alper ÖZMEN

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Bülent TAVLI

Tarih: Mart 2021

Karasal ortamdaki kablosuz algılayıcı ağlar hakkında birçok araştırma yapılmasına rağmen sualtı akustik algılayıcı ağlar (SAAA'lar) hakkında görece daha az araştırma yapılmıştır. Son yıllarda ise SAAA'lara olan ilgi çeşitli sebeplerden ötürü artmıştır. Sualtı ortamın karakteristik farklılıklarından ötürü, karasal ortamda yapılan araştırmalar SAAA'lara direkt uygulanamamaktadır. Elektromanyetik ve optik haberleşme suda verimli şekilde çalışmadığından ötürü SAAA'larda akustik haberleşme tercih edilmektedir. SAAA'lar genellikle zorlu sualtı ortamlara yerleştirilirler ve bu sebeple birçok güvenlik tehlikesiyle karşı karşıya kalırlar. Dahası, akustik haberleşmenin karakteristik özelliklerinden ötürü düşmanca saldırılara karşı savunmasızdırlar. En tehlikeli güvenlik tehditlerinden birisi de gizli dinleme saldırısıdır. Gizli dinleme saldırısı, saldırgan düğümün ağdaki algılayıcı düğümler arasındaki haberleşmeyi gizlice dinlemesi ile gerçekleşmektedir. İletim gücü seviyelerinin dikkatli şekilde atanması ve veri akış yollarının optimizasyonu gizli dinleme saldırılarının kapsamını hafifletmeye yardımcı olsa da, ağ yaşam süresini negatif olarak etkilemektedir. Bu çalışmada, SAAA'larda gizli dinleme potansiyeli

riskini minimize eden ve belli bir gizli dinleme riski altında ağ yaşam süresini maksimize eden iki optimizasyon modeli önerilmiştir. Sonuçlar göstermektedir ki, gizli dinleme riskinin minimize edildiği durumdaki ağ yaşam süresi, gizli dinleme kısıtının olmadığı durumdaki ağ yaşam süresinden oldukça kısadır. Benzer şekilde gizli dinleme riskine karşı önlemler gevşetildiğinde, SAAA'larda ağ yaşam süresi önemli derecede artmaktadır.

Anahtar Kelimeler: Sualtı akustik algılayıcı ağlar, Ağ yaşam süresi, Ağ güvenliği, Gizli dinleme saldırısı, Enerji verimliliği, Optimizasyon

ABSTRACT

MODELING THE TRADEOFF BETWEEN EAVESDROPPING AND NETWORK LIFETIME THROUGH A MIXED INTEGER PROGRAMMING APPROACH IN UNDERWATER ACOUSTIC SENSOR NETWORKS

Alper ÖZMEN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Electrical and Electronic Engineering

Supervisor: Prof. Dr. Bülent TAVLI

Date: March 2021

Although there are plenty of research on wireless sensor networks in the terrestrial environment, there are relatively little research on underwater acoustic sensor networks (UASNs). In recent years, UASNs attract considerable attention for a variety of reasons. Because of the characteristic differences of the underwater environment, the studies conducted in terrestrial environment cannot be directly applied to UASNs. In UASNs, acoustic communication is preferred rather than electromagnetic and optical communication which cannot work efficiently in underwater. UASNs are often placed in severe environments and therefore they face many safety hazards. Moreover, because of the harsh characteristics of the underwater environment, they are vulnerable to hostile attacks. One of the most dangerous security threats is the eavesdropping attack where an attacker node silently taps the information exchanged between the sensor nodes. While careful assignment of transmission power levels and optimization of data flow paths can help mitigate the scope of eavesdropping attacks, it can negatively impact network lifetime. In this study, two optimization models are proposed where the first model minimizes the eavesdropping risk in UASNs while the second model maximizes network lifetime under a precise level of an eavesdropping risk. The results show that the networks lifetime obtained when eavesdropping risk is minimized are considerably shorter than the network lifetime obtained in the absence

of eavesdropping constraint. Similarly, when the precautions against the eavesdropping risks are relaxed, network lifetime in UASNs increases significantly.

Keywords: Underwater acoustic sensor networks, Network lifetime, Network security, Eavesdropping attack, Energy efficiency, Optimization.

TEŞEKKÜR

Yüksek lisans çalışmamı tamamlamamda en büyük pay sahipleri olan değerli danışmanlarım Prof. Dr. Bülent TAVLI ve Doç. Dr. Hüseyin Uğur YILDIZ'a bu süreçte verdikleri katkı ve paylaştıkları tecrübeler için çok teşekkür ederim. Ayrıca kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bölümü öğretim üyelerine ve yüksek lisans eğitim hayatım boyunca yardım ve desteklerini esirgemeyen çok kıymetli Yağmur Peker, Duygu Özmen ve Burak Emre Ün'e çok teşekkür ederim. Bu zamanlara gelmemde çok emeği olan ve maddi manevi destekleriyle her zaman yanımda olan kıymetli aileme en içten teşekkürlerimi sunarım. Son olarak yüksek lisans eğitimimde araştırma bursu imkanı sağlayan TOBB Ekonomi ve Teknoloji Üniversitesi'ne ve yüksek lisans eğitimimi 2210-A programı ile destekleyen TÜBİTAK'a çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

TEZ BİLDİRİMİ ..... **iii**
ÖZET ..... **iv**
ABSTRACT ..... **vi**
TEŞEKKÜR ..... **viii**
İÇİNDEKİLER ..... **ix**
ŞEKİL LİSTESİ ..... **x**
ÇİZELGE LİSTESİ ..... **xi**
KISALTMALAR ..... **xii**
SEMBOL LİSTESİ ..... **xiii**
1. GİRİŞ **1**
1.1 Tezin Amacı ve Organizasyonu 3
1.2 Literatür Araştırması 4
2. SUALTI AKUSTİK ALGILAYICI AĞLAR **13**
2.1 Tanımı 13
2.2 Karakteristiği 14
2.3 Kullanım Alanları 15
3. MATEMATİKSEL PROGRAMLAMA VE OPTİMİZASYON **19**
3.1 Tarihi 19
3.2 Doğrusal Programlama 20
3.2.1 İkili tamsayı programlama 20
3.2.2 Tamsayı programlama 20
3.2.3 Karışık tamsayı programlama 21
3.3 Doğrusal Olmayan Programlama 22
3.4 MATLAB ve GAMS 22
4. SİSTEM MODELİ **25**
4.1 Problem Tanımı 25
4.2 Ağ Topolojisi 26
4.3 Sualtı Enerji Tüketim Modeli 27
4.4 Gizli Dinleme Eniyileme Modeli 29
4.5 Lineer Topolojide Gizli Dinleme Eniyileme Modeli 31
4.6 Ağ Yaşam Süresi Eniyileme Modeli 34
5. ANALİZ VE DEĞERLENDİRMELER **37**
6. SONUÇLAR **45**
KAYNAKLAR **47**
ÖZGEÇMİŞ **51**

ŞEKİL LİSTESİ

Sayfa

Şekil 1.1 : SAAA'larda konuşlanma kablolu, kablosuz, sabit, mobil olabilir veya sensörler farklı bağlantılarla kıyıya bağlanabilir ([6]'dan alınarak düzenlenmiştir)…… 3
Şekil 1.2 : Sybil saldırısı ([16]'dan alınarak düzenlenmiştir)……...7
Şekil 1.3 : Solucan deliği bağlantılı bir SAAA ([16]'dan alınarak düzenlenmiştir)….8
Şekil 2.1 : Temsili bir SAAA mimarisi ([30]'dan alınarak düzenlenmiştir)…….. 13
Şekil 2.2 : Sualtı akustik modem blok diyagramı ([31]'den alınarak düzenlenmiştir)……... 14
Şekil 2.3 : Boru hattı izlemesi için bir SAAA modeli ([34]'ten alınarak düzenlenmiştir)……... 17
Şekil 2.4 : SAAA uygulamalarının sınıflandırılması ([35]'ten alınarak düzenlenmiştir)……... 18
Şekil 3.1 : Basit bir TP modeli……21
Şekil 4.1 : SAAA'larda gizli dinleme saldırı modeli ([47]'den alınarak düzenlenmiştir)……... 25
Şekil 4.2 : Rastgele oluşturulmuş SAAA topolojisi……... 27
Şekil 4.3 : Lineer topolojiden oluşan SAAA……..32
Şekil 4.4 : Lineer topoloji paket veri akışları……..32
Şekil 4.5 : γ_{kj} değerleri…….. 33
Şekil 4.6 : $\widehat{\gamma_{kj}}$ değerleri…….. 34
Şekil 4.7 : ζ_k değerleri…… 34
Şekil 5.1 : Minimum toplam gizli dinleme sayısı……...38
Şekil 5.2 : ε_{min} gizli dinleme kısıtı altında maksimum ağ yaşam süresi……...….39
Şekil 5.3 : ε_{min} gizli dinleme kısıtı olmadan maksimum ağ yaşam süresi…… 40
Şekil 5.4 : Maksimum ağ yaşam süresine (L_{max}) ulaşabilmek için olması gereken gizli dinleme sayısı…… 41
Şekil 5.5 : Gizli dinleme sayısı minimize edildiğinde ağ yaşam süresindeki (L_{max}) yüzdesel azalış…… 42
Şekil 5.6 : Maksimum ağ yaşam süresine (L_{max}) ulaşabilmek için gizli dinleme sayısındaki (ε_{min}) yüzdesel artış……... 43

ÇİZELGE LİSTESİ

Sayfa

Çizelge 1.1 : SAAA'lar üzerine bilimsel dergilerde yayımlanan çalışmaları gösteren istatistiki çizelge [2] 1
Çizelge 1.2 : SAAA'larda saldırı tipleri ve karşı önlemler ([12]'den alınarak düzenlenmiştir). 6
Çizelge 4.1 : 10 farklı güç seviyesi ($\mathcal{L}$) için iletimde harcanan enerji ($E_T(l)$ - mJ) ve iletim menzili ($d_c(l)$ - m). 28
Çizelge 4.2 : Analizde kullanılan parametreler. 36

KISALTMALAR

AES : İleri Şifreleme Standartı (İng. Advanced Encryption Standard)
AUV : Otonom Su Aracı (İng. Autonomous Underwater Vehicle)
BIP : İkili Tamsayı Programlama (İng. Binary Integer Programming)
CDMA : Kod Bölmeli Çoklu Erişim (İng. Code Division Multiple Access)
CoMP : Koordine Edilmiş Çok Noktalı (İng. Coordinated Multipoint)
CTS : Gönderme İçin Temiz (İng. Clear To Send)
DC : Doğru Akım (İng. Direct Current)
DOP : Doğrusal Olmayan Programlama
DP : Doğrusal Programlama
ECDH : Elliptic-Curve Diffie Hellman
GAMS : Genel Cebirsel Modelleme Sistemi (İng. General Algebraic Modeling System)
GHz : Gigahertz
IP : Tamsayı Programlama (İng. Integer Programming)
İTP : İkili Tamsayı Programlama
KAA : Kablosuz Algılayıcı Ağ
KTDOP : Karışık Tamsayı Doğrusal Olmayan Programlama
KTDP : Karışık Tamsayı Doğrusal Programlama
KTP : Karışık Tamsayı Programlama
LP : Doğrusal Programlama (İng. Linear Programming)
MATLAB : Matris Laboratuvarı (İng. Matrix Laboratory)
MHz : Megahertz
MILP : Karışık Tamsayı Doğrusal Programlama (İng. Mixed Integer Linear Programming)
MINLP : Karışık Tamsayı Doğrusal Olmayan Programlama (İng. Mixed Integer Nonlinear Programming)
MIP : Karışık Tamsayı Programlama (İng. Mixed Integer Programming)
NLP : Doğrusal Olmayan Programlama (İng. Nonlinear Programming)
NUSL : Bahri Sualtı Akustik Laboratuvar (İng. Naval Underwater Sound Laboratory)
pH : Hidrojen Gücü (İng. Power Of Hydrogen)
RF : Radyo Frekansı (İng. Radio Frequency)
RSS : Alınan-İşaret-Gücü (İng. Received-Signal-Strength)
RTS : Gönderme İçin İstem (İng. Request To Send)
SAAA : Sualtı Akustik Algılayıcı Ağ
TDMA : Zaman Bölmeli Çoklu Erişim (İng. Time Division Multiple Access)
TP : Tamsayı Programlama
UASN : Sualtı Akustik Algılayıcı Ağ (İng. Underwater Acoustic Sensor Network)
USB : Evrensel Seri Veriyolu (İng. Universal Serial Bus)

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklama
$A(d_c(l))$	$d_c(l)$ mesafesi üzerinde gerçekleşen akustik zayıflama
$\alpha(f)$	Soğurma katsayısı
$d_c(l)$	l enerji seviyesindeki maksimum haberleşme menzili
d_e	SAAA'nın taban kenar uzunluğu
d_{max}	Efektif gizli dinleme yarıçapı
E_{bat}	Batarya enerjisi
f	Çalışma frekansı
h	SAAA'nın derinliği
L	Ağ yaşam süresi
$\mathcal{L}$	Güç seviye kümesi
L_{min}	Minimum gizli dinleme kısıtı altında ağ yaşam süresi
L_{max}	Gizli dinleme kısıtı olmadığında ağ yaşam süresi
l_p	Veri paketlerinin bit olarak büyüklüğü
P_0	Alıcı düğüm girişinde ihtiyaç duyulan güç
P_t	Belli bir mesafe üzerinden paket iletilmesi için gereken güç
V	Ağdaki tüm düğümlerin kümesi
W	Baz istasyonu hariç ağdaki tüm düğümlerin kümesi
x_{ij}^k	k düğümünde üretilip i düğümünden j düğümüne akan paket sayısı
$\mathcal{A}$	Baz istasyonunun veri üretemediğini ve hiçbir düğümün kendine veri iletemediğini gösteren sıralı küme
β_{ij}^l	Minimum güç seviyesi l kullanılarak i düğümünün j düğümüne veri aktarıp aktaramayacağını gösteren ikilik değer
γ_{kj}	k düğümünde üretilip j düğümüne iletilen paket sayısı
$\widehat{\gamma_{kj}}$	k düğümünde üretilen paketi j düğümünün duyup duymadığını gösteren ikilik değer
δ_{ij}^l	Güç seviyesi l kullanılarak i düğümünün j düğümüne veri aktarıp aktaramayacağını gösteren ikilik değer
ε_{max}	Maksimum ağ yaşam süresine ulaşabilmek için gereken gizli dinlme sayısı
ε_{min}	Toplam gizli dinleme sayısı
ζ_k	k düğümünde üretilen paketi duyan düğüm sayısı
κ	Dağılım faktörü
ξ	SAAA'ya konulan gizli dinleme limiti
ω_{il}^k	k düğümünde üretilip, l güç seviyesi kullanılarak i düğümü üzerinden ağa dağıtılan toplam paket sayısı
$\widehat{\omega_{il}^k}$	k düğümünde üretilip, l güç seviyesi kullanılarak i düğümü üzerinden paket dağıtılıp dağıtılmadığını gösteren ikilik değer

1. GİRİŞ

Kablosuz haberleşme teknolojisi ve mikro sensör konularındaki ilerlemeler ile az güç tüketen, küçük boyutlu ve uygun maliyetli cihazlar gündeme gelmiştir. Bu cihazların ortaya çıkışı ve yaygınlaşması kablosuz algılayıcı ağlara olan ilgiyi artırmıştır. Artan bu ilgi sayesinde ise konu hakkında birçok akademik araştırma yapılmış ve bu araştırmalar geniş yelpazeli ürünlerin ortaya çıkmasına fırsat tanımıştır [1]. Araştırmaların birçoğu karasal ortamdaki kablosuz algılayıcı ağlara (KAA'lar) odaklansa da okyanusların büyük ve bilinmez olması, suyun yüksek basıncından ötürü uzun süreler insanların suyun altında çalışamaz olması gibi zorlu sebeplerden ötürü son yıllarda Sualtı Akustik Algılayıcı Ağlar'a (SAAA'lara) olan ilgi her geçen gün artmaktadır. [2]'de verilen çizelgede (Çizelge 1.1) SAAA'lar üzerine bilimsel dergilerde yayımlanan çalışmaların son yıllarda giderek arttığı gözlemlenebilir.

Çizelge 1.1 : SAAA'lar üzerine bilimsel dergilerde yayımlanan çalışmaları gösteren istatistiki çizelge [2]

Journal/Proceedings	Publisher	2000-2007	2008-2009	2010-2011	2012-2013	2014-2015	Total
IEEE Supported Conferences	IEEExplore	165	93	98	99	98	553
Hindawi Journals	Hindawi	0	0	5	9	19	33
Proceedings of Intl. Conference	ACM Digital Library	3	4	2	14	8	41
Computer Communications	Elsevier	0	2	0	3	1	6
Ad hoc Networks	Elsevier	2	3	4	4	6	19
IEEE Journals	IEEE	45	14	27	28	40	154
Systems	John Wiley	0	0	0	0	4	4

SAAA'lar verilen spesifik görevleri gerçekleştirmek üzere belli bir okyanus altı alana konumlanmış çeşitli sensör ve araçlardan oluşmaktadır. Okyanus altında bulunan sensör düğümleri denizbilimsel verinin toplanması, kirlilik takibi, taktiksel gözlem yapmak amacıyla kullanılabilir. Dahası otonom sualtı araçları sayesinde doğal sualtı kaynaklarının veya batık enkazların bulunmasında kullanılabilir. SAAA'lar bu uygulamalar için kolaylaştırıcı ve gelecek vaat eden bir teknolojidir [3].

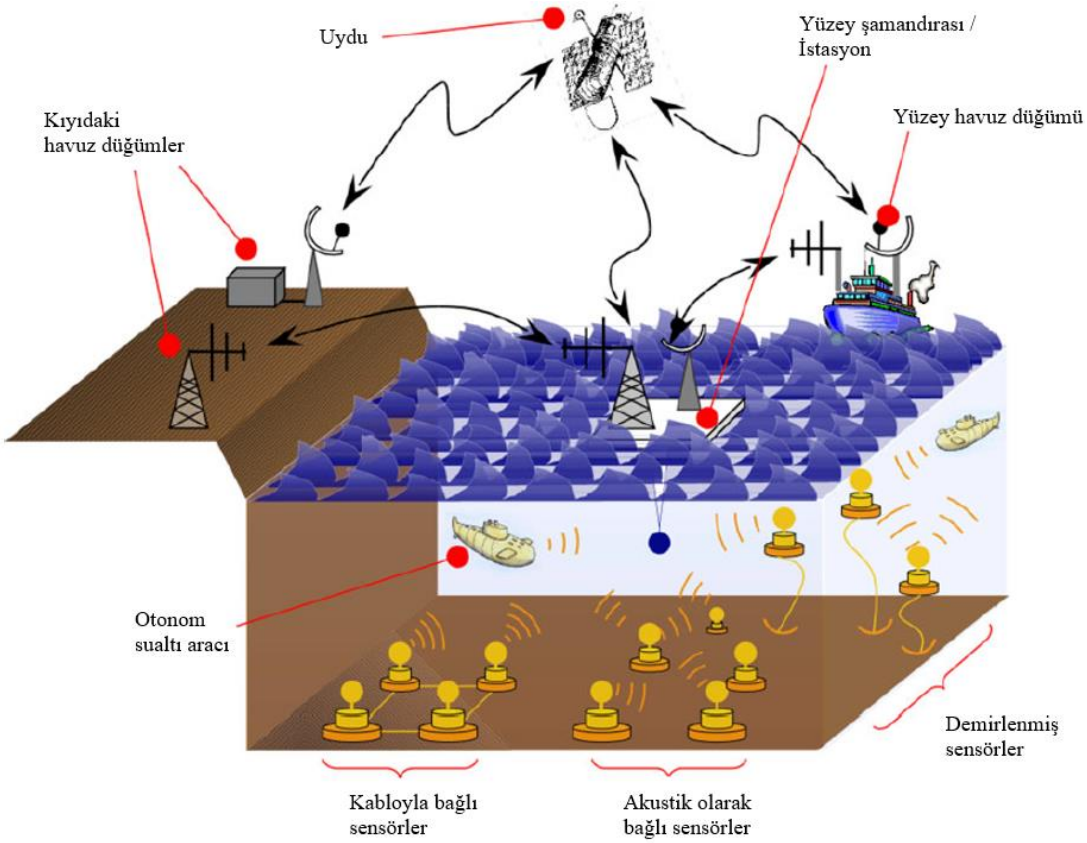
SAAA'larda tercih edilen yöntem akustik haberleşmedir. Bu yöntemde elektromanyetik dalgalar yerine akustik dalgalar kullanılmaktadır. Bu yüzden veri hızları daha düşüktür. Akustik haberleşme, elektromanyetik haberleşmeden farklı olsa

bile, temelde iki sistem de genlik, frekans veya faz modülasyonu kullanılarak kiplenen verinin bir taşıyıcı dalga (İng. carrier) ile iletilmesine dayanmaktadır [4].

Akustik haberleşmeyi etkileyen bazı zorluklar vardır. Bu zorlukların başında iletim kayıpları gelmektedir. İletim kayıpları, akustik zayıflama ve geometrik dağılımdan etkilenir. Akustik zayıflama, akustik enerjinin ısıya dönüşmesiyle gerçekleşir ve mesafe ve frekans ile doğru orantılı olarak artar. Geometrik dağılım ise ses enerjisinin yayılımını işaret etmektedir ve frekanstan bağımsız olarak yayılım mesafesiyle orantılı olarak artmaktadır. Diğer zorluk ise gürültü şeklinde ortaya çıkmaktadır. Gürültü, insan yapımı ve ortam gürültüsü olarak sınıflandırılabilir. İnsan gürültüsü daha çok makineler (gemiler, motorlar, pompalar vb.) kaynaklıyken, ortam gürültüsü ise çevresel sebeplerle gerçekleşen; suyun hareketleri, fırtına, rüzgâr ve yağmur kaynaklı gürültülerdir. Diğer zorluklar ise çok-yolluluk (İng. multi-path) ve yüksek yayılım gecikmesi olarak sayılabilir [5].

SAAA'ların sualtı ortamda konuşlanması farklı şekillerde gerçekleşebilir. Sualtında kablolu ağlar kullanılabilirken aynı zamanda kablosuz ağlar da kullanılabilmektedir. Şekil 1.1'de SAAA'ların birkaç konuşlanma şekli temsil edilmiştir. Sensörlerin demirli şamandıralara veya rıhtıma bağlanmasıyla sabit bir ağ yaratılabilirken, otonom su araçlarına (İng. autonomous underwater vehicles – AUVs) yüklenmiş sensörler ile mobil bir ağ da yaratılabilir. Mobilite, sınırlı donanım şartlarında (sensör adeti, batarya enerjisi vb.) maksimum sensör kapsama alanı sağlarken, yer saptama veya birbirine bağlı bir sensör ağı açısından zorluklar yaratabilmektedir. Sabit ağlarda ise ağ bağlantısı daha uzun süreler devam ettirilmektedir. Yine de bazı etkenlerle (rüzgâr, su akıntısı, şamandıra hareketleri vb.) sabit ağda küçük çaplı hareketler meydana gelebilmektedir [6].

İnsanlık ve endüstriyel sebeplerden ötürü artan petrol, doğalgaz gibi enerji kaynağı ihtiyacı ile yine aynı şekilde denizden çıkarılabilecek mineral ve maden ihtiyacı, yakın gelecekte denizlere ve SAAA'lara olan ilgiyi daha da artıracaktır. Dünya'nın yaklaşık yüzde 70'i su olduğundan ötürü bu alandaki araştırmalar belki de insan yaşamı için birçok şey vaat etmektedir [7].



Şekil 1.1 : SAAA'larda konuşlanma kablolu, kablosuz, sabit, mobil olabilir veya sensörler farklı bağlantılarla kıyıya bağlanabilir ([6]'dan alınarak düzenlenmiştir).

1.1 Tezin Amacı ve Organizasyonu

SAAA'larda bulunan sensör ve cihazlar zorlu bir ortama yerleştirildiklerinden ötürü, bataryalarını şarj etmek veya değiştirmek her zaman kolay değildir. Bu yüzden ağ yaşam süresi bu tip ağlarda çok daha fazla önem kazanmaktadır. SAAA'larda ağ yaşam süresini açıklayan farklı tanımlar bulunmaktadır. Bazı araştırmacılar ağ yaşam süresini; ağdaki ilk düğümün enerjisini bitirdiği zaman olarak alırken, diğerleri ağdaki tüm düğümlerin enerjisini tükettiği zaman olarak almaktadır. Bu sebepten ötürü ağ yaşam süresini artırmaya çalışan çalışmalardaki algoritmalar farklılığa uğrayabilmektedir. Birçok araştırmacı ağ yaşam süresini artırmak için tüm düğümlerin enerjisini aynı zamanda tüketmesi amacıyla ağdaki enerji tüketimini dengelemeye çalışırken, diğer grup ilk düğümün enerjisini bitirmesine izin vermektedir [8]. Enerji tüketiminin düşürülerek optimum iletim menzilinin bulunması ve ağ yaşam süresinin artırılması araştırmacılar tarafından çözülmesi gereken en önemli problemlerden biridir, zaten literatürde bu konu hakkında birçok araştırma yapılmıştır [9, 10, 11].

Sualtındaki algılayıcı düğümler, zorlu ortam ve barındırdığı karakteristiklerinden ötürü kötü niyetli saldırılara karşı savunmasızdır ve SAAA'lara karşı çok fazla güvenlik tehditi bulunmaktadır. Bu tez çalışmasında SAAA'lardaki bu iki önemli konu üzerine (ağ yaşam süresi ve güvenlik riski) bir çalışma gerçekleştirilmiştir. Çalışmada, sualtındaki algılayıcı düğümlere yapılan pasif saldırı tiplerinden gizli dinleme (İng. eavesdropping) riski azaltılarak, bu kısıt altında ağ yaşam süresini artıran çok amaçlı bir optimizasyon (İng multi-objective optimization) problemine çözüm bulunmaya çalışılmıştır. Düğüm sayısı ve ağ büyüklüğünün değişimi ile ağdaki toplam gizli dinleme sayısı incelenmiştir. Yine aynı parametreler ile gizli dinleme kısıtı altında ve kısıt kaldırıldığında ağ yaşam süresi incelenerek kıyaslamalar yapılmıştır.

Bu tez çalışmasının organizasyonu aşağıda anlatıldığı sıraya göre yapılmıştır.

1. bölümde, yapılan tez çalışması hakkında kısa bir bilgilendirmeye, tezin amacına ve literatür araştırmasına yer verilmiştir.

2. bölümde SAAA'ların kısa bir tanımı yapılmış, KAA'lar ile farklarından bahsedilerek karakteristiği incelenmiş ve son olarak da kullanım alanlarına değinilmiştir.

3. bölümde matematiksel programlama ve optimizasyon konusu anlatılıp, optimizasyonun tarihinden bahsedilmiştir.

4. bölümde bu tez çalışmasında kurulan sistem modeli denklemler ve örnekler ile detaylı şekilde açıklanmıştır.

5. bölümde, yapılan çalışmanın sonucu grafikler ile incelenerek, detaylı analiz ve değerlendirmeler yapılmıştır.

6. bölümde ise tez çalışmasnın sonuçları özetlenmiştir.

1.2 Literatür Araştırması

Güvenlik konusu ve kablosuz ağların maruz kaldıkları tehlikeleri en aza indirgemek, özellikle kritik görevlerde büyük önem kazanmaktadır. SAAA'larda güvenlik tehditleri ve bu ağların savunma mekanizmaları hakkında literatürde birçok çalışma bulunmaktadır. [12]'deki çalışmadan alınan çizelgede (Çizelge 1.2) her bir katman özelinde saldırı tipleri ve bu saldırıların karşı önlemleri gösterilmiştir.

Bunlardan bahsedilecek olursa; karıştırma (İng. jamming) saldırısı fiziksel katmandaki saldırı tiplerindendir. Bu atak tipinde saldırgan sürekli olarak gürültü ve anlamsız sinyaller basarak, ağdaki düğümlerin enerjisini boşa sarfettirerek paket gönderip-almasını engellemeye çalışır. Karıştırma saldırısına karşı önlem olarak ağda uyuma-uyanma modeli (İng. sleep-wakeup scheme) uygulanabilir. Bu modelde düğümler enerji tüketimini azaltmak için uyku moduna geçerler, sadece paket gönderip-alacakları zaman uyanırlar. Fiziksel katmandaki saldırı tiplerinden bir diğeri ise kurcalama (İng. tampering) saldırısıdır. Bu saldırı tipinde saldırgan düğümleri fiziksel olarak ele geçirip sorgulayabilir veya içindeki veriyi değiştirebilir. Buna önlem olarak ise ağda şifreleme algoritmaları kullanılabilir [13].

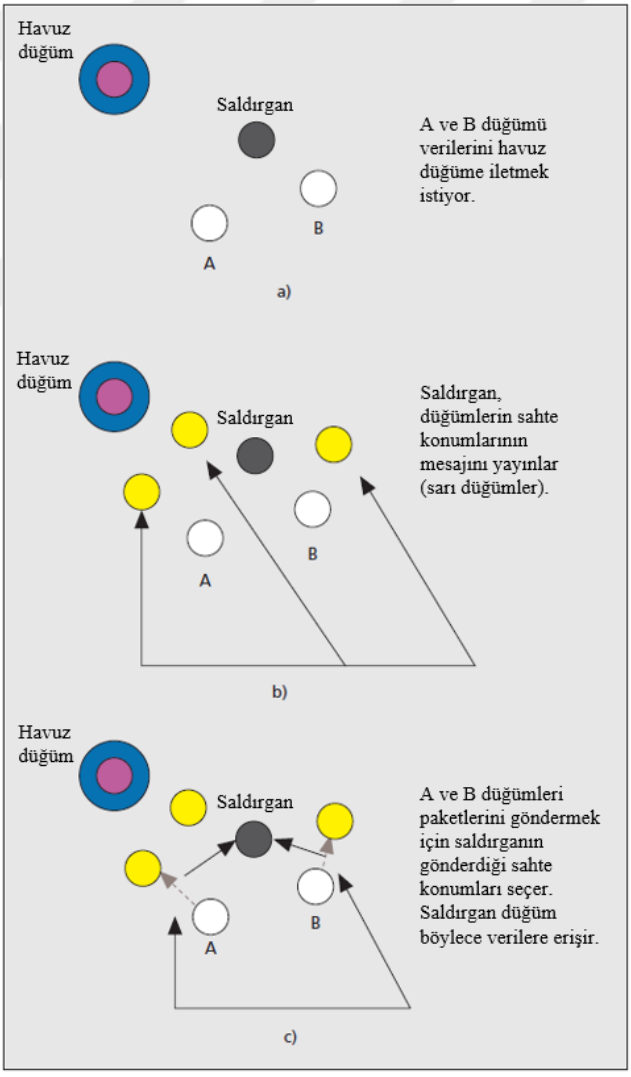
Veri bağı katmanındaki saldırı tipleri; çarpışma (İng. collision), tüketme (İng. exhaustion) ve adaletsizlik (İng. unfairness) saldırısı olarak gruplanabilir. İlk olarak çarpışma saldırısından bahsedilecek olursa; Gönderme İçin İstem/Gönderme İçin Temiz (İng. Request to Send – RTS / Clear to Send – CTS) el sıkışma mekanizması kablosuz ağlarda paket çarpışmalarını önlemek için kullanılan bir yöntemdir [14]. Bu mekanizmaya göre veri iletimi başlamadan önce haberleşme kanalı belli bir süre rezerve edilir ve haberleşme kanalında RTS veya CTS paketi görüldüğünde o süre içerisinde paket iletilmemesi gerekmektedir. Fakat saldırgan bu kuralı ihlal ederek paket gönderir, bu da alıcıda çarpışmaya sebep olur. Bu saldırı hata düzeltme kodu (İng. error correction code) ile önlenebilir [15]. Bir diğer saldırı tipi ise tüketme saldırısıdır. Tüketme saldırılarının amacı düğümlerin enerjisini tüketerek ağ yaşam süresini azaltmaktır. Temelde, saldırgan sürekli yeniden iletim isteği göndererek hedef düğümleri yormaya çalışır. Önlem olarak ağa yeniden iletim limiti koyulabilir, böylece bu limit aşıldığında düğümler saldırı olduğunu anlayacak ve paketleri tekrar iletmeyecektir [13]. Veri bağı katmanına yapılan son saldırı tipi ise adaletsizlik saldırısıdır. Bu tipte ise saldırgan algılayıcı düğümlerin kanala erişmesini tamamen değil de kısmen engelleyerek ağ performansını düşürmeyi hedefler. Önlem olarak paketlerin küçük parçalar halinde iletilmesi sağlanılarak, ağdaki düğümlerin kanala kısa bir süre erişmesi istenir. Böylece tüm düğümlerin kanala erişme fırsatı bulmasıyla adaletsizlik ortadan kalkmaktadır [15].

Çizelge 1.2 : SAAA'larda saldırı tipleri ve karşı önlemler ([12]'den alınarak düzenlenmiştir).

Katman	**Saldırı tipi**	**Karşı önlem**
Fiziksel katman	Karıştırma [13]	Uyuma-uyandırma modeli, çok frekanslı iletişim, farklı iletim önceliği kullanmak vb.
	Kurcalama [13]	Fiziksel hasar için algılama mekanizması, şifreleme algoritması vb.
Veri bağı katmanı	Çarpışma [15]	Hata düzeltme kodu
	Tüketme [13]	İletim hızını ve yeniden iletimi limitlemek
	Adaletsizlik [15]	Uzun paket kullanımından kaçınmak, paketlerin iletim önceliğini yeniden dağıtmak vb.
Ağ katmanı	Seçmeli yönlendirme [15]	Çok-yollu yönlendirme, itibar ve güven modeli vb.
	Sybil [16]	Düğümlerin kimlik doğrulaması
	Solucan deliği [17]	Ağ topolojisinin kurulması
	Havuz deliği [15]	Trafik izleme, kimlik doğrulama, çok-yollu yönlendirme vb.
İletim katmanı	Aşırı paket yollama [13]	Algılayıcı düğümlerin yayın aralığını sınırlandırmak

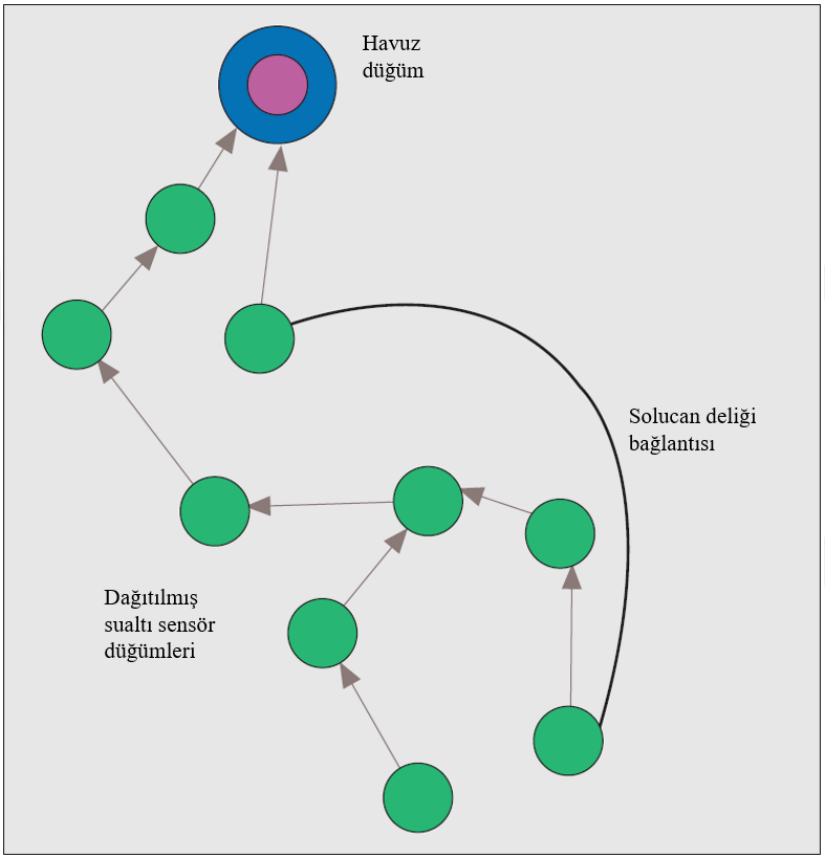
Ağ katmanı veri paketlerinin kaynak düğümden (İng. source node) havuz düğüme (İng. sink node) iletilmesinden sorumludur. Bu katmana seçmeli yönlendirme (İng. selective forwarding), sybil, solucan deliği (İng. wormhole) ve havuz deliği (İng. sinkhole) saldırıları yapılabilir. Seçmeli yönlendirme saldırısında, saldırgan ağdaki düğümlerden biri gibi davranarak iletim kanalında görev alır. Fakat röle düğüm olarak görevini tam olarak gerçekleştirmeyip, paketi hedef düğüme iletmek yerine imha eder. Ağdaki düğümlerin bunu algılayıp paketi yönlendirmek için başka yollar bulabileceğinden ötürü saldırgan bu riskten kaçınmak amacıyla paketleri seçerek imha ederken, bazılarını ise iletir. Önlem olarak çok yollu yönlendirme tekniğiyle, algılayıcı düğümler alternatifli olarak birden çok yol kullanır [15]. Bir diğer saldırı tipi olan sybil saldırısında, saldırgan birden fazla sahte kimlikle aynı anda farklı yerlerde gibi

davranarak ağ haberleşmesine erişebilir. Bu saldırı tipini özetleyen bir şema Şekil 1.2'de gösterilmiştir. Bu saldırı, algılayıcı düğümlerin kimlik doğrulamalarının yapılmasıyla önlenebilir [16]. Solucan deliği saldırısında ise, saldırgan ağdaki paketi bir noktadan alır, tünelden geçirerek ağdaki bir başka noktadan tekrar ağa sokar. Yönlendirme algoritması bu tünel yolunu tercih eder çünkü bu yol daha kısa görünmektedir, saldırgan bunun için daha iyi metriklere sahip kablosuz kanal veya kablolu kanal kullanabilir. Solucan deliği saldırısını görselleştiren bir şema Şekil 1.3'te gösterilmiştir. Bu saldırıdan kaçınmanın yollarından birisi olarak ağ topolojisi tabanlı bir yaklaşım kullanılabilir [17]. Son olarak havuz deliği saldırısında ise saldırgan daha hızlı ve kaliteli bir rota sunarak havuz düğümü üzerindeki tüm trafiği üzerine çeker. Bu saldırıya karşı yine düğümlerin kimlik doğrulaması yöntemi kullanılabilir [15].



Şekil 1.2 : Sybil saldırısı ([16]'dan alınarak düzenlenmiştir).

İletim katmanında ise ağa aşırı paket yollama (İng. flooding) saldırısı yapılabilir. Bu tip bir saldırıda; saldırgan, düğümlere çok fazla bağlantı isteği göndererek düğümlerin enerjisini tüketmeyi hedefler. Kod bölmeli çoklu erişim (İng. code division multiple access – CDMA) ve zaman bölmeli çoklu erişim (İng. time division multiple access – TDMA) gibi protokoller bu sorunu çözebilir [13]. Diğer bir yöntem olarak da düğümlerin yayın menzilleri kısılarak bu atağın önüne geçilebilir.



Şekil 1.3 : Solucan deliği bağlantılı bir SAAA ([16]'dan alınarak düzenlenmiştir).

Atak türüne göre saldırı aktif veya pasif olarak sınıflandırılabilir. Aktif atakta, saldırgan ağda iletilen paketi değiştirmeye, silmeye veya ağa paket enjekte etmeye çalışır [15]. Pasif atakta ise saldırgan, saldırıyı gerçekleştirirken herhangi bir sinyal göndermez. Gizli dinleme saldırısı bir pasif ataktır ve iki kanal arasında devam eden bir haberleşme kötü niyetli kişiler tarafından gizlice dinlenebilir. Saldırgan, haberleşen kanalların haberleşme menzili içerisindeyse kablosuz haberleşmenin de doğası gereği bu atağı kolayca gerçekleştirebilir [18, 19]. Saldırgan kendini açığa çıkarmadan ağı dinlediğinden ötürü gizli dinlemeyi saptamak çok zordur.

[20]'de yapılan çalışmada, gizli dinleme riskini azaltarak ağ güvenliğini artırmanın bir yolu olarak iletim yapan algılayıcı düğümlerin iletim güçlerinin azaltılması önerilmektedir, böylece azaltılan iletim gücü, daha kısa iletim menzili anlamına gelerek bu menzile girebilecek potansiyel saldırgan sayısını düşürmüş olmaktadır. Bu yöntem ayrıca kriptografi tabanlı çalışmalara göre daha az masraflı bir çözüm sağlamaktadır. Tabi iletim güçlerinin azaltılması ile paketin iletimi direkt havuz düğüme olmayacak ve araya birçok röle düğüm girebilecek, bu da batarya sürelerinin düşmesine sebep olacaktır.

Başka bir çalışmada ise ağda gizli dinleme saldırısı varken, gizli bir mesaj iki kaynak arasında güvenli şekilde iletilmek istenmektedir. Bu çalışmada, CDMA tabanlı analog ağ kodlayıcı (İng. analog network coding) aracılığıyla dost karıştırma yöntemine dayanan güvenli bir sualtı haberleşme şeması önerilmektedir. Önerilen şemada dost karıştırıcı (İng. jammer) kaynak, haberleşmesi istenen iki kaynak arasındaki şifreyi kullanarak yayın basar. Basılan yayını, saldırgan duysa bile deşifre edemezken, haberleşmek istenilen kaynak çözebilmektedir [21].

[22]'de sualtı ağlarda kulak misafirliğini azaltmak için Alınan-İşaret-Gücü (İng. Received-Signal-Strength – RSS) tabanlı şifre üretimi yaklaşımı önerilmektedir. Simetrik anahtar şifrelemesi (İng. symmetric key cryptography) yönteminde gönderici ve alıcı arasında şifre paylaşılması gerektiğinden ötürü ekstra anahtar dağıtım merkezine ihtiyaç duyulmaktadır. Açık anahtar şifrelemesinin (İng. public key cryptography) ise batarya kısıtı olan ağlarda kullanımının zorluk yaratmasından ötürü, önerilen yöntemin daha avantajlı olduğu savunulmaktadır.

Qiu Wang ve arkadaşları [23]'teki çalışmada SAAA'larda gizli dinleme olasılığını hesaplayan analitik bir model önermiştir. Çalışmada önerilen modelde izotropik hidrofon ve dizi hidrofon kullanan SAAA'lar kıyaslanılarak dizi hidrofon kullanılan ağda gizli dinleme riskinin düştüğü gösterilmiştir. Ayrıca önerilen analitik modele göre, gizli dinleme olasılığı algılayıcı düğüm yoğunluğunun artmasıyla artıp; rüzgâr hızı, sinyal frekansı ve yayılım faktörünün artmasıyla ise azalmaktadır. Bu sonuçlar detaylı grafiklerle çalışmada gösterilmiştir.

[24]'te koordine edilmiş çok noktalı (İng. coordinated multipoint – CoMP) iletişim kullanan dağıtık anten sisteminden (İng. distributed antenna elements) oluşmuş SAAA'larda gerçekleşebilecek gizli dinleme saldırısına karşı bir savunma

mekanizması geliştirilmektedir. Ses hızının suda yavaş olmasından ve sistem bileşenlerinin konumsal diversitelerinden (İng. spatial diversity) faydalanılarak bir sinyal hizalama (İng. signal alignment) stratejisi geliştirilmiştir. Sinyaller saldırgan düğüm üzerinde çarpışıp üst üste binerken; haberleşilmesi istenen düğümlerde çarpışma olmadan, haberleşme uygun şartlarda sağlanmaya devam etmektedir.

[25]'te yapılan çalışmada SAAA'larda kümelenmiş yıldız topolojisi yerine hibrit ağ topolojisi önerilmektedir. Kümelenmiş yıldız topolojisinde, tüm ağ trafiği küme içerisindeki havuz düğüm üzerinden döner ve ağda yoğun trafik olduğunda bu düğüm cevap veremez hale geldiğinden küme içerisindeki düğümler bağlantılarını kaybederler. Böyle bir durumda, önerilen hibrit mimari ile paketler müsait durumdaki mümkün olan en yakın havuz düğümüne yönlendirilir. Bu hibrit mimari kullanılan SAAA'larda, paket iletim oranı ve enerji verimliliğini artıran Janus tabanlı yönlendirme protokolü (İng. routing protocol) tanıtılmaktadır. Daha sonra bu çalışmada, tanıtılan protokolün güvenlik açıklığı sorgulanmakta ve gizli dinleme riskini minimize edecek Elliptic-Curve Diffie Hellman (ECDH) anahtar değişim modeli önerilmektedir. ECDH modeli, kaynak ve havuz düğümlerin paketlerini eş anahtarlar ile ileri şifreleme standartı (İng. advanced encryption standard – AES) kullanılarak şifrelemesine dayanmaktadır.

Gizli dinleme saldırısında, saldırganın trafiği analiz ederek veya paketleri takip ederek düğümlerin konum bilgisine ulaşması mümkündür. [26]'da yapılan çalışmada SAAA'larda havuz düğümünün lokasyon bilgisini saldırgandan saklayan bir ağ güvenliği şeması çizilmiştir. Çizilen bu şemada önerilen metot rastgele yönlendirme ve yönlü yönlendirme fazlarından oluşur. Rastgele yönlendirme fazında, saldırganın yolu karıştırması amaçlanarak ağa rastgele sahte paketler sürülürken, yönlü yönlendirme fazında ise sanal daire yaratılarak saldırganların havuz düğümünün yönünü kaybetmesi amaçlanır.

[27]'de SAAA'larda gizli dinleme saldırılarının; bir silahı, savunma mekanizmasına dönüştürülerek önlenmesi önerilmektedir. İki düğüm arasındaki haberleşmeyi saldırganın duymaması için yardımcı bir düğümden faydalanılır. Yapılan bu çalışmada yardımcı düğüm, saldırganın sinyal alımını engellemek için karıştırıcı sinyal basar. Belirlenen tasarıma göre; ağdaki diğer düğümler tarafından veri paketi ve karıştırıcı sinyal aynı güce sahip olduğundan ötürü ayırt edilemezken, haberleşilmek istenen

düğümde farklı güçlere sahiptir ve genlik modülasyonu tabanlı metotla ayrıştırılmaktadır.

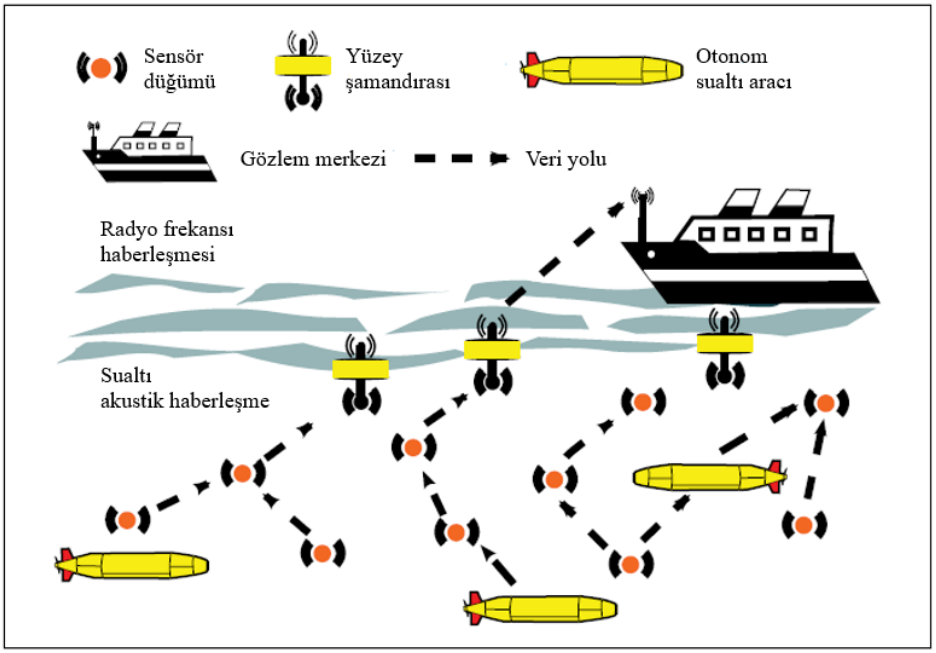
[28]'deki çalışmada SAAA'ların güvenlik açıklarını araştırmak için, aktif saldırı yöntemlerinden karıştırma ile pasif yöntemlerden gizli dinlemenin kombin edilmesiyle oluşturulan bir hibrit atak modeli önerilmektedir.

Bu tez çalışmasında ise [29]'da yapılan KAA'ların gizli dinleme ve ağ yaşam süresi arasındaki ilişkiyi irdeleyen çalışma genişletilerek, bu ödünleşme SAAA'lar için araştırılmıştır.

2. SUALTI AKUSTİK ALGILAYICI AĞLAR

2.1 Tanımı

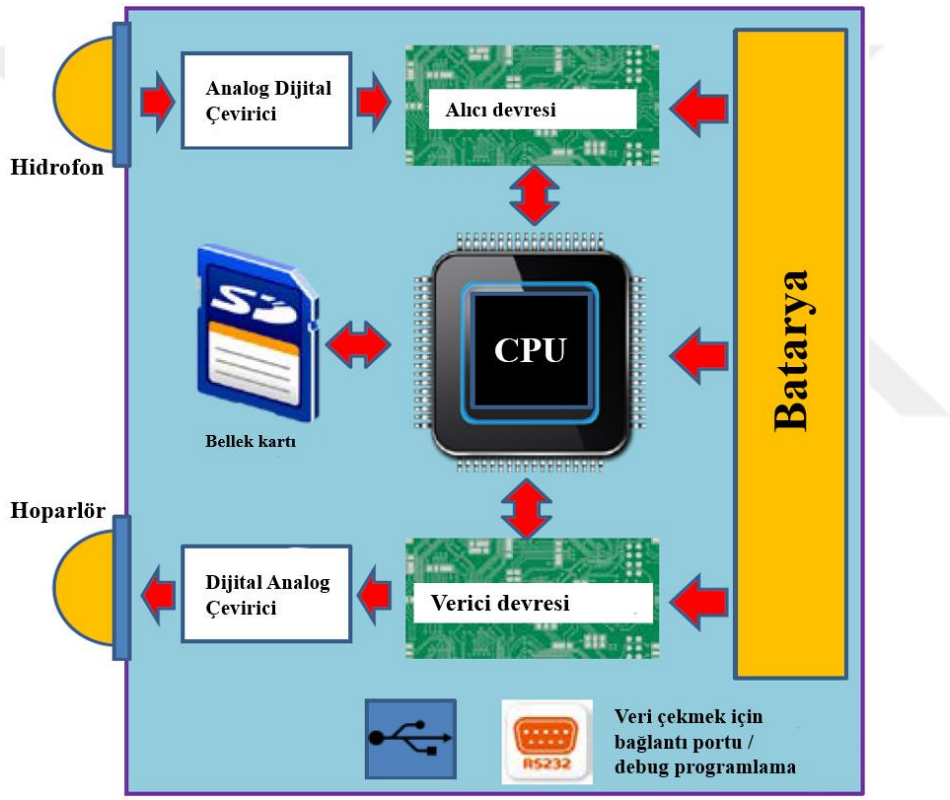
SAAA'lar, sualtındaki spesifik bir ortama, belli bir görevi yapmak amacıyla yerleştirilmiş algılayıcı düğümlerinden oluşmaktadır. SAAA'larda bulunan algılayıcı düğümler konuşlandığı ortamdan topladığı sıcaklık, basınç, ses gibi verileri daha ileri işlenmek üzere havuz düğümlere iletir [15]. Bu iletim, kaynak düğümden havuz düğüme direkt olabileceği gibi röle düğümler aracılığıyla da yapılabilir. Şekil 2.1'de temsili bir SAAA mimarisi verilmiştir. Verilen topolojide, her bir algılayıcı düğüm çevresindeki bölgeyi izlemekten sorumludur ve toplanan veriler yüzeyde bulunan bir şamandıraya çok atlamalı sualtı akustik haberleşme kanalıyla iletilmektedir. Yüzey şamandırası tarafından akustik haberleşme yoluyla düğümlerden toplanan veri radyo haberleşmesiyle gözlem merkezine aktarılmaktadır [30].



Şekil 2.1 : Temsili bir SAAA mimarisi ([30]'dan alınarak düzenlenmiştir).

Sualtı akustik kanalı oldukça değişkendir ve sinyal iletimi; suyun sıcaklığı, basıncı veya tuzluluğu gibi çevresel faktörlere göre değişebilir. Bu nedenle bu cihazların nasıl geliştirildiğini ve ulaşabilecekleri maksimum mesafe ve veri aktarım hızlarını bilmek önemlidir. Bu yüzden cihazların donanımsal yapısı önem kazanmaktadır. Bir sualtı

akustik modemde batarya ve DC/DC çeviriciden oluşan güç ünitesi, işlemci, hidrofon ve hoparlör, ortamdan alınan akustik sinyalleri işlemciye vermek üzere analog dijital çevirici ve son olarak işlemciden çıkan sinyalleri sualtı ortama basmak için dijital analog çevirici devresi bulunur. Şekil 2.2'de bir sualtı akustik modemin blok diyagramı verilmiştir. Kablosuz olmasından ötürü, sualtı cihazları büyük oranda batarya bağımlıdır. Akustik modemlerde veri kablosuz bağlantı kullanılarak iletilir, fakat ticari modemlerin birçoğu içerideki veriyi almak için RS232 veya USB portu da bulundurmaktadır. Günümüzdeki akustik modemler çok fazla güç tüketir ve uzun süreli kullanım için çok uygun değildir. Bu yüzden enerji verimli yönlendirme algoritmaları önem kazanmaktadır [31].



Şekil 2.2 : Sualtı akustik modem blok diyagramı ([31]'den alınarak düzenlenmiştir).

2.2 Karakteristiği

Sualtı haberleşmesi ile ilgili bilinen ilk çalışmalar 2. Dünya Savaşı yıllarına dayanmaktadır. 1945 yılında, o zamanki adıyla Naval Underwater Sound Laboratory (NUSL) tarafından denizaltındaki mürettebat ile haberleşmek için sualtı telefonları geliştirilip kullanılmıştır [32]. O günden bugüne, SAAA'lar özelinde birçok çalışma yapılmasına rağmen bu konu, sualtı haberleşmesinin zorluklarından ötürü karasal

ortamdaki KAA'lar kadar çok araştırılmamıştır. KAA'lar ile SAAA'lar arasındaki karakteristik farklılıklarından ötürü de KAA'larda yapılan çalışmalar, SAAA'lar için direkt olarak uygulanabilir olamamaktadır.

KAA'lar ile SAAA'lar arasında karakteristik olarak büyük farklar bulunmaktadır. Bunlardan bahsedilecek olursa [12, 33]:

- KAA'lar için 2 boyutlu ağ topolojisi üzerinden mimari oluşturulurken, SAAA'larda derinlik de işin içine girdiğinden dolayı genelde 3 boyutlu mimari oluşturulmaktadır.
- KAA'larda oluşturulan topoloji büyük oranda sabit kalırken, SAAA'ların topolojisi suyun hareketinden dolayı hayli dinamik olabilmektedir.
- KAA'lardaki algılayıcı düğümlere kıyasla çok daha maliyetli olması sebebiyle SAAA'lardaki algılayıcı düğümlerin dağılımı çok daha geniş alana yayılır.
- KAA'larda haberleşme amacıyla kullanılan yüksek frekanslı (radyo frekans – RF) dalgalar su içerisinde hızlı bir şekilde zayıflamaya (İng. attenuation) uğrarlar. Optik sinyaller ise su içerisinde zayıflamadan ziyade saçılmaya (İng. scattering) uğradığından, SAAA'larda akustik haberleşme tercih edilir.
- Karada MHz ve GHz mertebesinde yüksek frekanslı sinyaller kullanılmaktadır. Yüksek frekanslı sinyallerin ise suda hızlıca absorbe edilmesinden ötürü SAAA'larda daha düşük frekans kullanılmaktadır.
- Radyo dalgalarının havadaki hızı, ışığın hızına yakın ve 3 x 10^8 m/s iken, sesin sudaki hızının 1500 m/s olmasından ötürü SAAA'lardaki yayılım gecikmesi (İng. propagation delay) çok daha fazladır.
- Son olarak SAAA'larda düşük bant genişliği ve yüksek paket hata oranı olmasından ötürü bağlantı kalitesi daha düşüktür.

2.3 Kullanım Alanları

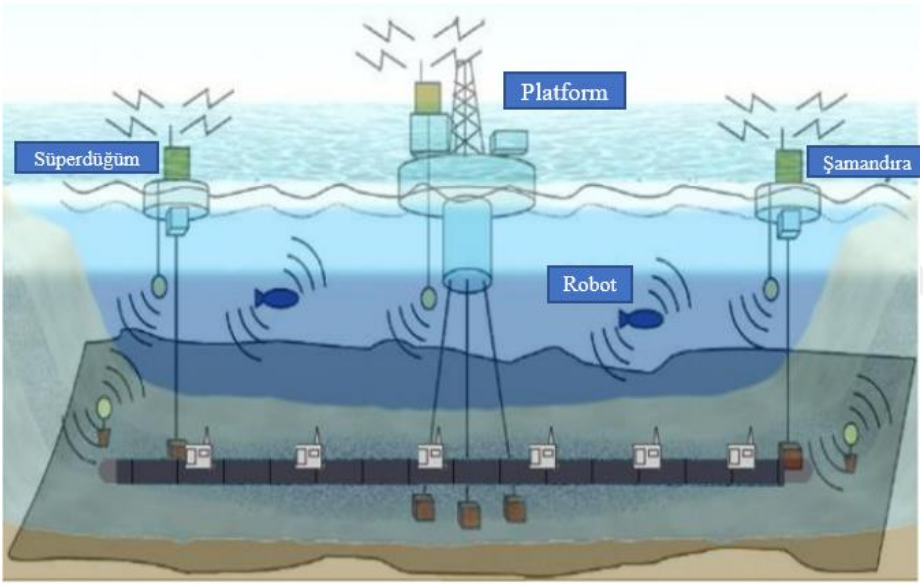
SAAA'ların kullanım alanı gittikçe yaygınlaşmaktadır. Yeni kullanım alanları, konunun akademik olarak daha çok ilgi çekmesine sebep olmuştur. SAAA'ların kullanım alanlarından örnekler aşağıda verilmiştir:

- **Sualtı Ortam İzleme Uygulamaları:** Sualtına yerleştirilmiş algılayıcı düğümler aracılığıyla sualtında ortam gözlemesi yapılabilir. Dünyamızın yaklaşık yüzde 70'inin su olmasından ötürü, su insan yaşamında çok önemli bir yer edinmektedir. Bu yüzden sualtı gözlemlerin insanlık için önemli sonuçlar verebilmesi mümkündür. Balık üretimi ve yetiştiriciliği önemli ekonomik alanlardandır. Sualtı gözlemlerde suyun kalitesinin; pH ve barındırdığı kimyasallar açısından incelenmesiyle ortamın balıkların yaşamına uygun olup olmadığı bilimsel olarak verilerle takip edilip, üretimde verim artırılabilir. Yine sualtı habitatı incelenerek, deniz biyolojisi alanındaki çalışmalar için veri toplanabilir. Doğadaki insan varlığından ötürü su kirliliği her geçen gün daha da artmaktadır. Sualtı ortam izlemesiyle su kirliliği incelenip, gereken önlemlerin alınması mümkündür [34].
- **Sualtı Keşif Uygulamaları:** Belli bölgelere yerleştirilmiş sualtı algılayıcı düğümler ile deniz içerisindeki doğal kaynaklar araştırılabilir, deniz altına döşenecek kablolar için rota belirlenebilir ve petrol, doğalgaz boru hatları gözlemlenebilmektedir [35].

  Sismik izleme yöntemiyle okyanus altı sahalardan petrol çıkarımı SAAA'lar için gelecek vaat eden bir uygulamadır. Kara ortamındaki petrol sahaları yıllık, 3 aylık hatta aylık periyotlarla gözlemlenebilirken, sualtı petrol sahalarını izlemek çok daha zorludur. Genelde bu sahaların izlenmesinde özel ekipmanlarla donatılmış gemiler ve özel eğitimli personel kullanılmaktadır. Böyle bir çalışmayı yürütmenin operasyonel maliyetleri çok yüksektir. Günümüzde enerjinin artan ihtiyacından ötürü bu çalışma birçok ülke tarafından denizlerde yürütülmektedir. Buna kıyasla SAAA'lar çok daha düşük maliyete sahiptir ve sualtı sahalarda daha uzun süreler gözlem yapabilmektedir. Böyle bir sistem petrol rezervuarlarının daha sık gözlemlenmesine ve petrol üretiminin artmasına yardımcı olur [4].
- **Askeri Uygulamalar:** Askeri açıdan kritik bölgelere konumlandırılan sualtı algılayıcı düğümler ile denizaltı gibi araçlar tespit edilebilir, askeri gözetleme yapılabilir veya saldırı tespit sistemleri kurulabilir [33].
- **Yardımcı Yön Bulma Uygulamaları:** Algılayıcı düğümler denizde seyahat eden bir gemi için su altındaki tehlikeleri keşfedebilir; sığ sulardaki

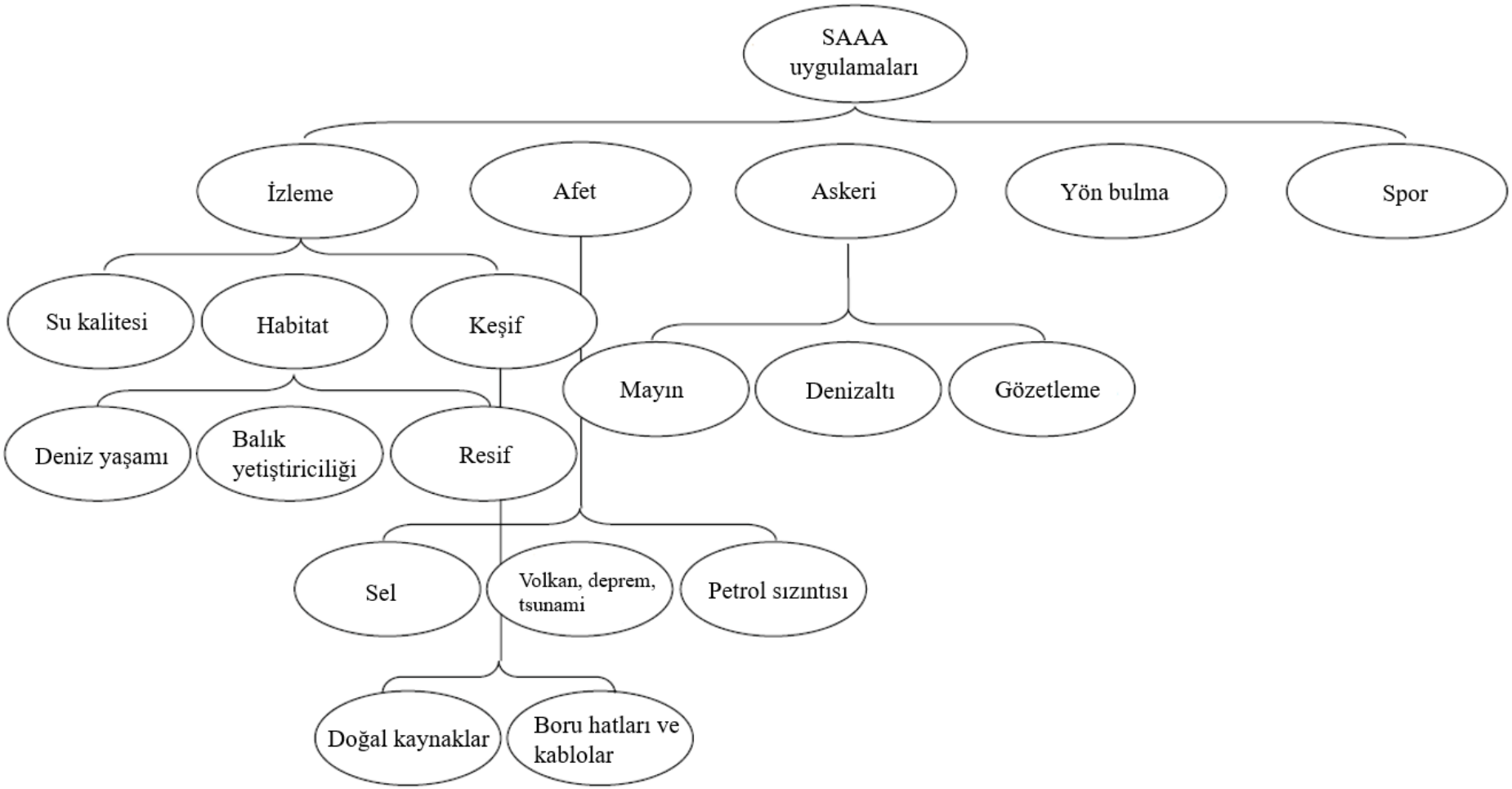
kayaları, balık sürüsünü tespit edebilir veya demirleme yeri bulabilir. Dahası, tespiti zor olan batık enkazları aramak için yardımcı olabilir [33].

- **Afet Önleme Uygulamaları:** Doğal afetler genelde kaçınılmazdır. Özellikle deniz kaynaklı afetler çok tehlikeli ve yıkıcı bir etkiye sahiptir. Suların yükselmesi sonucu oluşan sel felaketinin zararları, önceden uyarı sistemleri sayesinde azaltılabilir. Yine, yer kabuğundaki değişikliklerden ötürü sualtında oluşan depremler ve bunun sonucunda meydana gelen tsunami büyük yıkıcılığa sahiptir ve böyle bir felaket ansızın gerçekleşebilir. [36]'da, sualtına yerleştirilmiş sismik basınç sensörleri kullanılarak, sensörlerin üzerindeki basınç bilgisinin üst sensör düğümüne iletilmesi sistemine dayanan, tsunamiyi erken tahmin etme amaçlı bir çalışma gerçekleştirilmiştir.



Şekil 2.3 : Boru hattı izlemesi için bir SAAA modeli ([34]'ten alınarak düzenlenmiştir).

SAAA'ların uygulama alanlarını gösteren kapsamlı bir şema Şekil 2.4'te gösterilmiştir.



Şekil 2.4 : SAAA uygulamalarının sınıflandırılması ([35]'ten alınarak düzenlenmiştir).

3. MATEMATİKSEL PROGRAMLAMA VE OPTİMİZASYON

Optimizasyon bir problem karşısında, alternatif çözümler arasından en iyi çözümü bulmak olarak tanımlanabilmektedir. Bu problemler belli kısıtlar içerebilir ve çözüm bu kısıtlar içerisinde bulunmaya çalışılır. Optimizasyon problemi, en basitinden birçok kişinin günlük hayatında karşılaştığı, belli kısıtlar içerisinde kalarak en optimal kararı vermeye çalıştığı problemlerdir. Üretim, ekonomi, mühendislik, askeri ve daha birçok alanda optimizasyon çözümlerinden faydalanılmaktadır. Örnek verilecek olursa, birçok şubesi bulunan bir işletmenin belli bir lokasyonda yeni bir şube açması kararı optimizasyon modelleri ile değerlendirilerek karar verilmektedir. Bu karar verilirken yeni şube açma giderleri ve yeni lokasyondaki potansiyel müşteriler gibi veriler değerlendirilerek sonuca ulaşılır. Savaş durumundaki bir ordunun lojistik desteğini hangi rota üzerinden askerlerine ulaştıracağı konusu da bir optimizasyon problemidir. Yine, üniversitelerde ders programının hazırlanması da; her akademisyenin aynı anda tek bir derste olabileceği, üniversitedeki sınıf sayısı, verilmesi gereken ders sayısı, derslerin birbiriyle çakışmama durumları gibi birçok kısıttan oluşan ve her yeni okul döneminde çözülmesi gereken bir optimizasyon problemidir. Kısıt sayısı ve değişken sayısı arttıkça bu problemleri el ile çözmek zorlaşır. Bu yüzden sistematik algoritmalara ihtiyaç duyulur. Modern dünyada, karmaşık optimizasyon problemleri matematiksel terimler ile ifade edilerek matematiksel modellere dönüştürülür. Bu modeller, optimizasyon problemlerini çözmek için geliştirilen algoritmaları barındıran çözücüler (İng. solver) aracılığıyla bilgisayarlar tarafından hızlıca çözümlenir.

3.1 Tarihi

Optimizasyonun tarihi çok eski değildir. Başlangıç olarak genelde 1947 tarihi, 2. Dünya Savaşı'nın hemen sonrası düşünülmektedir. 1947 yılından önce de bu konu hakkında bazı çalışmalar gerçekleştirilmiştir. Leonid Kantorovich tarafından 1939 yılında "The Mathematical Method of Production Planning and Organization" isimli önemli bir çalışma gerçekleştirilmiş fakat ideolojik sebeplerden dolayı bu çalışma göz ardı edilmiştir [37]. Yine, 1941 yılında Frank L. Hitchcock tarafından sunulan "The

Distribution of a Product from Several Sources to Numerous Localities" isimli çalışma ulaşım probleminin (İng. transportation problem) çözümünde önemli bir katkı sunmuş fakat bu çalışma da 1950'lere kadar pek ilgi çekmemiştir [38]. Birçok teknolojinin ortaya çıkışı gibi yine askeri sebepler, optimizasyon alanının da gelişmesinde ve ilgi çekmesinde etkili olmuştur. 2. Dünya Savaşı zamanında Amerikan ordusunda program planlayıcısı rolünde görev alan George B. Dantzig'den; savaş sonrasında, planlama süreçlerini mekanize edip hızlandıracak bir çalışma yapılması istenmiştir. Bu çalışma sonrasında George B. Dantzig 1947 yılında ünlü "simpleks algoritmasını" sunmuştur [39].

3.2 Doğrusal Programlama

Doğrusal Programlama (DP) (İng. linear programming – LP) modeli, doğrusal bir amaç fonksiyonunun doğrusal eşitlik veya eşitliksizlerden oluşan kısıtlar altında maksimum ya da minimum olacak şekilde optimize edildiği modeldir. Doğrusal programlamada, tüm karar değişkenleri gerçel sayıdır yani değişkenler 4.3 ve 9.854 gibi ondalıklı değerler alabilir.

3.2.1 İkili tamsayı programlama

İkili tamsayı programlama (İTP) (İng. binary integer programming – BIP) modelinde tüm karar değişkenleri ikili olmalıdır yani değişkenler sadece 0 ya da 1 değerini alabilir. Bu, bir durum karşısında evet/hayır kararı veya anahtarlardan oluşan bir devrede hangi anahtarların açık/kapalı olduğunun seçimi gibi bir problemi temsil edebilir [40].

3.2.2 Tamsayı programlama

Tamsayı programlama (TP) (İng. integer programming – IP) modelinde tüm karar değişkenleri tamsayıdır. Bir fabrikada, hangi gün kaç işçinin çalışacağının optimize edilmesi TP modeli ile çözülebilir. Çünkü insan sayısı 7.4 gibi ondalıklı sayılar olamaz. Şekil 3.1'de basit bir TP modeli verilmiştir. Verilen problem önce matematiksel modele çevrilmektedir daha sonra bu matematiksel model üzerinden bilgisayarlar aracılığıyla hızlıca çözüm bulunabilmektedir.

Optimizasyon Problemi:
Bir fabrikada m_1, m_2 ve m_3 modelinde 3 çeşit tişört üretilmektedir. 1 adet m_1 model tişörtün üretilmesi için 85 m^2, 1 adet m_2 model için 43 m^2 ve 1 adet m_3 model için ise 32 m^2 kumaş harcanmaktadır. Fabrikada günlük harcanması gereken kumaş miktarı ise 5000 m^2 'dir. Tezgahta ise m_1, m_2 ve m_3 model tişörtler için üretim bandındaki günlük sınır sırasıyla 35, 52 ve 60 adettir. m_1 modelinden 24 lira, m_2 modelinden 13 lira ve m_3 modelinden 8 lira kar edilmektedir. Bu durumda fabrika, maksimum kar için nasıl bir üretim modeli çıkarmalıdır.

Amaç Fonksiyonu:

$$\text{Enbüyükle } 24m_1 + 13m_2 + 8m_3 \tag{3.1}$$

Kısıtlar:

$$85m_1 + 43m_2 + 32m_3 \leq 5000 \tag{3.2}$$

$$m_1 \leq 35, \quad m_2 \leq 52, \quad m_3 \leq 60 \tag{3.3}$$

$$m_1 \geq 0, \quad m_2 \geq 0, \quad m_3 \geq 0 \tag{3.4}$$

Şekil 3.1 : Basit bir TP modeli

3.2.3 Karışık tamsayı programlama

Karışık tamsayı proglamlama (KTP) (İng. mixed integer programming – MIP) modelinde karar değişkenlerinden bazıları gerçel sayılar olabilirken, bazıları ise tam sayı olur. Tüm kısıtlar ve amaç fonksiyonu doğrusal ise o zaman model karışık tamsayı doğrusal programlama (KTDP) (İng. mixed integer linear programming – MILP) olur. Aksine, kısıtlar veya amaç fonksiyonun doğrusal olmadığı durumda ise model karışık tamsayı doğrusal olmayan programlama (KTDOP) (İng. mixed integer nonlinear programming – MINLP) olmaktadır. KTDOP modelinin çözümü daha zor ve zaman alıcıdır [40]. Fakat genelde KTP denildiğinde, KTDP akla gelmektedir. Bu tez çalışmasında da KTP modeli, DP alt modeli olarak düşünülmüştür.

3.3 Doğrusal Olmayan Programlama

Doğrusal olmayan programlama (DOP) (İng. nonlinear programming – NLP) modelinde amaç fonksiyonu veya kısıtlardan biri/birkaçı doğrusal değildir. İçinde yaşadığımız Dünya çoğunlukla doğrusal değildir bu yüzden DOP modeli fazlasıyla gerçek dünyada yer edinir. Örnek verilecek olursa; bir şirket tarafından yürütülen projelerde çalışan sayısını iki katına çıkarmak proje bitim süresini yarıya düşürmez. Doğrusal olmayan modeller çok daha fazla gerçekçilik ve incelik sağlasa da, birçok sebepten ötürü hiçbir zaman doğrusal modeller kadar popüler olamamıştır. Bu sebeplerden bazıları bilgisayar teknolojisinin her geçen gün ilerlemesiyle yavaş yavaş ortadan kaybolurken, bazıları ise doğrusal olmayan fonksiyonların karmaşık karakteristiği gereği sorun olmaya devam etmektedir [41].

3.4 MATLAB ve GAMS

MATLAB (İng. matrix laboratory), Mathworks firması tarafından sunulan, sinyal işleme, kontrol sistemleri, derin öğrenme, makine öğrenmesi ve daha birçok alanda kullanılan bir programlama ve sayısal hesaplama ortamıdır [42]. GAMS (İng. General Algebraic Modeling System) ise derleyici ve 3. parti şirketler tarafından sağlanan çözücülerden oluşan yüksek seviye bir modelleme sistemidir ve matematiksel optimizasyon problemlerinin çözümü için kullanılır. GAMS'in bünyesinde barındırdığı çözücülere IBM firması tarafından sağlanan CPLEX çözücüsü [43] ve FICO firması tarafından sağlanan XPRESS çözücüsü [44] örnek verilebilir. Bu tez çalışmasında CPLEX çözücüsünden faydalanılmıştır. GAMS ile gerçek dünyadaki optimizasyon sorunları hızlıca bilgisayar koduna dönüştürülür ve daha sonra derleyici, bu kodu çözücülerin anlayacağı bir formata çevirir. Bu mimari sayesinde modeldeki formülasyonu değiştirmeden sadece bir satır kodda yapılacak değişiklik ile kullanılacak çözücü değiştirilebilir. Bu durum kullanıcıya büyük esneklik sağlamaktadır [45].

İki program arasındaki arayüz sayesinde GAMS, MATLAB kullanıcılarına uygulamanın tüm optimizasyon olanaklarını kullanma imkanı sağlarken, aynı zamanda GAMS modellerinin doğrudan MATLAB içerisinde görselleştirilmesine imkan tanımaktadır. MATLAB'ın görselleştirme araçları sayesinde modellerin geniş

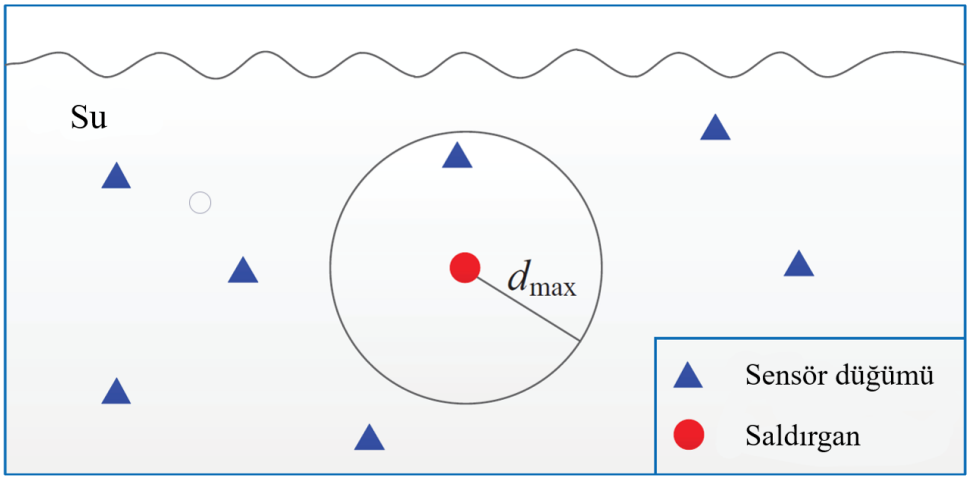
çeşitlilikteki çizim ve görselleri sonuçların kolay bir şekilde yorumlanması ve analiz edilmesine fırsat tanımaktadır [46].

4. SİSTEM MODELİ

Tez çalışmasının bu bölümünde; problem tanımı (bkz. Bölüm 4.1), ağ topolojisinin tanımı (bkz. Bölüm 4.2), sualtı enerji tüketim modeli (bkz. Bölüm 4.3), gizli dinleme eniyileme modeli (bkz. Bölüm 4.4) ve son olarak da gizli dinleme eniyileme modelinin lineer topoloji için çözümü (bkz. Bölüm 4.5) ile ağ yaşam süresi eniyileme modeli (bkz. Bölüm 4.6) açıklanmıştır.

4.1 Problem Tanımı

SAAA'lar yerleştirildikleri konum ve kullanıldıkları amaç itibariyle kritik görevlerde yer alabilmektedir. Bu yüzden ağ güvenliği bu tarz sistemlerde önem kazanmaktadır. Ağ güvenliğine zarar verebilecek ataklardan birisi de gizli dinleme saldırısıdır. Gizli dinleme saldırısı, ağdaki haberleşmenin gizlice istenmeyen düğümler tarafından dinlenmesidir. Saldırganın gizli dinlemeyi yapabilmesi için haberleşmenin yapıldığı menzil içerisinde olması gerekmektedir. Şekil 4.1'de efektif gizli dinleme alanı d_{max} yarıçaplı çember ile sınırlandırılmaktadır. d_{max} aynı zamanda saldırganın gizli bir şekilde bilgiye erişebileceği maksimum gizli dinleme mesafesidir [47].



Şekil 4.1 : SAAA'larda gizli dinleme saldırı modeli ([47]'den alınarak düzenlenmiştir).

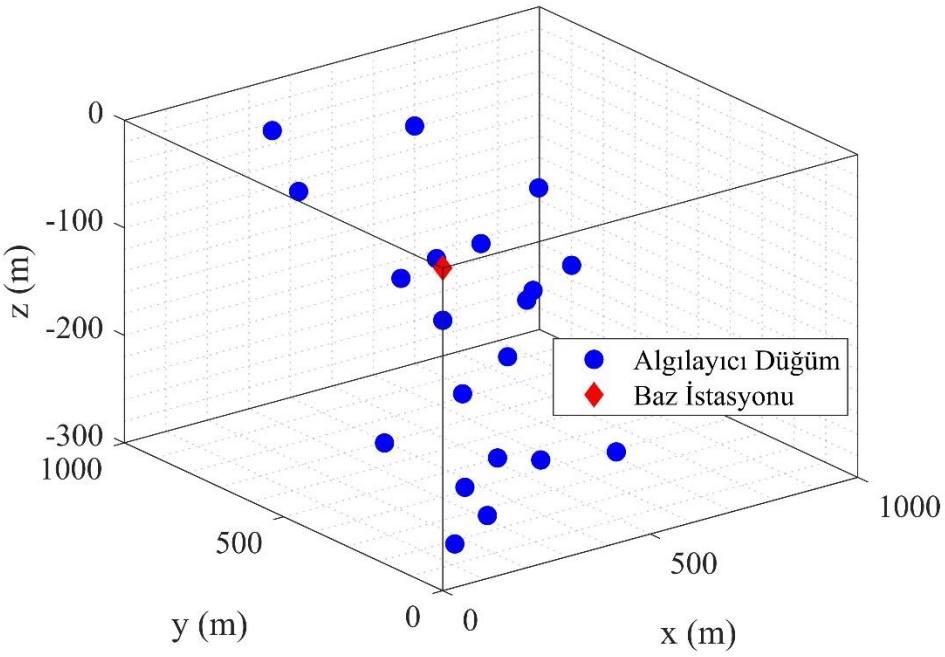
Ayrıca SAAA'larda en önemli performans metriklerinden birisi de ağ yaşam süresidir. Gizli dinleme riskini minimize edecek paket yönlendirme yolları aranırken ağ yaşam

süresinde ciddi ölçüde kayıp olabilmektedir. Bu tez çalışmasında, bu iki metrik arasındaki ödünleşme problemi detaylıca incelenmiştir.

4.2 Ağ Topolojisi

Bu tez çalışmasında düşünülen SAAA, $|W|$ adet algılayıcı düğüm ve bir adet baz istasyonundan oluşmaktadır. Algılayıcı düğümlerin sudan kaynaklı hareketleri ihmal edilerek, statik oldukları kabul edilmektedir. Ağ topolojisi $G = (V, \mathcal{A})$ şeklinde yönlü bir grafik olarak kabul edilir. V kümesi SAAA'daki baz istasyonu (düğüm-0) dahil tüm düğümleri temsil eder. Bu kümeden baz istasyonu çıkarılmasıyla geriye kalan düğümleri ise W kümesi temsil etmektedir, $W = V \setminus \{1\}$. $\mathcal{A} = \{(i,j): i \in W, j \in V - i\}$ sıralı bir kümedir. $\mathcal{A}$ kümesi, baz istasyonunun bir havuz düğümü olduğunu ve veri üretemediğini aynı zamanda hiçbir düğümün kendine veri iletemediğini göstermektedir [48]. Algılayıcı düğümler $d_e \times d_e \times h$ m^3 hacimli kare prizma şeklindeki bir sualtı ağ içerisinde, düzgün bir şekilde (İng. uniform distribution) dağıtılmıştır. Bu hacimde h değeri suyun derinliğini temsil etmektedir. Baz istasyonu, su yüzeyinde asılı şekilde ve ağın üst köşe noktasında konumlanmaktadır. Algılayıcı düğümlerin düzgün dağıtılmasıyla oluşturulmuş örnek bir topoloji Şekil 4.2'de verilmiştir. Bu SAAA'da 20 algılayıcı düğüm ve 1 adet baz istasyonu $1000 \times 1000 \times 300$ m^3 hacimli bir ağ içerisinde haberleşmektedir [49]. Ağ topolojisinin oluşturulması MATLAB programı aracılığıyla yapılmıştır. Her bir algılayıcı düğümün x, y, z koordinatları rastgele şekilde program tarafından oluşturularak algılayıcı düğümlerin konumları kararlaştırılmaktadır. Daha sonra ise algılayıcı düğümlerin birbirlerine mesafeleri hesaplanmaktadır.

Her bir algılayıcı düğüm E_{bat} başlangıç batarya gücüne sahiptir. $\mathcal{L}$ kümesi ise veri iletimi için gereken güç seviyelerini göstermektedir. Bu tez çalışmasında 10 ayrık güç seviyesi ($|\mathcal{L}| = 10$) seçilmiştir, yani böylece 10 farklı iletim menzili olduğu kabul edilmiştir. Algılayıcı düğümlerin iletim güçleri, hedef düğüm ile olan mesafelerine göre belirlenir. $d_c(l)$, güç seviyesi-l için maksimum iletim menzili olarak tanımlanır. SAAA'daki operasyon, ilk düğümün gücü bitene kadar devam eder. İlk düğümün gücünü bitirmesiyle ağdaki haberleşmenin durduğu kabul edilir, bu süreye ise ağ yaşam süresi (İng. network lifetime) adı verilmektedir.



Şekil 4.2 : Rastgele oluşturulmuş SAAA topolojisi

4.3 Sualtı Enerji Tüketim Modeli

Bu bölümde yapılan çalışmada [8, 49, 50]'deki çalışmalarda kullanılan sualtı enerji tüketim modelinden faydalanılmıştır. Modele göre bir düğümden başka bir düğüme belli bir mesafe, $d_c(l)$, üzerinden veri paketi iletilmesi için verici tarafında $P_t = A\big(d_c(l)\big)\, x\, P_0$ güce ihtiyaç duyulmaktadır. Bu denklemde P_0 alıcı düğümün girişinde ihtiyaç duyulan güç değeriyken, $A\big(d_c(l)\big)$ akustik zayıflamadır ve (4.1) numaralı denklemdeki gibi hesaplanmaktadır [8].

$$A\big(d_c(l)\big) = d_c(l)^{\kappa} \times \nu^{10^{-3} d_c(l)} \tag{4.1}$$

Yukarıdaki denklemde κ dağılım faktörüdür (İng. spreading factor). Bu faktör, sinyal yayılımının geometrisini temsil etmektedir. Genel olarak 3 başlığa ayrılmaktadır. Küresel dağılım (İng. spherical spreading), akustik enerjiyi etkileyen su yüzeyi veya deniz tabanı gibi sınırlar olmadığında, ses dalgasının kaynaktan tüm yönlere eşit olarak yayıldığı durumdaki seviye düşüşünü tanımlar. Silindirik dağılım (İng. cylindrical spreading) ise, akustik enerjinin alt veya üst sınırlarla karşılaşmasından ötürü tüm yönlerde eşit dağılmadığı durumu ifade eder [51, 52]. Küresel dağılım için $\kappa = 2$, silindirik dağılım için $\kappa = 1$ ve pratik dağılım için $\kappa = 1.5$ alınır.

$\nu = 10^{\alpha(f)/10}$ ise frekans bağımlı terimdir. Bu ifadede, $\alpha(f)$ soğurma katsayısı (İng. absorption coefficient) olup birimi dB/km iken, f ise çalışma frekansı ve birimi kHz'dir. Sualtı akustik haberleşme kanalında yol kaybı sadece düğümler arasındaki mesafeye değil, aynı zamanda iletilen sinyal frekansına bağlıdır. Thorp'un ifadesini kullanarak $\alpha(f)$ aşağıdaki gibi bulunur [53].

$$\alpha(f) = \frac{0.11f^2}{1+f^2} + \frac{44f^2}{4100+f^2} + 2.75 \cdot 10^{-4} f^2 + 0.003 \quad (4.2)$$

Gönderici düğüm tarafından (İng. transmitter node), güç seviyesi-l kullanılarak, 1-bit veri iletmek için harcanan enerji (4.3) numaralı denklemde verilmiştir.

$$E_T(l) = d_c(l)^k \times \nu^{10^{-3} d_c(l)} \times P_0 \times t \quad (4.3)$$

1-bit veriyi almak için alıcı düğüm tarafından harcanan enerji ise güç seviyesinden bağımsızdır. Bu değer (4.4)'te ifade edilmiştir.

$$E_R = P_r \times t \quad (4.4)$$

Bu eşitlikte, P_r alıcı düğüm platformuna bağlı olan sabit bir parametredir. Son olarak düğüm-i, iletim gücü seviyesini (İng. transmission power level) düğüm-j ile arasındaki mesafeye (d_{ij}) göre ayarlamaktadır. Dolayısıyla, gönderici düğümün veri iletmek için harcadığı iletim enerjisi, gönderici ve alıcı arasındaki mesafeye bağlıdır ve aşağıdaki denkleme göre belirlenmektedir.

$$E_{T,ij}^{opt} = argmin_{l \in \mathcal{L},\, d_{ij} \le d_c(l)} \; E_T(l) \quad (4.5)$$

Çizelge 4.1 : 10 farklı güç seviyesi ($\mathcal{L}$) için iletimde harcanan enerji ($E_T(l)$ - mJ) ve iletim menzili ($d_c(l)$ - m).

l	$E_T(l)$	$d_c(l)$	l	$E_T(l)$	$d_c(l)$
1 (l_{min})	0.1151	100	6	3.4160	600
2	0.3747	200	7	4.9543	700
3	0.7922	300	8	6.9666	800
4	1.4037	400	9	9.5675	900
5	2.2579	500	10 (l_{max})	12.8968	1000

(4.1)'den (4.5)'e kadar olan denklemler kullanılarak, düğümlerin iletim yaparken harcadıkları enerji hesaplanmıştır. Gönderici ve alıcı düğümler arasındaki mesafe

aralıklarına göre, 10 farklı güç seviyesi seçilmiştir. Görsel kolaylık açısından bu çalışma Çizelge 4.1'de gösterilmiştir. Bu çizelgede gönderici düğümün alıcı düğüme gönderdiği paket başına harcadığı enerji gösterilmektedir.

4.4 Gizli Dinleme Eniyileme Modeli

Sualtı haberleşme için kurulan ve sualtı algılayıcı düğümlerden oluşan bir ağın, gizli dinleme riskini en aza indirecek şekilde haberleşmesi istenmektedir. Bu yüzden bu alt bölümde ortaya konulan KTP modelinin amaç fonksiyonu, ağdaki gizli dinleme sayısını minimize etmek olacaktır. Gizli dinleme riski, ağdaki diğer düğümlerin kendi aralarındaki iletimlerine kulak misafiri olan algılayıcı düğümlerin toplam sayısı olarak modellenmekte ve ε_{min} değişkeni ile temsil edilmektedir. Dolayısıyla, bu modelin amaç fonksiyonu aşağıdaki şekilde tanımlanmıştır.

$$\text{Enküçükle } \varepsilon_{min} \tag{4.6}$$

Bu modelin kısıtları (4.7)'den (4.15)'e kadar olan denklemler ile tanımlanmıştır. Düğüm-k tarafından üretilen ve düğüm-i'den düğüm-j'ye ((i,j) bağlantı yolu üzerinden) akan toplam paket sayısı, x_{ij}^{k} tamsayı karar değişkeni (İng. integer decision variable) ile temsil edilmektedir. Her kaynak düğümdeki ($i = k$), baz istasyonundaki ($i = 0$) ve röle düğümlerdeki ($i \neq k$) akış dengeleme kısıtı aşağıdaki gibi ifade edilmiştir.

$$\sum_{j \in V,\ i \neq j} x_{ij}^{k} - \sum_{j \in W,\ i \neq j} x_{ji}^{k} = \begin{cases} 1 & eğer\ i = k\ ise \\ -1 & eğer\ i = 0\ ise \\ 0 & diğer\ durumlarda \end{cases} \tag{4.7}$$

$$\forall i \in V, \forall k \in W$$

Ağdaki toplam gizli dinleme sayısını hesaplamak için, algılayıcı düğümlerin her turda tek bir paket ürettiği varsayılmaktadır. Optimizasyon problemi çözdürülürken anlam ifade etmeyen paket iletim döngüleri oluşmaması için (4.8) nolu kısıt eklenmiştir. Bu kısıt ile, herhangi bir kaynak düğüm tarafından üretilen paketin, tekrar bu kaynak düğüme iletilme durumunun önüne geçilmiştir.

$$\sum_{j \in W} x_{jk}^{k} = 0,\ \forall k \in W \tag{4.8}$$

Düğüm-k tarafından üretilen ve güç seviyesi-l'yi kullanarak, düğüm-i üzerinden ağa dağıtılan toplam paket sayısı, ω_{il}^{k} tamsayı karar değişkeni ile (4.9) numaralı kısıtta ifade edilmektedir. Bu kısıtta, β_{ij}^{l}, düğüm-i minimum güç seviyesi-l'yi kullanarak düğüm-j'ye paket iletebiliyorsa değeri 1, diğer durumda 0 olan ikilik sistemdeki bir parametreyi (İng. binary parameter) ifade etmektedir. Bu parametre MATLAB tarafından oluşturulmaktadır.

$$\omega_{il}^{k} = \sum_{j \in V} x_{ij}^{k}\, \beta_{ij}^{l},\ \forall (i,k) \in W,\ \forall l \in \mathcal{L} \tag{4.9}$$

(4.10) numaralı kısıt oluşturulurken büyük M yönteminden (İng. big M method) faydalanılmıştır. Bu kısıt kullanılarak, ω_{il}^{k} tamsayı karar değişkeni, $\widehat{\omega_{il}^{k}}$ ikili karar değişkenine (İng. binary decision variable) çevrilmiştir. Yani $\omega_{il}^{k} > 0$ ise $\widehat{\omega_{il}^{k}} = 1$, değilse $\widehat{\omega_{il}^{k}} = 0$ olmaktadır.

$$\begin{aligned} \omega_{il}^{k} &\leq M \times \widehat{\omega_{il}^{k}},\ \forall (i,k) \in W,\ \forall l \in \mathcal{L} \\ \omega_{il}^{k} &\geq \widehat{\omega_{il}^{k}},\ \forall (i,k) \in W,\ \forall l \in \mathcal{L} \end{aligned} \tag{4.10}$$

Düğüm-k tarafından üretilen ve düğüm-j'ye iletilen toplam paket sayısı, γ_{kj} tamsayı karar değişkeni ile (4.11) numaralı kısıtta ifade edilmektedir. Bu kısıtta, δ_{ij}^{l}, düğüm-i güç seviyesi-l'yi kullanarak düğüm-j'ye paket iletebiliyorsa değeri 1, diğer durumda 0 olan ikilik sistemdeki bir parametreyi ifade etmektedir. Aynı zamanda bu parametre de, β_{ij}^{l}'de olduğu gibi, MATLAB tarafından oluşturulmaktadır.

$$\gamma_{kj} = \sum_{i \in W} \sum_{l \in \mathcal{L}} \widehat{\omega_{il}^{k}} \times \delta_{ij}^{l},\ \forall k \in W,\ \forall j \in V \tag{4.11}$$

Denklem (4.12)'de yine büyük M yöntemi kullanılarak, γ_{kj} tamsayı karar değişkeni, $\widehat{\gamma_{kj}}$ ikili karar değişkenine çevrilmiştir. Aslında γ_{kj}, düğüm-k'da üretilen paketi düğüm-j'nin kaç defa duyduğunu göstermektedir. Eğer düğüm-j, aynı paketi birden fazla duymuşsa bir kez gizli dinleme sayılması bu kısıt ile sağlanmıştır. Bu kısıt matematiksel olarak bir başka gösterimle ifade edilecek olursa; $\gamma_{kj} > 0$ iken $\widehat{\gamma_{kj}} = 1$, değilken $\widehat{\gamma_{kj}} = 0$ olmaktadır.

$$\gamma_{kj} \leq M \times \widehat{\gamma_{kj}},\ \forall k \in W,\ \forall j \in V$$
$$\gamma_{kj} \geq \widehat{\gamma_{kj}},\ \forall k \in W,\ \forall j \in V \tag{4.12}$$

Düğüm-k tarafından üretilen pakete kulak misafiri olan toplam algılayıcı düğüm sayısı, tamsayı karar değişkeni ζ_k ile denklem (4.13)'te ifade edilmiştir.

$$\zeta_k = \sum_{j \in V} \widehat{\gamma_{kj}},\ \forall k \in W \tag{4.13}$$

SAAA'daki toplam gizli dinleme sayısı ise, (4.14) numaralı denklemde gösterildiği üzere, ζ_k 'nın tüm kaynak düğümler üzerinden toplanmasıyla elde edilir.

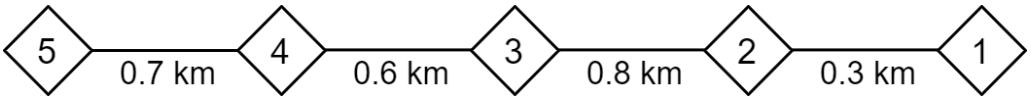
$$\varepsilon_{min} = \sum_{k \in W} \zeta_k \tag{4.14}$$

Daha önce de belirtildiği gibi, bu modelin amaç fonksiyonu ε_{min}'i minimize etmektir. Bu fonksiyon ile, ağda haberleşme yapılırken, gizli dinleme sayısı minimum olacak şekilde paket iletim yollarını ayarlanmaktadır. Son olarak, bu modelde kullanılan karar değişkenleri (İng. decision variables) için belirlenen sınırlar ise (4.15) numaralı denklem ile gösterilmektedir.

$$x_{ij}^k \geq 0,\ \forall (i,k) \in W, \forall j \in V$$
$$\omega_{il}^k \geq 0,\ \forall (i,k) \in W,\ \forall l \in \mathcal{L}$$
$$\gamma_{kj} \geq 0,\ \forall k \in W,\ \forall j \in V$$
$$\zeta_k \geq 0,\ \forall k \in W \tag{4.15}$$
$$\widehat{\omega_{il}^k} \in \{0,1\},\ \forall (i,k) \in W,\ \forall l \in \mathcal{L}$$
$$\widehat{\gamma_{kj}} \in \{0,1\},\ \forall (k,j) \in W$$

4.5 Lineer Topolojide Gizli Dinleme Eniyileme Modeli

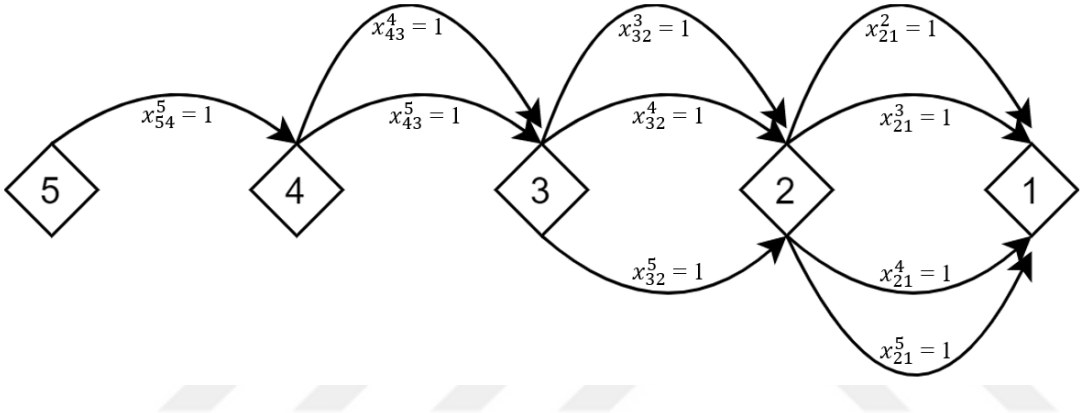
Bir önceki bölümde verilen KTP modelinin daha iyi anlaşılması açısından bu alt bölümde, lineer topoloji üzerinden gizli dinleme eniyileme modelinin çözümü anlatılmış ve bazı değişkenler örneklerle açıklanmıştır.



Şekil 4.3 : Lineer topolojiden oluşan SAAA

Şekil 4.3'te 1 boyutlu lineer topolojiden oluşan bir SAAA örneği gösterilmiştir. Bu topolojide 1 nolu algılayıcı düğüm; havuz düğüm, diğer bir ifadeyle baz istasyonudur. Tüm düğümler verilerini direkt veya röle düğümler aracılığıyla 1 nolu düğüme aktarmaktadır.

Bu topoloji Bölüm 4.4'teki KTP modeline yerleştirilip, çözüm alındığında paket veri akışları (x_{ij}^{k}) Şekil 4.4'teki gibi olmaktadır.



Şekil 4.4 : Lineer topoloji paket veri akışları

Bu şekil incelendiğinde SAAA'daki gizli dinleme sayısının en aza indirgenmesi için:

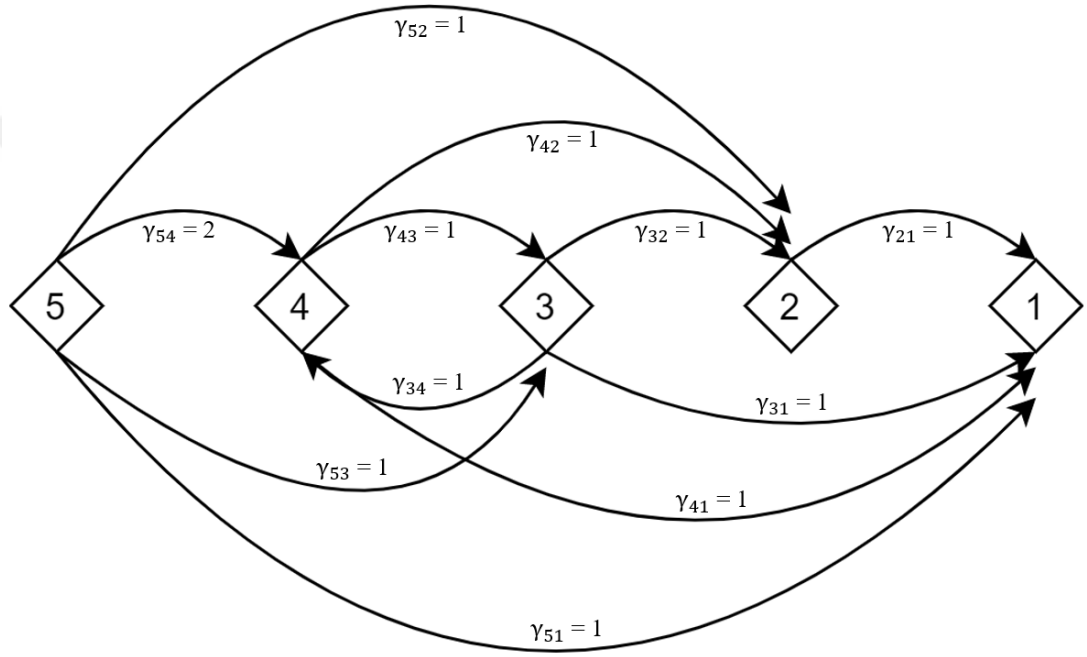
- 2. düğüm paketini direkt 1. düğüme,
- 3. düğüm paketini 2. düğüm aracılığıyla 1. düğüme,
- 4. düğüm paketini 3. düğüme, oradan 2. düğüme ve son olarak 1. düğüme,
- 5. düğüm paketini 4. düğüme, oradan 3. düğüme, sonra 2. düğüme ve son olarak 1. düğüme iletmektedir.

Bu iletimler yapılırken, iletim menzili içerisinde kalan düğümler ağda iletilen veriyi duyacaktır. İletimlere göre gizli dinleme sayısı bulunacak olursa;

- 2. düğümün verisini, sadece 1. düğüm duymaktadır.
- 3. düğümün verisini; 1, 2 ve 4. düğümler duymaktadır. 4. düğümün duymasının sebebi 3. düğüm 0.8 km uzağındaki 2. düğüme veri aktarmak için sinyal gönderdiğinde, 0.6 km uzağındaki 4. düğümün iletim menzili içerisinde kalmasıdır.

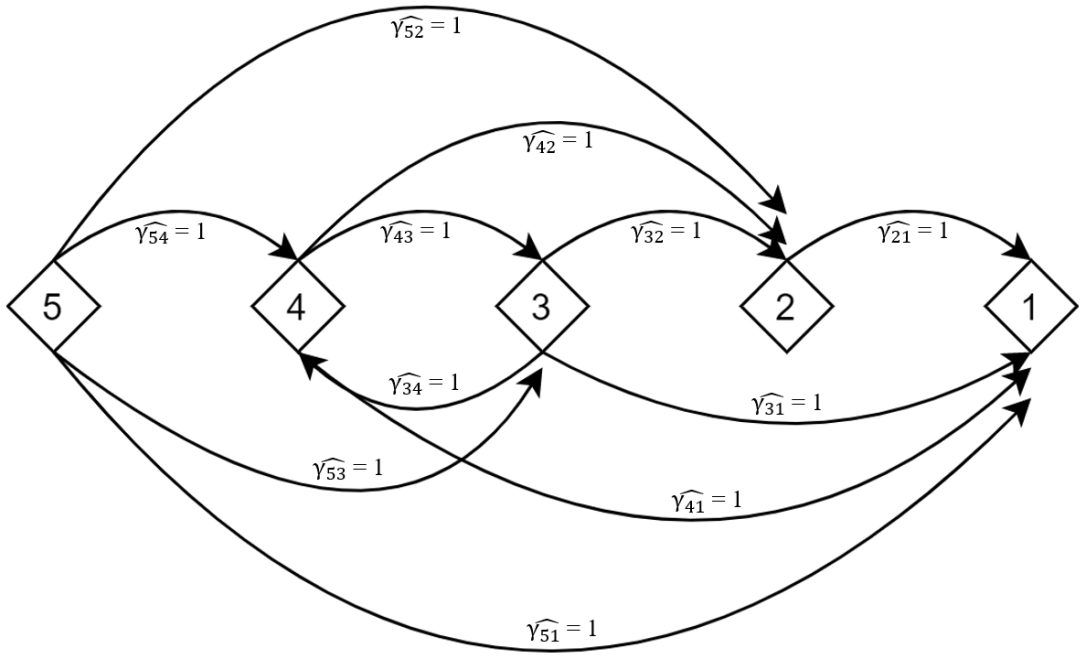
- 4. düğümün verisini; 1, 2 ve 3. düğümler duymaktadır. 5. düğümün duymamasının sebebi, 4. düğüm 0.6 km uzağındaki 3. düğüme veri aktarmak için sinyal gönderdiğinde, 0.7 km uzağındaki 5. düğümün iletim menzili dışında kalmasıdır.
- Son olarak 5. düğümün verisini ise; 1, 2, 3 ve 4. düğümler duymaktadır.

Denklem (4.11)'deki γ_{kj} değişkenin aldığı değerler ise Şekil 4.5'te lineer topoloji üzerinde gösterilmiştir. γ_{kj} değişkeni k'da üretilen paketi j düğümünün kaç kez duyduğudur.



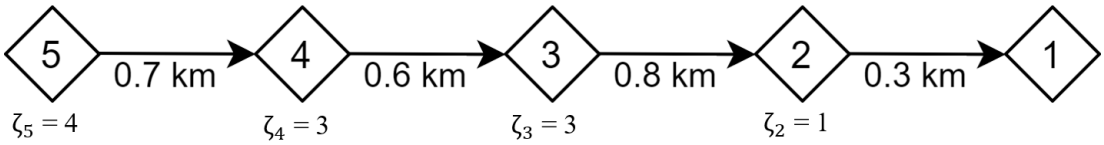
Şekil 4.5 : γ_{kj} değerleri

Şekil 4.5'e bakıldığında γ_{43} = 1'dir, yani 4 numaralı düğümde üretilen veriyi 3 numaralı düğüm 1 kez duymuştur. γ_{54} = 2'dir, diğer bir ifadeyle 5 numaralı düğümde üretilen veriyi 4 numaralı düğüm 2 kez duymuştur. Bu duyumlardan ilki 5. düğüm paketi 4. düğüme iletirken olurken, diğeri ise 3. düğümden 2. düğüme iletim sırasında 4. düğümün aynı paketi tekrar duymasıyla gerçekleşmektedir. Fakat aynı paketin tekrar duyulması gizli dinleme açısından bir kez sayılacaktır. Bu durum için KTP modeline eklenen (4.12) numaralı denklem ile γ_{kj} tamsayı karar değişkeni, $\widehat{\gamma_{kj}}$ ikili karar değişkenine çevrilmiştir ve lineer topoloji için $\widehat{\gamma_{kj}}$ değerleri Şekil 4.6'da gösterilmiştir. Şekil 4.5 ve Şekil 4.6 incelendiğinde γ_{54} = 2 iken $\widehat{\gamma_{54}}$ = 1 olduğu gözlemlenmektedir.



Şekil 4.6 : $\widehat{\gamma_{kJ}}$ değerleri

Şekil 4.7, düğüm k tarafından üretilen pakete kulak misafiri olan düğüm sayısını gösteren ζ_k değişkenini lineer topoloji üzerinde göstermektedir. Şekle göre ζ_4 = 3 iken, ζ_5 = 4'tür. Daha önce de bahsedildiği gibi 4 nolu düğümde üretilen paketi duyan düğümler; 1, 2 ve 3 olmak üzere toplam 3 düğümken, 5 nolu düğümde üretilen paketi duyan düğümler; 1, 2, 3 ve 4 olmak üzere toplam 4 düğümdür. Bu değerler de Şekil 4.7'i doğrulamaktadır.



Şekil 4.7 : ζ_k değerleri

Son olarak (4.14) numaralı denklemde ζ_k değerlerinin k üzerinde toplanmasıyla elde edilen ε_{min} değeri 1+3+3+4 değerlerinin toplanmasıyla elde edilen 11'dir ve bu ağda gerçekleşebilecek minimum gizli dinleme sayısı bu sayıdır.

4.6 Ağ Yaşam Süresi Eniyileme Modeli

Bu alt bölümde ortaya konulan KTP modeli ile belli bir gizli dinleme risk seviyesinde, ağın yaşam süresi maksimize edilmeye çalışılmaktadır. Gizli dinleme risk seviyesi, ağdaki toplam kulak misafirliği sayısına bir sınır tanımlayarak belirlenmektedir. Bu

model, Bölüm 4.4'te anlatılan modelin devamı niteliğindedir. Önceki modelin amaç fonksiyonu olan ağdaki minimum toplam gizli dinleme sayısı, bu modele kısıt olarak verilmektedir. Bu gizli dinleme kısıtı altında aynı ağın; ağ yaşam süresini, L (tur olarak), maksimize yapacak şekilde haberleşmesi istenir. Kurulan modelin amaç fonksiyonu ise aşağıdaki denklemde verilmiştir.

$$\text{Enbüyükle } L \tag{4.16}$$

Düğümlerin her turda bir paket ürettiği varsayıldığından ötürü, ağ yaşam süresi boyunca düğümlerin üretiği toplam paket sayısı L'ye eşit olacaktır. Bu yaklaşım göz önünde bulundurularak, bu model için (4.7)'deki akış dengeleme kısıtı aşağıdaki gibi güncellenir.

$$\sum_{j\in V,\ i\neq j} x_{ij}^{k} - \sum_{j\in W,\ i\neq j} x_{ji}^{k} = \begin{cases} L & eğer\ i = k\ ise \\ -L & eğer\ i = 0\ ise \\ 0 & diğer\ durumlarda \end{cases} \tag{4.17}$$

$$\forall i \in V, \forall k \in W$$

Kısıt (4.18) ile her bir düğümün paket gönderirken ve alırken harcadığı enerjilerin toplamının, başlangıç batarya enerjisinden küçük olması sağlanmıştır.

$$\mathrm{l}_p \sum_{k\in W} \left(\sum_{j\in V} E_{T,ij}^{opt} x_{ij}^{k} + E_R \sum_{j\in W} x_{ji}^{k} \right) \leq E_{bat},\ \forall i \in W \tag{4.18}$$

Bu kısıtta, l_p her bir paketin kaç bitten oluştuğunu belirtirken, E_R ve $E_{T,ij}^{opt}$ değerleri ise sırasıyla (4.4) ve (4.5) numaralı denklemlerde tanımlanmıştır. (4.19) numaralı kısıtta ise, ağdaki toplam gizli dinleme sayısı belli bir sabit (ξ) ile sınırlandırılmıştır. Modele verilen bu sabit değer ile ağdaki gizli dinleme risk seviyesi belirlenmektedir. Bu tez çalışmasında sabit değer olarak, ağdaki minimum gizli dinleme sayısı verilmiştir.

$$\sum_{k\in W} \zeta_k \leq \xi \tag{4.19}$$

Bölüm 4.4'te tanımlanan KTP modelinin kısıtları olan (4.8)−(4.13) arası ve (4.15) numaralı kısıtlar aynı zamanda bu KTP modelinde de kullanılmaktadır. Son olarak analizde kullanılan parametreler görsel kolaylık açısından Çizelge 4.2'de listelenmiştir.

Çizelge 4.2 : Analizde kullanılan parametreler.

Parametreler	**Tanım**	**Değer**
d_c	Maksimum haberleşme menzili (m)	$\{100, 200, \dots, 1000\}$
d_e	Ağın taban kenar uzunluğu (km)	$\{0.4, 0.7, \dots, 1.9\}$
E_{bat}	Batarya enerjisi (KJ)	25
f	Çalışma frekansı (kHz)	25
h	Ağın derinliği (m)	300
κ	Dağılım faktörü	1.5
$\lvert\mathcal{L}\rvert$	Toplam güç seviyesi sayısı	10
l_p	Paket boyutu (bit)	1024
$\lvert W\rvert$	Algılayıcı düğüm sayısı	$\{10, 20, 30\}$
P_0	Alıcı düğümün girişinde istenen güç değeri (J/bit)	1×10^{-7}
P_r	Alınma sabiti (J/bit)	0.2×10^{-7}

5. ANALİZ VE DEĞERLENDİRMELER

Tez çalışmasının bu bölümünde, gizli dinleme kısıtı ile ağ yaşam süresi arasındaki ilişki sayısal değerler ve grafikler ile analiz edilerek sonuçlar değerlendirilmiştir. Problemlerin çözümünde, MATLAB ve GAMS programları kullanılmıştır. Ağ topolojisinin oluşturulması ve KTP modellerinin çözümü için ihtiyaç duyulan parametreler MATLAB programı ile oluşturulup, `gdx` dosya formatında GAMS programına aktarılmıştır. Diğer bir deyişle; Bölüm 4.2'de anlatılan ağ topolojisi ve Bölüm 4.3'te anlatılan algılayıcı düğümlerin enerji tüketim değerleri MATLAB aracılığıyla oluşturulurken, Bölüm 4.4'te ve 4.6'da anlatılan KTP modellerinin çözümünde ise GAMS'den faydalanılmıştır. Ayrıca bu modelleri çözerken kullanılan parametreler Çizelge 4.2'de listelenmiştir. Oluşturulan bir SAAA için, bu tez çalışmasındaki iki KTP modeli aşağıdaki sıraya göre çözdürülmüştür:

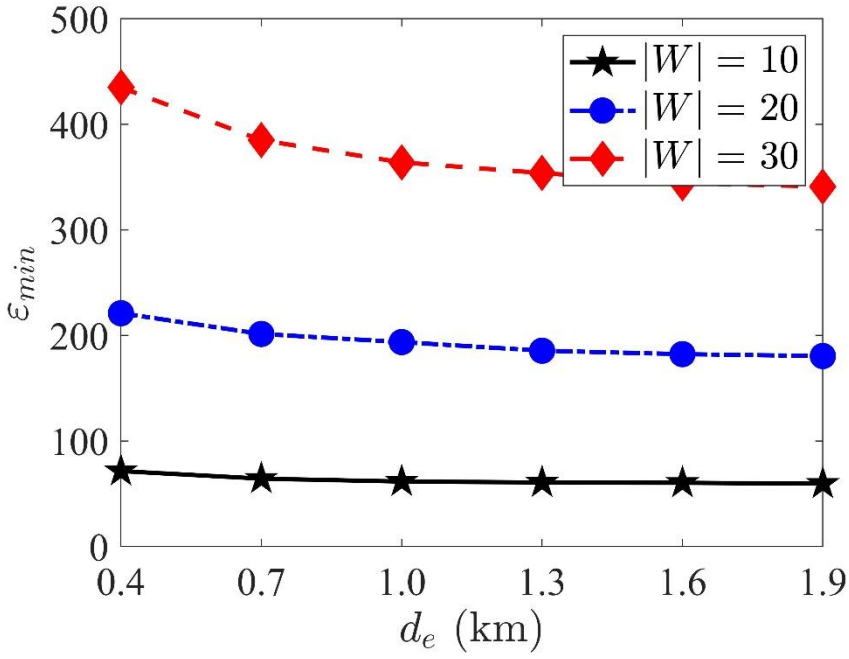
1. SAAA'daki toplam gizli dinleme sayısını enküçüklemek için Bölüm 4.4'teki KTP modeli çözdürülmüştür. Bu modelin çözümüyle bulunan ε_{min} değeri SAAA'da haberleşme sağlanırken, ağda oluşabilecek minimum gizli dinleme sayısını temsil etmektedir. Diğer bir deyişle ilgili ağda ε_{min} değerinin daha altında bir gizli dinleme sayısı ile ağda kopma olmadan haberleşilmesi imkansızdır.

2. Adım 1'in sonunda elde edilen ε_{min} değeri, (4.19) numaralı kısıttaki ξ sabiti yerine yazılarak ($\xi = \varepsilon_{min}$) Bölüm 4.6'daki KTP modeli çözdürülmüştür. Böylece, Kısıt (4.16)'daki amaç fonksiyonunun optimum değeri bulunur ve bu değer $L = L_{min}$ olarak tanımlanır. Diğer bir deyişle, bulunan bu değer (L_{min}) gizli dinleme riski (limiti) minimum iken SAAA'da gerçekleşen ağ yaşam süresidir.

3. Bölüm 4.6'daki KTP modeli, (4.19) numaralı kısıttaki ξ'nin sabit bir değer yerine serbest karar değişkeni (İng. free decision variable) olarak seçilmesiyle tekrar çözdürülmüştür. Bunun sonucunda, Kısıt (4.16)'daki amaç fonksiyonunun optimum değeri bulunur ve bu değer $L = L_{max}$ olarak tanımlanır. Bulunan bu değer (L_{max}) ağda gizli dinleme kısıtı olmadan,

algılayıcı düğümlerin özgür bir şekilde haberleştiği durumdaki ağ yaşam süresini göstermektedir. Ayrıca, serbest karar değişkeninin optimum değeri $\xi = \varepsilon_{max}$ olarak bulunur. Bu değer ($\xi = \varepsilon_{max}$) ise, SAAA'daki maksimum ağ yaşam süresine ulaşabilmek için ağda olması gereken gizli dinleme sayısını göstermektedir.

GAMS'den alınan sonuçlar, istenilen şekilde grafiklerini çizdirmek ve kolayca yorumlanmak amacıyla `gdx` dosya formatında tekrar MATLAB'a aktarılmaktadır. İstatiksel olarak anlam ifade etmesi amacıyla, bu bölümde verilen tüm grafikler rastgele oluşturulmuş 100 topolojinin ortalaması alınarak çizdirilmiştir.

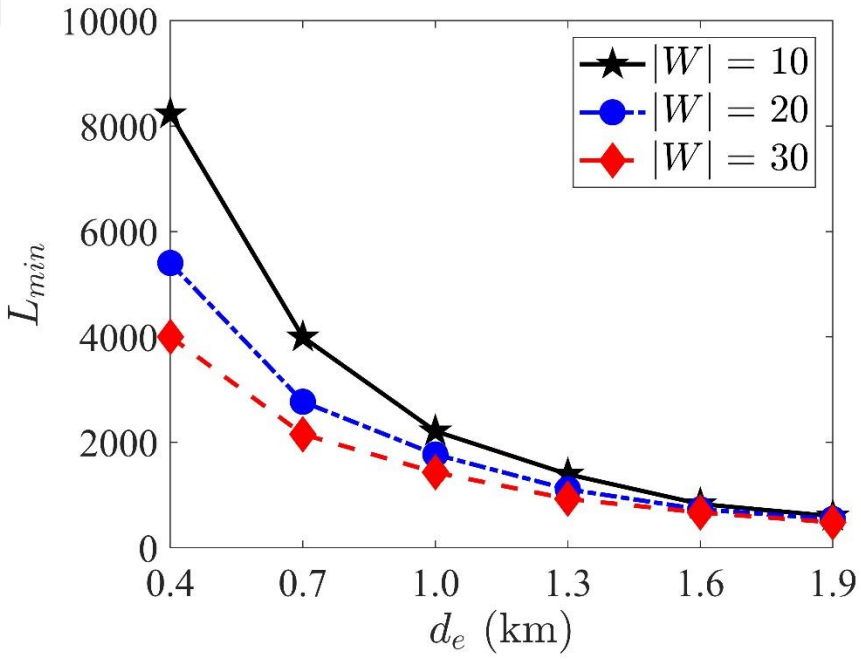


Şekil 5.1 : Minimum toplam gizli dinleme sayısı

Şekil 5.1'de verilen grafik, ağdaki 3 farklı algılayıcı düğüm sayısı için (3 farklı $|W|$ değeri) seçilen d_e değerlerine göre ağda gerçekleşen minimum gizli dinleme sayısını (ε_{min}) göstermektedir. ε_{min} maksimum değerini en yoğun ağda ($|W| = 30$ ve $d_e = 0.4$ km iken) 435 olarak olarak alırken, minimum değerini en seyrek ağda ($|W| = 10$ ve $d_e = 1.9$ km iken) 60 olarak almıştır. Grafik incelendiğinde, d_e sabit iken $|W|$ arttıkça ε_{min}'in arttığı gözlenir. Yani sabit büyüklükteki ağda algılayıcı düğüm yoğunluğu arttıkça, ağdaki toplam gizli dinleme sayısı artmaktadır. Örneğin, $d_e = 1.0$ km iken $|W| = 10$, 20 ve 30 için ε_{min} sırasıyla 62, 194 ve 364 olarak gerçekleşir. Bunun sebebi olarak yoğun bir ağda algılayıcı düğümlerin birbirinin iletim menziline daha fazla girmesinden ötürü, iletilen bir paketin diğer düğümler tarafından duyulma

sayısının artması gösterilebilir. Diğer yandan, $|W|$ sabit tutulurken d_e arttıkça, ε_{min} belli bir d_e değerine kadar azalmakta, sabit bir d_e değerinden sonra ise belli bir değere yakınsamaktadır. Bunun sebebi olarak ise, ağ seyrekleştikçe gizli dinleme sayısını azaltacak yeni haberleşme bağlantılarının kolayca kurulamaması gösterilebilir.

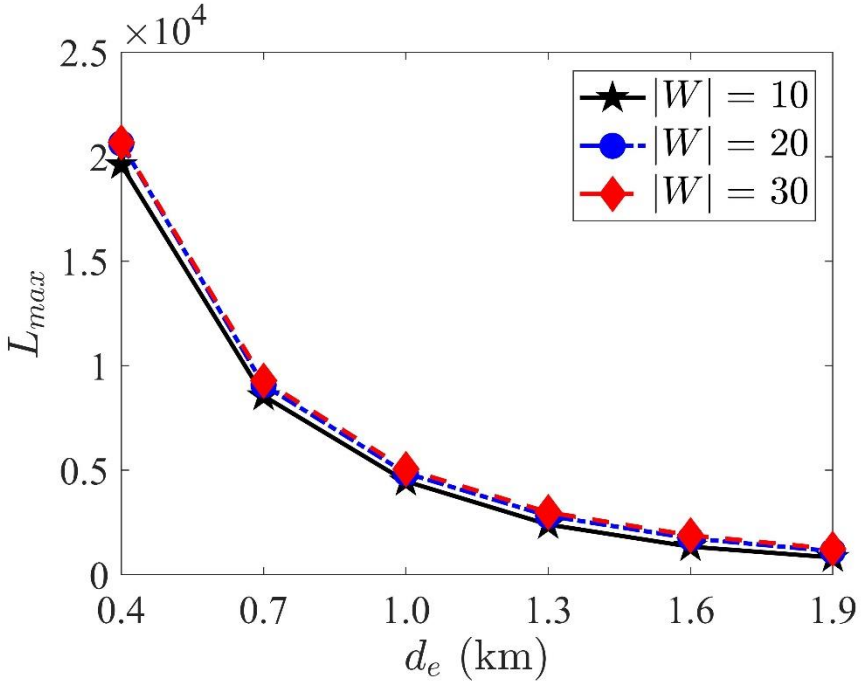
Şekil 5.2'de verilen grafik, minimum gizli dinleme kısıtı (ε_{min}) altında gerçekleşen maksimum ağ yaşam süresini göstermektedir. Grafiğe bakıldığında, d_e sabit iken $|W|$ azaldıkça L_{min}'in arttığı gözlemlenmiştir. Diğer bir ifadeyle, sabit bir ağ büyüklüğü için ağdaki düğüm yoğunluğu azaldıkça ağ yaşam süresi artmaktadır. Bunun sebebi olarak, yoğun ağlarda gizli dinleme kısıtının görece daha fazla olmasından ötürü ağ yaşam süresinin daha fazla düşmesi gösterilebilir. L_{min} maksimum değerini ($|W| = 10$ ve $d_e = 0.4$ km iken) 8232 tur olarak olarak alırken, minimum değerini ($|W| = 30$ ve $d_e = 1.9$ km iken) 482 tur olarak almıştır. Diğer yandan, $|W|$ sabit tutulurken d_e arttıkça L_{min} azalmaktadır. Çünkü ağdaki algılayıcı düğüm sayısı ($|W|$) sabit iken ağ büyüklüğü artarsa, mesafeler arttığından ötürü, algılayıcı düğümler iletimlerini yapabilmek için daha çok enerji harcamaktadırlar. Bu da bataryanın hızlı tüketilip, ağ yaşam süresinin düşmesine sebep olmaktadır.



Şekil 5.2 : ε_{min} gizli dinleme kısıtı altında maksimum ağ yaşam süresi

Şekil 5.3'te verilen grafik, gizli dinleme kısıtı (ε_{min}) kaldırıldığında, gerçekleşen maksimum ağ yaşam süresini göstermektedir. L_{max} maksimum değerini en yoğun ağda ($|W| = 30$ ve $d_e = 0.4$ km iken) 20680 tur olarak olarak alırken, minimum

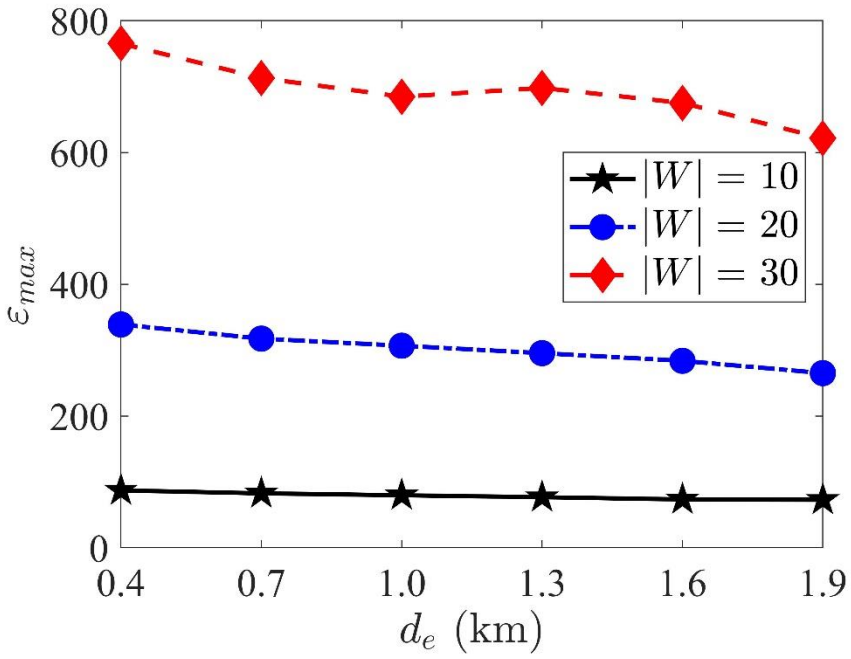
değerini en seyrek ağda ($|W| = 10$ ve $d_e = 1.9$ km iken) 826 tur olarak almaktadır. Grafik incelendiğinde, d_e sabit iken $|W|$ arttıkça küçük bir L_{max} artışı gözlemlenmiştir. Bunun sebebi olarak, röle düğüm sayısının fazla olmasından ötürü algılayıcı düğümlerin ağ yaşam süresini artırabilmek için, iletim esnasında daha fazla alternatif yol bulabilmesi gösterilebilir. Fakat genel olarak aynı d_e değeri için, L_{max} değerleri birbirine çok yakındır. Diğer yandan, $|W|$ sabit tutulurken d_e arttıkça L_{max} azalır. Şekil 5.2'de de açıklandığı gibi sabit algılayıcı düğüm sayısı ($|W|$) için ağ büyüklüğü artışı düğüm mesafelerinin artışına, bu da batarya süresinin düşmesine neden olmaktadır. Şekil 5.2 ve Şekil 5.3 genel eğilim olarak ağ büyüklüğünün artmasıyla ağ yaşam sürelerinin düşmesi açısından benzerlik sağlamaktadır. Diğer taraftan ise sabit bir ağ içerisinde Şekil 5.2'de daha seyrek ağda ağ yaşam süresi yüksekken, Şekil 5.3'te daha yoğun ağda ağ yaşam süresi daha yüksektir. Bunun sebebi olarak ise gizli dinleme kısıtı varken ve daha seyrek ağda bu kısıtın daha hafif olmasından ötürü ağ yaşam süresini fazla düşürememesi gösterilebilir. Gizli dinleme kısıtı kaldırıldığında ise daha yoğun ağlar, bahsedildiği gibi, daha fazla alternatif rota bularak ağ yaşam süresini artırabilmektedir.



Şekil 5.3 : $\varepsilon_{\min}$ gizli dinleme kısıtı olmadan maksimum ağ yaşam süresi

Şekil 5.4'te verilen grafik, maksimum ağ yaşam süresine ulaşabilmek için olması gereken gizli dinleme sayısını (ε_{max}) göstermektedir. Bu grafiğin eğilimi Şekil 5.1'deki grafiğin eğilimine benzemektedir. ε_{max} maksimum değerini en yoğun ağda

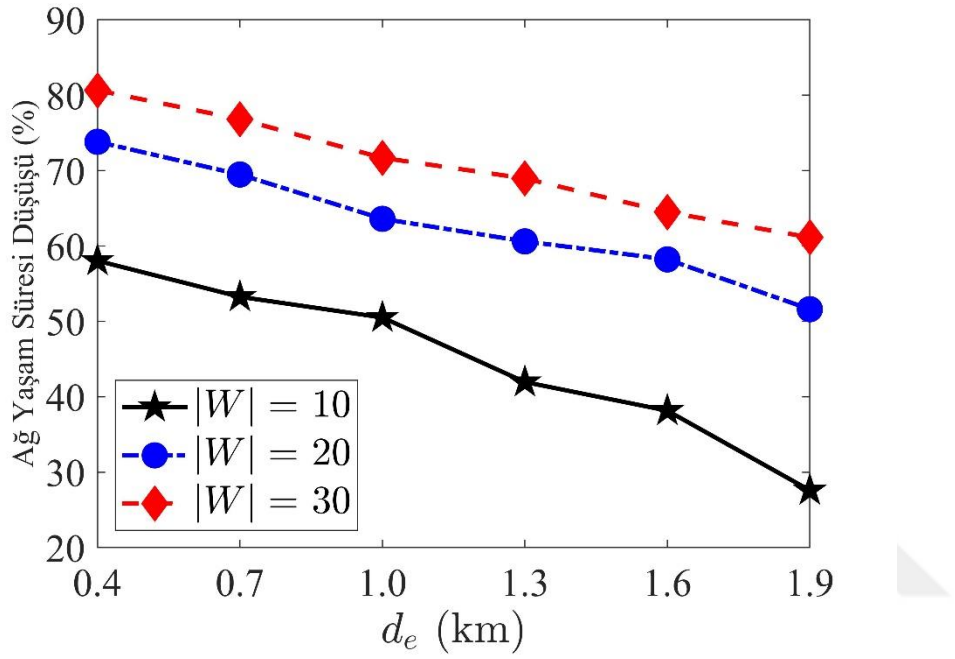
($|W| = 30$ ve $d_e = 0.4$ km iken) 765 olarak olarak alırken, minimum değerini en seyrek ağda ($|W| = 10$ ve $d_e = 1.9$ km iken) 73 olarak almaktadır. Grafik incelendiğinde d_e sabit iken, $|W|$ arttıkça ε_{max}'ın arttığı gözlemlenir. Çünkü daha yoğun bir ağda, iletilen bir paketin diğer düğümler tarafından duyulma sayısı daha fazla olacaktır. Diğer yandan, $|W|$ sabit tutulurken d_e arttıkça, ε_{max} genel olarak (bir nokta hariç) azalma eğilimindedir. Bunun sebebi olarak ise ağ seyrekleştikçe düğüm mesafelerinin artmasından ötürü düğümlerin menzilden çıkarak, gizli dinleme sayılarının düşmesi gösterilebilir.



Şekil 5.4 : Maksimum ağ yaşam süresine (L_{max}) ulaşabilmek için olması gereken gizli dinleme sayısı

Şekil 5.5'teki grafik, gizli dinleme sayısı ε_{min} ile sınırlandığında, maksimum ağ yaşam süresi (L_{max}) üzerinde gerçekleşen yüzdesel azalışı göstermektedir. L_{max} üzerinde gerçekleşen yüzdesel azalış $100 \times \frac{|L_{max} - L_{min}|}{L_{max}}$ olarak hesaplanmaktadır. Grafiğe bakıldığında, L_{max}'daki minimum ve maksimum azalmalar sırasıyla %27.60 – %61.14 ($d_e = 1.9$ km için) ve %58.04 – %80.64 ($d_e = 0.4$ km için) aralıklarında gerçekleşmektedir. Sabit bir d_e değeri için $|W|$ arttıkça, L_{max}'daki düşüş yüzdesi artmaktadır çünkü fazla sayıda algılayıcı düğüm olması ile ağın ömrü uzatılmaya çalışılırken gizli dinleme risklerini en aza indirecek enerji açısından verimli yönlendirme yolları bulunamaz. Örneğin, $d_e = 0.4$ km iken L_{max}'daki düşüş yüzdesi $|W| = 10$, 20 ve 30 için sırasıyla %58.04, %73.82 ve %80.64 olarak ve $d_e = 1.9$ km

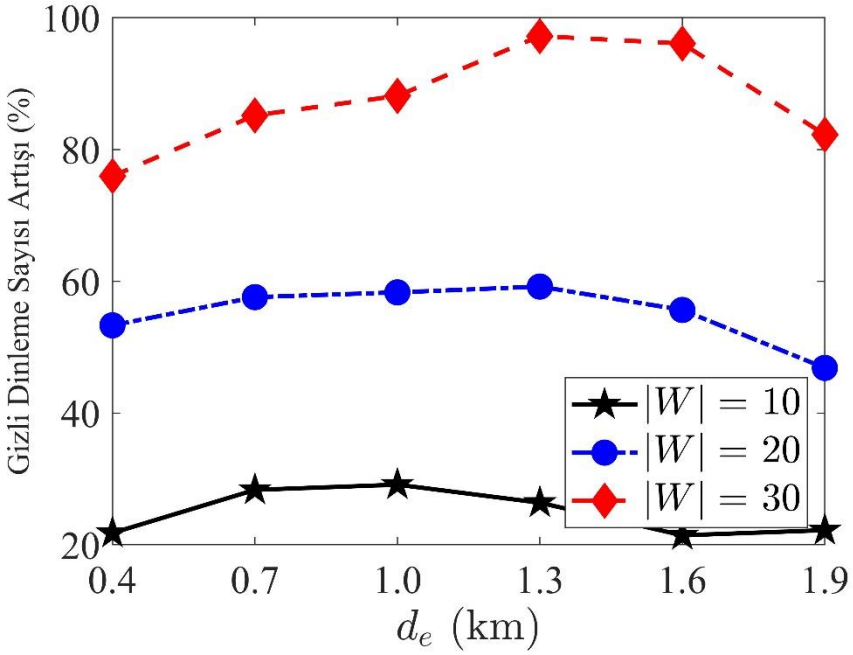
için L_{max}'daki düşüş yüzdesi $|W| = 10$, 20 ve 30 için sırasıyla %27.60, %51.62 ve %61.14 olarak gözlemlenir. Diğer taraftan ise, sabit bir $|W|$ değeri için d_e arttıkça, L_{max}'daki yüzdesel düşüş azalmaktadır çünkü daha seyrek ağlarda toplam gizli dinleme sayısını ε_{min}'e limitlemek, ağ yaşam süresi üzerinde görece daha hafif etkiye sahiptir. Örneğin, $|W| = 30$ için, d_e arttıkça, L_{max}'daki yüzdesel azalış %80.64'ten (d_e = 0.4 km iken), %61.14'e (d_e = 1.9 km iken) düşmektedir.



Şekil 5.5 : Gizli dinleme sayısı minimize edildiğinde ağ yaşam süresindeki (L_{max}) yüzdesel azalış

Şekil 5.6'da verilen grafik, maksimum ağ yaşam süresine (L_{max}) ulaşabilmek için gizli dinleme sayısında (ε_{min}) yüzdesel olarak ne kadar artış yapılması gerektiğini göstermektedir. ε_{min} üzerinde gerçekleşen yüzdesel artış $100 \times \frac{|\varepsilon_{max} - \varepsilon_{min}|}{\varepsilon_{min}}$ olarak hesaplanmaktadır. L_{max}'a ulaşmak için ε_{min}'de olması gereken yüzdesel artış, sabit bir d_e değeri için $|W|$ arttıkça, artmaktadır. Örneğin, d_e = 0.4 km olan bir ağda L_{max}'a ulaşmak için, ε_{min} değeri $|W| = 10$, 20 ve 30 için sırasıyla %21.78, %53.30 ve %75.95 olarak artırılmalıdır. Diğer taraftan, $|W|$ sabit durumdayken, L_{max}'ı elde etmek için ε_{min}'de olması gereken yüzdesel artış belli bir ağ büyüklüğün kadar artıp sonra azalmaktadır. Her bir $|W|$ değeri için ε_{min}'deki yüzdesel artışın en yüksek değerleri %97.21 (d_e = 1.3 km ve $|W|$ = 30 iken), %59.19 (d_e = 1.3 km ve $|W|$ = 20 iken) ve %29.12 (d_e = 1 km ve $|W|$ = 10 iken) olarak gerçekleşir. Bu sonucun arkasındaki temel sebep olarak belli bir d_e değerine kadar ε_{min} değerlerinin, ε_{max} değerlerinden

daha sert düşmesi gösterilebilir. İlgili d_e değeri geçildikten sonra ise bu durum tersine dönmektedir.



Şekil 5.6 : Maksimum ağ yaşam süresine (L_{max}) ulaşabilmek için gizli dinleme sayısındaki (ε_{min}) yüzdesel artış

6. SONUÇLAR

Bu tez çalışmasında, SAAA'larda gizli dinleme riskini minimize etmenin ağ yaşam süresi üzerindeki etkisi 2 KTP modeli üzerinden araştırılmıştır. Sonuçlar göstermektedir ki; gizli dinleme riskinin minimize edildiği durumda, gizli dinleme kısıtının olmadığı durumdaki ağ yaşam süresinden %80.64'e kadar daha düşük ağ yaşam süreleri elde edilebilmektedir. Dahası, gizli dinleme kısıtının olmadığı durumdaki maksimum ağ yaşam süresine ulaşmak için, ağdaki minimum gizli dinleme sayısını %97.21 seviyelerine kadar artırma ihtiyacı doğmaktadır. Bununla birlikte seyrek ağlarda, minimum gizli dinleme kısıtından ötürü gerçekleşen maksimum ağ yaşam süresindeki düşüş daha azdır.

Genel olarak sonuçlar özetlenecek olursa:

- SAAA'nın topoloji büyüklüğü sabit iken algılayıcı düğüm sayısı arttıkça, ağdaki gizli dinleme sayısı (ε_{min}) artarken; diğer yandan algılayıcı düğüm sayısı sabit tutularak ağ büyüklüğü artırıldığında, ağdaki gizli dinleme sayısı belli bir ağ büyüklüğüne kadar azalıp, sabit bir ağ büyüklüğü değerinden sonra ise belli bir değere yakınsamaktadır.

- SAAA'nın topoloji büyüklüğü sabit iken algılayıcı düğüm sayısı azaldıkça, gizli dinleme kısıtı altındaki ağ yaşam süresi artarken; diğer yandan algılayıcı düğüm sayısı sabit tutulurken ağ büyüklüğü arttıkça, gizli dinleme kısıtı altındaki ağ yaşam süresi azalmaktadır.

- SAAA'nın topoloji büyüklüğü sabit iken algılayıcı düğüm sayısı artırıldığında, küçük bir ağ yaşam süresi (L_{max}) artışı gözlemlenirken; diğer yandan algılayıcı düğüm sayısı sabit tutularak ağ büyüklüğü artırıldığında ise ağ yaşam süresi azalmaktadır.

- SAAA'nın topoloji büyüklüğü sabit iken algılayıcı düğüm sayısı arttıkça, maksimum ağ yaşam süresine ulaşabilmek için gereken gizli dinleme sayısının (ε_{max}) arttığı gözlemlenirken; diğer yandan algılayıcı düğüm sayısı sabit

tutularak ağ büyüklüğü artırıldığında, ε_{max} genel olarak (bir nokta hariç) azalma eğilimindedir.

- SAAA'nın topoloji büyüklüğü sabit iken algılayıcı düğüm sayısı arttıkça, maksimum ağ yaşam süresindeki (L_{max}) düşüş yüzdesi artarken; diğer yandan algılayıcı düğüm sayısı sabit tutularak ağ büyüklüğü artırıldığında, maksimum ağ yaşam süresindeki yüzdesel düşüş azalmaktadır.
- Maksimum ağ yaşam süresine ulaşmak için ağdaki gizli dinleme sayısında olması gereken yüzdesel artış, sabit bir SAAA topoloji büyüklüğü için algılayıcı düğüm sayısı arttıkça artmaktayken; diğer yandan algılayıcı düğüm sayısı sabit tutulduğunda, maksimum ağ yaşam süresini elde etmek için ağdaki gizli dinleme sayısında olması gereken yüzdesel artış belli bir ağ büyüklüğü değerine kadar artıp sonra azalmaktadır.

KAYNAKLAR

[1] **Kumar, P., Kumar, P., Priyadarshini, P., & Srija.** (2012). Underwater acoustic sensor network for early warning generation. *2012 Oceans*, (pp. 1-6). Hampton Roads, VA, USA.

[2] **Amoli, P.** (2016). An Overview on Current Researches on Underwater Sensor Networks: Applications, Challenges and Future Trends. *International Journal of Electrical and Computer Engineering (IJECE), 6*, 955.

[3] **Akyildiz, I., Pompili, D., & Melodia, T.** (2004). Challenges for Efficient Communication in Underwater Acoustic Sensor Networks. *Association for Computing Machinery, 1*(2), 3-8.

[4] **Heidemann, J., Ye, W., Wills, J., Syed, A., & Li, Y.** (2006). Research challenges and applications for underwater sensor networking. *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.* Las Vegas, NV, USA.

[5] **Akyildiz, I., Pompili, D., & Melodia, T.** (2006). State of the Art in Protocol Research for Underwater Acoustic Sensor Networks. *ACM SIGMOBILE Mobile Computing and Communications Review, 11*, 7-16.

[6] **Heidemann, J., Stojanovic, M., & Zorzi, M.** (2012). Underwater sensor networks: Applications, advances and challenges. *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 370*(1958), 158-175.

[7] **Li, N., Martínez, J.-F., Meneses, J., & Eckert, M.** (2016). A Survey on Underwater Acoustic Sensor Network Routing Protocols. *Sensors, 16*, 414.

[8] **Jinfeng, D., Zhongwen, G., Jiabao, C., & Guangxu, Z.** (2008). Optimum Transmission Range for Underwater Acoustic Sensor Networks. *2008 International Conference on Information Networking.* Busan, South Korea.

[9] **Mohammadi, Z., Soleimanpour-Moghadam, M., Askarizadeh, M., & Talebi, S.** (2020). Increasing the Lifetime of Underwater Acoustic Sensor Networks: Difference Convex Approach. *IEEE Systems Journal, 14*(3), 3214-3224.

[10] **Yang, H., Zhou, Y., Hu, Y.-H., Wang, B., & Kung, S.-Y.** (2018). Cross-Layer Design for Network Lifetime Maximization in Underwater Wireless Sensor Networks. *2018 IEEE International Conference on Communications (ICC).* Kansas City, MO, USA.

[11] **Kartha, J., Jabbar, A., Baburaj, A., & Jacob, L.** (2015). Maximum lifetime routing in underwater sensor networks using mobile sink for delay-tolerant applications. *TENCON 2015 - 2015 IEEE Region 10 Conference.* Macao, China.

[12] **Han, G., Jiang, J., Sun, N., & Shu, L.** (2015). Secure communication for underwater acoustic sensor networks. *IEEE Communications Magazine, 53*(8), 54-60.

[13] **Cong, Y., Yang, G., Wei, Z., & Zhou, W.** (2010). Security in Underwater Sensor Network. *2010 International Conference on Communications and Mobile Computing.* Shenzhen, China.

[14] **Sawwashere, S., & Nimbhorkar, S.** (2014). Survey of RTS-CTS Attacks in Wireless Network. *Fourth International Conference on Communication Systems and Network Technologies.* Bhopal, India.

[15] **Yang, G., Dai, L., & Wei , Z.** (2018). Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks. *Sensors, 18*(11), 3907.

[16] **Domingo, M.** (2011). Securing underwater wireless communication networks. *IEEE Wireless Communications, 18*(1), 22-28.

[17] **Hu, Y.-C., Perrig, A., & Johnson, D.** (2006). Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 370-380.

[18] **Yang, G., Dai, L., Si, G., Wang, S., & Wang, S.** (2019). Challenges and Security Issues in Underwater Wireless Sensor Networks. *Procedia Computer Science, 147*, 210-216.

[19] **Jiang, S.** (2019). On Securing Underwater Acoustic Networks: A Survey. *IEEE Communications Surveys & Tutorials, 21*(1), 729-752.

[20] **Kao, J.-c., & Marculescu, R.** (2006). Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks. *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks.* Reston, VA, USA.

[21] **Kulhandjian, H., Melodia, T., & Koutsonikolas, D.** (2014). Securing underwater acoustic communications through analog network coding. *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, (pp. 266-274). Singapore.

[22] **Lu, Y., Pu, L., Peng, Z., & Shi, Z.** (2016). RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements. *IEEE Communications Magazine, 54*(2), 32-38.

[23] **Wang, Q., Dai, H.-N., Li, X., Wang, H., & Hong, X.** (2016). On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks. *Sensors, 16*, 721.

[24] **Wang, C., & Wang, Z.** (2016). Signal Alignment for Secure Underwater Coordinated Multipoint Transmissions. *IEEE Transactions on Signal Processing, 64*(23), 6360-6374.

[25] **Ghannadrezaii, H., & Bousquet, J.-F.** (2018). Securing a Janus-Based Flooding Routing Protocol for Underwater Acoustic Networks. *OCEANS 2018 MTS/IEEE.* Charleston, SC, USA.

[26] **Feng, X., Wang, Z., & Han, N.** (2019). Protection Research of Sink Location Privacy in Underwater Sensor Networks. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* Paris, France, France.

[27] **Ye, Y., Peng, Z., Kumar P, A., A. R., V., & Hong, X.** (2019). Active Jamming for Eavesdropping Prevention in Underwater Wireless Networks. *WUWNET'19: International Conference on Underwater Networks & Systems.* Atlanta, GA, USA.

[28] **Li, X., Zhou, Y., Yan, L., Zhao, H., Yan, X., & Luo, X.** (2020). Optimal Node Selection for Hybrid Attack in Underwater Acoustic Sensor Networks: A Virtual Expert-Guided Bandit Algorithm. *IEEE Sensors Journal, 20*(3), 1679-1687.

[29] **Karakurt, Y., Yıldız, H. U., & Tavlı, B.** (2018). The impact of mitigation of eavesdropping on wireless sensor networks lifetime. *2018 26th Signal Processing and Communications Applications Conference (SIU).* İzmir, Türkiye.

[30] **Coutinho, R., Boukerche, A., Vieira, L., & Loureiro, A.** (2016). Design guidelines for opportunistic routing in underwater networks. *IEEE Communications Magazine, 54*(2), 40-48.

[31] **Sendra, S., Lloret, J., Jimenez, J., & Parra, L.** (2016). Underwater Acoustic Modems. *IEEE Sensors Journal, 16*(11), 4063-4071.

[32] **Quazi, A., & Konrad, W.** (1982). Underwater acoustic communications. *IEEE Communications Magazine, 20*(2), 24-30.

[33] **Akyildiz, I., Pompili, D., & Melodia, T.** (2005). Underwater Acoustic Sensor Networks: Research Challenges. *Ad Hoc Networks, 3*(3), 257-279.

[34] **Murad, M., Sheikh, A., Manzoor, M., Felemban, E., & Qaisar, S.** (2014). A Survey on Current Underwater Acoustic Sensor Network Applications. *International Journal of Computer Theory and Engineering, 7*, 51-56.

[35] **Felemban, E., Shaikh, F., Qureshi, U., Sheikh, A., & Qaisar, S.** (2015). Underwater Sensor Network Applications: A Comprehensive Survey. *International Journal of Distributed Sensor Networks*, 1-14.

[36] **Casey, K., Lim, A., & Dozier, G.** (2008). A Sensor Network Architecture for Tsunami Detection and Response. *International Journal of Distributed Sensor Networks, 4*, 27-42.

[37] **Kantorovich, L.** (1960). Mathematical Methods of Organizing and Planning Production. *Management Science, 6*(4), 363-505.

[38] **Hitchcock, F.** (1941). The Distribution of a Product from Several Sources to Numerous Localities. *Journal of Mathematics and Physics, 20*, 224-230.

[39] **Dantzig, G.** (2002). Linear Programming. *Operations Research, 50*(1), 42-47.

[40] **Chinneck, J.** (2006). *Practical Optimization: A Gentle Introduction.* Carleton University.

[41] **Nash, S.** (1998). Nonlinear Programming. *OR/MS Today, 25*(3), 36-45.

[42] **"*MATLAB - Mathworks*"** [Çevrimiçi]. Url: www.mathworks.com/products/matlab.html. [1 Ocak 2021'de erişildi].

[43] **"*IBM® Cplex Solver*"** [Çevrimiçi]. Url: https://www.ibm.com/tr-tr/analytics/cplex-optimizer. [7 Şubat 2021'de erişildi].

[44] **"*FICO® Xpress Solver*"** [Çevrimiçi]. Url: https://www.fico.com/en/products/fico-xpress-solver. [6 Şubat 2021'de erişildi].

[45] **"*GAMS*"** [Çevrimiçi]. Url: www.gams.com/products/gams/gams-language. [1 Ocak 2021'de erişildi].

[46] **Ferris, M., Jain, R., & Dirkse, S.**, "*GDXMRW: Interfacing GAMS and MATLAB*" [Çevrimiçi]. Url: http://pages.cs.wisc.edu/~ferris/matlab/gdxmrw.pdf. [7 Şubat 2021'de erişildi].

[47] **Wang, Q., & Dai, H.-N.** (2017). On modeling of eavesdropping behavior in underwater acoustic sensor networks. *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM).* Macau, China.

[48] **Yıldız, H. U., Tavlı, B., & Yanıkömeroğlu, H.** (2016). Transmission Power Control for Link-Level Handshaking in Wireless Sensor Networks. *IEEE Sensors Journal, 16*(2), 561-576.

[49] **Khan, J., & Cho, H.-S.** (2014). A data gathering protocol using AUV in underwater sensor networks. *OCEANS 2014 - TAIPEI.* Taipei, Taiwan.

[50] **Khan, M., Javaid, N., Majid, A., Imran, M., & Alnuem, M.** (2016). Dual Sink Efficient Balanced Energy Technique for Underwater Acoustic Sensor Networks. *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA).* Crans-Montana, Switzerland.

[51] **Brennan, C.**, "R2Sonic LLC Multibeam Training – Basic Acoustic Theory," [Çevrimiçi]. Url: https://www.r2sonic.com/wp-content/uploads/2020/03/Basic-Acoustic-Theory.pdf. [23 Ocak 2021'de erişildi].

[52] **Sehgal, A., Cernea, D., & Birk, A.** (2010). Modeling underwater acoustic communications for multi-robot missions in a robotics simulator. *OCEANS'10 IEEE SYDNEY.* Sydney, NSW, Australia.

[53] **Stojanovic, M.** (2006). On the Relationship Between Capacity and Distance in an Underwater Acoustic Communication Channel. *ACM SIGMOBILE Mobile Computing and Communications Review, 11*, 41–47.