TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GİZLİ ANAHTAR ŞİFRELEMESİ KULLANAN SUALTI AKUSTİK ALGILAYICI AĞLARDA KRİTİK DÜĞÜMLERİN AĞ YAŞAM SÜRESİNE ETKİLERİNİN ÖZGÜN BİR ENİYİLEME ÇERÇEVESİ TASARLANARAK İRDELENMESİ

YÜKSEK LİSANS TEZİ

Burak Emre ÜN

Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Bülent TAVLI

NİSAN 2022

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Burak Emre ÜN

ÖZET

Yüksek Lisans Tezi

GİZLİ ANAHTAR ŞİFRELEMESİ KULLANAN SUALTI AKUSTİK ALGILAYICI AĞLARDA KRİTİK DÜĞÜMLERİN AĞ YAŞAM SÜRESİNE ETKİLERİNİN ÖZGÜN BİR ENİYİLEME ÇERÇEVESİ TASARLANARAK İRDELENMESİ

Burak Emre ÜN

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

Danışman: Ünvan. Prof. Dr. Bülent TAVLI

Tarih: Mart 2022

Okyanuslar ve denizler dünya yüzeyinin yaklaşık yüzde yetmişini kaplamaktadır. Günümüzde sualtı yaşamı hala birçok bilinmezlik barındırmasıyla sayısız keşif imkanı sağlamaktadır. 20 yy. sonlarına doğru yarı iletken teknolojisinin ilerlemesi üretim maliyetlerinin büyük ölçüde azaltmıştır. Donanımların maliyetlerinin düşmesi algılayıcı ağların popülerliğini arttırmıştır. Fakat sualtındaki yüksek basınç, aşınma vb. zorlu koşullar nedeniyle bu tarz ortamlara uygun algılayıcıları tasarlamak zorlu ve maliyetli bir iştir. Buna ek olarak algılayıcıları bu bölgelere yerleştirmek ve bakımını yapmak kalifiye ve maliyetli işçilik gerektirmektedir.

Sualtı Akustik Algılayıcı Ağlar (SAAA) genellikle zor ortamlara seyrek olarak dağıtılırlar. Bir kere dağıtıldıktan sonra algılayıcılara erişim kısıtlıdır. Algılayıcı düğümler arası gönderilen verilerin güvenliği veri paketlerinin şifrelenmesi ile sağlanır. Su altına dağıtılan algılayıcı düğümlerin sınırlı donanımları sebebiyle hafızaları kısıtlıdır. Hafıza kısıtı nedeniyle her düğümde gizli anahtar kümesinin sadece belirli bir kısmı bulunur. Güvenli bağlantının sağlanabilmesi için sadece iki

düğüm birbirine veri gönderebilecek mesafede olması yetmez ayrıca aynı gizli anahtarı da bulundurması gerekir. Ana istasyon tüm gizli anahtarları barındırdığı için algılayıcı düğümler topladıkları verileri direkt olarak ana istasyona gönderebilirler. Buna ek olarak topladıkları verileri aynı gizli anahtarı paylaştığı yani güvenli bağlantı kurabildiği diğer algılayıcı düğümler üzerinden de ana istasyona gönderebilirler. Ağdaki düğümlerin hepsi güvenli bağlantı kuramadıkları için birbirleriyle haberleşemezler. Bu durum ana istasyona giden veri aktarım yollarının (diğer düğümler üzerinden) azalmasına sebep olur. Güvenli bağlantı kısıtından dolayı azalan veri aktarım yolları nedeniyle düğümler veri paketlerini aktarırken enerji olarak en verimli yolu kullanamazlar ve aktarım sırasında olması gerekenden daha fazla enerji harcarlar. Algılayıcı sensörlerin bataryaları limitli olması nedeniyle aktarım için harcadıkları enerji arttıkça ağın yaşam süresi kısalır. Azalan veri aktarım yolları ağı kritik düğüm saldırılarına daha açık hale getirir. Ağdaki en kritik düğümün etkisiz hale getirilmesi ağın yaşam süresini önemli ölçüde azaltmaktadır. Bu çalışmada gizli anahtar şifrelemesi kullanan Sualtı Akustik Algılayıcı Ağlarda kritik düğümün ağ yaşam süresine etkileri doğrusal programlama (DP) modeli oluşturularak ağın büyüklüğü, anahtar paylaşma olasılıkları ve kritik düğüm sayısı gibi farklı parametrelerle incelenmiştir.

Anahtar Kelimeler: Sualtı akustik algılayıcı ağlar, Ağ güvenliği, Gizli anahtar şifrelemesi, Düğüm yakalama saldırıları, Kritik düğümler, Akustik haberleşme kanalı, Yaşam süresi eniyileme, Doğrusal programlama (DP).

ABSTRACT

Master of Science

DESIGN OF A NOVEL OPTIMIZATION FRAMEWORK FOR THE ANALYSIS OF THE IMPACT OF CRITICAL NODES ON NETWORK LIFETIME OF UNDERWATER ACOUSTIC SENSOR NETWORKS UTILIZING PRIVATE KEY CRYPTOGRAPHY

Burak Emre ÜN

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 2022

Oceans and seas cover approximately 70% of the earth's surface. However, there are still a lot of unknowns about underwater life, which means there are a lot of opportunities for exploration. Semiconductor technology progressed rapidly toward the end of the twentieth century, lowering production costs dramatically. Due to harsh conditions such as high pressure, abrasion, and other factors, designing sensors suitable for such environments is a difficult and costly task. Furthermore, deploying and maintaining sensors in these areas necessitates highly skilled and expensive labor. Underwater Acoustics Sensor Networks (UASN) are usually deployed sparsely in harsh underwater environments. Their access is restricted once the network is deployed. The encryption of the data packets ensures the security of the data sent between the nodes. Because sensor nodes have limited memory, each node only has a subset of the keys distributed across the entire network. In a secure communication scheme, two nodes must not only be at a certain distance from each other to send data, but they must also share the same secret key. As a result, only a portion of the physical

links are available and can be used for secure communications. Since the sink node contains all the secret keys in the pool, the sensor nodes can send the data they collect directly to the sink node. In addition, they can send their gathered data to the sink node via other sensor nodes that have established a secure connection. Due to the secure connection constraint, available data transmission paths are limited, and nodes are unable to use the best transmission path when transferring data packets, consuming more energy than they should. Because the sensor's batteries are limited, the network's lifetime shortens as more energy is consumed for transmission. The effects of incapacitating the critical node on network lifetime in UASNs with incomplete secure connectivity were investigated using a linear programming (LP) model with various parameters such as network size, key sharing probabilities, and the number of critical nodes.

Keywords: Underwater acoustic sensor networks, Network security, Private key cryptography, Node capture attacks, Critical nodes, Acoustic communication channel, Network lifetime optimization, Linear programming (LP)

TEŞEKKÜR

Hayatım boyunca desteklerini esirgemeyen aileme ve tez çalışmalarım boyunca fikirleri, yönlendirmeleri, katkı ve yardımlarıyla sürekli desteklerini hissettiğim değerli danışmanlarım Prof. Dr. Bülent TAVLI ve Doç. Dr. Hüseyin Uğur YILDIZ'a sonsuz şükranlarımı sunarım. Ayrıca yüksek lisans hayatım boyunca desteklerini esirgemeyen TOBB Ekonomi ve Teknoloji Üniversitesi Elektrik ve Elektronik Bölümü öğretim üyelerine, Alper ÖZMEN, Duygu ÖZMEN ve Mert KAYIŞ'a çok teşekkür ederim. Son olarak çalışanlarını geliştirme hedefiyle akademik programları destekleyen ASELSAN'a teşekkür ederim.

İÇİNDEKİLER

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

KISALTMALAR

DP	**:** Doğrusal Programlama
GAMS	**:** Genel Cebirsel Modelleme Sistemi (İng. General Algebraic Modeling System)
GPS	**:** Küresel Konumlandırma Sistemi (İng. Global Positioning System)
IoT	**:** Nesnelerin İnterneti (İng. Internet of Things)
KAA	**:** Kablosuz Algılayıcı Ağ
LP	**:** Doğrusal Programlama (İng. Linear Programming)
MAC	**:** Ortam Erişim Kontrolü (İng. Medium Access Control)
MATLAB	**:** Matris Laboratuvarı (İng. Matrix 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
TCP	**:** Aktarım Kontrol Protokolü (İng. Transmit Control Protocol)
UASN	**:** Sualtı Akustik Algılayıcı Ağ (İng. Underwater Acoustic Sensor Network)

SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
$A(d_{ij}, f)$	d_{ij} mesafesinde f frekansında gerçekleşen akustik zayıflama
$\alpha(f)$	Soğurma katsayısı
d_e	SAAA'nın taban kenar uzunluğu
d_{ij}	Düğüm-i ile düğüm-j arsaındaki mesafe
d_{max}	Maksimum haberleşme mesafesi
ε_{bat}	Batarya enerjisi
f	Çalışma frekansı
h	SAAA'nın derinliği
t	Ağ yaşam süresi
P_{ksp}	Anahtar dağılım oranı
P_0	Alıcı düğüm girişinde ihtiyaç duyulan güç
$\mathcal{V}$	Ağdaki tüm düğümlerin kümesi
$\mathcal{W}$	Ana istasyon hariç ağdaki tüm düğümlerin kümesi
$\mathcal{A}$	Ana istasyon düğümü, tüm algılayıcı düğümleri ve birbirleriyle olan bütün bağlantıları ifade eden küme
s_i	Veri oluşturma hızı
N_c	Ele geçirilen düğüm sayısı
κ	Dağılım faktörü
$\tilde{\varepsilon}$	Ortalama enerji tüketim fazlalığını
$\tilde{d}_s$	Ele geçirilen düğümün ana istasyona göre ortalama normalize edilmiş uzaklığı

1. GİRİŞ

Yarı iletken teknolojisinin hızla gelişmesiyle kablosuz algılayıcı ağların oluşturulması için gereken uygun maliyetli, haberleşme ve veri toplama/işleme algoritmalarını çalıştırmak için yeterli miktarda işlem gücüne sahip küçük boyutlu cihazların sayısı gün geçtikçe artmaktadır. Bu cihazlarla birlikte Nesnelerin İnterneti (İng. Internet of Things IoT), kablosuz algılayıcı ağlara olan ilgi artmıştır. 20. yy. sonlarına doğru bu alanlardaki hem akademik araştırmalar hemde ticari kullanımları hızla artmıştır. Bu araştırmaların birçoğu bu tez kapsamında kablosuz algılayıcı ağlar (KAA'lar) olarak bahsedeceğimiz Karasal Kablosuz Algılayıcı Ağlara odaklanmıştır. Çünkü sualtı ortamın zorlu yapısı, veri iletimindeki sıkıntılar, ekipman maliyetleri, düğümlerin bakımı ve yerleştirilmesi gibi durumlar KAA'lara göre daha zordur. [1]'de yapılan çalışmada Sualtı Akustik Algılayıcı Ağlar (SAAA'lar) hakkında bilimsel dergilerde yayınlanan çalışmaların yıllara göre dağılımı verilmiş ve arttığı gözlemlenmiştir.

KAA'lar SAAA'lara göre uzun süredir çalışılan ve daha iyi bilinen bir konudur. Fakat KAA'da edinilen kazanımların birçoğu direkt olarak SAAA'lara aktarılamamaktadır. Genel hatlarıyla birbirlerine benzeselerde haberleşme ortamı ve haberleşmede kullanılan dalga tipleri gibi farklılıklara sahiptirler. Bu nedenle KAA'larda çözüme kavuşturulmuş birçok problemin SAAA'lar için tekrar değerlendirilmesi gerekmektedir.

SAAA'lar gerçekleştirilecek uygulamaya göre sualtına genelde seyrek dağıtılarak yerleştirilen algılayıcı düğümler ve su yüzeyine kalacak şekilde yerleştirilmiş bir ya da daha fazla sayıda ana istasyondan oluşurlar. Algılayıcı düğümler çoğunlukla seyrek dağıtıldıkları için her düğüm topladığı verileri ana istasyona direkt iletebilecek mesafede olmayabilir. Bu yüzden birden fazla atlamaya dayalı iletişim modelleri kullanır. Topladığı verileri iletmek isteyen algılayıcı düğüm ana istasyona erişemeyeceği mesafede ise verileri başka bir algılayıcı düğüm üzerinden ana istasyona iletir. SAAA'larda zorlu kanal koşulları nedeniyle elektromanyetik dalgalar yerine akustik dalgalar tercih edilir. Elektromanyetik dalgalar ve akustik dalgalar arasında fiziksel farklılıklar bulunsada temelde veri iletirken iki dalga tipindede veri

taşıyıcı dalgaya uygulanan faz, frekans veya genlik modülasyonlarıyla iletilir. Akustik haberleşme kaynaklı veri iletim sürelerindeki yüksek ve değişken gecikme, sınırlı bant genişliği, yüksek hata oranları ve sualtı ortamının değişkenliği KAA'lar için geliştirilmiş birçok iletim modeli SAAA'larda kullanılamalasına sebep olmaktadır. Son yıllardaki SAAA'lara artan ilgi sualtı haberleşmesine uygun tasarlan haberleşme protokollerinin artması sağlayacaktır. Bu sayede dünya yüzeyinin yaklaşık %70'ini kaplayan okyanus ve denizlerin araştırılması için yeni ufuklar açacaktır.

1.1 Tezin Amacı

Tezin amaçları ve özgün değeri şu maddelerle özetlenebilir:

1. Literatürde, SAAA'larda anahtar havuzunun kısıtlı olduğu (yani düğümlerin ancak ağdaki tüm düğümlerin bir alt kümesiyle doğrudan iletişim kurabilme durumunda ki bu güvenlik açısında gerekli bir durumdur) durumda ağ yaşam süresi henüz irdelenmemiştir. Her düğüm ağdaki tüm diğer düğümlerle doğrudan haberleşebilseydi eğer tek bir düğümün bir saldırganın kontrolüne geçmesiyle ağın tüm güvenlik altyapısı anlamsızlaşırdı. Dolayısıyla irdelenecek olan ilk konu; iki düğümün doğrudan haberleşmesi olasılığının yaşam süresine etkisinin irdelenmesidir. Doğrudan haberleşme olasılığı da toplam anahtar havuzu büyüklüğü ile her bir düğümdeki anahtar havuzunun büyüklüğü ile ilintilidir. Sonuçta, SAAA'larda iki düğüm arası doğrudan haberleşebilme olasılığı ile ağ yaşam süresi arasındaki ödünleşmenin eniyi şartlar altında karakterize edilip modellenmesi literatürde daha önce incelenmemiş özgün bir konudur.
2. Gizli haberleşme için kısıtlı büyüklükteki anahtar havuzu kullanılması ağdaki çoğu fiziksel bağın (İng. physical link) mantıksal bağ (İng. logical link) olarak kullanılamaz olmasına neden olmaktadır. Dolayısıyla böylesi bir ağda bazı düğümlere (tüm düğümlerin birbirleriyle haberleşebilmesi durumuna göre) aşırı yüklenilmesi olasılığı yükselmektedir. Sonuçta SAAA'larda sınırlı anahtar havuzu kullanılması nedeniyle kritiklik durumu artan düğümlerin (ki belki de bu düğümler mantıksal olarak haberleşememe durumu olmasaydı kritik düğümler olmayabilirlerdi) kaybının SAAA yaşam süresine etkileri literatürde daha önce hiç araştırılmamış özgün bir araştırma konusudur.

Bu tez kapsamında yukarıdaki iki araştırma sorusu tümleşik olarak irdelenmiş ve elde edilen bulgular değerlendirilmiştir.

1.2 Tezin Organizasyonu

Yapılan tez çalışmasının organizasyonu aşağıdaki şekilde yapılmıştır;

1. bölümde bu tez çalışmasının amacı, organizasyonu ve literatür araştırılmasına yer verilmiştir.
2. bölümde SAAA'lara genel bakış, KAA'lardan farkları ve karakteristiği, kullanım alanlarına yer verilmiştir.
3. bölümde matematiksel programlama ve optimizasyon konularının tarihi, kullanılan temel matematiksel programlama türleri, problemleri çözümlemek için kullanılan MATLAB ve GAMS programları hakkında kısaca bilgilere yer verilmiştir.
4. bölümde bu tez çalışması kapsamında oluşturulan problemin tanımı, ağ topolojisi, anahtar dağılımı, enerji tüketim modeli, düğüm etkisiz hale getirme algoritması ve ağ yaşam süresinin en iyileme modeli anlatılmıştır.
5. bölümde yapılan çalışma sonrası ortaya çıkarılan bulgular incelenmiş ve değerlendirmeler yapılmıştır.
6. bölümde bu tez kapsamında elde edilen sonuçlar özetlenmiştir.

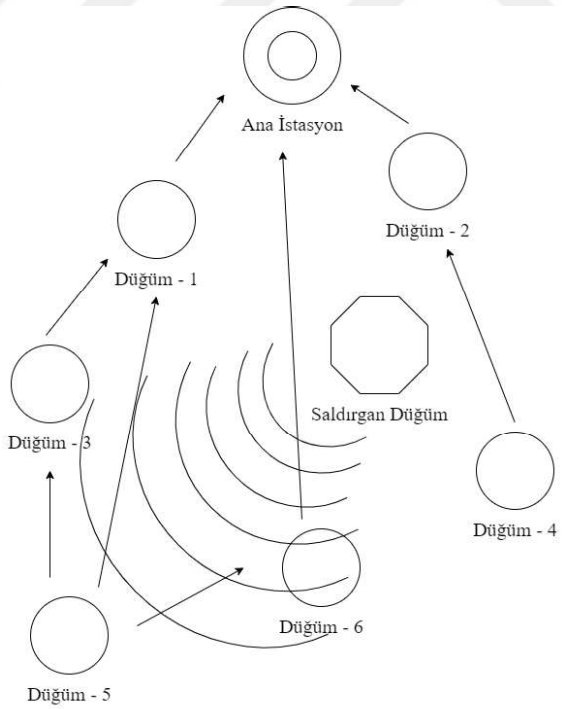
1.3 Literatür Araştırması

SAAA'lar yapıları, işlevleri, işlem güçleri ve enerji sınırlamaları gibi özellikler açısından KAA'lar ile benzerdir. Fakat algılayıcı düğümler birbirleri ile haberleşirken elektromanyetik dalgalar yerine akustik dalgaları kullanmasından dolayı çeşitli zorluklar vardır. Bunların başlıcaları;

- Akustik dalgaların sualtında yayılma hızları elektromanyetik dalgaların havada yayılmasına göre çok yavaştır.
- Akustik haberleşme kanalları düşük bant genişliğine sahiptir. Çok-yolluluk ve zayıflama gibi etkiler bağlantı kalitesini ciddi ölçüde düşürmektedir.

- Sualtında bulunan algılayıcı düğümler akıntılar ve çevresel etkenlerden dolayı oldukça hareketlidir. Küresel Konumlandırma Sistemi (İng. Global Positioning System - GPS) 1.5 GHz frekansında çalıştığı için sualtında kullanılamaz. Bu yüzden sualtında bulunan algılayıcı düğümlerin konumlarının hassas olarak bilinmesi karasal olanlara göre daha zordur.
- Sualtı donanımlarının maliyetleri karasal donanımlara oranla daha yüksek olduğu için seyrek yerleştirilirler.
- Akustik haberleşme elektromanyetik haberleşmeye göre daha fazla enerji harcar. Genellikle sualtı algılayıcı düğümleri arasındaki mesafe fazla olduğu için verilerin iletilmesi sırasında yüksek miktarda enerji kullanılır.

Bu zorluklar dikkate alındığında çeşitli ağ güvenliği problemleri oluştuğu görülmektedir. Literatürde bu konu hakkında [2-6] gibi geniş çaplı yapılmış birçok araştırma bulunmaktadır. Katman tiplerine göre sınıflandırılmış saldırı tipleri Çizelge 1.1'de verilmiştir. Bu saldırı tiplerine değinecek olursak;

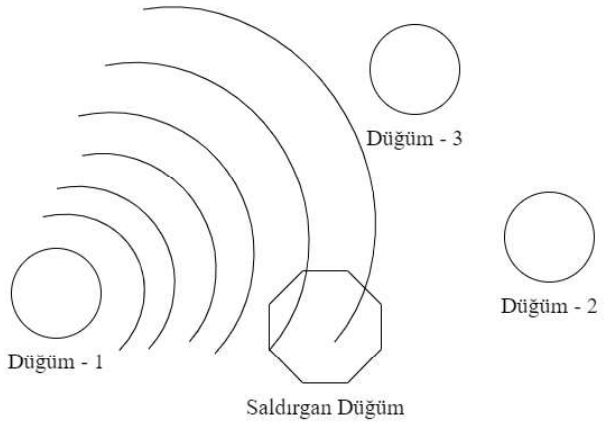


Şekil 1.1 : SAAA'larda temsili bir karıştırma saldırısı

- Fiziksel Katman Saldırıları: Akustik dalgaların düşük bant genişliği ve yüksek iletim mesafelerinden yararlanılarak yapılan saldırılardır. Bunlara örnek olarak

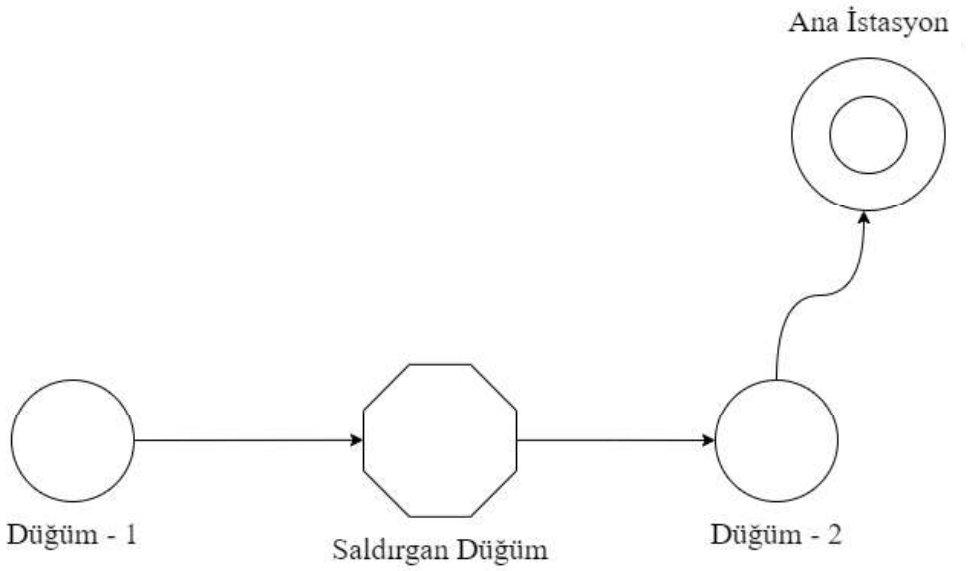
karıştırma (İng. Jamming) ve gizli dinleme (İng. Eavesdropping) saldırıları örnek olarak gösterilebilir.

- Karıştırma Saldırısı: Saldırgan düğüm hedef düğüme aynı frekans bandında anlamsız sinyaller gönderir. Akustik kanal bant genişliği düşük olduğu için SAAA'lar bu saldırılara oldukça dayanıksızdır. Akılsız (İng. Dummy) ve aldatıcı (İng. Deceptive) olmak üzere iki tip karıştırma saldırısı vardır. Akılsız karıştırma saldırının önüne geçebilmek için algılayıcı düğüm karıştırıldığını anlayarak uyku durumuna geçer. Aralıklı olarak karıştırmanın bitip bitmediğini kontrol eder. Karıştırma bittikten sonra topladığı verileri iletmeye devam eder. Aldatıcı karıştırma saldırısında karıştırıcı ağın durumunu dinleyerek veri iletilmeye başlandığı anda veri iletmeye başlar. Bu tip saldırıları tespit etmek oldukça zordur. Farklı frekans bantları kullanılarak karıştırıcı alt edilmeye çalışılır. Şekil 1.1'de gösterildiği gibi saldırgan düğüm kullanılan akustik kanala yüksek güç göndererek düğüm-3, düğüm-5 ve düğüm-6'nın diğer düğümlerle haberleşmesini engellemiştir.
- Gizli Dinleme Saldırısı: Bu saldırı tipinde saldırgan düğüm ağdaki verileri toplar. Bu saldırıyı tespit etmek olanaksızdır. Çünkü saldırgan düğüm ağa müdahale etmez akustik dalgaların doğası gereği iki düğüm arasında gönderilen sinyali toplar. Şekil 1.2'de gösterildiği gibi düğüm-1 tarafından yapılan yayınları saldırgan düğüm akustik haberleşmenin yapısı gereği kanala müdahale yapmadan verileri gizlice dinleyebilir.



Şekil 1.2 : SAAA'larda temsili bir gizli dinleme saldırısı

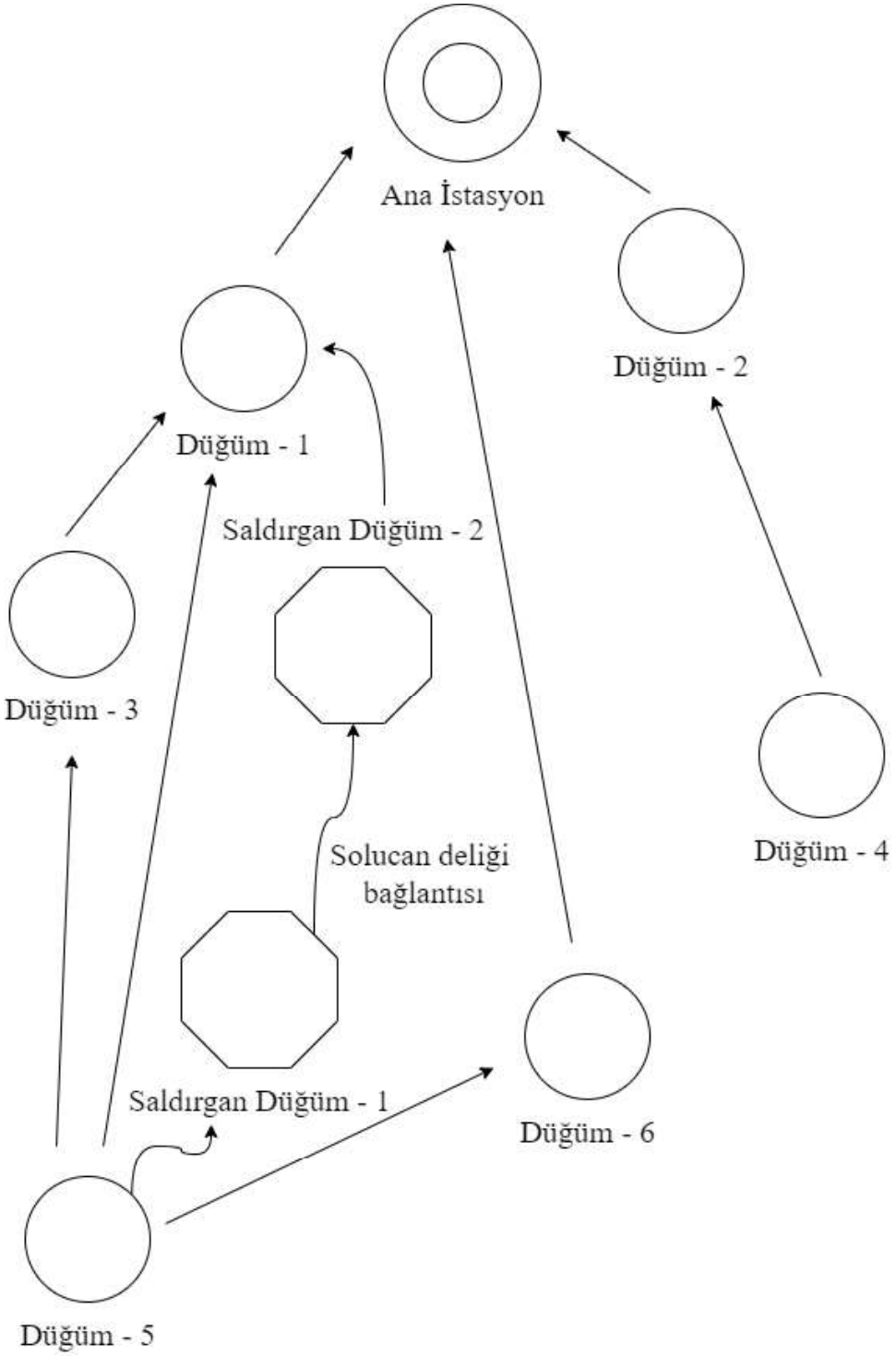
- Veri Bağı Katmanı Saldırıları: Karıştırma saldırılarına benzer saldırgan düğüm iki düğüm arasında iletilecek veriyi geciktirir ya da yanlış bilgiler ekler. Bu tip saldırılar düğümlerin ağ topolojisini karıştırmasına sebep olur. Düğümlerin aralarındaki mesafeyi olduğundan kısa az zannederek veri gönderirken daha düşük güçle iletmesi sağlar ve veri ana istasyona ulaşamadan ortadan kaybolur. Ya da düğümler arasındaki mesafeyi olduğundan uzak göstererek düğümün veri gönderirken fazla enerji tüketmesine ve bataryasını erken bitirmesine sebep olur. Bunlara örnek olarak solucan deliği, tekrarlama ve sybil saldırısı verilebilir.
    - Tekrarlama Saldırısı: Saldırgan düğüm ağda bulunan iki düğüm haberleşirken araya girer. Gönderici düğümden aldığı mesajı sahte gecikme ve sinyal gücü ile alıcı düğme iletir. Bu saldırı iki düğümün birbirini yanlış konumlandırmasına sebep olur. Şekil 1.3'te gösterildiği gibi saldırgan düğüm, düğüm-1 ile düğüm-2 arasına girerek tekrarlama saldırısını gerçekleştirir.



Şekil 1.3 : SAAA'larda temsili bir tekrarlama saldırısı

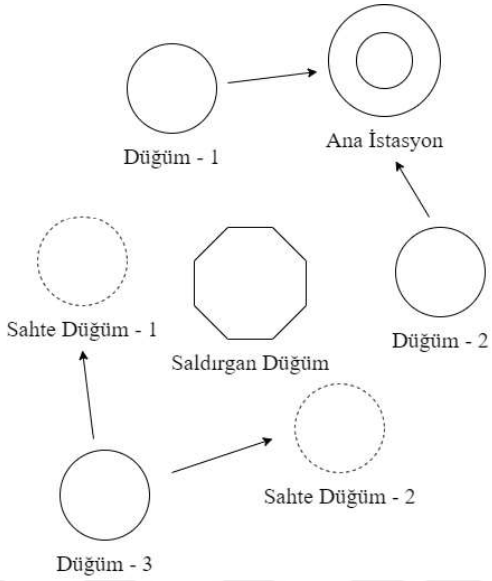
- Solucan Deliği Saldırısı: Saldırgan düğüm gönderi düğümden aldığı veriyi bant dışı daha düşük gecikmeli bir yolla solucan deliği bağlantısından gönderir. Bağlantının diğer tarafında bulunan başka bir saldırgan düğüm bu veriyi ağa yayar. Bu ağda bulunan düğümlerin birbirleri olduğundan yakın görmesine ve yanlış konumlandırmalarına

sebep olur. Şekil 1.4'te gösterildiği gibi saldırgan düğüm, düğüm-5'den aldığı veriyi solucan deliği bağlantısını kullanarak düğüm-1'e aktarmıştır.



Şekil 1.4 : SAAA'larda temsili bir solucan deliği saldırısı

- Sybil Saldırısı: Saldırgan düğün birden fazla kimlikle kendini ağda bulunmadığı konumlarda göstererek algılayıcı düğümlerin olmayan noktalara veri göndermesine sebep olur. (Şekil 1.5)



Şekil 1.5 : SAAA'larda temsili bir sybil saldırısı

- Zaman Senkronizasyonu ve MAC Saldırıları: Tekrarlama, solucan deliği ve sybil saldırıları ile aynı zamanda ağda bulunan zaman senkronizasyonu da bozulabilir. Saldırgan düğüm algılayıcı düğüme sürekli veri gönderme isteği (İng. Request to Send - RTS) göndererek enerjisini erken tüketmesini sağlar.

- Ağ Katmanı Saldırıları: Gönderilen paketi yönlendirme ve engelleme gibi saldırıları içerir. Bunlara örnek olarak kara/havuz delik (İng. Black/Sink Hole) ve seçmeli yönlendirme verilebilir.

  - Kara Delik Saldırısı: Saldırgan düğüm ağa daha kısa gözüken sahte yollar sunarak trafiği üzerine çeker. Bu şekilde gelen verileri analiz eder ve istediği paketleri iptal eder.

  - Seçmeli Yönlendirme Saldırısı: Saldırgan düğüm veriyi gönderen düğüme paketi aldığına dair bilgi döner. Elde ettiği paketi değiştirerek alıcı düğüme yanlış veri yollar ya da gelen paketi iptal eder. Bu şekilde gönderen düğüm paketin ulaştığını düşünmesine rağmen paket alıcı düğüme ulaşmamıştır.

- İletim Katmanı Saldırıları: Bu katmandaki saldırıların çoğu TCP üzerinden gerçekleşir. Saldırgan düğüm TCP üzerinden hedefteki düğüme sürekli bağlantı isteği yollar ve bu sayede hedefteki düğümün hafızasını doldurur. Ya da hedefteki düğüme sahte alındı bilgisi (İng. Acknowledgment) yollayarak gereksiz tekrar geri gönderimleri tetikler.

KAA'larda güvenliği sağlamak için düğüm yakalama saldırılarını tespit edecek sağlam ve güvenilir algoritmalar gereklidir. [7]'de çeşitli güvenlik önlemleri incelenmiştir. Varolan önlemlerin düğüm yakalama saldırılarını anlık olarak tespit edemediği ve bu alanda daha fazla çalışmaya ihtiyaç duyulduğu belirtilmiştir.

Ele geçirilmiş düğümlerle uğraşmak genellikle kablosuz algılayıcı ağ güvenliğinin önündeki en büyük zorluklardan biridir. [8]'de algılayıcı düğümlerin düşük maliyetlerinden ötürü düğüm yakalama saldırılarının etkisini azaltmak için tek seferlik algılayıcı konsepti geliştirilmiştir. Buradaki temel fikir düğüm içerisine yüklenen tek seferlik şifre ile düğüm ele geçirilse bile ağa en fazla bir adet yanlış mesaj gönderebilmesidir. Orman yangınlarını tespit gibi görevler için kullanılacak ağlarda algılayıcıların düşük maliyetlerinden yararlanarak oluşacak yangını o bölgeden gelen tek bir alarm mesajıyla değilde birden fazla algılayıcının belirli bir zaman içerisinde alarm mesajı göndermesiyle tespit edilebileceği vurgulanmıştır. Bu şekilde düğüm ele geçirilip alarm mesajı gönderilse bile sistem yanlış alarm üretmeyecektir. Tek seferlik algılayıcı konsepti algılayıcı düğümlerin sürekli mesaj göndermesi ve gönderdiği verinin güvenliğinin sağlanması gereken uygulamalar için uygun değildir.

Çoğu KAA uygulamasında düğümlerin hassas konum bilgisi gerekmektedir. Kullanılan konumlandırma algoritmalarının çoğunda yeri önceden bilinen düğümler kullanılarak geri kalan düğümlerin konumları belirlenmektedir. Fakat bu algoritmalar bazı düğümlerin düşman tarafından ele geçirilip yanlış bilgi ilettikleri durumda çalışmamaktadır. [9]'da bu tür düğüm yakalama ataklarına karşın az hesaplama gerektiren güvenli bir hassas konumlandırma algoritması geliştirilmiştir. Geliştirilen algoritma benzerleri ile karşılaştırıldığında daha az işlem gücü gerektirmesine karşın benzer hatta daha iyi sonuçlar vermektedir. Ayrıca geliştirilen algoritma hareketli ağlar için konumu önceden bilinen noktalara ihtiyaç duymadan düğümlerin göreceli konumlarını bulabilmektedir.

[10] numaralı çalışmada rastgele ve önden dağıtılmış anahtarlar kullanan ağlarda düğüm yakalama saldırısı sürecini modellemek için matris tabanlı bir yöntem geliştirilmiştir. Bu yöntemde düğümler ve iletim yollarını belirlemek için bir matrisler oluşturulur. En az enerji ile en efektif şekilde düğüm yakalamaya odaklanan algoritma oluşturulmuştur. Simulasyon sonuçları incelendiğinde enerji tüketimi ve saldırı süresinde düşüş sağlanarak saldırının verimliliği arttırılmıştır.

[11]'de düğüm yakalama saldırılarının tespiti için karma işlev tabanlı anahtarlar (İng. Hash-based keys) ve yapay rastsal fonksiyonlar (İng. pseudo random functions) kullanan yeni bir yaklaşım geliştirmiştir. Bu yaklaşımda düğümün üzerine yerleştirilen modül düğümde bulunan hafızayı kontrol eder ve doğrular. Bu sayede düşman tarafından ele geçirilen düğümün hafızasına eklenen kötücül yazılımları tespit eder. Yapılan deneysel çalışmalarla yakalanan düğümün bu kontrolden kaçmasının mümkün olmadığı gösterilmiştir. Ayrıca bu protokol ile yakalanan düğümün diğer düğümlerin verilerini açığa çıkarması da engellenmiş olur.

Algılayıcı düğümlerin yapısı ve hafıza kısıtları göz önünde bulundurulduğunda anahtar dağıtım modelleri oldukça basit olmalıdır. [12]'de algılayıcı ağlar için hem operasyonel hemde güvenlik gereklerini sağlayacak yeni bir anahtar dağıtım modeli geliştirilmiştir. Bu model yüksek hesaplama gücü ve haberleşme gerektirmeden anahtarların algılayıcı düğümlere dağıtımı, iptali ve yeniden anahtar dağıtımını sağlamaktadır. Bu yaklaşım oldukça ölçeklenebilir ve esnektir. Hedeflenen uygulamaya göre gereken hafıza ve istenilen bağlantı olasılığı ayarlanabilir. Temelde düğümler ilgili alana dağıtılmadan önce düğümlere anahtar havuzundan belirlenen miktarda rastgele anahtarlar dağıtılır. Aynı anahtarı paylaşan düğümler birbiriyle haberleşebilir. Bu modelde iki düğümün birbiriyle haberleşme olasılığı yani aynı anahtarı paylaşma olasılığı matematiksel olarak hesaplanabilir.

[13] numaralı çalışmada hareketli SAAA'lar için yeni bir anahtar dağıtım modeli geliştirilmiştir. Sonuçlar incelendiğinde hareketler geçici olarak ağ bağlantısında düşüşlere sebep olsa da oluşturulan model bağlantı performansının zamanla iyileşmesine izin vermektedir. Ayrıca oluşturulan modelle birlikte düğüm yakalama saldırılarına dirençli bir ağ oluşturulmuş. Yakalanan düğüm çevresindeki çok az sayıda bağlantının gizliliği ifşa edilmiş olur.

[14]'te SecFUN isimli SAAA için esnek ve ayarlanabilir bir güvenlik çerçevesi (İng. Security Framework) oluşturulmuştur. Her düğüm ana istasyonla aynı grup anahtarını ve bir gizli anahtarı paylaşır. Enerji tüketimi ve gecikme gibi parametrelerin analizi yapılmıştır. Sonuçlar incelendiğinde tam teşekküllü ve esnek SAAA'ların güvenlik çözümlerine uygun bir çözüm geliştirilmiştir.

SAAA'lar akustik haberleşmenin yapısı gereği gizlice dinleme ve sahte veri enjekte etme gibi tehditlere açıktır. Birçok farklı gizli anahtar yaklaşımının yanı sıra alınan sinyal gücü tabanlı anahtar üretimi anahtar dağıtımı gibi ihtiyaçları ortadan kaldırmaktadır. Çeşitli alınan sinyal gücü tabanlı anahtar üretimi yaklaşımları KAA'lar için oluşturulmuştur. [15]'te alınan sinyal gücü tabanlı anahtar üretimin sualtı ortamlar ve SAAA'lar için performans analizi yapılmış ve başlıca zorlukları incelenmiştir. Akustik dalgaların iletim gecikmelerinden dolayı RF dalgalara göre daha düşük anahtar oluşturma hızına sahiptirler. Ayrıca bu durum paylaşılan anahtarda yüksek bit uyumsuzluğuna sebep olmaktadır. Çok kanallı haberleşme modeli kullanarak birbiriyle haberleşen düğümler çoklu kanallardaki gizli bitleri kullanması sağlanarak anahtar oluşturma verimliliğini önemli ölçüde artırılmıştır. Ayrıca gelen sinyal filtreden geçirilerek iki düğüm arasındaki farklılıklar büyük ölçüde azaltılmıştır.

[16]'da ağdaki her bir düğüme kaç tane ve hangi anahtarın dağıtılacağına karar vermek için yeni bir deterministik altıgen tabanlı anahtar dağıtım yaklaşımı önerilmiştir. Önerilen yaklaşımın performans ve güvenlik özelliklerini analiz edilmiş ve altıgen tabanlı anahtar dağıtım yaklaşımının diğer yaklaşımlarla benzer olduğu gösterilmiştir.

SAAA'larda iletişim güvenliğini artırmak için [17]'de önerilen model tek yönlü karma işlev (İng. one-way hash function) ve kaotik haritalar (İng. chaotic maps) gibi temel şifreleme işlevlerini kullanarak karşılıklı kimlik doğrulama ve anahtar anlaşması sağlamıştır. Yapılan analizlerde düğüm yakalama saldırıları gibi birçok saldırıya karşı güvenli olduğu gösterilmiştir. Ayrıca yapılan performans analizi sonucunda diğer kaynak kısıtlı modellere göre daha verimli olduğu görülmüştür. [18]'de ise quantum ve simetrik şifreleme kullanılarak ağın güvenliği artırılmıştır.

Çizelge 1.1 : Ağ Katmanlarına Göre Tehditler ve Savunma Stratejileri ([5]'ten alınarak düzenlenmiştir.)

Katman	**Ana İşlev**	**Tipik Tehditler**	**Savunma Stratejileri**
Fiziksel	Sinyal haberleşmesi	Karıştırma [19] ve gizli dinleme [20]	Karıştırma tespit, verileri şifreleme
Veri Bağı	Ortam Erişim Kontrolü (İng. Medium Access Control - MAC), hata kontrolü	Tekrarlama, Solucan deliği [21], Sybil [3], Zamanlama senkronizasyonu ve Sürekli Veri Gönderme İsteği Saldırısı	Anormallik Tespiti, kimlik doğrulama
Ağ	Adresleme ve Yönlendirme	Kara Delik ve Seçmeli Yönlendirme Saldırısı [4]	Yönlendirme doğrulaması, çok-yollu yönlendirme
İletim	Uçtan uca iletim kontrolü, Akış ve Yığılma kontrolü	Sahte alındı ürteme, aktarım kontrol protokolü (İng. Transmit Control Protocol - TCP) oturumu ele geçirme	Uçtan uca kimlik doğrulama ve şifreleme

2. SUALTI AKUSTİK ALGILAYICI AĞLAR

2.1 Genel Bakış

Sualtı araştırmaları tarih boyunca insanlığın hep ilgisini çekmiş fakat zorlu şartları sebebiyle karasal ortam araştırmalarının gerisinde kalmıştır. Son yıllarda SAAA'lara artan ilgi ve ekipmanların gelişmesiyle araştırması maliyetli ve zorlu olan alanları incelemek için kullanılmaya başlanmıştır. Bunlara örnek olarak sualtı yaşamının izlenmesi, batık aramaları, sualtında bulunan kabloların ve boru hatlarının izlenmesi, su kirliliği takibi gibi sivil alanlara ek olarak yasaklı bölge kontrolü ve belirli alanların savunması gibi askeri uygulamalar verilebilir.

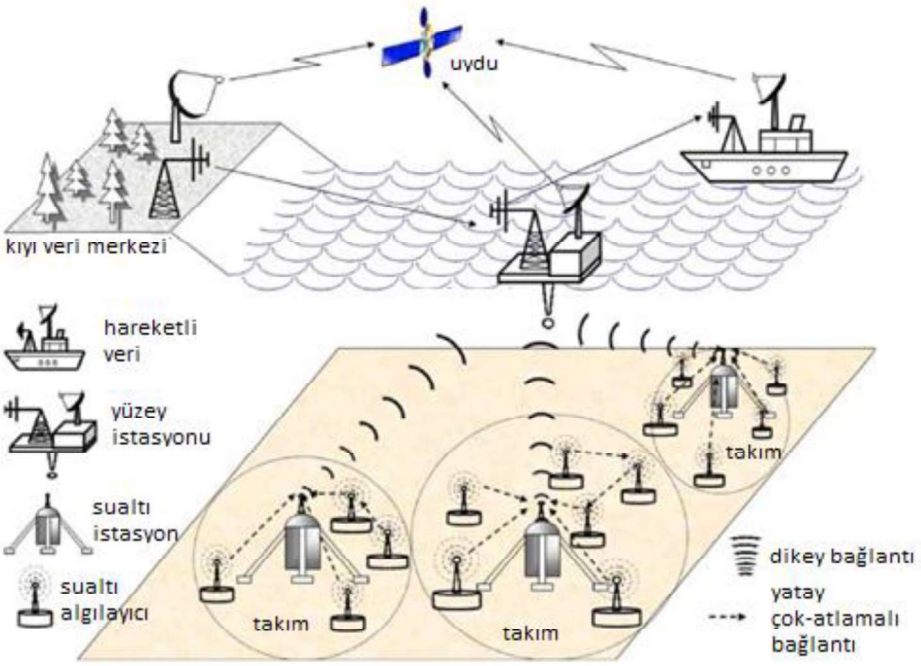
Yapılan ilk sualtı gözlemlerinde algılayıcılar belirlenen alana yerleştirilip belirlenen süre tamamlanana ya da bataryası bitene kadar bırakılır. Verileri üzerine yerleştirilen depolama birimine kaydetmesi sağlanır [22]. Bu yöntemin dezavantajları aşağıdaki gibi sıralanabilir.

1. Veriler sonradan toplandığı için gerçek zamanlı gözlem yapılamaz.
2. Algılayıcı yerleştirdikten sonra üzerinde herhangi bir iyileştirme, görev değişikliği ya da ek görev atama gibi değişiklikler yapılamaz.
3. Algılayıcı yerleştirildikten sonra cihaz donanımında ya da yazılımında oluşacak hata toplanana kadar farkedilemez.
4. Yapılacak ölçümde toplanacak verinin yoğunluğu ve sıklığı gibi parametreler algılayıcı düğümlerin depolama alanları ile sınırlıdır.

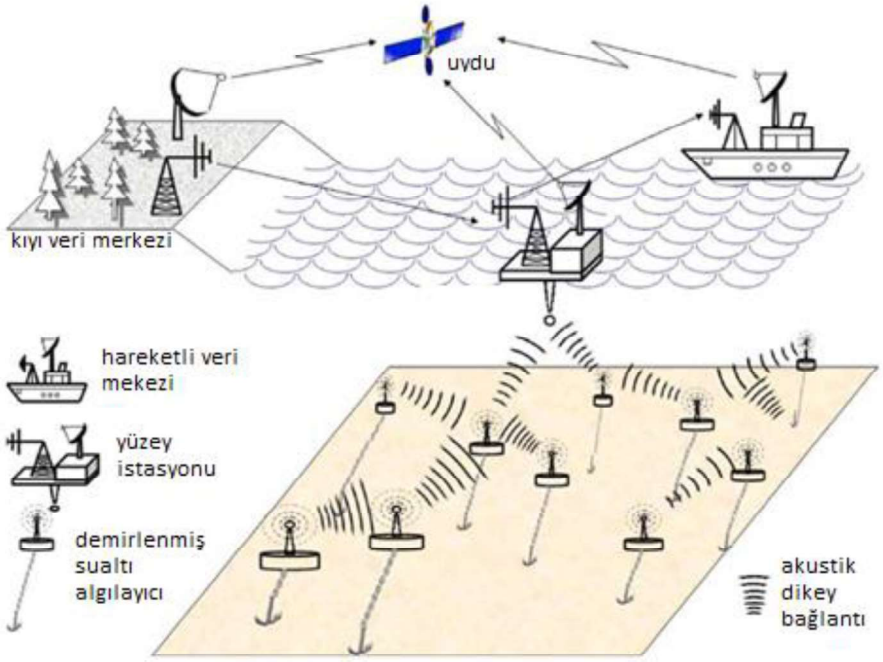
Bu yetenekleri kazandırmak amacıyla oluşturulan SAAA'lar genelde iki (Şekil 2.1) veya üç boyutlu (Şekil 2.2) olarak su altına yerleştirilirler. Su altına yerleştirilen algılayıcı düğümler topladıkları verileri direkt ya da başka bir algılayıcı düğüm üzerinden su yüzeyinde bulunan ana istasyona aktarırlar. Ağın tasarımına göre ana istasyon sayısı değişebilir. Ana istasyonda toplanan veriler RF dalgalar kullanılarak kıyıdaki ya da gemideki veri merkezlerine iletilir.

Algılayıcı düğümlerin topladıkları verileri direkt ana istasyona göndermesi ağ modelini kolaylaştırsa da enerji verimliliği açısından diğer algılayıcı düğümler üzerinden çok atlamalı şekilde ana istasyona iletmesi daha çok tercih edilir. Bunun yanı sıra algılayıcı düğümler topladıkları verileri ana istasyona direkt iletmeye çalışırken yüksek güç kullanacaktır. Bu nedenle ortaya çıkabilecek akustik dalgalardaki çarpışma durumları ağın işlem hacmini düşürecektir. Algılayıcı düğümlerin verileri alma ve gönderme, algılama ve işleme olmak üzere dört temel işlevi vardır. Sualtı algılayıcı düğümler için en çok enerji tüketen işlev verileri göndermektir. Bu işlevleri yerine getirebilmek için Şekil 2.3'de gösterilen altı temel bloktan oluşur. Bu blokların işlevleri aşağıdaki gibi kısaca özetlenebilir;

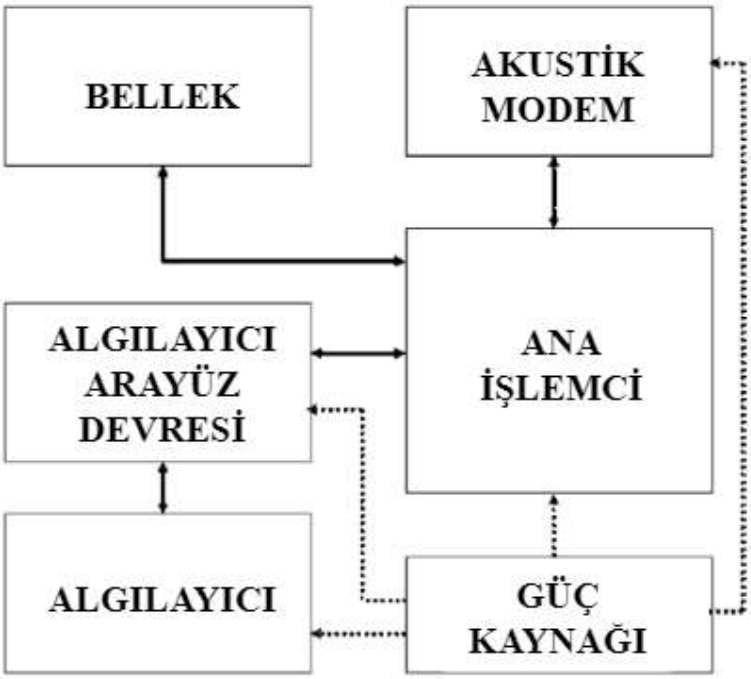
- Ana kontrolcü/işlemci: Algılayıcı düğüm üzerindeki tüm işlemleri kontrol eder. Sensör arayüz devresi üzerinden gerekli sensör okumalarını yapar ve bunları hafızaya kaydeder. Akustik modem üzerinden diğer sensörlerden gelen verileri işler. Gelen veriler ve kendi oluşturduğu verileri başka bir algılayıcı düğüme ya da ana istasyona gönderir.
- Hafıza: Sensörlerden ve diğer algılayıcı düğümlerden gelen verileri kaydetmeye yarar.
- Akustik Modem: Algılayıcı düğümün diğer düğümler ve ana istasyona olan haberleşmesinin fiziksel katmanını halleder. Ana kontrolcü tarafından oluşturulan dijital sinyaller analog sinyallere akustik modem üzerinden iletilir.
- Sensör Arayüz Devresi: Algılayıcı düğüm üzerinde bulunan bir ya da daha fazla sensörün ana kontrolcü ile haberleşmesi için gerekli devredir.
- Sensör: Algılayıcı düğümün ortamdan sıcaklık, basınç, suyun pH değeri gibi çeşitli verileri toplamasına yarayan donanımlardır. Teledyne Benthos [23] ve Aquatec [24] gibi firmaların örnek ürünleri vardır.
- Güç kaynağı: Algılayıcı düğüm içerisinde bulunan bataryadan gerekli enerjiyi alarak ana kontrolcü, sensör arayüz devresi ve sensörlerin çalışması için gereken voltaj çevrimlerini yapan bloktur.



Şekil 2.1 : Örnek iki boyutlu SAAA modeli ([25]'ten alınarak düzenlenmiştir.)



Şekil 2.2 : Örnek üç boyutlu SAAA modeli ([25]'ten alınarak düzenlenmiştir.)



Şekil 2.3 : Sualtı algılayıcı düğüm blok diyagramı ([25]'ten alınarak düzenlenmiştir.)

2.2 Kablosuz Algılayıcı Ağlar ile Farkları ve Karakteristiği

SAAA'lar ile KAA'lar birçok yönden birbirlerine benzeseler de temelde kilit farklılıkları vardır. Bunlardan ilki iletişim ortamıdır. KAA'lar tarafından kullanılan yüksek frekanslı elektromanyetik dalgalar sualtında hızla sönümlendikleri için sualtı haberleşmesinde kullanılmaz. Bu nedenle sualtı haberleşmesinde yüksek frekanslı elektromanyetik dalgalar yerine düşük frekanslı akustik dalgalar kullanılır. Fakat akustik dalgalar elektromanyetik dalgalardan oldukça yavaştır [25]. İkinci büyük fark sualtındaki algılayıcı düğümler karasal algılayıcı düğümlere göre bulundukları ortamdan dolayı daha fazla hareket ederler. Kullanılan akustik dalgalar sebebiyle KAA'lara göre bant genişliği çok düşüktür. Bu nedenle veri aktarım hızları da düşmektedir. Örneğin 1 km uzaklıktaki bir yere veri aktarım hızı yaklaşık 40 kb/s'dir [26].

Sualtı algılayıcı düğümlerin üzerinde oluşan paslanma, tortu birikimi, yosunlanma ve aşınma gibi etkiler veriler iletilirken hataya oranını artırır. Ayrıca deniz dibi ve deniz üstü dalgalar akustik dalgaları etkileyerek beklenenden farklı davranma ihtimali artırır.

Bu tarz etkiler sualtı haberleşmesinde yüksek hata oranlarına dolayısıyla veri kayıplarına neden olabilir. Basınç, sıcaklık ve tuzluluk arttıkça akustik dalgaların yayılım hızını artar [27].

Akustik dalgalar ile iletişimdeki zorluklara baktığımızda değişken ve yüksek iletim gecikmesi, doppler yayılımı, çok yolluluk, gürültü ve iletim yolu kayıpları öne çıkar. Bu etkiler sualtı haberleşmesinin zamansal ve mekansal değişimini belirler. Bu değişkenlik akustik haberleşmedeki bant genişliğini sınırlar ve büyük ölçüde mesafe ve frekansa bağımlı hale getirir.

Bu zorlukları incelendiğinde etkileri aşağıdaki gibi sıralanabilir; [25]

- İletim yolu kaybı
    - Temelde yayılan akustik dalganın ilerlerken ısı enerjisine dönüşerek sönümlenmesi ile oluşur. Ayrıca suyun derinliği, deniz dibi ve yüzeyinden kaynaklanan yankılanmalar, su yüzeyinin dalgalanması nedeniyle oluşabilecek dağılma ve kırılım gibi sebepler akustik dalganın zayıflamasında önemli rol oynar.
    - Geometrik yayılma frekanstan bağımsız olarak uzaklıkla artar. Genelde iki tip yayılma kullanılır. Bunlardan biri sığ sularda yatay olarak yayılma olarak adlandırılan silindirik yayılmadır. Diğeri ise derin sularda noktasal kaynak gibi davranarak yayılan küresel yayılmadır.
- Gürültü
    - Makine ve gemi motoru nedeniyle oluşan insan kaynaklı gürültüler.
    - Okyanus ya da denizde oluşan biyolojik ve sismik hareketler nedeniyle oluşan ortam gürültüsüdür.
- Çok yolluluk
    - İletim anında yansımalar sonucu akustik dalgalar üst üste binerek sinyalin bozulmasına sebep olur.
    - Alıcı ve göndericinin konumuna göre değişiklik gösterir.

- Değişken ve yüksek iletim gecikmesi
    - Akustik dalglar su altında yavaş iletilirler ve sıcaklık, tuz, derinlik gibi faktörlere bağlı olarak hızları değişir.
    - Bu yüksek gecikme ağdaki veri aktarım hızını büyük ölçüde azaltır ve verimli bir haberleşme protokolü tasarlamayı zorlaştırır.
- Doppler etkisi
    - Alıcı tarafında sembollerin birbirine karışmasına sebep olur. Bunları karışıklıkları gidermek için komplike sinyal işleme algoritmaları gerekir.

2.3 Kullanım Alanları

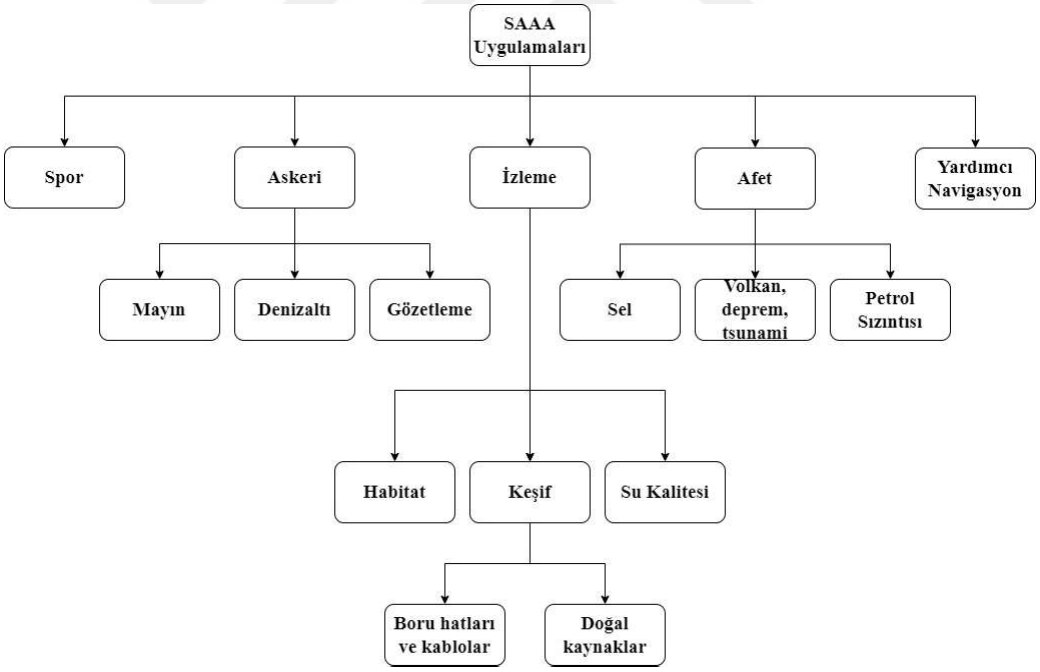
Şekil 2.4'de kapsamlı bir biçimde SAAA'ların uygulama alanları gösterilmiştir. Bu uygulama alanlarını kısaca açıklayacak olursak;

- İzleme Uygulamaları: Sualtı canlılarını ve okyanus akıntılarının takibi, kimyasal, biyolojik vb. kirlilik analizleri için kullanılabilirler [28]. Örneğin;
    - [29]'da alabalık çiftlikleri için su kalitesini izleyen bir uygulama geliştirilmiştir.
    - [30]'da içme suyu depolarındaki suyun kalitesini gözlemlemek için iki farklı yaklaşım geliştirmiştir.
    - [31]'de okyanus kirliliği ve batık tespiti için bir sistem geliştirilmiştir.
- Afet Uygulamaları: Oluşacak afetlerin birkaç saniye önce bile olsa tespit edilmesi birçok zararı engelleyebilir. Örneğin gelgit sebebiyle anlık su yükselmeleri ile oluşan seller, okyanus ve deniz tabanlarındaki depremlerden kaynaklı tsunami oluşumlarını erken tespit ederek oluşacak hasarların engellemesi için kullanılabilir [32].
- Askeri Uygulamalar: Mayın tarama, dost ve düşman tespiti, sınır ihlalleri tespiti gibi uygulamalarda kullanılabilirler [33].
- Yardımcı Navigasyon Uygulamaları: Sığ sularda ilerleyen gemiler için kayalıklar gibi tehlikelerden uzak durarak yollarına devam etmelerini, demir

atmak için en uygun noktayı seçmelerini, o bölgede yapacağı batık çalışması için ön bilgi toplamalarını sağlayabilir. Örneğin;

- [34]'te demir atmak için uygun noktayı bulan bir algoritma geliştirilmiştir.
- [35]'te sualtı konumlandırması için algoritma geliştirilmiştir.

- Spor Uygulamaları: Spor uygulamaları için oluşturulan ağlar genelde iki boyutlu olup kullanıldığı alanlar küçük olduğu için ağlar oluşturulurken akustik dalgaların yanı sıra optik ve RF dalgalarda kullanılan uygulamalar vardır. Örneğin;
  - [36]'da bir ya da daha fazla yüzücünün performans analizi yapılmıştır.
  - [37]'de yüzücülerin havuzdaki konumlarını bulmaya yönelik çalışmalar yapılmıştır.



Şekil 2.4 : SAAA uygulamalarının sınıflandırılması ([38]'den alınarak düzenlenmiştir).

3. MATEMATİKSEL PROGRAMLAMA VE OPTİMİZASYON

3.1 Tarihi ve Genel Bakış

Optimizasyon kavramı günümüze dek farklı araştırmacılar tarafından pek çok kez tanımlanmaya çalışılmıştır. Herhangi bir sistemin girdilerini olabilecek en verimli şekilde kullanarak hedef çıktıları elde etmeyi sağlayan yöntemsel çalışmalardır. Genel olarak, optimizasyon, bir dizi kısıtlamaya tabi olan bir fonksiyonun minimize veya maksimize edilmesi problemidir. Optimizasyon sorunları her yerde mevcuttur. Örneğin günlük hayatımızda sıkça kullandığımız navigasyon uygulamalarında istenilen yere en kısa mesafede ya da en kısa sürede ulaşmamızı sağlayan rota belirleme algoritmalarında kullanılmaktadır [39].

Optimizasyon süreci model oluşturma ve analiz olarak temel iki bileşenden oluşmaktadır. Model oluşturulurken istenen girdi parametreleri değişkenler (bilinmeyenler) olarak, amaç fonksiyonu maksimize ya da minimize edilmesi gereken değeri, problemdeki tüm kısıtlarda matematiksel bir kısıtlama olarak ifade edilir [39, 40]. Model oluşturma aşaması, gerçek hayat sorunlarının sayılarla ifade edilmesidir. Analiz aşaması ise oluşturulan matematiksel modelin gereklerini sağlayan en iyi çözümün elde edilmesidir. Model oluşturma alanında ilk çalışmalar Leontief'in ekonomi alanında yaptığı çalışmalardır. Kantorovich ise çalışmalarında üretim alanında optimizasyon ihtiyacını ortaya koymuştur. Çalışmalarında farklı üretim alanı sorunları için optimizasyon algoritmaları geliştirmiştir [40]. Günümüz optimizasyon çalışmalarının temeli 1947'de B. George Dantzig'in çalışmasıyla başladığı varsayılmakla beraber tartışmalı bir konudur. Bununla birlikte, diğer birçok bilim insanının da konuya önemli katkılarda bulunduğu söylenmelidir ve bazıları B. G. Dantzig'in katkısından önce gelir. Fakat tartışmaya açık olmayan durum B. G. Dantzig'in optimizasyon ve doğrusal programlamaya yaptığı önemli katkıdır [41].

Optimizasyon kavramı birçok karmaşık karar veya tahsis probleminin analizinin altında yatmaktadır. Tartışılması zor olan konuların anlaşılması için basit bir anlatım sunar. Karmaşık bir karar problemiyle karşı karşıya kalındığında değişken etkileşimlerin, kısıtlamaların ve uygun hedeflerin tam olarak temsil edilmesi çoğu

zaman için mümkün değildir. Bu nedenle, tüm nicel analiz tekniklerinde olduğu gibi, oluşturulan optimizasyon modeli yalnızca bir yaklaşım olarak kabul edilmelidir.

Oluşturulan modelin analizi sonrası çözümün kabul edilebilirliği tasarım faaliyetine çok sayıda gereksinim ve kısıtlama getirir. Bu nedenle, tüm bu farklı gereksinimler/kısıtlamalar altında uygulanabilir bir tasarım oluşturmak zaten zor bir iştir ve oluşturulan uygulanabilir tasarımın aynı zamanda 'en iyi' olmasını sağlamak da oldukça zordur. [42]

Optimizasyon modellerinin temel faydası, olası çözümleri, bunları gerçekten oluşturmadan ve denemeden hızlı ve güvenli bir şekilde değerlendirmektir. Diğer faydalarına değinirsek;

- Düşünce sürecini yapılandırır. Karar vericiyi problemi kısa ve düzenli bir şekilde düşünmeye zorlar. Karar verici, hangi faktörleri kontrol edeceğini belirler; yani, karar değişkenlerinin ne olduğunu, çözümün nasıl değerlendirileceğini yani amaç fonksiyonunu belirler. Son olarak, karar verici karar ortamını başka bir deyişle kısıtlamaları tanımlar.
- Sistemin objektifliğini artırır. Tüm kriterler açıkça belirtildiği için matematiksel modeller daha objektiftir.
- Karmaşık sorunları oldukça izlenebilir duruma getirir. Optimizasyon modelleri kompleks sorunları çözmeyi kolaylaştırır.
- Sorunları bilgisayar ile çözüme uygulanabilir hale getirir. Gerçek hayattaki problemlerin matematiksel model olarak oluşturulup, matematiksel analiz ve çözüm yöntemlerini kullanarak çözülmesini sağlar.

Matematiksel modellemenin oldukça fazla avantajı olmasına karşın dezavantajları da bulunmaktadır. Modelin oluşumu en önemli adımdır. Sorunlar çok karmaşık olmaya yatkın olduğundan, problemi yanlış modellemek optimizasyon için en başta hata yapılmasını bu durum da en uygun çözüm çıktısının oluşamamasını sağlamaktadır. Bir diğer dezavantajı ise karar verme sürecinde modellemenin oynadığı rolü anlamamaktır. Bir modelin çözümü her zaman gerçek sorun için en uygun çözüm olmayabilir. Matematiksel modeller doğru kararlara ulaşmada yardımcı olacak unsurlardır. Fakat, son karara ulaşan tek faktör değildir. Çözümleri nicel kriterlerle değerlendirir. Bu durumlarda, kararda niteliksel unsurlar da dikkate alınmalıdır.

3.2 Doğrusal Programlama

Doğrusal programlama, optimizasyon süreçleri için kullanılan başlıca tekniklerin en sık şekilde kullanılanıdır. Doğrusal programlamada, gerçek dünya süreçlerinin altında yatan tüm modeller doğrusaldır, bu sebepten dolayı doğrusal programlama, doğrusal modeller yardımıyla planlama olarak düşünülebilir [43].

Doğrusal programlama, kaynakların verimliliğini üst seviyeye ulaştırmak amacıyla 2. Dünya Savaşı esnasında geliştirildi. Programlama kavramı, oldukça verimli şekilde planlamak ya da insanları mümkün olacak en uygun biçimde yerleştirmek yani işleri/işçileri çizelgelemek gibi çalışmaları kast eden askeri bir kavramdı. 1947'de B. George Dantzig, doğrusal yapılara sahip programlama problemlerini çözmek için verimli bir algoritma olan Simplex yöntemini geliştirdi [44].

Dönemin ekonomistlerinin aksine B. G. Dantzig doğrusal programlamanın yalnızca ekonomik çalışmaların analizinde kullanmanın yanı sıra belli başlı gerçek dünya sorunlarının çözümlerini analiz etmek amacıyla kullanılabilecek bir çeşit model olarak görmüştür. Yaklaşımına tutarlı olacak şekilde doğrusal programlama modellerini analiz etmek amacıyla bir algoritma olan Simpleks Algoritmasını geliştirmiştir. Günümüzde hala karışık tam sayılı ve doğrusal programlamada öncelikli hesaplama aracı olacak şekilde kullanımı devam etmektedir [41]. Simpleks algoritmasından sonra 1984'te Karmarkar'ın iç nokta yöntemini geliştirmesi de doğrusal programlama çalışmaları için önemli bir atılım sayılır [43].

3.2.1 İkili tamsayı programlama

Matematiksel yöntemlerden ikili tam sayı programlama yöntemi için bütün karar faktörleri ikili sistemde olmalıdır. Bu durum değişkenlerin sıfır veya bir değerini alabileceği anlamına gelmektedir. İkili sistemde optimizasyon amacıyla çözülebilecek gerçek zaman problemleri için evet – hayır şeklinde kararlar üretmesi gerekmektedir. Bu elektrik devrelerinde devre kesici elemanların (ayırıcı, kesici veya adi anahtar) hangilerinin açık ya da kapalı olacağının belirlenmesi ve bu sayede belirli şartlarda hangi konumların enerji verilerek besleneceğinin belirlenmesinin seçimi benzeri problemlerin temsil edilmesinde yararlanılabilir.

3.2.2 Tamsayılı programlama

Matematiksel yöntemlerden tamsayılı programlama modelinde değişkenlerinin tamamı tamsayılı değerler almalıdır. Örneğin herhangi bir üretim tesisi için gerekli işçi sayısını belirleme sürecinin optimize edilmesi tamsayılı programlama modeli ile çözülebilir.

3.2.3 Karma tamsayılı programlama

Bu model için karar faktörlerinden bazıları reel sayılar olabildiği gibi değişkenlerin bir kısmı tam sayıdır. Kısıt ve amaç fonksiyonlarının durumuna göre doğrusal olan ve doğrusal olmayan karma tamsayılı programlama çeşitleri vardır. Genel kullanımda karma tamsayılı programlama denildiğinde doğrusal olan kastedilmektedir. Bu modelde optimizasyon süresini kısaltmak için dal – sınır veya kesme düzlemi yöntemlerinden yararlanılabilir [45].

3.3 Doğrusal Olmayan Programlama

Matematiksel programlamada oluşturulan modeldeki kısıtlardan bir veya daha fazlası ya da amaç fonksiyonu doğrusal değilse bu tarz modellere doğrusal olmayan programlama modeli denir. Doğrusal olmayan programlama modellerinin çözümleri doğrusal programlama modellerine göre çok daha zordur. Bunun bazıları aşağıdaki gibidir;

- Global optimum ile lokal optimum noktasını birbirinden ayırmak zordur.
- Optimum nokta doğrusal programlama modellerindeki gibi sadece uç noktalarda olmak zorunda değildir.
- Birbirinden ayrık olurlu bölgeler (İng. feasible regions) bulunabilir. Belirli bir olurlu bölge içerisindeki optimum nokta bulunsa bile incelenmemiş ayrık başka bir olurlu bölgenin olmadığına emin olunamaz.

Gerçek dünyada karşılaştığımız problemlerin çoğu doğrusal değildir. Örneğin bir yazılım geliştirme projesinde yazılımcı sayısını iki katına çıkarmak proje süresini yarıya düşürmez.

Gerçek dünyaya daha yakın modelleme imkânı sunsalar da doğrusal olmayan programlama modelleri çözümlerindeki zorluklar sebebiyle doğrusal modeller kadar popüler olamamıştır.

3.4 MATLAB ve GAMS

Mathworks şirketi tarafından model oluşturmak, algoritma geliştirmek ve verileri analiz etmek amaçlı geliştirilen MATLAB (MATrix LABoratory) kontrol sistemleri, sinyal işleme, derin öğrenme gibi birçok farklı alanda kullanılmaktadır [46]. GAMS optimizasyon ve matematiksel programlama için kullanılan üst düzey modelleme sistemidir. İçerisinde birçok çözücü ve bir dil derleyicisi barındırır. GAMS modelleme dili modelleyen kişiye gerçek dünya problemlerini hızlı bir şekilde bilgisayar koduna dönüştürme imkânı verir. GAMS dil derleyicisi bu kodu şirketler tarafından optimizasyon problemleri için geliştirilen çözücülerin anlayacağı hale getirir. Bu yapı sayesinde modelde herhangi bir değişiklik yapmadan farklı çözücülere geçme imkânı sunar [47]. En popüler çözücülere örnek olarak FICO tarafından geliştirilen XPRESS [48], GUROBI Optimization tarafından geliştirilen GUROBI [49] ve IBM tarafından geliştirilen CPLEX [50] verilebilir.

MATLAB ve GAMS arasındaki arayüz sayesinde, MATLAB üzerinden GAMS'in sağladığı tüm optimizasyon imkanları kontrol edilebilir. Ayrıca GAMS tarafından çözülen optimizasyon probleminin sonuçları MATLAB'a aktarılarak MATLAB içerisinde bulunan çeşitli görselleştirme ve raporlama araçları ile sonuçlar analiz edilebilir [51].

4. SİSTEM MODELİ

4.1 Problem Tanımı

Sualtı Akustik Algılayıcı Ağlar (SAAA), algılayıcıların sualtında belirli noktalara dağıtılmasıyla oluşur [52]. Sualtı haberleşmede elektromanyetik dalgalar yerine akustik dalgalar kullanılır çünkü elektromanyetik dalgalar tuzlu suda çok hızlı bir şekilde sönümlenmesine karşın akustik dalgalar suda daha az sönümlenmektedir [53, 54]. Algılayıcılar dağıtıldıkları bölgelerden çeşitli verileri toplayarak birbirleri üzerinden veya direkt olarak ana istasyona toplanan verileri iletebilirler [55-57]. Bu ağlar sualtına yerleştirildikleri için zorlu kanal şartlarına maruz kalırlar ve erişimleri kısıtlıdır [58, 59]. Sürekli batarya değişimi yapılmayacağı için ağ yaşam süresi sistem tasarımında oldukça önemli bir parametredir [60, 61]. Fakat askeri sistemler gibi güvenlik gerektiren uygulamalarda ağ yaşam süresinden ödün verilerek algılayıcıların topladıkları verilerin güvenliğini sağlamak, fiziksel ve siber saldırıların etkisini azaltmak için çeşitli önlemler alınmaktadır [2, 3, 62]. Kullanılan güvenlik önlemlerinden bir tanesi olan gizli anahtar şifrelemesinde ağdaki düğümler (İng. nodes) sadece uygun anahtarı bulunduran düğümlerle haberleşebilmektedir [63, 64]. Düğümlerin birbirleriyle haberleşmesi kısıtlı olduğundan bir veya daha fazla düğümün fiziksel koşullar ya da siber saldırılar sonucu servis dışı kalması ağ yaşam süresini önemli ölçüde azaltabilme potansiyeline haizdir [65]. Bu durum ağdaki veri akışının kopmasına veya düğümlerin verileri iletmek için daha fazla enerji harcayarak beklenenden önce bataryasının bitmesine sebep olmaktadır [66, 67]. Tez kapsamında SAAA'lar için gizli anahtar şifrelemesi kullanan bir ağ modellenecektir. Gizli anahtar paylaşma olasılığının ağ yaşam süresine etkisi incelenecektir. Farklı anahtar paylaşma olasılıkları için kritik düğümler bulunacak ve bu düğümlerin etkisiz hale getirilmesinin ağ yaşam süresine etkileri incelenecektir. Bu analizlerin tamamı eniyi (İng. optimal) karar verme süreçlerinin sağlandığı durumlar için yapılacaktır (örn. Doğrusal Programlama - DP). Böylece verilen kısıtlar altında eniyi durumda analizler sunulacaktır.

4.2 Ağ Topolojisi

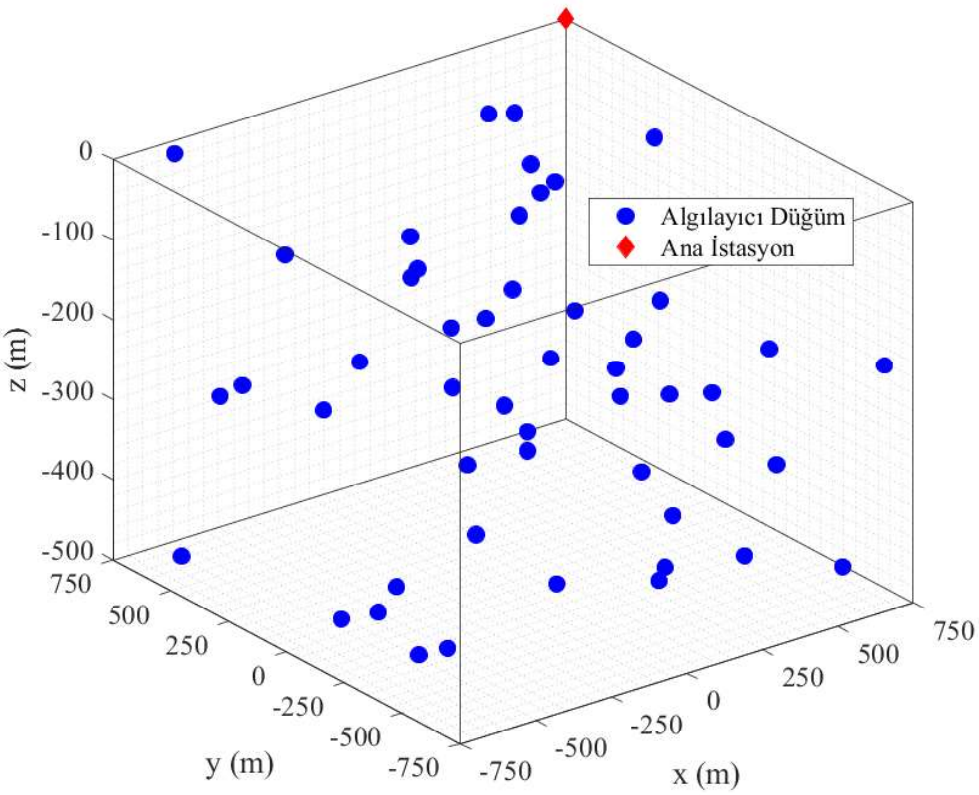
Bu tez kapsamında oluşturulan SAAA'da $|\mathcal{W}|$ adet algılayıcı düğüm ve bir adet ana istasyon düğümü (düğüm-1) vardır. Ağdan bulunan tüm algılayıcı düğümler $\mathcal{W}$ kümesi ile ifade edilmekte olup suyun hareketlerinden bağımsız olarak konumları statik olarak kabul edilmiştir. Ağ topolojisini $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ şekilde yönlü çizge olarak kabul edilir. $\mathcal{V}$ kümesi tüm algılayıcı düğümler ve ana istasyon düğümünü (düğüm-1) temsil eder. Ağ topolojisi ve $\mathcal{V}$ kümesi incelendiğinde $\mathcal{W}$ kümesinin $\mathcal{W} = \mathcal{V}/\{1\}$ olduğu görülecektir. $\mathcal{A}$ kümesi ana istasyon dahil tüm düğümlerin birbirleriyle olan bütün bağlantıları ifade edecek şekilde $\mathcal{A} = \{(i,j) : \in \mathcal{W}, j \in \mathcal{V} - i\}$ olarak tanımlanır. Aşağıda $\mathcal{A}$ kümesinin tanımı gereği oluşan ağ topolojisi için oldukça önemli sonuçlar belirtilmiştir;

- Tüm algılayıcı düğümler ana istasyon düğümüne (düğüm-1) veri gönderebilir.
- Ana istasyon düğümü (düğüm-1) hiçbir algılayıcı düğüme veri gönderemez.
- Hiçbir algılayıcı düğüm kendi kendine veri gönderemez.

Tüm algılayıcı düğümleri için aşağıdaki tanımlamalar yapılmıştır;

- Batarya seviyeleri eşit kabul edilmekte olup başlangıçtaki enerji miktarı ε_{bat} şeklinde tanımlanmıştır.
- Maksimum transfer mesafesi d_{max} olacaktır.
- Düğümler veri iletirken kaynak ve hedef düğüm arasındaki mesafeye göre iletim gücünü mesafenin artışına göre sürekli bir biçimde ayarlayacaktır.

Algılayıcı düğümler kenar uzunluğu d_e ve yüksekliği h olacak şekilde $d_e \times d_e \times h\, m^3$ hacimli kare prizma içerisine tekdüze dağılım (İng. uniform distribution) kullanılarak yerleştirilecektir. Algılayıcı düğümlerin konumu su içerisinde statik kabul edilecektir. Ana istasyon suyun yüzeyine ve kare prizmanın köşelerinden birine yerleştirilecektir. Şekil 4.1'de 50 algılayıcı düğüm ve bir adet ana istasyondan oluşan örnek bir SAAA verilmiştir.



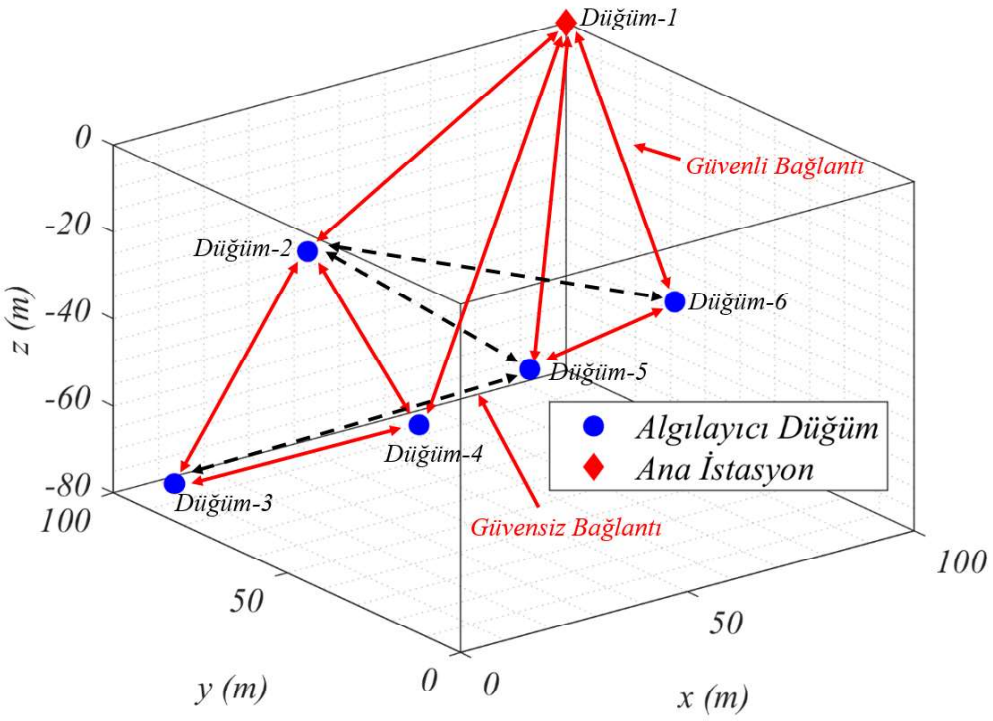
Şekil 4.1 : Örnek SAAA ağ topolojisi.

4.3 Anahtar Dağılımı

Gerçek dünyada karşılaştığımız problemlerin çoğu doğrusal değildir. Örneğin bir yazılım geliştirme projesinde yazılımcı sayısını iki katına çıkarmak proje süresini yarıya düşürmez. [12]'de verilen yöntem anahtar dağılımı için etkili ve basit bir yöntemdir. Üçüncü parti bir şirket tarafından oluşturulan anahtarlar bu tez kapsamında Anahtar Havuzu olarak adlandıracağımız bir havuzda toplanır. Ana istasyon anahtar havuzu içerisindeki tüm anahtarlara sahiptir. Bu nedenle tüm algılayıcı düğümlerle iletişim kurabilir. Her algılayıcı düğüme anahtar havuzu içerisinden belirli bir oranda rastgele seçilen anahtarlar atanır. İki algılayıcı düğümün birbirine veri gönderebilmesi için en az bir adet ortak anahtara sahip olması gereklidir. [12]'de verilen yöntemde iki algılayıcı düğümün en az bir anahtar paylaşma olasılığının matematiksel olarak hesaplanabileceği gösterilmiştir. Algılayıcı düğüm başına atanan anahtar sayısı (k) ve havuzundaki toplam anahtar sayısı yani anahtar havuzu büyüklüğü (P) ile düğüm sayısından bağımsız bir şekilde anahtar paylaşma olasılığı hesaplanabilir (Denklem 4.1'de verilmiştir).

$$P_{ksp} = \frac{k!\,(P-k)!\,(P-k)!}{P!\,k!\,(P-2k)!} \tag{4.1}$$

Şekil 4.2'de gizli anahtar şifrelemesi kullanan beş adet algılayıcı düğüm ve bir adet ana istasyondan oluşan örnek bir SAAA modeli verilmiştir. Bu örnek modelde kırmızı düz çizgilerle gösterilmiş (3,2), (3,4), (5,6) ve tüm düğümlerin ana istasyonla olan bağlantıları güvenlidir. Kesikli siyah çizgiler ile belirtilen diğer bağlantılar güvensizdir yani iki düğüm arasında ortak anahtar bulunmamaktadır. Gösterim kolaylığı olması açısından tüm bağlantılar gösterilmemiştir. Düğüm-3'ün uzaklığı yüzünden ana istasyonla direkt bağlantısı bulunmamaktadır. Düğüm-4'ün bulunduğu konum gereği topladığı verileri ana istasyona direkt iletmek yerine düğüm-2 üzerinden göndermesi enerji verimliliği açısından daha iyidir. Örneğin düğüm-3'ün topladığı verileri ana istasyona güvenli bir şekilde gönderebilmesi için çok atlamalı olarak sırasıyla 4 ve 2 nolu düğümler üzerinden göndermelidir. Bunun yanı sıra düğüm-4'e baktığımızda topladığı verileri direkt ana istasyona iletebilir ya da enerji verimliliği açısından düğüm-2 üzerinden de gönderebilir.



Şekil 4.2 : Örnek SAAA ağ topolojisi

4.4 Sualtı Enerji Tüketim Modeli

Bu tez kapsamında sualtında bir bit veri göndermek ve almak için gerekli enerji tüketimi hesabını [68] ve [69]'da belirtilen enerji dağılım modelinden faydalanılarak yapılmıştır. Denklem 4.2 ve denklem 4.3'e bakıldığında sualtı akustik haberleşmedeki iletim yolu kaybının sadece mesafeye değil ayrıca kullanılan akustik dalganın frekansınada bağlı olduğu görülür.

Düğüm-*i* ve düğüm-*j* arasındaki akustik iletim yolu kaybı (4.2) nolu denklemde hesaplanmaktadır.

$$A(d_{ij}, f) = (d_{ij})^{\kappa} \times \alpha(f)^{10^{-3} \times d_{ij}} \qquad (4.2)$$

(4.2) nolu denkleme bakıldığında iki düğüm arasındaki mesafe d_{ij}, sinyal yayılımının geometrisini belirten dağılım faktörü κ (İng. spreading factor), soğurma katsayısı $\alpha(f)$ ile ifade edilmiştir. d_{ij} hesaplanırken m cinsinden iki düğüm arasındaki öklid uzaklığı hesaplanır. κ yani dağılım faktörü ise genelde üç farklı değer alır [70]. Bunlar;

- Akustik sinyalin su yüzeyi ve deniz dibi gibi üst ve alt sınırlarla karşılaşmadan her yöne eşit yayılmasına küresel dağılım denir. Küresel Dağılım için $\kappa = 2$ alınır.
- Akustik sinyal su yüzeyi ve deniz dibi gibi üst ve alt sınırlarla karşılaştığından eşit yayılamaz bu dağılıma silindirik dağılım denir. Silindirik dağılım için $\kappa = 1$ alınır.
- Pratik dağılım için $\kappa = 1.5$ alınır.

(4.3) nolu denklemde soğurma katsayısını $(\alpha(f))$ bulmak için kullanılan Thorp'un denklemi verilmiştir.

$$10log_{10}\alpha(f) = \frac{0.11f^2}{1+f^2} + \frac{44f^2}{4100+f^2} + 2.75 \cdot 10^{-4}f^2 + 0.003 \qquad (4.3)$$

(4.3) nolu denklem kullanılarak hesaplanan soğurma katsayının birimi dB/km'dir. Ayrıca denklemde kullanılan f akustil dalganın frekansını belirtir ve birimi kHz'dir.

1-bit veri göndermek için gönderici düğüm tarafından tüketilen enerji (4.4) nolu denklemde verilmiştir. Bu denklemde P_0 olarak gösterilen değer alıcı düğüme ulaşması istenilen güç seviyesidir ve sabittir. Bu nedenle gönderici düğüm tarafından

veri iletimi sırasında harcanan enerji alıcı düğüm ile arasındaki mesafeye göre değişmektedir.

$$E_{tx}(d_{ij}) = A(d_{ij}, f) \times P_0 \tag{4.4}$$

1-bit veri almak için gereken enerji (4.5) nolu denklemde gösterilmiştir. Bu denklemde P_r olarak belirtilen değer sabittir ve kullanılan düğüm platformuna göre değişmektedir.

$$E_{rx} = P_r \tag{4.5}$$

4.5 Gizli Anahtar Şifrelemesi Kullanan Sualtı Akustik Algılayıcı Ağlarda Ağ Yaşam Süresini Eniyilemek için Doğrusal Programlama Modeli

Bu bölümde gizli anahtar şifrelemesi kullanan sualtı akustik algılayıcı ağlarda ağ yaşam süresini eniyilemek için oluşturulan doğrusal programlama modeli anlatılacaktır. Oluşturulan DP modelinde amaç fonksiyonu ağ yaşam süresini (ilk algılayıcı düğüm pil enerjisi tüketene kadar geçen süre) maksimize etmektir. Ağ yaşam süresi (6.1) nolu denklemde *t* ile olarak ifade edilir ve birimi saniyedir. DP modelinde düğüm-*i*'den düğüm-*j*'ye iletilen bit sayısı, g_{ij} sürekli karar değişkeni (İng. continuous decision variable) ile ifade edilmektedir. Ağ yaşam süresi boyunca düğüm-*i* tarafından tüketilen enerjiyi ise ϵ_i sürekli karar değişkeni ile ifade edilmektedir.

$$Enbüyükle\ t \tag{4.6}$$

(4.7)'den (4.14)'e kadar olan denklemler DP modelinin kısıtları ifade etmektedir.

$$\sum_{j \in \mathcal{V}} g_{ij} - \sum_{j \in \mathcal{W}} g_{ji} = \begin{cases} s_i \times t, \forall i \in \mathcal{W} \\ -\sum_{j \in \mathcal{W}} s_j \times t, i = 1 \end{cases} \tag{4.7}$$

Denklem 4.7 tüm algılayıcı düğümler ve ana istasyon için akış dengesini ifade etmektedir. Bu kısıtta s_i algılayıcı düğümler için veri üretim hızını saniye başına bit sayısı olarak ifade etmektedir. Bu kısıt incelendiğinde tüm algılayıcı düğümler için düğümden çıkan veri miktarının düğüme gelen veri miktarı ve düğümün ürettiği veri miktarının toplamı olduğu görülecektir.

$$g_{ij} \geq 0,\ \forall (i,j) \in \mathcal{A} \tag{4.8}$$

Denklem 4.8 ağ trafiğinin daima pozitif olmasını sağlar.

$$g_{ii} = 0,\ \forall i \in \mathcal{W} \tag{4.9}$$

Denklem 4.9'da olası veri döngüleri engellenmiştir. Düğüm-i oluşturduğu veriyi kendine iletemez.

$$\sum_{j \in \mathcal{V}} g_{1j} = 0 \tag{4.10}$$

Denklem 4.10'da ana istasyonun herhangi bir algılayıcı düğüme veri göndermesi engellenmiştir. Bu sayede ana istasyon veri göndermek yerine sadece veri toplayabilir.

$$g_{ij} = 0 \text{ if } d_{ij} > d_{max},\ \forall (i,j) \in \mathcal{A} \tag{4.11}$$

Denklem 4.11'de düğümler için maksimum gönderim mesafesinin sınırlı olmasını sağlar.

$$\sum_{j \in \mathcal{V}} E_{tx}(d_{ij}) \times g_{ij} + E_{rx} \sum_{j \in \mathcal{W}} g_{ji} = \varepsilon_i\ ,\ \forall i \in \mathcal{W} \tag{4.12}$$

Denklem 4.12'de ağ yaşam süresi boyunca tüm algılayıcı düğümler için veri alma ve gönderme için harcanan toplam enerji hesaplanır. Burada E_{tx} ve E_{rx} 1-bit veri gönderme ve alma için harcanan enerjidir. Bu enerjiler denklem 4.4 ve denklem 4.5'te gösterilmiştir.

$$\varepsilon_i \leq \varepsilon_{bat},\ \forall i \in \mathcal{W} \tag{4.13}$$

Denklem 4.13 her algılayıcı düğüm için algılayıcı düğümün harcayabileceği toplam enerjinin başlangıçtaki batarya enerjisinden küçük ya da eşit olmasını sağlar.

$$g_{ij} = \begin{cases} g_{ij} & eğer\ \beta_{ij}\ \leq P_{ksp} \\ 0 & diğer\ durumlarda \end{cases},\ \forall (i,j) \in \mathcal{A} \tag{4.14}$$

Son olarak denklem 4.14 verinin güvenli bağlantılar üzerinden iletilmesini sağlar. Bu kısıtta β_{ij}'nin (0,1) aralığında rastgele tekdüze bir değer olduğu varsayılmıştır. Eğer düğüm-*i* ve düğüm-*j* ortak bir anahtar paylaşıyorsa (yani $\beta_{ij} \leq P_{ksp}$) veri güvenli bir

şekilde iletilebilir. Ortak anahtar bulunmuyorsa veri iletilmez. İki düğüm arasındaki bağlantının simetrik olduğu ($\beta_{ij} = \beta_{ji}$) varsayılmıştır.

Bu DP modeli ağ içindeki akışı herhangi bir algılayıcı düğüm enerjisini erken harcamayacak şekilde ayarlarken aynı zamanda algılayıcı düğüm ve baz istasyonu arasındaki optimal güvenli yolu seçerek ağ yaşam süresini enbüyüklemektedir.

4.6 Düğüm Etkisiz Hale Getirme Modeli

Bu tez kapsamında düğümün etkisiz hale gelmesinin sebebinin düğüm yakalama saldırılarından olduğunu varsayıyoruz. Bununla beraber etkisiz hale getirilen algılayıcı düğümlerin fiziksel olarak imha edilmiş ve barındırdığı gizli anahtarların açığa çıkmadığını varsayıyoruz. Ağdan çıkarıldığında ağ yaşam süresini en çok azaltan düğüme kritik düğüm denir. Algılayıcı düğüm etkisiz hale getirme ve kritik düğümü bulmak için geliştirilen model Algoritma 1'de verilmiştir. Geliştirdiğimiz model ağdan çıkarıldığında ağ yaşam süresini en aza indiren düğümü yani kritik düğümü bulmaktadır. İlk olarak tekdüze dağılım ile rastgele oluşturulmuş ağ için kaç adet kritik düğüm bulunacağı (Nc) belirlenir. Sonrasında sıralı bir şekilde algılayıcı düğümler tek tek etkisiz hale getirilir yani ağdan çıkarılırlar (satır 2-4). Çıkarılan düğüm v_i olarak ifade edilir ve potansiyel bir kritik düğüm olarak kabul edilir. v_i'nin ağdan çıkarılmasıyla birlikte Bölüm 4.5'te anlatılan DP modeli çözülür ve ağ yaşam süresi hesaplanır (satır 5). Çıkarılan her algılayıcı düğüm için DP modeli çözülür ve hesaplanan ağ yaşam süresi t_i olarak ifade edilir ve değeri kaydedilir (satır 6). Tüm T_i değerleri hesaplandıktan sonra minimum t_i değeri bulunur (satır 8). Bu küme içerisindeki en düşük ağ yaşam süresi T_k olarak ifade edilen kümeye eklenir. T_k kümesi kritik düğümler ele geçirildikten sonraki ağ yaşam sürelerini ifade eder (satır 9). Ayrıca minimum t_i'yi sağlayan kritik düğüm, v_i, C_k olarak adlandırılan etkisiz hale getirilen düğümler kümesine eklenir (satır 10). İlk kritik düğüm bulunduktan sonra ağdan çıkarılarak ağ topolojisi güncellenir (satır 11). Kalan $Nc - 1$ sayıdaki kritik düğümler yukarıda anlatılan prosedür tekrar edilerek bulunur. Son olarak etkisiz hale getirilen kritik düğümler (C) ve kritik düğümler etkisiz hale getirildikten sonraki ağ yaşam süreleri (T) analiz edilmek için ilgi yere gönderilir (satır 13).

Çizelge 4.1 : Düğüm Etkisiz Hale Getirme Algoritması

Algoritma 1 Düğüm Etkisiz Hale Getirme Modeli

Girdi: $\mathcal{G} = (\mathcal{V}, \mathcal{A})$: Ağ topolojisini temsil eden yönlü çizelge, Nc: Etkisiz hale getirilecek kritik düğüm sayısı

Çıktı: C: Etkisiz hale getirilen kritik düğümler, T: C'deki kritik düğümler etkisiz hale getirildikten sonraki ağ yaşam süreleri

1: $C = \{C_k\}_{k=1}^{Nc} = \emptyset$ ve $T = \{T_k\}_{k=1}^{Nc} = \emptyset$ olacak şekilde tanımlanır.

2: **for** $k = 1$ to Nc **do**

3: **for i =** 2 to $|\mathcal{V}|$ **do**

4: Düğüm-i (v_i) ağdan kaldırılır.

5: Bölüm 4.5'te anlatılan DP modeli v_i olmadan çözülür.

6: Hesaplanan ağ yaşam süresi t_i olarak kaydedilir.

7: **end for**

8: Minimum t_i ve ona karşılık değerine karşılık gelen i değeri bulunur.

9: Minimum t_i değeri T_k kümesin eklenir. $T_k \leftarrow min_i\{t_i\}$

10: Bulunan kritik düğüm (Minimum t_i değerini sağlayan düğüm) C_k kümesine eklenir. $C_k \leftarrow v_j,\ j = argmin_i\{t_i\}$

11: Ağ topolojisi bulunan kritik düğüm çıkarılacak şekilde güncellenir. $\mathcal{G} \leftarrow \mathcal{G} \setminus C_k$

12: **end for**

13: **return** $C = \bigcup_{k=1}^{Nc} C_k$ *ve* $T = \bigcup_{k=1}^{Nc} T_k$

5. ANALİZLER

DP modeli CPLEX çözücüsü kullanılarak GAMS üzerinde çözdürülmüştür. Rastgele oluşturulmuş 50 adet ağ topolojisinin ortalaması alınarak sonuçların istatistiksel olarak anlamlı hale gelmesi hedeflenmiştir. MATLAB üzerinde analizler yapılırken sırasıyla aşağıdaki adımlar izlenmiştir;

1. Bölüm 4.2'de tanımlanan ağ topolojisi oluşturulmuştur.
2. Bölüm 4.3'te anlatılan anahtar dağılımı kullanılarak oluşturulan ağ topolojisinde düğümler arası anahtar paylaşma oranları belirlenmiştir.
3. Düğümler arası mesafeler hesaplandıktan sonra Bölüm 4.4'te anlatılan sualtı enerji tüketim modeli kullanılarak düğümler arası veri gönderme ve alma işlemleri için gereken enerji miktarları hesaplanmıştır.
4. Oluşturulan ağ topolojisi için hesaplanan değerler MATLAB üzerinden GAMS modeline aktarılarak ağ yaşam süresi maksimize edecek şekilde eniyilenmiştir. Ağ yaşam süresi ve algılayıcı düğümlerin kalan batarya enerjileri analiz için GAMS üzerinden tekrar MATLAB'a aktarılmıştır.
5. Bölüm 4.6'da belirtilen düğüm etkisizleştirme algoritması ile oluşturulan ağ topolojisi için kritik düğümler bulunmuştur.
6. Tüm sonuçlar toplandıktan sonra verileri daha kolay analiz edebilmek için sonuçlar grafik üzerinde incelenmiştir.

Yapılan analizler sırasında Çizelge 5.1'deki parametreler kullanılmıştır. Verilen grafiklerde bulunan üç eğri etkisiz hale getirilen düğüm sayısını (N_C) temsil etmektedir. Yapılan analizlerde anahtar paylaşma oranı sabit tutulurken etkisiz hale getirilen düğüm sayısı artırılmıştır. Ayrıca ağ yaşam süresi olarak tanımladığımız süre ilk düğümün enerjisi bitene kadar geçen süredir.

Çizelge 5.1 : Analizde Kullanılan Parametreler

Parametreler	**Tanım**	**Değer**
d_{max}	Maksimum haberleşme mesafesi (m)	1000 [71]
d_e	Ağın taban kenar uzunluğu (m)	{500, 1000, 1500}
ε_{bat}	Batarya enerjisi (KJ)	10
f	Çalışma frekansı (kHz)	10
h	Ağın derinliği (m)	500
κ	Dağılım faktörü	1.5 [71]
N_c	Ele geçirilen düğüm sayısı	{0, 1, 2, 3} [67]
P_{ksp}	Anahtar paylaşma oranı	{0.25, 0.5, 0.75, 1} [65]
$\|\mathcal{W}\|$	Algılayıcı düğüm sayısı	50 [67]
P_0	Alıcı düğümün girişinde istenen güç değeri (J/bit)	1×10^{-7} [71]
P_r	Alınma sabiti (J/bit)	0.2×10^{-7} [71]
s_i	Veri oluşturma hızı (bps)	1 [65]

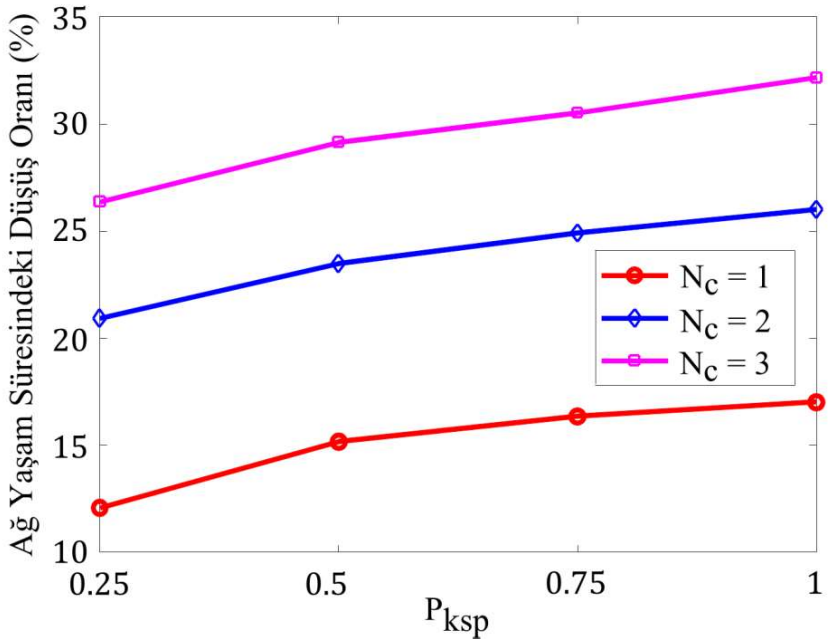
5.1 Ağ Yaşam Süresindeki Düşüş Oranı

Bu analizde farklı anahtar paylaşma olasılıkları için düğüm etkisizleştirme saldırısı altında bulunan bir SAAA'daki ağ yaşam süresindeki düşüşü incelenmiştir. Ayrıca bu analiz üç farklı ağ yoğunluğu için tekrarlanmış ve sırasıyla Şekil 5.1, 5.2 ve 5.3'de gösterilmiştir.

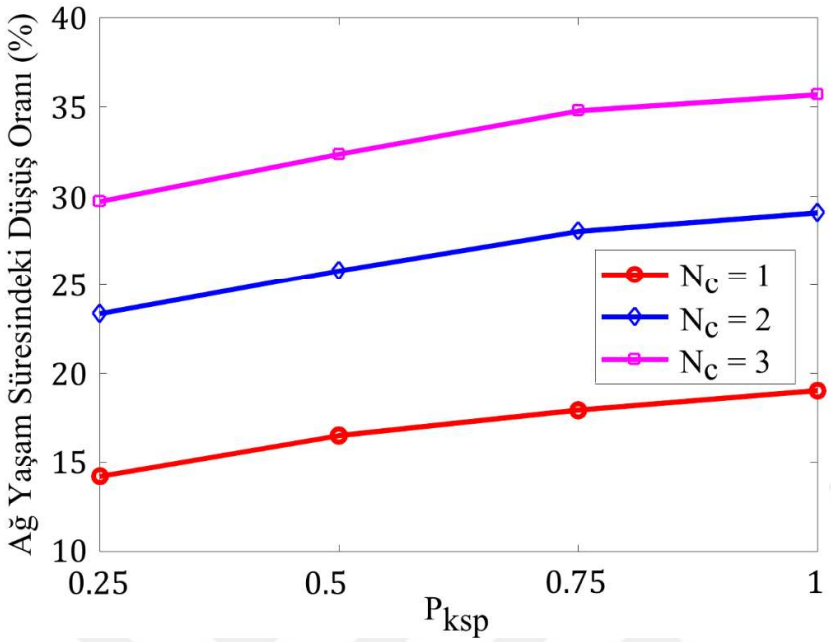
Ağ yaşam süresi düşüş oranı hesaplanırken herhangi bir düğüm saldırısı olmadığı durumdaki ağ yaşam süresi referans alınmıştır. Bu referansa göre sabit anahtar paylaşma olasılığı için etkisiz hale getirilen kritik düğüm sayısının ağ yaşam

süresindeki düşüşe etkisi gösterilmiştir. Ağ yaşam süresindeki en az düşüş oranları $P_{ksp} = 0.25$, en yüksek düşüş oranları ise $P_{ksp} = 1$ iken görülmüştür. Sonuçlar incelendiğinde ağ yaşam süresindeki azalmanın en az %12 ($N_C = 1$ ve $P_{ksp} = 0.25$ iken Şekil 5.1) ve en fazla %47 ($N_C = 1$ ve $P_{ksp} = 1$ iken Şekil 5.3) olduğu gözlemlenmiştir. Kritik düğüm sayısı sabit kalırken anahtar paylaşma oranı arttıkça ağ yaşam süresindeki düşüş artmaktadır. Örneğin Şekil 5.3'de $N_C = 3$ iken anahtar paylaşma oranı 0.25'den 1'e doğru artarken ağ yaşam süresindeki düşüş oranı da %41'den %47'ye kadar artmıştır. Bu durum anahtar paylaşma oranı yükseldikçe artan mantıksal bağlardır (İng. Logical Link). Bu yüzden literatürde sıcak nokta (İng. Hot-Spot) [72] olarak tanımlanan bölge büyümektedir. Bu nedenle sıcak nokta içerisinde bulunan bir ya da daha fazla düğümün etkisiz hale getirilmesi ağ yaşam süresini büyük ölçüde etkilemektedir.

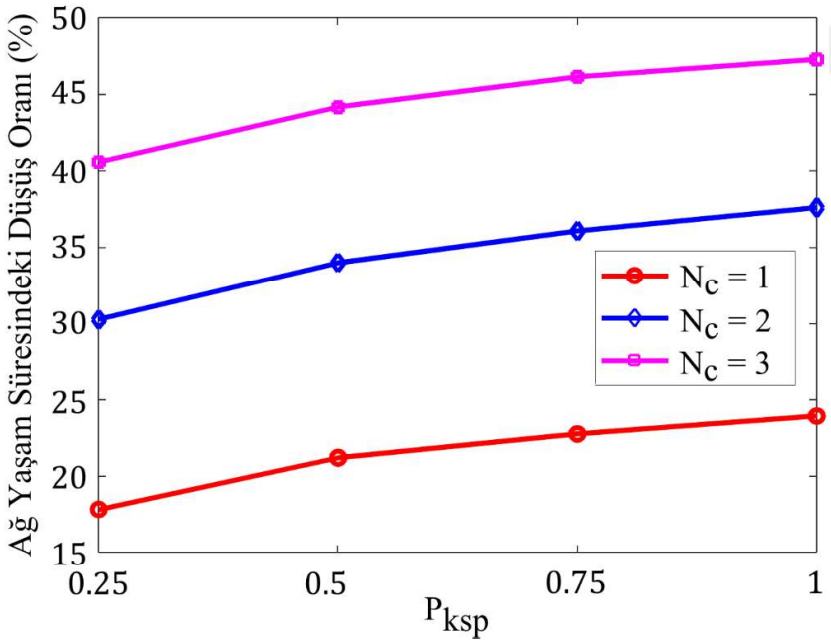
Sabit anahtar paylaşım oranı için etkisiz hale getirilen düğüm sayısının ağ yaşam süresine etkisi incelendiğinde etkisiz hale getirilen düğüm sayısı arttıkça ağ yaşam süresindeki düşüş oranı da artmaktadır. Şekil 5.1'e bakıldığında anahtar paylaşım oranı 0.25 iken, ele geçirilen düğüm sayısı arttıkça ağ yaşam süresindeki düşüş oranı %12'de %26'ya çıkmıştır. Bu analizlere bakıldığında ağın seyrekliği arttıkça ağ yaşam süresindeki düşüş oranı ciddi miktarda artmaktadır.



Şekil 5.1 : $\boldsymbol{d_e = 500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Ağ Yaşam Süresindeki Düşüş Oranı (%)



Şekil 5.2 : $\boldsymbol{d_e = 1000}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Ağ Yaşam Süresindeki Düşüş Oranı (%)



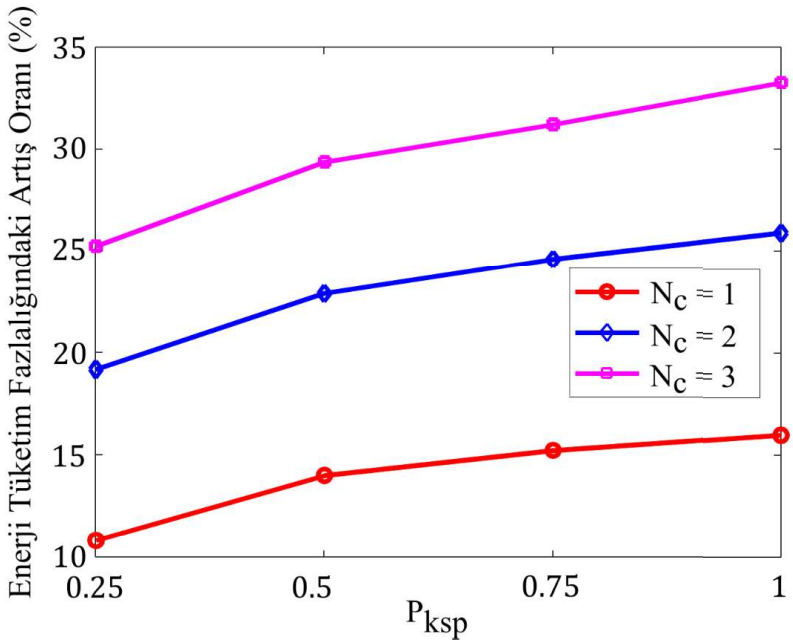
Şekil 5.3 : $\boldsymbol{d_e = 1500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Ağ Yaşam Süresindeki Düşüş Oranı (%)

5.2 Enerji Tüketim Fazlalığı Artış Oranı

Bu analizde farklı anahtar paylaşma olasılıkları için düğüm etkisizleştirme saldırısı altında bulunan bir SAAA'daki ortalama enerji tüketim fazlalığı incelenmiştir. Birim

zamanda düğüm başına tüketilen ortalama enerji olarak ifade edilen ortalama enerji tüketim fazlalığını $\tilde{\varepsilon}$ ile gösterilir ve (5.1) nolu denklem ile hesaplanır. Denklemde i düğümünün ağ ömrü boyunca harcadığı enerji ε_i olarak ifade edilmiştir. Bu analiz üç farklı ağ yoğunluğu için tekrarlanmış ve sırasıyla Şekil 5.4, 5.5 ve 5.6'de gösterilmiştir. Ortalama enerji tüketim fazlalığı hesaplanırken herhangi bir düğüm saldırısı olmadığı durumdaki ortalama enerji tüketim fazlalığı alınmıştır. Bu referansa göre sabit anahtar paylaşma olasılığı için etkisiz hale getirilen kritik düğüm sayısının ortalama enerji tüketim fazlalığına etkisi gösterilmiştir. Yapılan analizler incelendiğinde ortalama enerji tüketim fazlalığındaki değişimin minimum %11 ($N_C = 1$ ve $P_{ksp} = 0.25$ iken Şekil 5.4) ve maksimum %46 ($N_C = 1$ ve $P_{ksp} = 1$ iken Şekil 5.6) olduğu gözlemlenmiştir.

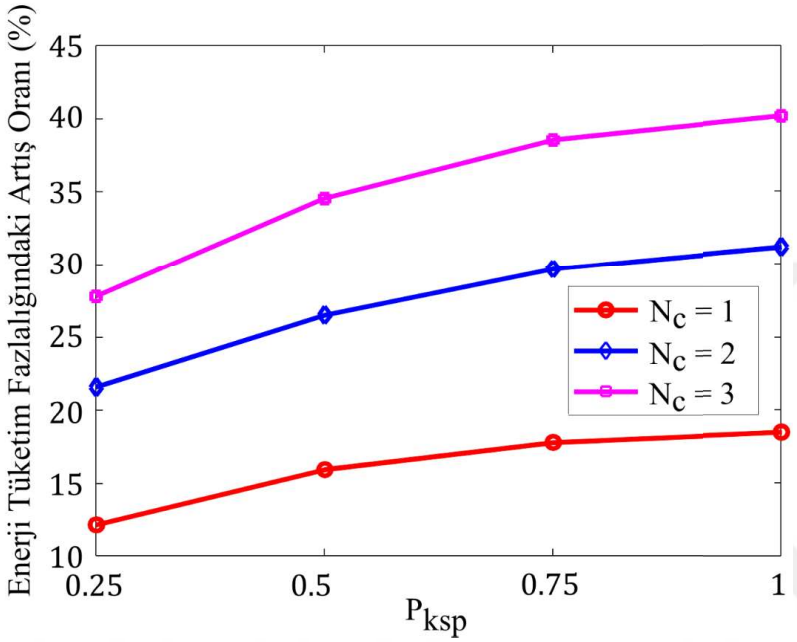
$$\tilde{\varepsilon} = \frac{\sum_{i \in W} \varepsilon_i}{t \times |W|} \tag{5.1}$$



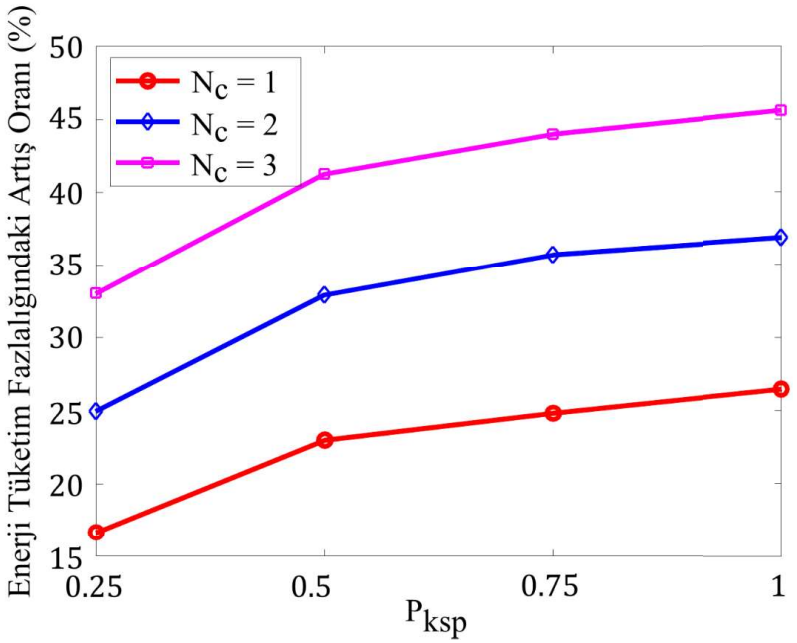
Şekil 5.4 : $\boldsymbol{d_e = 500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Enerji Tüketim Fazlalığındaki Artış Oranı (%)

Kritik düğüm sayısı sabit kalırken anahtar paylaşma oranı arttıkça ortalama enerji tüketim fazlalığı artmaktadır. Örneğin Şekil 6.3'de $N_C = 3$ iken anahtar paylaşma oranı 0.25'ten 1'e doğru artarken ortalama enerji tüketim fazlalığındaki artış oranı da sırasıyla %33, %41, %44 ve %46 olmuştur.

Sabit anahtar paylaşım oranı için etkisiz hale getirilen düğüm sayısı arttıkça ortalama enerji tüketim fazlalığı da artmaktadır. Şekil 5.4'e bakıldığında anahtar paylaşım oranı 0.25 iken, ele geçirilen düğüm sayısı arttıkça ortalama enerji tüketim fazlalığındaki artış oranı %11'den %25'e çıkmıştır.



Şekil 5.5 : $\boldsymbol{d_e = 1000}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Enerji Tüketim Fazlalığındaki Artış Oranı (%)



Şekil 5.6 : $\boldsymbol{d_e = 1500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre Enerji Tüketim Fazlalığındaki Artış Oranı (%)

5.3 Ortalama Normalize Edilmiş Uzaklık

Bu analizde farklı anahtar paylaşma olasılıkları için etkisiz hale getirilen kritik düğümlerin ana istasyona olan ortalama normalize edilmiş uzaklıkları incelenmiştir. Bu analiz üç farklı ağ yoğunluğu için tekrarlanmış ve sırasıyla Şekil 5.7, 5.8 ve 5.9'da gösterilmiştir. Ana istasyona göre ortalama normalize edilmiş uzaklık $\tilde{d}_s$ ile gösterilir. Ortalama normalize edilmiş uzaklık hesaplanırken etkisiz hale getirilmiş tüm kritik düğümler (C kümesi) için normalize edilen uzaklıkların ortalaması alınır. Bu hesaplama (5.2) nolu denklem ile gösterilmiştir.

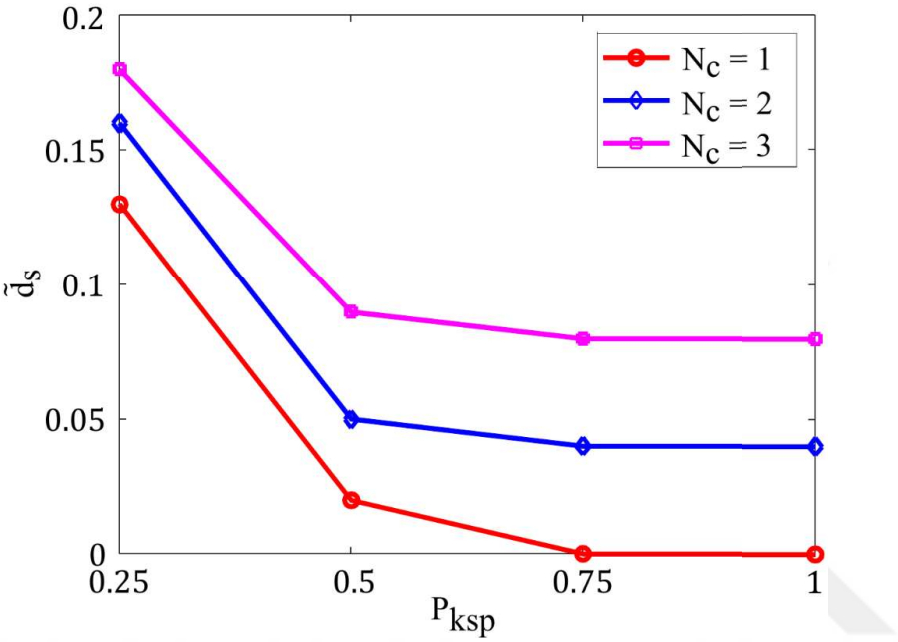
$$\tilde{d}_s = \frac{1}{N_C} \sum_{\kappa \in C} \frac{d_{k1} - \min\limits_{i \in W}\{d_{i1}\}}{\max\limits_{i \in W}\{d_{i1}\} - \min\limits_{i \in W}\{d_{i1}\}} \tag{5.2}$$

(5.2) nolu denklemde min olarak gösterilen ifade ana istasyona en yakın olan düğümün uzaklığını belirtir. Aynı şekilde max olarak gösterilen ifade ana istasyona en uzaktaki düğümün uzaklığını belirtir.

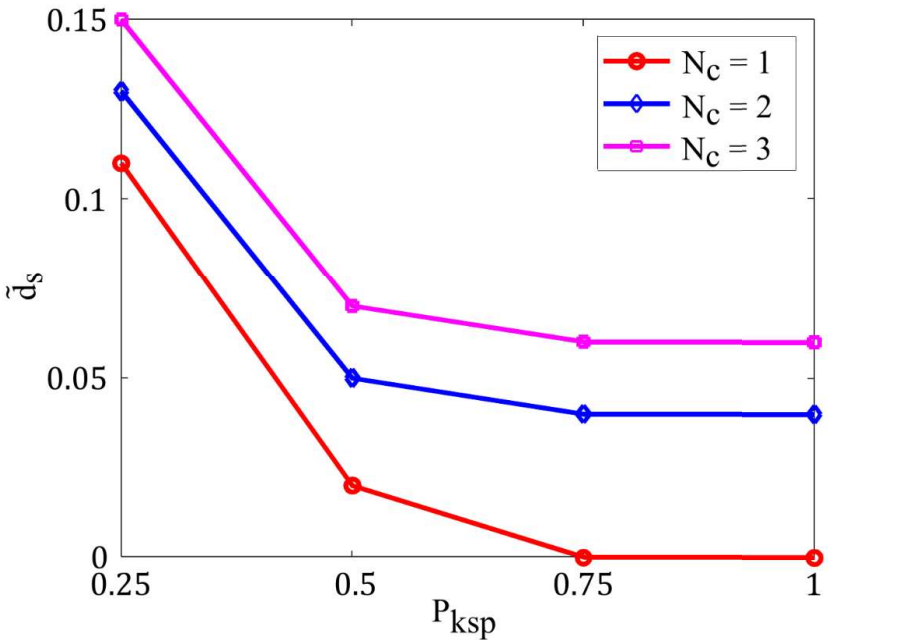
d_{k1}, etkisiz hale getirilen kritik düğümle ana istasyon arasındaki mesafe olarak ifade edilir. Örneğin bir adet kritik düğüm için eğer $\tilde{d}_s = 0$ ise kritik düğüm ana istasyona en yakın düğümdür. Eğer $\tilde{d}_s = 1$ ise kritik düğüm ana istasyona en uzak düğümdür. Sonuçlar incelendiğinde ortalama normalize edilmiş uzaklığın en fazla anahtar paylaşma oranı 0.25 iken olduğu görülmüştür ve bu değerler d_e = 500, 1000 ve 1500 için sırasıyla 0.18, 0.15 ve 0.11'dir. Anahtar paylaşma oranı arttıkça ortalama normalize edilmiş uzaklık azalmaktadır. Başka bir deyişle anahtar paylaşma oranı arttıkça ana istasyona yakın olan düğümlerin kritik düğüm olma ihtimali artmaktadır. Ayrıca, $P_{ksp} \geq 0.75$ olduğu durumda $\tilde{d}_s$ nin önemi kalmamaktadır. Ağın seyrekliğinden bağımsız olarak $P_{ksp} \geq 0.75$ ve $N_C = 1$ için $\tilde{d}_s = 0$ olmuştur. Yani her daim ana istasyona en yakın düğümün kritik olduğunu göstermektedir. Bu sonuçlardan çıkarılan diğer iki bulgu ise;

1. Etkisiz hale getirilen düğüm sayısı arttıkça (N_C) ortalama normalize edilmiş uzaklıkta ($\tilde{d}_s$) artar. Çünkü ana istasyona en yakın düğüm haricindeki diğer tüm düğümler ortalamayı arttıracaktır.
2. Ağ seyrekliği arttıkça ortalama normalize edilmiş uzaklık ($\tilde{d}_s$) düşer. Çünkü algılayıcı düğümlerin veri iletim mesafeleri sınırlıdır. Ağ büyüdükçe ve

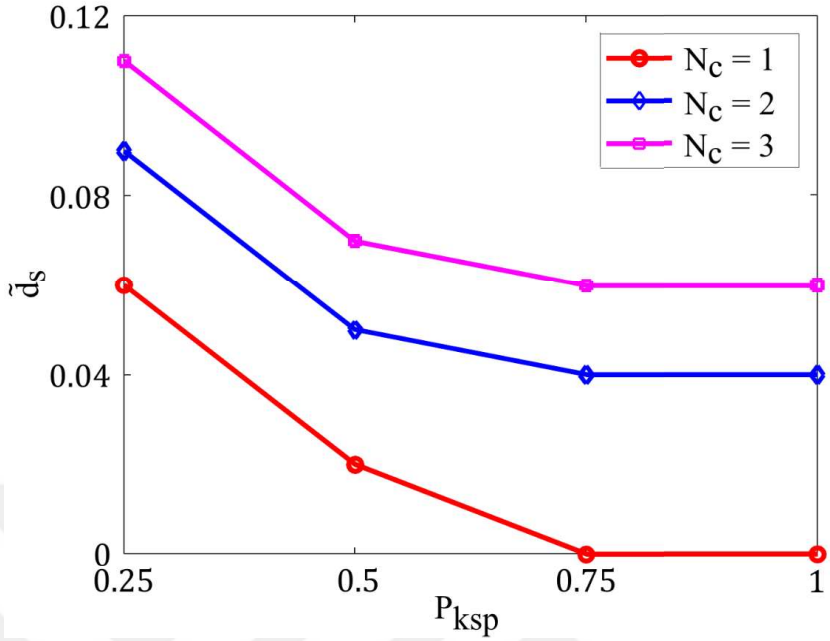
seyrekleştikçe ana istasyona yakın düğümlerin kendi ürettikleri veri haricinde diğer düğümlerden gelen verileri de yönlendirmesi gerekir. Bu nedenle kritik düğümün ana istasyona yakın olma ihtimali aynı anahtar paylaşma oranına sahip daha yoğun ağlara göre daha yüksektir.



Şekil 5.7 : $\boldsymbol{d_e = 500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre $\boldsymbol{\tilde{d}_s}$



Şekil 5.8 : $\boldsymbol{d_e = 1000}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre $\boldsymbol{\tilde{d}_s}$



Şekil 5.9 : $\boldsymbol{d_e = 1500}$ iken $\boldsymbol{P_{ksp}}$ ve $\boldsymbol{N_C}$'ye göre $\boldsymbol{\tilde{d}_s}$

6. SONUÇLAR

Bu tez çalışmasında gizli anahtar şifrelemesi kullanan SAA'larda kritik düğümün etkisiz hale getirilmesinin ağ yaşam süresine etkileri incelenmiştir. Problemin çözülmesi için düğümler arası güvenli haberleşme kanalları oluşturan ve ağ yaşam süresini eniyileyen bir doğrusal programlama modeli geliştirildi. Ağ yaşam süresini en aza indiren kritik düğümü bulma algoritması ile oluşturulan DP modeli ağ yoğunluğu, anahtar paylaşma oranı ve etkisiz hale getirilen kritik düğüm sayısı gibi çeşitli parametrelerle analiz edildi. Sonuçlar incelendiğinde kritik düğümün etkisizleştirilmesi ağ yaşam süresini en az %12 (yoğun ağlar için) en fazla %47 (seyrek ağlar için) oranında düşürmektedir. Ayrıca kritik düğümün etkisizleştirmesi ağdaki ortalama enerji tüketim fazlalığını %11 ila %46 artırmıştır. Kritik düğümün ana istasyona yakınlığı incelendiğinde %18 olduğu görülmüştür.

Sonuçlar özetlenecek olursa:

- Kritik düğüm sayısı sabit kalırken anahtar paylaşma oranı arttıkça ağ yaşam süresindeki düşüş oranı ve ortalama enerji tüketim fazlalığı artmaktadır.
- Sabit anahtar paylaşım oranı için etkisiz hale getirilen düğüm sayısının ağ yaşam süresine etkisi incelendiğinde düğüm sayısı arttıkça ağ yaşam süresindeki düşüş oranı ve ortalama enerji tüketim fazlalığı artmaktadır.
- Ağ seyrekliği ve anahtar paylaşma oranı arttıkça ana istasyona yakın olan düğümlerin kritik düğüm olma ihtimali artmaktadır.

KAYNAKLAR

[1] **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.

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

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

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

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

[6] **Alharbi, A., Muzzammil, M.** (2022). A Survey on the Security of Routing Protocols for Underwater Acoustic Sensor Networks. *International Journal of Computer Science and Network Security*, *22*(1), 453-464.

[7] **Bharathi, M. V., Tanguturi, R. C., Jayakumar, C., Selvamani, K.** (2012). Node capture attack in wireless sensor network: A survey. *2012 IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, India.

[8] **Bicakci, K., Gamage, C., Crispo, B., Tanenbaum, A. S.** (2005). One-Time sensors: a novel concept to mitigate node-capture attacks. *European Workshop on Sec. in Ad-hoc Sens. Netw.*, Springer, Berlin, Heidelberg.

[9] **Garg, R., Varna, A. L., Wu**, **M.** (2012). An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*, *7*(2), 717-730.

[10] **Lin, C., Wu**, **G.** (2013). Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. *The Journal of Supercomputing*, *66*, 989-1007.

[11] **Agrawal, S., Das, M. L., Lopez**, **J.** (2019). Detection of Node Capture Attack in Wireless Sensor Networks. *IEEE Systems Journal*, *13*(1),238-247.

[12] **Eschenauer, L., Gligor**, **V. D.** (2002). A key-management scheme for distributed sensor networks. *In Proceedings of the 9th ACM conference on Computer and communications security*.

[13] **Kalkan, K., Levi**, **A.** (2014). Key distribution scheme for peer-to-peer communication in mobile underwater wireless sensor networks. *Peer-to-Peer Networking and Applications*, *7*, 698-709.

[14] **Ateniese, G., Capossele, A., Gjanci, P., Petrioli, C., Spaccini**, **D.** (2015). SecFUN: Security framework for underwater acoustic sensor networks. *OCEANS,* Genova.

[15] **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.

[16] **Hassan, M. A. H., Abdullah-Al-Wadud, M., Mehedi, M., Almogren, A. S., Alamri, A., Kamal, A. R. M., Mamun-Or-Rashid**, **M.** (2018). A key distribution scheme for secure communication in acoustic sensor networks. *Future Gener. Comput. Syst.*, *86*, 1209-1217.

[17] **Zhang, S., Du, X., Liu**, **X.** (2020). A Secure Remote Mutual Authentication Scheme Based on Chaotic Map for Underwater Acoustic Networks. *IEEE Access, 8*, 8285-48298.

[18] **Ma, H., Teng, J., Hu, T., Shi, P., Wang**, **S.** (2020). Co-communication Protocol of Underwater Sensor Networks with Quantum and Acoustic Communication Capabilities. *Wireless Personal Communications, 113*, 337-347.

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

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

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

[22] **Proakis, J. G., Sözer, E. M., Rice, J. A., Stojanovic**, **M.** (2001). Shallow water acoustic networks. *IEEE Communications Magazine, 39*, 114-119.

[23] "**Teledyne Benthos**" [Çevrimiçi]. Url: http://www.teledynemarine.com/benthos. [15 Mart 2022'de erişildi].

[24] "**AQUATEC**" [Çevrimiçi]. Url: https://www.aquatecgroup.com/. [15 Mart 2022'de erişildi].

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

[26] **Ayaz, M., Baig, I., Abdullah, A. B., Faye**, **I.** (2011). A survey on routing techniques in underwater wireless sensor networks. *Journal of Network and Computer Applications, 34*, 1908-1927.

[27] **Liu, L., Zhou, S., Cui**, **J.H.** (2008). Prospects and problems of wireless communication for underwater sensor networks. *Wireless Communications and Mobile Computing, 8*, 977-994.

[28] **B. Zhang, G. S. Sukhatme and A. A. G. Requicha**, (2004). Adaptive sampling for marine microorganism monitoring. *2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS),* Sendai, Japan.

[29] **Yalçuk, A., Postalcioglu**, **S.** (2014). Evaluation of pool water quality of trout farms by fuzzy logic: monitoring of pool water quality for trout farms," *International Journal of Environmental Science and Technology, 12*, 1503-1514.

[30] **Tuna, G., Arkoc, O., Gulez**, **K.** (2013). Continuous Monitoring of Water Quality Using Portable and Low-Cost Approaches. *International Journal of Distributed Sensor Networks,9*.

[31] **Khan, A., Jenkins**, **L.** (2008). Undersea wireless sensor network for ocean pollution prevention. *3rd International Conference on Communication Systems*

Software and Middleware and Workshops (COMSWARE '08), Bangalore, India.

[32] **Soreide, N., Woody, C., Holt**, **S.** (2001). Overview of ocean based buoys and drifters: present applications and future needs. *MTS/IEEE Oceans 2001. An Ocean Odyssey. Conference Proceedings, 4*, Honolulu, HI, USA.

[33] **Cayirci, E., Tezcan, H., Dogan, Y., Coskun**, **V.** (2006). Wireless sensor networks for underwater survelliance systems. *Ad Hoc Networks, 4*, 431-446.

[34] **Guo, Y., Liu**, **Y.** (2013). Localization for anchor-free underwater sensor networks. *Computers & Electrical Engineering, 39*, 1812-1821.

[35] **Carroll, P., Mahmood, K., Zhou, S., Zhou, H., Xu, X., Cui**, **J.-h.** (2012). On-demand asynchronous localization for underwater sensor networks. *Proceedings of the IEEE Oceans,* Hampton Roads, VA, USA.

[36] **Le Sage, T., Bindel, A., Conway, P., Slawson, S., West**, **A.** (2011). Development of a wireless sensor network for embedded monitoring of human motion in a Harsh environment. *IEEE 3rd International Conference on Communication Software and Networks,* Xi'an, China.

[37] **Marshall**, **J.** (2015). Magnetic Field Swimmer Positioning. *IEEE Sensors Journal, 15*(1), 172-179.

[38] **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.

[39] **Guenin, B., Könemann, J., Tunçel**, **L.** (2014). *A Gentle Introduction to Optimization*, Cambridge: Cambridge University Press.

[40] **Türkay**, **M.,** "Optimizasyon Modelleri ve Çözüm Metodları," [Çevrimiçi]. Url: http://home.ku.edu.tr/~mturkay/indr501/Optimizasyon.pdf. [15 Mart 2022'de erişildi].

[41] **Bixby**, **R. E.** (2012). A Brief History of Linear and Mixed-Integer Programming Computation. *Documenta Mathematica, Extra Volume: Optimization Stories*, 107–121.

[42] **Kulkarni, A., Krishnasamy, G., Abraham**, **A.** (2016). Introduction to Optimization. *Cohort Intelligence: A Socio-inspired Optimization Method*, Cham, Springer, 1-7.

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

[44] **C. Lewis**, "Linear Programming: Theory and Applications," [Çevrimiçi]. Url: https://www.whitman.edu/Documents/Academics/Mathematics/lewis.pdf. [15 Mart 2022'de erişildi].

[45] **Kocaarslan, İ., Tiryaki**, **H.** (2015). Yük Dağıtım Sistemlerinde Karışık Tamsayı Programlama Algoritması ile Optimizasyon. *Uluslararası Muhendislik Arastirma ve Gelistirme Dergisi, 7*, 1-10.

[46] **"*MATLAB - Mathworks*"** [Çevrimiçi]. Url: www.mathworks.com/products/matlab.html. [15 Mart 2022'de erişildi].

[47] **"*GAMS*"** [Çevrimiçi]. Url: www.gams.com/products/gams/gams-language. [15 Mart 2022'de erişildi].

[48] **"*FICO® Xpress Solver*"** [Çevrimiçi]. Url: https://www.fico.com/en/products/fico-xpress-solver. [15 Mart 2022'de erişildi].

[49] "**GUROBI**" [Çevrimiçi]. Url: https://www.gurobi.com/products/gurobi-optimizer/. [15 Mart 2022'de erişildi].

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

[51] **Ferris, M., Jain, R., Dirkse, S.**, "*GDXMRW: Interfacing GAMS and MATLAB*" [Çevrimiçi]. Url: http://pages.cs.wisc.edu/~ferris/matlab/gdxmrw.pdf. [15 Mart 2022'de erişildi].

[52] **Sozer, E., Stojanovic, M., Proakis**, **J.** (2000). Underwater acoustic networks. *IEEE Journal of Oceanic Engineering, 25*(1), 72-83.

[53] **A. A. Aziz, Y. A. Sekercioglu, P. Fitzpatrick and M. Ivanovich**, "A Survey on Distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials,* vol. 15, no. 1, pp. 121-144, 2015.

[54] **G. Han, J. Jiang, N. Bao, L. Wan and M. Guizani**, "Routing protocols for underwater wireless sensor networks," *IEEE Communications Magazine,* vol. 53, no. 11, pp. 72-78, 2015.

[55] **K. Chen, M. Ma, E. Cheng, F. Yuan and W. Su**, "A Survey on MAC Protocols for Underwater Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials,* vol. 16, no. 3, pp. 1433-1447, 2014.

[56] **Jouhari, M., Ibrahimi, K., Tembine, H., Ben-Othman**, **J.** (2019). Underwater Wireless Sensor Networks: A Survey on Enabling Technologies, Localization Protocols, and Internet of Underwater Things. *IEEE Access, 7*, 96879-96899.

[57] **Erol-Kantarci, M., Mouftah, H. T., Oktug**, **S.** (2011). A Survey of Architectures and Localization Techniques for Underwater Acoustic Sensor Networks. *IEEE Communications Surveys and Tutorials, 13*(3), 487-502.

[58] **Islam, T., Park**, **S.-H.** (2020). A Comprehensive Survey of the Recently Proposed Localization Protocols for Underwater Sensor Networks. *IEEE Access, 8*, 179224-179243.

[59] **Luo, H., Wu, K., Ruby, R., Liang, Y., Guo, Z., Ni**, **L. M.** (2018). Software-Defined Architectures and Technologies for Underwater Wireless Sensor Networks: A Survey. *IEEE Communications Surveys and Tutorials, 20*(4), 2855-2888.

[60] **Ghoreyshi, S. M., Shahrabi, A., Boutaleb**, **T.** (2017). Void-Handling Techniques for Routing Protocols in Underwater Sensor Networks: Survey and Challenges," *IEEE Communications Surveys and Tutorials, 19*(2), 800-827.

[61] **Sandeep, D., Kumar**, **V.** (2017). Review on Clustering, Coverage and Connectivity in Underwater Wireless Sensor Networks: A Communication Techniques Perspective. *IEEE Access, 5*, 11176-11199.

[62] **Qiu, T., Zhao, Z., Zhang, T., Chen, C., Chen**, **C. L. P.** (2020). Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Transactions on Industrial Informatics, 16*(7), 4297-4307.

[63] **Huang, Y., Zhou, S., Shi, Z., Lai**, **L.** (2016). Channel Frequency Response-Based Secret Key Generation in Underwater Acoustic Systems. *IEEE Transactions on Wireless Communications, 15*(9), 5875-5888.

[64] **Xu, M., Liu**, **L.** (2018). SenseVault: A Three-tier Framework for Securing Mobile Underwater Sensor Networks. *IEEE Transactions on Mobile Computing, 17*(11), 2632-2645.

[65] **Yildiz, H. U., Ciftler, B. S., Tavli, B., Bicakci, K., Incebacak**, **D.** (2018). The Impact of Incomplete Secure Connectivity on the Lifetime of Wireless Sensor Networks. *IEEE Systems Journal, 12*(1), 1042-1046.

[66] **Yuksel, A., Uzun, E. Tavli**, **B.** (2015). The impact of elimination of the most critical node on Wireless Sensor Network lifetime. *IEEE Sensors Applications Symposium (SAS),* Zadar, Croatia.

[67] **Yildiz, H. U., Tavli, B., Kahjogh, B. O. Dogdu**, **E.** (2017). The Impact of Incapacitation of Multiple Critical Sensor Nodes on Wireless Sensor Network Lifetime. *IEEE Wireless Communications Letters, 6*(3), 306-309.

[68] **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.

[69] **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.

[70] **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.

[71] **Özmen A.**, **Yıldız H.U**., **Tavlı B.**, (2020). Impact of Minimizing the Eavesdropping Risks on Lifetime of Underwater Acoustic Sensor Networks, *2020 28th Telecommunications Forum (TELFOR)*, November 24-25, Belgrade, Serbia.

[72] **Perillo, M., Cheng, Z. Heinzelman**, **W.** (2005) An analysis of strategies for mitigating the sensor network hot spot problem. *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services,* San Diego, CA, USA.