T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ ALGILAYICI AĞLARDA YENİ BİR HİBRİT SALDIRI TESPİT SİSTEMİNİN GELİŞTİRİLMESİ

Hamza ELBAHADIR

Yüksek Lisans Tezi

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
Donanım Bilim Dalı

OCAK 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

KABLOSUZ ALGILAYICI AĞLARDA YENİ BİR HİBRİT SALDIRI TESPİT SİSTEMİNİN GELİŞTİRİLMESİ

Tez Yazarı
Hamza ELBAHADIR

Danışman
Doç. Dr. Ebubekir ERDEM

OCAK 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Kablosuz Algılayıcı Ağlarda Yeni Bir Hibrit Saldırı Tespit Sisteminin Geliştirilmesi
Yazarı:	Hamza ELBAHADIR
İlk Teslim Tarihi:	24.12.2021
Savunma Tarihi:	28.01.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

İmza

Danışman: Doç. Dr. Ebubekir ERDEM — Onayladım
Fırat Üniversitesi Mühendislik Fakültesi

Başkan: Doç. Dr. Taner TUNCER — Onayladım
Fırat Üniversitesi Mühendislik Fakültesi

Üye: Dr. Öğr. Üyesi Cengiz HARK — Onayladım
Malatya Turgut Özal Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Kablosuz Algılayıcı Ağlarda Yeni Bir Hibrit Saldırı Tespit Sisteminin Geliştirilmesi " Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

28.01.2022

Hamza ELBAHADIR

ÖNSÖZ

Fiziksel ortamlardaki sıcaklık, basınç, titreşim, hız gibi verileri algılamak ve sonuçlar üretmek amacıyla günümüzde çok çeşitli alanlarda yaygın olarak kullanılan kablosuz algılayıcı ağlar (KAA); askeri, istihbari ve sağlık gibi kritik öneme sahip alanlarda da kullanılmaktadır. Bununla birlikte, gerek altyapı mimarisinin geleneksel ağlara göre farklılık göstermesi gerekse de donanımsal kısıtlarından dolayı KAA'lar için özgün güvenlik mekanizmaları geliştirilmelidir.

Teknolojik gelişmelere paralel olarak, KAA'lara yönelik güvenlik önlemleri geliştirilmiştir. Saldırı tespit sistemleri (STS), algılayıcı ağların güvenliğini sağlamak için etkili mekanizmalardan biridir. Bununla birlikte, günümüz şartlarında, saldırı tespiti için önerilen algılama metotları, etkili bir güvenlik için tek başına yeterli değildir. Ayrıca mevcut çalışmaların azımsanmayacak bir kısmında, STS'lerde kullanılan veri kümeleri güncelliğini yitirmiş olduğundan, elde edilen sonuçlar, güncel saldırılar karşısında tutarlı sonuçlar vermeyecektir. Söz konusu eksiklikler ve dezavantajlar, KAA güvenliği için etkili bir STS modeli ortaya konmasını gerekli kılmıştır. Bu tezde, KAA güvenliği için çeşitli algılama yöntemlerini ihtiva eden hibrit bir saldırı tespit sistemi modellenmiş olup, KAA'ların donanımsal kısıtları göz önünde bulundurularak, hesaplama karmaşıklığını ve tüketim belleğini azaltan veri madenciliğine dayalı ön işleme adımları kullanılmıştır. Geliştirilen modelde, normal ve saldırı trafiğinin ayırt edilebilmesi için makine öğrenme algoritmaları kullanılmış, saldırı profilleri oluşturmak için en güncel veri kümesi ile çalışılmıştır. Benzetim sonuçları, modellenen sistemin, yüksek doğruluk oranına ve düşük işlem süresine ulaştığını göstermektedir.

Bu tez çalışmasının her aşamasında beni yönlendiren ve bilimsel bir bakış açısı kazanmama vesile olan danışman hocam sayın Doç. Dr. Ebubekir ERDEM'e katkılarından dolayı müteşekkirim. Tez süresince desteğini esirgemeyen ve her koşulda yanımda olan değerli aileme ve yakın çalışma arkadaşlarıma teşekkür ederim.

Hamza ELBAHADIR
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Kablosuz Algılayıcı Ağlarda Yeni Bir Hibrit Saldırı Tespit Sisteminin Geliştirilmesi

Hamza ELBAHADIR

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Ocak 2022, Sayfa: xii + 106

Kablosuz algılayıcı ağlar (KAA); fiziksel ortamlardaki sıcaklık, basınç, titreşim, hız gibi değişkenleri algılamak ve sonuçlar üretmek için günümüzde birçok alanda kullanılmaktadır. Söz konusu ağlar, kritik ve hayati öneme sahip askeri, istihbari, sağlık ve doğal afetler gibi veri güvenliğin sağlanmasının önem arz ettiği alanlarda da kullanılmaktadır. Bununla birlikte KAA'lar, geleneksel ağlardan farklı alt yapı özelliklerine ve donanım kısıtlarına sahip olduğundan dolayı, bu ağlara yönelik etkili güvenlik önlemlerinin alınması elzemdir. Gelişen teknoloji ve değişen şartlar ile birlikte KAA'lara yönelik güvenlik önlemleri geliştirilmiştir. Saldırı tespit sistemleri, KAA güvenliğini sağlamak için geliştirilen etkili güvenlik çözümlerinden biri olmakla birlikte, günümüz şartlarında, STS'ler için önerilen algılama metotlarının, güvenliği sağlamak için tek başlarına yeterli olmayışı ve mevcut çalışmaların büyük bir kısmında güncelliğini yitirmiş veri kümelerinin kullanılması, KAA güvenliği için etkili ve güncel bir STS modeli ortaya konmasını gerekli kılmıştır. Bu tezde, STS'ler için önerilen algılama metotlarının hibrit olarak kullanıldığı bir model geliştirilmiş; modelde, KAA'ların kaynak kısıtlarına binaen, veri madenciliğine dayalı ön işleme adımları uygulanmıştır. Önerilen yaklaşımda, normal ve saldırı trafiğinin ayırt edilebilmesi için makine öğrenme algoritmaları kullanılmış, ağın eğitimi için en güncel veri kümesi referans alınmıştır. Benzetim sonuçları, önerilen modelin KAA'lar için kullanılabilecek performans ve güvenilirlikte olduğunu göstermiştir.

Anahtar Kelimeler: Kablosuz algılayıcı ağlar, saldırı tespit sistemi, makine öğrenmesi, hibrit sistem

ABSTRACT

Development of a New Hybrid Intrusion Detection System in Wireless Sensor Networks

Hamza ELBAHADIR

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Computer Engineering

January 2022, Pages: xii + 106

Wireless sensor networks (WSNs) are used in many areas today to detect variables such as temperature, pressure, vibration, speed in physical environments and to produce results. These networks are also used in critical and vital areas such as military, intelligence, health and natural disasters, where data security is important. However, since WSNs have different infrastructure features and hardware constraints than traditional networks, it is essential to take effective security measures for these networks. With the developing technology and changing conditions, security measures have been developed for WSNs. One of the effective security mechanisms recommended for WSNs is intrusion detection system (IDS). However, in today's conditions, the detection methods recommended for IDSs are not sufficient on their own to ensure security and the use of outdated data sets in most of the existing studies has necessitated an effective and up-to-date IDS model for WSN security. In this thesis, a model has been developed in which the proposed detection methods for WSNs are used as hybrids. In the model, due to resource constraints of WSNs, preprocessing steps based on data mining were applied. In the proposed approach, machine learning algorithms are used to distinguish between normal and attack traffic, and the most up-to-date data set are taken as reference for training the network. The simulation results have shown that the proposed model has the performance and reliability that can be used for WSNs.

Keywords: Wireless sensor networks, intrusion detection system, machine learning, hybrid system

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

KISALTMALAR

KAA	: Kablosuz Algılayıcı Ağ
STS	: Saldırı Tespit Sistemi
IDS	: Intrusion Detection System
GPS	: Global Positioning System
ANDES	: Anomaly Detection System
AIS	: Artifical Immune System
HMM	: Hidden Morcov Model
DoS	: Denial of Service
YSA	: Yapay Sinir Ağı
MANET	: Mobile Ad Hoc Network
MAC	: Media Access Control
AMoF	: Accumulated Measure of Fluctuation
LB-IDS	: Layer Trust-Based Intrusion Detection System
IWD	: Intelligent Water Drops
SVM	: Support Vector Machine
IoT	: Internet of Things
KB	: Küme Başı
MEMS	: Mikroelektromekanik Sistem
RF	: Radio Frequency
OSI	: Open Systems Interconnection
LEACH	: Low-Energy Adaptive Clustering Hierarchy
ULEACH	: Unequal Low-Energy Adaptive Clustering Hierarchy
HEED	: Hybrid Energy Efficient Distributed Clustering
UHEED	: Unequal Hybrid Energy Efficient Distributed Clustering
EDUC	: Energy-Driven Unequal Clustering
EEUC	: Energy Efficient Unequal Clustering
ULCA	: Unequal Layered Clustering Approach
EAUFC	: Energy Aware Unequal Fuzzy Clustering
EEHMC	: Energy Efficient Hybrid Multi Hop Clustering
HADCC	: Hybrid Advanced Distributed and Centralized Clustering
ECR	: Energy Consumption Ratio
VM	: Verifiable Multilateration
SERLOC	: Secure Range-Independent Localization
PDR	: Packet Delivery Ratio
FHSS	: Frequency Hopping Spread Spectrum
RTS	: Request to Send
CTS	: Clear to Send
DCF	: Distribute Coordination Function
CSMA/CA	: Carrier Sense Multiple Access with Collision Avoidance
MAC	: Message Authentication Code
RAEED	: Robust formally Analysed protocol for wirEless sEnsor networks Deployment
ACL	: Access Control List
MIC	: Message Integrity Code
PAN	: Personal Area Network
GTS	: Guaranteed Time Slot

1. GİRİŞ

Teknolojinin baş döndürücü hızla geliştiği ve anlamlı verinin kritik değere sahip olduğu günümüz dünyasında, fiziksel ortamlardan veri toplamak ve ilgili verileri işlemek, araştırmacıların yoğunlaştığı bir alan haline gelmiştir. Kablosuz algılayıcı ağlar, hızlı konuşlandırma, kendi kendine organize olabilme ve hata toleransı gibi avantajlı özelliklerinden dolayı ilk dönemlerde özellikle askeri alanlarda; komuta ve kontrol, haberleşme, gözetleme, keşif gibi amaçlarla kullanılmıştır [1].

Teknolojinin gelişmesi ve donanım maliyetlerinin düşmesine paralel olarak KAA'lar; sıcaklık, basınç, titreşim, hız, nem, ses, yön gibi birçok çevresel koşulları elde etmek amacıyla çok çeşitli alanlarda kullanılmaya başlanmıştır. KAA'ların uygulama alanları arasında, endüstriyel uygulamalar, akıllı ev ve alanlar, çevresel izleme, bilimsel çalışmalar gibi alanlar bulunmaktadır. Bununla birlikte sağlık hizmetleri, felaket algılama, askeri ve istihbari faaliyetler gibi kritik alanlarda da KAA'lar, yaygın olarak kullanılmaktadır. Verinin güvenli bir şekilde elde edilmesi ve transferinin kritik öneme sahip olduğu alanlarda, KAA güvenliği hayati önem taşımaktadır.

KAA'ların sınırlı enerji, hafıza ve hesaplama kapasitesi gibi donanımsal kısıtlar ile iletişim ortamı ve altyapısının geleneksel ağlardan farklı olması ve savunmasız bölgelere yerleştirilmesi gibi faktörler, KAA'ları saldırıya açık hale getirmektedir. Üstelik KAA'ların söz konusu kısıtları ve geleneksel ağlardan farklı altyapı ve mimariye sahip olmaları nedeniyle, KAA'lara yönelik farklı güvenlik çözümlerinin geliştirilmesi zaruridir. Araştırmacılar, KAA güvenliğini sağlayabilmek için birtakım güvenlik mekanizmaları önermişlerdir.

Silva vd. [2], spesifikasyona dayalı, dağıtılmış bir merkezi saldırı tespit mekanizması sunmuşlardır. Bu mekanizmada izleme düğümü adı verilen düğümler, herhangi bir düğümün herhangi bir kuralı ihlal edip etmediğini kontrol eder. Her düğüm için bir hata sayacı vardır. Bir düğüm, herhangi bir kuralı ihlal ederse, ilgili sayaç artırılır. Sayaç değeri, "t" zaman aralığında belirli bir "th" eşiğini aşarsa, o düğüm hakkında bir uyarı oluşturulur. Yazarlar, C++'da geliştirdikleri simülatör ile çalışmalarını test ederler. Sonuçlar, önerdikleri metodolojinin enerji açısından verimli olduğunu ve kara delik, seçici yönlendirme ve solucan deliği saldırıları için %100 algılama oranına ulaştığını göstermektedir.

Roman vd. [3], "bekçi köpeği" olarak bilinen bir komşu izleme tekniğini tanıtmışlardır. Onlara göre, saldırı tespit sistemi (STS) ajanı her algılayıcı düğüme kurulur ve radyo menzilinde bulunan düğümler ile komşusu olan düğümlerden gelen verileri denetler. Herhangi bir düğümün anormal çalışması durumunda uyarı üretilir.

Loo vd. [4], sabit genişlikli kümeleme algoritmasını önermişlerdir. Algoritmaya göre, STS ajanı her düğüme kurulur ve tüm düğümler izleme düğümleri olarak işlev görür. Bu yaklaşımda; alınan, gönderilen ve toplu yayın olarak yayınlanan paket sayısı gibi toplam 12 özellik tanımlanır. Bu özellikler, normal mesajlaşmada her bir komşu düğüm için ortalama veya standart sapmayı

belirlemek için kullanılır. Bu değerler, çeşitli saldırı senaryoları simüle edilerek hesaplanır ve kümelere yerleştirilir. Bu kümeler analiz edildikten sonra, tehlike altındaki düğümler tespit edilir. Bu modelin dezavantajı, özellik tanımlaması ve bu özelliklerin belirli saldırıları tanımlamak için kullanılmasıdır. Yazarlara göre, önerdikleri metodoloji, düşük yanlış pozitif oranı elde ederken simüle edilmiş yönlendirme saldırılarını verimli bir şekilde tespit edebilir.

Drozda ve Szczerbicka [5], yapay bağışıklık sistemi (Artifical Immune System, AIS) tabanlı bir algılama mekanizması sunar. Bu mekanizma, hesaplama açısından daha ucuzdur ve daha iyi algılama performansı sağlar. Bu metodolojiye göre, mesajlar göz önünde bulundurarak önce normal davranış öğrenilir, akabinde saldırı tespiti gerçekleştirilir. Yazarlar, önerilen metodolojileri için tasarım ilkelerini açıklarlar ve yaklaşımlarının etkinliğini göstermek için Network Simulator 2 (NS-2) uygulamasında simülasyon yaparak deneyler gerçekleştirirler.

Gupta vd. [6], saldırıları tespit etmek için merkezi bir anormallik tespit mekanizması (Anomaly Detection System, ANDES) önermişlerdir. ANDES, ulaşılabilir olup olmadığını bulmak için her düğüme rotalar oluşturur. ANDES, veri düzleminden ve yönetim düzleminden toplanan verilerle anormal düğümleri tespit eder.

Krontiris vd. [7], seçici yönlendirme ve kara delik saldırılarının tespiti için spesifikasyona dayalı bir kooperatif yerel denetim mekanizması önermişlerdir. Yaklaşımlarına göre, STS ajanı her algılayıcı düğüme kurulur ve düğümün mesajlarının kurallara uyup uymadığını kontrol eder. Spesifikasyonları ihlal ederse, kooperatif tespit motoruna bir uyarı gönderilir. Bu bileşen daha sonra o düğümün durumunu kontrol etmek için diğer düğümlerle iletişim kurar. Düğümlerin çoğu bu düğümün kötülüğünü doğrularsa, bir uyarı oluşturulur.

Bojkovic vd. [8], KAA'ların genel işleyişini etkileyen bir dizi saldırıyı kısaca incelemiştir. Onlara göre, "STS, az gelişmiş bir hizmettir, bir düğümün bir düşman tarafından altüst edilmesi ve kontrol edilmesi olasılığının olduğu senaryolar için yararlıdır". Gizli markov modeli (Hidden Morcov Model, HMM) kullanan bir algılama tekniği önerirler.

Rajasegarar vd. [9], anomali tabanlı tespit mekanizmaları üzerine bir araştırma yapmışlardır. Çalışmaları yalnızca anomali tabanlı tekniklere odaklanmaktadır.

Shaikh vd. [10], güvenliği ihlal edilmiş düğümleri tanımlamak için bir algoritma önermişlerdir. Tehlikeye giren düğümler, normal düğüm(ler) hakkında yanlış alarmlar oluşturabildiğinden, bu düğümleri tespit için dağıtılmış işbirlikçi STS'ler geliştirmişlerdir. Tespit yöntemi iki aşamalı olarak çalışır. Öncelikle herhangi bir anormal düğümün bildirilmiş olup olmadığına bakılır. Bilgi mevcut değilse tehdit düzeyine göre n sayıda komşuyu rastgele seçer ve onay talebi paketleri gönderir. Herhangi bir düğüm, onay talebi paketini aldığında karar aşaması etkinleşir. Bu aşama; rastgele seçilen düğümlerden alınan yanıtlara göre, doğrulama (düğüm anormal), fikir birliği yok (tanımlanmamış) ve geçersiz kılma (uyarıyı gönderen düğüm tehlikeye

atılmış) olmak üzere üç kararlı sistemdir. Önerilen bu model, tehlikeye atılmış düğümleri tespit etmeye yardımcı olmakla birlikte enerji tüketimini, hesaplama ve kontrol ek yükünü de artırır.

Ahmed vd. [11], bir başka anormal düğüm algılama tekniği önermişlerdir. Güvenliği ihlal edilen düğümleri belirlemek için hem imza hem de anomali tabanlı teknikleri kullanırlar. Bu teknikte, algılayıcı ağ, çiftlere bölünmüştür. Her algılayıcı düğüm, eşleştirme düğümünün davranışını denetler. Bu yaklaşımın, çiftlerin oluşturulması ve anormal aktivite için tespit mekanizması olmak üzere iki zorluğu vardır.

Li vd. [12], grup bazlı bir tespit mekanizması sunmuşlardır. Bu mekanizmada, algılayıcı ağ n sayıda gruba bölünmüştür. Yazarlar, belirli bir grubun tüm düğümlerinin, ortamın bazı belirli özelliklerini algılamak gibi aynı görevi yerine getirmesi gerektiğini varsayar. Bununla birlikte algılanan bilgiler, belirli bir eşik değeri ile birbirinden farklı olmalıdır. Başlangıçta, algılayıcı düğümler, algılanan veriler arasındaki benzerlik temelinde birlikte gruplandırılır. Bu bilgiler, saldırı senaryoları sırasında belirli bir düğümün, anormal aktivitesini tespit etmek için kullanılabilir. Belirli bir düğümün arızalı olduğu tespit edilirse, yönlendirme tablosundan kaldırılır. Yazarlar, önerilen metodolojiyi uyguladıktan sonra düşük yanlış alarm oranı bulduklarını belirtmektedirler.

Zhang vd. [13], tehlike altındaki işaret düğümlerini verimli bir şekilde tespit eden grafik tabanlı bir yaklaşım sunarlar. STS ajanının, işaret düğümlerine kurulduğu varsayılır. İşaret düğümleri, algılayıcı düğümlere konum bilgisi sağlar. Güvenliği ihlal edilmiş bir işaret düğümü, diğer düğümler hakkında yanlış bilgi iletir ve yönlendirme protokolünün performansını düşürür. Baz istasyonu, bu uyarıları herhangi bir güvenli aktarım protokolü ile alır. Verimli miktarda veri toplandıktan sonra, bilgilerin güvenilir bir kaynaktan alınıp alınmadığını bulmak için önerilen grafik teorisine dayalı tespit mekanizmasını uygular. Bu yaklaşımın yazarları, uygulamaya bağlı bir çerçeve önermektedir. Odak noktaları ister güvenilir ister riskli olsun, bilgi kaynağını tanımlamaktır. Küresel konumlandırma sistemi (Global Positioning System, GPS), her bir algılayıcı düğüme kurulursa pahalıdır. İşaret düğümü kavramı, konuma dayalı yönlendirmeye sahip ağlar için kaynak açısından verimlidir.

Tiwari vd. [14] tarafından önerilen STS mekanizması, davranışları normal veya anormal olarak belirleyen kuralların tanımlandığı, spesifikasyona dayalı yaklaşımı izler. Kara delik ve seçici yönlendirme saldırılarını tespit etmek için düğüm tarafından bırakılan mesajların sayısı kullanılır. Küme başı, kendi kümesinde paketleri gönderip alan düğümlerin yasal olup olmadığına ilişkin kararları almakla sorumludur.

Farid vd. [15], farklı tipteki ağ saldırılarının tespiti için veri madenciliği yöntemlerinden Bayes sınıflandırıcı ve karar ağacı kullanmışlardır. Önerilen algoritma, öznitelikle uğraşma, eksik öznitelik değerleriyle başa çıkma ve eğitim verilerindeki gürültüyü azaltma gibi veri madenciliğinin bazı zorluklarını da ele almaktadır.

Mamun vd. [16], farklı STS yaklaşımlarını kıyaslayarak, yeni bir STS önermişlerdir. Bu mimaride, algılayıcı ağın toplam alanı birkaç bölgeye bölünür. Her bölgedeki algılayıcı düğümler, bir küme düğümü tarafından izlenir. İki veya daha fazla küme düğümü, bölgesel bir düğüm tarafından izlenir. Buna karşılık, bölgesel düğümler baz istasyonu tarafından kontrol edilir ve izlenir.

Chitrakar ve Huang [17], anormal davranış tespiti için hibrit bir yöntem önermişlerdir. Yazarlar, k-Medoid tabanlı kümeleme tekniği ile Naïve Bayes sınıflandırma tekniğini birleştirerek hibrit öğrenme yaklaşımını uygulamaya çalışmışlardır.

Coppolino vd. [18], veri madenciliği tekniklerini kullanarak KAA'da gelişmiş bir STS modeli önermektedirler. Önerilen STS'de merkezi ve yerel ajanlar olmak üzere iki tür ajan sınıflandırılmıştır. Merkezi ajan, sunucuda saldırı tespiti için nihai kararı veren baz istasyonu olarak konumlandırılırken, yerel ajanlar düğümlerde bulunur.

Sajjad vd. [19], komşu düğümün güven hesaplamasına dayalı bir saldırı tespit tekniği sunmaktadır. Önerilen STS'de her bir düğüm, komşu düğümlerin güven düzeyini gözlemler. Bu güven değerlerine dayanarak; komşu düğümler güvenilir, riskli veya kötü niyetli olarak ilan edilebilir. Önerilen şema, ağ istatistiklerini ve kötü niyetli düğüm davranışını analiz ederek Hello taşkını, sıkışma ve seçici yönlendirme saldırılarını başarıyla algılar. Benzetim sonuçları, ağın komşu düğüm güven yönetimine dayalı anormallik algılama tekniği uygulandığında daha iyi performans verdiğini göstermektedir.

Balakrishnan ve Rino [20], kurala dayalı bir anormallik tespit şeması kullanarak, izinsiz girişleri belirlemeye ve tespit etmeye çalışmışlardır. Anormallik algılama, tanımlanan kurallar çerçevesinde gerçekleştirilir. Çalışmada, ağdaki farklı düğümler arasından bir dizi küme başı seçilir ve geri kalan düğümler, bunlarla kümelenir. Küme başları, kendi küme üyelerinden izinsiz girişleri algılama verilerini alır. Ayrıca küme başları, yönlendirme yapısının omurgasını oluşturdukları için diğer küme başlarına yönelik saldırıları da algılayabilir. Bununla birlikte küme başları, kendi küme üyeleri tarafından izlenir. Küme başlarından herhangi biri anormal olarak algılanırsa, küme başı izleme ekibi tarafından iptal edilir. Kötü niyetli küme başının tanımlanması ve iptal edilmesinden sonra, küme üyeleri arasından başka bir küme başı seçilir. Yazarlar algoritmanın performansını değerlendirmek için C++ ile uygulanan özel geliştirilmiş bir simülasyon aracı kullanmışlardır.

Almomani vd. [21], dört tür hizmet reddi saldırısının (blackhole, grayhole, flooding ve scheduling) daha iyi tespit edilmesine ve sınıflandırılmasına yardımcı olmak amacıyla, KAA'lar için özel bir veri kümesi geliştirmişlerdir. Toplanan veri kümesine WSN-DS (Wireless Sensor Network-Dataset) adı verilir. Yapay sinir ağı (YSA), farklı hizmet reddi saldırılarını (Denial of Service, DoS) tespit etmek ve sınıflandırmak için veri kümesi ile eğitilmiştir. Sonuçlar, WSN-DS'nin, STS'nin daha yüksek sınıflandırma doğruluk oranı elde etme yeteneğini geliştirdiğini göstermektedir.

Ozcelik vd. [22], kümelenmiş ağlar için hibrit bir saldırı tespit sistemi önermişlerdir. Önerilen yöntemin ana fikri, her düğümün komşularını gözetlemesine dayanmaktadır. Söz konusu mekanizma için, beş işlevsel itibar ölçütü tanımlanmıştır. Baz istasyonu, işlevsel itibar değerlerini ve kötüye kullanım algılama kurallarını birleştirerek kötü niyetli düğümleri tespit eder. Benzetim sonuçlarına göre önerilen yaklaşım, enerji tüketimini artırmadan merkezi bir şekilde kötü niyetli düğümleri tespit ederek ağ ömrünü uzatır ve algılanan veri tazeliğini iyileştirir. Yapılan çalışmada, enerji tüketimine dair sonuçlar verilmesine rağmen, saldırı türleri ve bu saldırıları tespit oranlarına değinilmemiştir.

Amouri vd. [23], KAA ve mobil özel amaçlı ağlar (Mobile Ad Hoc Network, MANET) için çapraz katmanlı, anormallik tabanlı bir STS önermişlerdir. Bu çalışmada önerilen saldırı tespit şeması, katmanlar arası özellik toplama ve paket sayılarına dayanmaktadır. Önerilen STS'de kullanılan veri toplama şeması, rastgele izlemeye ve komşu düğümlerin trafik aktivitesini gizlice dinlemeye dayanır. Yazarlar, kötü niyetli düğümleri tespit etmek için iki seviyeli bir tespit şeması kullanmaktadırlar. İlk seviye, rastgele modda çalışan özel algılayıcılardan oluşur. Her bir algılayıcı, çeşitli ağ katmanlarından bilgi yakalar ve miktarları hesaplar. Burada karar ağacı tabanlı bir sınıflandırıcı (C4.5 veya rastgele orman) kullanılır. Bu miktarlar daha sonra, birikmiş dalgalanma ölçüsünü (Accumulated Measure of Fluctuation, AMoF) hesaplayan bir süper düğümde toplanır. Yazarlara göre, AMoF'nin yeni bir özellik olarak kullanılması, özellikle küçük boyutlu veri kümeleri için umut verici sonuçlar vermiştir.

Acharya ve Singh [24], KAA'larda saldırı tespiti için akıllı su damlaları (Intelligent Water Drops, IWD) algoritmasına dayanan bir model önermişlerdir. Çalışmada, gürültülü ve ilgisiz özellikler içeren veri kümelerinin, sınıflandırıcı tarafından genellikle düşük algılama ve yüksek yanlış sınıflandırma oranlarına yol açtığına vurgu yapılmıştır. Önerilen yöntemde, seçilen özelliklerin değerlendirilmesi için sınıflandırıcı olarak destek vektör makinesi (Support Vector Machine, SVM) ile birlikte özellik alt kümesi seçimi için IWD algoritması kullanılır. Deneysel sonuçlar, önerilen modelin mevcut yaklaşımlardan daha yüksek algılama oranı, düşük yanlış alarm oranı ve gelişmiş doğruluk açısından daha iyi performans gösterdiğini göstermektedir.

Ghugar vd. [25], KAA'ların farklı katmanlarının güvenilirliğini göz önünde bulunduran bir STS yaklaşımı (Layer Trust-Based Intrusion Detection System, LB-IDS) sunmuşlardır. Yazarlar; temel olarak, fiziksel katman güveni, MAC katmanı güveni ve ağ katmanı güveni gibi üç katmandaki güvenilirliği dikkate almaktadırlar. Bir algılayıcı düğümün, belirli bir katmandaki güveni, o katmanın temel güven ölçümleri alınarak hesaplanır. En sonunda, algılayıcı düğümünün genel güven değeri, her katmanın bireysel güven değerlerini birleştirerek tahmin edilir. Güven eşiği uygulanan algılayıcı düğüm, güvenilir veya kötü niyetli olarak algılanır. Simülasyonlar kullanılarak fiziksel katmanda sıkışma saldırısı, MAC katmanında geri çekilme saldırısı ve ağ katmanında düden saldırısı uygulanmıştır. Ayrıca, bir saldırganın aynı anda MAC katmanına ve ağ katmanına

saldırdığı simüle edilerek, bir çapraz katman saldırısı uygulanmıştır. LB-IDS'nin performansı; tespit doğruluğu, yanlış pozitif oranı ve yanlış negatif oranı gibi üç performans parametresinin sonuçları Wang'ın planının sonuçlarıyla karşılaştırılarak değerlendirilir. Benzetim sonuçlarına göre LB-IDS, Wang'ın şemasına kıyasla daha iyi bir performans göstermektedir.

Darabi [26], KAA güvenliği için anomali ve imza tabanlı algılama metotlarının kullanıldığı hibrit bir saldırı tespit sistemi önermiştir. Önerilen yaklaşımda, ağ trafiğinde gezen paketler, algılama metotlarıyla filtreden geçirilerek, normal veya saldırı şeklinde tanımlama yapılır. Farklı sınıflandırma algoritmalarının performans değerleri, verilen benzetim sonuçlarıyla gösterilmiştir. Ayrıca önerilen yaklaşımın, diğer çalışmalara göre kıyası ve üstünlükleri çeşitli parametrelere göre gösterilmiştir. Söz konusu çalışmanın en büyük dezavantajı, güncelliğini yitirmiş KDDCup'99 veri kümesinin kullanılmasıdır.

Yang vd. [27], ağda bulunan kötü amaçlı düğümleri daha verimli bir şekilde tanımlamayı amaçlayan yeni bir algoritma önermişlerdir. Önerilen yaklaşımda, küme başı düğümleri, gelişmiş LEACH yönlendirme protokolüne göre seçildikten sonra ağdaki diğer düğümler, kümeler oluşturur ve paket dağıtım yollarını belirler. Akabinde her düğüm, paketi alıcı düğüme göndermeden önce düğüm numarasını ve itibar değerini pakete ekler. Daha sonra havuz düğüm, paketlerden elde edilen düğüm numaralarıyla, kaynak düğüm numaralarını karşılaştırır ve şüpheli düğümlerin listesini oluşturur.

Paul vd. [28], internete entegre edilmiş KAA'lara yönelik çeşitli saldırıları tespit edebilmek için bir STS önermişlerdir. Çalışmada KAA'ların, nesnelerin interneti (Internet of Things, IoT) yapısına dahil edilmesine yönelik yöntemler ve söz konusu yapının güvenlik gereksinimleri ele alınmış, hizmet reddi saldırılarına yönelik STS önerilmiştir. Önerilen yaklaşım, nöro-bulanık teknikler kullanılarak tasarlanmış anomali tabanlı bir sistemdir.

Gandhimati ve Murugaboopathi [29], küme tabanlı KAA'larda kötü amaçlı düğümlerin tespiti için mobil aracılar kullanılmasını önermişlerdir. Bu yöntemde tüm algılayıcı düğümleri doğrulamak yerine yalnızca küme başları doğrulanır. Önerilen yaklaşımda önce belirlenen kurallar ile anomali tespiti, akabinde kümeleme ve küme başı seçimi, son adımda ise verilerin baz istasyonuna iletilmesi gerçekleştirilir.

Narayanan vd. [30], KAA'lar için tehlikeli iki saldırı tipi olan kara delik ve solucan deliği saldırılarına karşı Naive Bayes sınıflandırıcısını kullanmışlardır. Yazarlar, yetki kodunu kullanarak kara delik saldırılarının analiz edilebileceğini belirtmişlerdir. Kara delik saldırısı durumunda, yetki kodu olmayan bir düğüm, kötü niyetli düğüm olarak kabul edilmekte ve ağdan atılmaktadır. Benzer şekilde solucan deliği ve sahte hedef saldırılarının, veri iletim süresi yardımıyla tespit edilebileceğini göstermişlerdir. Paket belirli bir süre içinde hedefe ulaşmazsa, ağda solucan deliği oluşumu otomatik olarak algılanmaktadır. Önerilen yöntem, ağ simülatörü (NS2) üzerinde deneysel olarak doğrulanmıştır. Önerilen yöntemin ana avantajı, iletişim yükünü azaltmaktır.

Bu tez çalışmasında, literatürde bulunan mevcut çalışmaların eksik yönleri göz önünde bulundurularak, KAA güvenliği için etkili ve güncel bir saldırı tespit modeli ortaya konmuştur. Ortaya konan modelin katkıları şu şekilde sıralanabilir.

- Saldırı tespiti için önerilen algılama metotları, günümüz şartlarında tek başına yeterli güvenliği sağlayamadığı için, söz konusu metotlar birleştirilerek hibrit bir model önerilmiştir. Algılama metotlarından birinin tespit edemediği veya yanlış alarm oluşturduğu durumda diğer metodun devreye girmesiyle daha etkili bir saldırı tespiti sağlanmıştır.
- Hibrit bir modelin güvenliği garanti altına almakla birlikte, donanım kaynaklarını daha fazla kullanacağı öngörülerek, sistemin hesaplama karmaşıklığı ve kaynak kullanımını minimize etmek amacıyla, veri kümesi üzerinde, veri madenciliği ön işleme adımları uygulanmıştır.
- KAA güvenliği için yapılan mevcut çalışmaların aksine, saldırı profilleri oluşturmak ve makine öğrenmesi için ağı eğitmek amacıyla güncel bir veri kümesi olan IDS2018 kullanılmıştır. Güncelliğini yitirmiş veri kümelerinden elde edilen sonuçların, yeni nesil saldırılara karşı yetersiz ve güvensiz olacağı muhakkaktır.
- Normal ve saldırı trafiğini analiz edebilmek için farklı makine öğrenme algoritmaları ile sınıflandırmalar yapılmış ve çeşitli parametrelere göre algoritmaların performans değerleri sunulmuştur.
- En iyi performansa sahip makine öğrenme algoritması tespit edilmiş, ilgili algoritmanın daha iyi sonuçlar üretebilmesi için birtakım optimizasyonlar yapılmıştır.

Bu tez çalışması, altı bölümden oluşmaktadır.

Bölüm 1'de, tezin konusu açıklanmış, önemine ve başlıca amacına değinilmiştir. Literatürde yapılan mevcut çalışmalar incelenerek, eksik ve zayıf yönleri belirtilmiş ve tezde yapılan çalışmalara yer verilerek, tezin katkıları ele alınmıştır.

*Bölüm 2'*de, KAA'ların karakteristik özelliklerine, donanımsal kısıtlarına ve mimari yapılarına değinilmiştir. KAA'ların genel işleyişi ve mimarileri, bu bölümde detaylı bir şekilde incelenmiştir.

Bölüm 3'te, KAA'ların güvenlik ilkelerine, katmanlarına yönelik gerçekleştirilen saldırı tiplerine ve geliştirilen güvenlik mekanizmalarına değinilmiştir. KAA güvenliği için etkili bir güvenlik çözümü olan STS'ler ele alınmış, STS bileşenleri ve çalışma prensipleri incelenmiştir.

Bölüm 4'te, tezde kullanılan materyal ve metotlar ele alınmıştır. STS geliştirmek için kullanılan materyaller, önerilen algılayıcı ağ modeli ve geliştirilen saldırı tespit sistemi modeli irdelenmiştir. Modellenen STS'de kullanılan algılama metotlarının çalışma mekanizmaları, KAA performansı için veri kümesine uygulanan ön işleme adımları, normal ve saldırı trafiğini

sınıflandırmak için makine öğrenme algoritmalarının kullanılması ve optimize edilmesi gibi işlemler, bu bölümde icra edilmiştir.

Bölüm 5'te, ön işleme adımlarının ve algoritmaların uygulanması neticesinde elde edilen bulgular incelenmiş, algoritmaların birbirlerine üstünlükleri kıyaslanmıştır.

Bölüm 6'da, önerilen modelin genel değerlendirmesi yapılmıştır. Ayrıca tezin teknik, akademik ve ekonomik etkilerine/katkılarına değinilmiştir. Akabinde teze konu olan model ile ilgili geleceğe dair birtakım önerilerde bulunulmuştur.

2. KABLOSUZ ALGILAYICI AĞLARIN ÖZELLİKLERİ

KAA'lar, kullanım amaçlarına bağlı olarak, birbirine bağlı yüzlerce hatta binlerce algılayıcı düğümden oluşan ve önceden tasarlanan ağ topolojilerinin aksine, yapılarını dinamik olarak organize eden ağlardır. KAA'lar, fiziksel koşulları izlemek ve değerlendirmek için kullanılan büyük, maliyetli ve uygulaması zor geleneksel algılayıcı sistemlerin aksine basit, maliyeti düşük, yüksek performansa sahip ve kurulumu kolay ağlardır. Bununla birlikte her türlü çevresel koşullara uygulanabilme özelliği sayesinde, verinin güvenli elde edilmesinin ve iletilmesinin hayati öneme sahip olduğu alanlar da dahil olmak üzere çok yaygın kullanım alanına sahiptir [31].

KAA'lar geniş alanlara uygulanan dağıtık ağlar olup, yoğun bir bakıma ihtiyaç duymazlar. Söz konusu ağları oluşturan düğümlerin her biri nispeten küçük bir alandan veri toplasa da düğümlerin eş zamanlı ve kooperatif olarak çalışmaları neticesinde makro düzeyde geniş bir ağ kapsamı elde edilmiş olur. Teorik olarak sınırsız bir alana uygulanabilme özelliğine sahip olan KAA'lar, maliyet ve kurulum kolaylığı açısından avantajlı olduğu gibi güvenilirlik, esneklik ve hata toleransı bakımından da geleneksel ağlara kıyasla çok daha iyi performans göstermektedirler. Zira geleneksel makrosensör ağlarda herhangi bir düğümün hata vermesi, o lokasyonda sistemin işlevini yitirmesi anlamına gelirken, KAA'larda ise mikrosensör düğümü hata verse bile ilgili lokasyondan veri akışı devam eder. Bu avantajlarına rağmen KAA'ların sınırlı enerji ve hesaplama gücü ile iletişim mimarisi, geniş bir coğrafyada yüksek sayıda algılayıcı düğüm kullanımını gerektirir [32].

KAA'ların etkin ve verimli bir şekilde uygulanabilmesi için karakteristik özelliklerinin ve mimari yapılarının bilinmesi gereklidir. Bu bölümde KAA'ların genel çalışma prensipleri hakkında bilgi verilerek, karakteristik özellikleri ve mimari yapıları ele alınmıştır.

2.1. Kablosuz Algılayıcı Ağların Karakteristik Özellikleri

KAA'lar, belirli bir fiziksel ortamdan çeşitli verileri elde etmek ve değerlendirmek amacıyla kablosuz olarak birbirine bağlı yüzlerce hatta binlerce algılayıcı düğümden oluşmaktadır. Mekânsal olarak dağıtık halde bulunan her bir düğüm, ağdaki diğer düğümlerle iletişim kurabilen ve iş birliği halinde çalışabilen bir yapıya sahiptir. Mikro düzeyde işlev gören düğümlerin, büyük ölçeklere uygulanması ve dinamik bir topoloji kullanmaları, kısıtlı donanımsal kaynaklarına ve enerjiye sahip olmaları, yaşam sürelerinin öngörülemezliği, çoğunlukla savunmasız alanlara kurulu olması gibi karakteristik özellikleri, bu ağlara özgü güvenlik çözümleri üretilmesini gerekli kılmaktadır.

2.1.1. Kısıtlı Kaynak

KAA tasarımında, maliyeti azaltmak ve düğüm sayısını artırarak daha geniş coğrafi alanlara kurulum yapabilmek için, algılayıcı düğümlerin boyutunun küçültülmesi ve doğal olarak

kaynakların sınırlandırılması gerekir. Düğümlerin fiziksel olarak boyutlarının küçültülmesine paralel olarak enerji kapasiteleri de azalır. Ağı oluşturan düğümler, sınırlı işlem ve hesaplama kapasitesine, düşük depolama alanına ve kısıtlı iletişim bant genişliğine sahiptir. Bu sınırlamalar nedeniyle geleneksel ağlarda kullanılan güvenlik mekanizmalarını, KAA'lar için kullanmak mümkün değildir. KAA'ların temel kaynak kısıtları şu şekildedir:

Enerji

KAA'nın en önemli kısıdı hiç şüphesiz, enerjidir. Zorlu ortamlarda veya askeri amaçlı gibi bazı KAA uygulamalarında, düğümlerin güç kaynaklarının yenilenmesi imkânsız olabilir. Dolayısıyla ağın sürdürülebilir olması, düğümlerin pil ömrüne doğrudan bağımlıdır. Algılayıcı düğümlerdeki enerji tüketimi; verinin algılanması, algılayıcı düğümler arasındaki iletişim ve mikroişlemci hesaplaması için kullanılmaktadır. [33, 34]'teki çalışmalar ile KAA'larda iletilen her bir bitin, yaklaşık 800-1000 mikroişlemci talimatını yürütmek kadar enerji tükettiği bulunmuştur. Söz konusu çalışmalar, KAA'larda iletişimin, hesaplamadan daha maliyetli olduğunu göstermektedir. Gerek ağa yönelik saldırılar sonucu düğümlerin aşırı trafiğe zorlanması gerekse de geliştirilen güvenlik mekanizmalarının neden olacağı ek yük, daha fazla enerji tüketimine sebep olacaktır. Bu sebeple KAA'ların donanım kısıtları ve enerji maliyetleri göz önünde bulundurularak güvenlik çözümleri geliştirilmelidir.

Donanımsal Kısıtlar

Algılayıcı düğümlerde donanımsal kısıtlamalar, temelde hesaplama ve bellek birimlerine yöneliktir. Fiziksel ortamlardan elde edilen verilerin hesaplanması için düğümlere gömülü işlemciler bulunmaktadır. Bu işlemciler, geleneksel işlemciler kadar güçlü olmadığından, hesaplama karmaşıklığı gerektiren güvenlik mekanizmaları KAA'lara uygulanamaz.

Algılayıcı düğümlerdeki bellek ise genellikle flash bellek ve RAM'den oluşmaktadır. Flash bellek, uygulama kodunu saklamak için; RAM ise uygulama programlarını, algılayıcının elde ettiği verileri ve ara hesaplamaları depolamak için kullanılır. Bununla birlikte düğümün bellek miktarı düşük olduğundan, işletim sistemi ve uygulama kodu yüklendikten sonra, algoritmaları çalıştırmak için sınırlı bellek miktarı kalır [35]. Gerek hesaplama kapasitesinin düşüklüğü gerekse de depolama biriminin kapasitesi göz önünde bulundurulduğunda, geleneksel ağlara uygulanan güvenlik mekanizmaları ile hesaplama karmaşıklığı gerektiren algoritmalar, KAA'lara uygulanamaz.

İletim Ortamı

Algılayıcı düğümlerin paket iletim aralığı hem teknik olarak hem de enerji tasarrufu ihtiyacı ile sınırlıdır. Düğümün gerçek sinyal iletim menzili, kurulu olduğu lokasyondaki hava ve arazi şartları gibi çevresel faktörler ile doğrudan ilgilidir [35].

KAA'ların paket tabanlı yönlendirmesi, bağlantısız protokollere dayandığından dolayı doğası gereği güvenilmezdir. Ayrıca kablosuz iletim ortamı ve paketlerin kanalda sıkışması/çarpışması durumları da iletişimi güvensiz kılmaktadır. Geliştirilen güvenlik mekanizmaları ise ek maliyete yol açmaktadır [36].

KAA'ların iletim ortamıyla ilgili bir başka handikap ise paketin gecikmesi ile ilgilidir. Bir KAA'da çok sekmeli yönlendirme (multi-hop routing), ağ tıkanıklığı ve ara düğümlerdeki işleme, paket iletiminde daha yüksek gecikme süresine yol açabilir. Bu durum, senkronizasyonun elde edilmesini zorlaştırır. Kriptografik anahtar dağıtımına dayanan bazı güvenlik mekanizmaları, senkronizasyon sorunlarından dolayı güvenlik açısından kritik olabilir [37]. Tablo 2.1'de bazı algılayıcı düğümlerin donanımsal özellikleri gösterilmiştir [38].

Tablo 2.1. Bazı algılayıcı düğümlerin donanımsal özellikleri

Ad	CPU	Hız	Enerji RX	Enerji TX	Program Hafızası	Veri Hafızası	Flash
Eyes	TI MSP430F149	5 MHz	1.8-4.8 mA	5.33-12 mA	4 kB (EEPROM)	N/A	60 kB
iMote2	Intel PXA271 Xscale	13-416 MHz	44-66 mA	44-66 mA	N/A	N/A	32 MB
Iris	Atmel ATmega1281	16 MHz	16 mA	10-17 mA	4 kB (EEPROM)	512 kB (Serial Flash)	128 kB
Mica	Atmel ATmega128L	8 MHz	5 mA	7-12 mA	4 kB (EEPROM)	4 Mbit (External Flash)	128 kB
Mica2	Atmel ATmega128L	8 MHz	9.6 mA	16.5 mA	4 kB (EEPROM)	N/A	128 kB
Mica2Dot	Atmel ATmega128L	8 MHz	10 mA	27 mA	4 kB (EEPROM)	512 kB (Serial Flash)	128 kB
MicaZ	Atmel ATmega128L	8 MHz	19.7 mA	11-17.4 mA	4 kB (EEPROM)	512 kB	128 kB
Rene 2	Atmel ATmega163	8 MHz	1.8-3.8 mA	12 mA	512 B (EEPROM)	N/A	16 kB
Shimmer	TI MSP430F1611	8 MHz	18.8-50 mA	17.4-50 mA	N/A	2 GB (microSD)	48 kB
SunSpot	Atmel ARM920T	180 MHz	18.8-19.7 mA	17.4 mA	N/A	N/A	4 MB
Telos/ Tmote	TI MSP430F149	8 MHz	18.8-23 mA	17.4-21 mA	512 kB (EEPROM)	N/A	60 kB
TMote Sky/ TelosB	TI MSP430F1611	8 MHz	19.7-23.0 mA	17.4 mA	1 MB (External Flash)	N/A	48 kB

2.1.2. Ölçeklenebilirlik

Kablosuz algılayıcı ağlar, kişisel sağlık uygulamaları gibi kısıtlı düğüm sayısı gerektiren alanlardan; çevresel izleme, felaket durumlarını tespit, saha gözetimi gibi geniş ölçekli alanlara

kadar birçok fiziki ortamdan veri toplayabilmektedir. KAA'ların geniş ölçekli alanlarda etkin bir şekilde kullanılabilmesi için, hedef lokasyona yüzlerce hatta binlerce algılayıcı düğümün konuşlandırılması gerekir.

KAA'ların donanımsal kısıtlarından kaynaklı sınırlı sinyal kapasiteleri ve yüksek ölüm oranları da ağın içerisinde bulunan algılayıcı düğümlerin sayısını arttıran faktörlerdendir [39]. Bir kablosuz algılayıcı ağın yoğunluğu 2.1'deki denkleme göre hesaplanabilir [40].

$$\mu(R) = (N \cdot \pi R^2)/A \tag{2.1}$$

Denklemde bulunan N, A lokasyonuna konuşlandırılan algılayıcı düğüm sayısını, R radyo iletim aralığını göstermektedir. $\mu(R)$ ise ağ yoğunluğunu, nominal kapsama alanı başına düşen düğüm sayısı cinsinden ifade etmektedir.

2.1.3. Hata Toleransı

Fiziksel ortamdan algılanan verilerin devamlılığının sağlanması ve söz konusu verilerin güvenli olarak baz istasyonuna iletilmesi için, algılayıcı düğümlerin sürekli işlevsel tutulması önemlidir [41]. Bununla birlikte KAA'ların, savunmasız/zorlu ortamlara konuşlandırılmaları, kısıtlı pil ömrü ve diğer donanımsal kısıtları, donanım bileşenlerinde meydana gelen arızalar, iletim ortamından kaynaklı problemler, çevresel faktörler veya algılayıcı düğümlere fiziksel müdahaleler gibi birçok nedenden dolayı algılayıcı düğüm devre dışı kalabilir [42, 43].

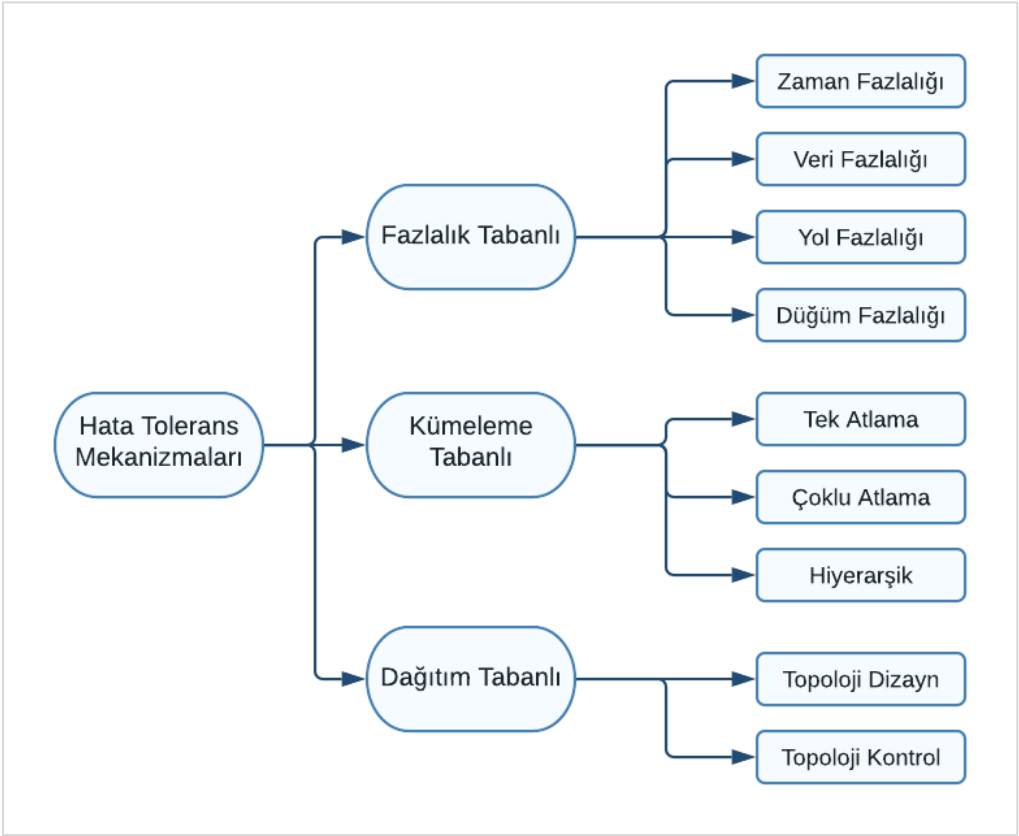
Hata toleransı, KAA'larda verilerin güvenli iletimi için kritik öneme sahiptir. Algılayıcı düğümlerdeki herhangi bir arıza, kesinti veya kötü niyetli saldırılara karşı sistemin işlevini kesintisiz olarak sürdürebilmesi ve hazır durumda bulunması gereklidir. Örneğin, afet yönetimi gibi bazı kritik görev uygulamalarında, hayatta kalanları kurtarma potansiyelini artırmak ve kurtarma ekibinin güvenliğini sağlamak için sistemin güvenliği ve sürdürülebilirliği hayati önem taşımaktadır [44]. Bu nedenle hata toleransı, KAA tasarımının önemli bir bileşenidir.

KAA'larda güvenilirlik veya bir düğümün hata toleransı, Denklem 2.2'de hesaplanmıştır [45]. Söz konusu hesaplamada, belirli bir zaman aralığı içerisinde hata olmaması olasılığını yakalamak için Poisson dağılımı kullanılmıştır.

$$R_k(t) = e^{-\lambda_k t} \tag{2.2}$$

$R_k(t)$ ağın güvenilirliğini yani düğümün hata toleransını göstermektedir. λ_k, k düğümünün hata oranı, t ise zaman periyodudur.

KAA'larda hata toleransını sağlayabilmek için çeşitli mekanizmalar önerilmiş olup, tüm bu yöntemler temelde üç kategoride sınıflandırılabilir: Fazlalık tabanlı mekanizmalar, kümeleme tabanlı mekanizmalar ve dağıtım tabanlı mekanizmalar [41]. Hata tolerans mekanizmaları, Şekil 2.1'de gösterilmiştir.



Şekil 2.1. Hata tolerans mekanizmaları

Fazlalık Tabanlı Mekanizmalar

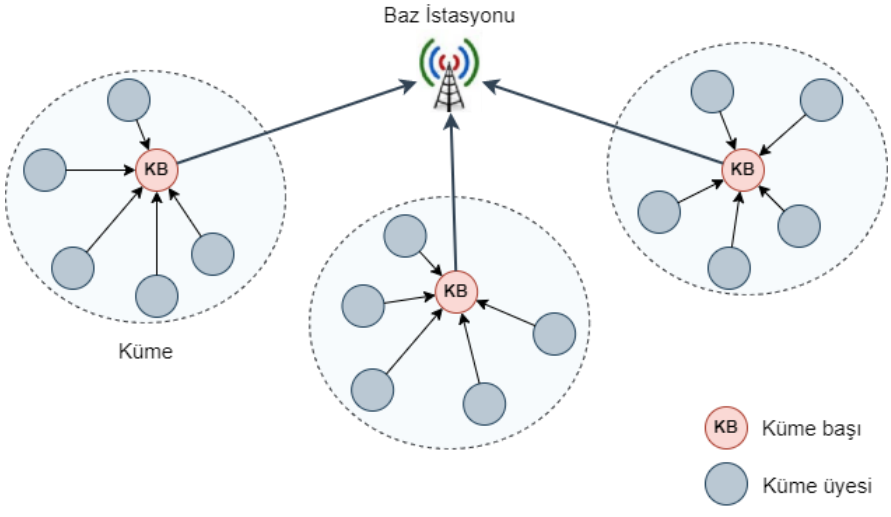
Fazlalık, fiziksel bir ortamı algılayarak benzer sonuçlar üretebilen ek veya yinelenen kaynaklar olarak tanımlanabilir [46]. Araştırmacılar, hata toleransını sağlayabilmek için; zaman fazlalığı, veri fazlalığı, yol fazlalığı, düğüm fazlalığı gibi fazlalığa dayalı çeşitli mekanizmalara dayalı yöntemler önermişlerdir [47, 48]. Söz konusu teknikler, kaynakların yinelenerek kullanılmasına ve hata durumunda alternatif kaynaklardan gelen verilerle güvenilir sonuçlar elde edilmesine dayanır. Örneğin düğüm fazlalığı mekanizmasında, belirli bir lokasyondaki ölçümler, yoğun bir şekilde konuşlandırılmış algılayıcı düğümlerle sağlanır. Aynı yerde, aynı değişkeni ölçen düğümlerden birine yönelik kötü niyetli saldırı durumunda bile veriler, diğer düğümler tarafından algılanmaya ve iletilmeye devam edecektir. Aynı konumda konuşlandırılmış A ve B düğümlerinin kapsama ve kesişim alanları Şekil 2.2'de gösterilmiştir.

Şekil 2.2. A ve B düğümlerinin kapsama ve kesişim alanları

Fazlalık tabanlı mekanizmalar, hata toleransını önemli ölçüde sağlamakla birlikte bazı dezavantajları da söz konusudur [46]. Kısıtlı donanımsal kaynaklara sahip KAA'lar için ağ trafiğinin ve enerji tüketiminin artması, bu yöntemin handikaplarındandır. Örneğin; düğümlerin birbirlerine yakın olduğu ve algılanan verilerde önemli miktarda fazlalığın olduğu bir mekanizmada, ağ trafiğinin ve pil tüketiminin artması kaçınılmaz olacaktır.

Kümeleme Tabanlı Mekanizmalar

Kümeleme, KAA'ların kullanım ömrünü ve sürdürülebilirliğini arttırmak için önerilen etkili yaklaşımlardan biridir. Ağda bulunan algılayıcı düğümlerin gruplar halinde çalışmasını esas almaktadır. Kümelenmiş bir KAA topolojisinde; algılayıcı düğümler, düğümlerden oluşan kümeler, kümelerde bulunan düğümleri organize eden ve baz istasyonuyla veri iletişimini sağlayan küme başı düğümler bulunmaktadır. Kümelenmiş bir KAA topolojisi Şekil 2.3'te gösterilmiştir



Şekil 2.3. Kümelenmiş KAA topolojisi

Algılayıcı düğümlerin konuşlandırıldığı zorlu ortamlar, kaynak kısıtlamaları ve düğümler arasındaki dengesiz iş yükü, kümelenmiş KAA'ların kullanılabilirliğini olumsuz anlamda etkileyen ve hatalara karşı savunmasız hale getiren faktörlerdir [49]. Bu nedenle KAA tasarımında hata toleransını sağlamak için kümeleme tabanlı mekanizmalar önerilmiştir. Söz konusu yöntemler arasında; küme üyelerini izleyerek arızalı düğümleri tespit etme, küme başı düğümlerinin arızalanması veya enerjilerinin tükenmesi durumunda yeni küme başı düğümü seçme, düğümler arasında yük dengeleme gibi yöntemler bulunmaktadır [49-55].

Dağıtım Tabanlı Mekanizmalar

Dağıtım tabanlı mekanizmalar, kablosuz algılayıcı ağların konuşlandırılması aşamasında tasarlanan topolojiye ve kurulum sonrasında topolojinin kontrolüne dayanmaktadır. Ağın etkili bir şekilde tasarlanması hata toleransını doğrudan etkilediği gibi algılayıcı düğümlerin arızalanması, fiziki müdahalelere maruz kalması ve diğer koşullar nedeniyle topoloji kontrol algoritmalarının geliştirilmesi de hata toleransı için kritiktir [41].

2.1.4. Topoloji

Bir kablosuz algılayıcı ağ, kurulum amacı ve konuşlandırılacağı lokasyona göre yüzlerce hatta binlerce düğümden oluşabilir. Bir algılama alanındaki düğüm yoğunluğu, 20 düğüm/m3 olabilir [56]. Yoğun bir şekilde konuşlandırılan düğümler ile tatmin edici boyutta veri elde edilse bile sürdürülebilir bir sistem oluşturmak için gerek ağın donanımsal kısıtlarına gerekse de zorlu çevresel koşullara yönelik önlemler alınması gerekir. Ağın hesaplama, iletim ve hata tolerans kapasitesi gibi parametreleri, algılayıcı düğümlerin enerji tüketimini doğrudan etkileyen faktörlerdir. Söz konusu faktörlerin ihmal edilmesi durumunda kısa bir süre hayatta kalan, enerji verimsiz bir sistem ortaya çıkması kaçınılmazdır. Dolayısıyla algılayıcı ağın tasarımında, çevresel faktörler ve donanımsal kısıtlar göz önünde bulundurularak optimum enerji tüketen bir yapı ortaya konmalıdır.

Belirli bir lokasyona, çok sayıda düğümü yoğun bir şekilde konuşlandırmak, topoloji bakımının da dikkatli bir şekilde ele alınmasını gerektirir. Düğümler, belirli bir alana tek tek yerleştirilebileceği gibi toplu olarak rastgele dağıtılabilir. Düğümlerin konuşlandırılmasından sonra düğümlerin arızalanması, iletim ortamındaki gürültüler, fiziksel müdahaleler veya enerjilerinin tükenmesi gibi sebeplerle topoloji değişebilir. Bu gibi durumlarda ağa ek algılayıcı düğümler konuşlandırılabilir [36].

Kablosuz algılayıcı ağlar, konuşlandırıldıkları lokasyonlarda birbirleriyle ve baz istasyonuyla iletişim kurabilmek için çeşitli topolojileri kullanırlar. Bu topolojiler; yıldız, ağaç, doğrusal, halka, dairesel, örgü ve ızgara şeklindedir [57].

2.1.5. Güvenlik

Kablosuz algılayıcı ağlar, farklı türdeki fiziksel ortamlarda ve çeşitli alanlarda yaygın bir şekilde kullanıldığından, elde edilen verilerin güvenliği önem kazanmaktadır. Özellikle veri gizliliğinin kritik olduğu alanlarda, ağ güvenliğini sağlamak elzemdir. Örneğin, askeri amaçlı kullanılan bir ağda; iletişim, izleme/gözetleme, hedef alandan bilgi toplama vb. faaliyetlerde, verinin gizliliği ve güvenli iletimi son derece önemlidir. Benzer şekilde çevresel algılama ve felaketten korunma amacıyla kullanılan ağlarda gerek afetleri önlemek gerekse de afet durumunda etkili bir kurtarma operasyonu sağlayabilmek için algılanan verilerin korunması gerekir. Sağlık uygulamalarında kişilerin fizyolojik veya psikolojik verileri, ticari uygulamalarda sır niteliği taşıyan veriler gibi birçok alandan elde edilen veriler için gizlilik ve güvenlik, kritik öneme sahiptir.

Kablosuz algılayıcı ağların statik bir topoloji yerine kendi kendine organize olan dinamik bir topolojiye sahip olmaları ve dolayısıyla topolojilerinin sıklıkla değişmeleri, donanımsal kısıtları ve kendilerine özgü mimarileri nedeniyle geleneksel ağlara uygulanan güvenlik çözümlerinden farklı yöntemler geliştirilmelidir.

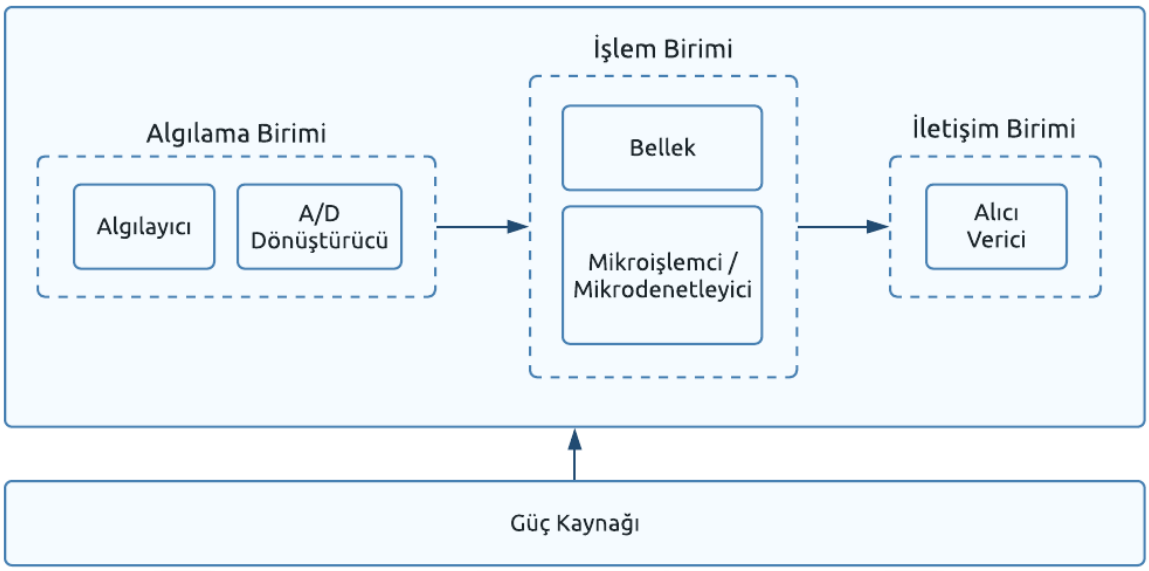
Bir kablosuz algılayıcı ağın güvenliğinin etkili bir şekilde sağlanabilmesi için dışarıdan ve içeriden gelen saldırılara karşı önlemler alınması gerekir. Bununla birlikte iletilen verilerin gizliliği, bütünlüğü ve tazeliği de garanti altına alınmalıdır. Ayrıca düğümlere fiziki müdahalelerin yapılması veya arıza durumuna karşı da gerekli tedbirler alınmalıdır. KAA güvenliği 3. bölümde detaylı olarak incelenmiştir.

2.2. Kablosuz Algılayıcı Ağların Mimari Özellikleri

Bir kablosuz algılayıcı ağ, birbirine bağlı birkaç ile binlerce algılayıcı düğümden oluşur. Algılayıcı düğümler, fiziksel ortamlardan çeşitli tipteki verileri algılayan, diğer düğümler ve baz istasyonu ile iletişim kabiliyetine sahip düğümlerdir. Algılayıcı düğümlerin temeli, 1998 yılında geliştirilen akıllı toz (Smart Dust) projesine dayanmaktadır. Akıllı toz projesi; sıcaklık, manyetizma, ışık, titreşim ve kimyasalları algılama kapasitesine sahip algılayıcılar, robotlar veya diğer cihazlar gibi birçok küçük mikroelektromekanik sistemden (MEMS) oluşan bir sistemdir [58, 59]. Kablosuz algılayıcı ağların mimarileri, algılayıcı düğüm mimarisi ile ağ ve haberleşme mimarisini ele almaktadır.

2.2.1. Algılayıcı Düğüm Mimarisi

Algılayıcı düğümler; verileri algılama, algılanan verileri işleme ve gerek diğer düğümlerle gerekse de baz istasyonuyla iletişime geçebilmek için birtakım temel bileşenlere ihtiyaç duyarlar. Bu bileşenler; algılama birimi, işlem birimi, iletişim birimi ve güç kaynağıdır. Şekil 2.4'te bir algılayıcı düğümün bileşenleri gösterilmiştir.



Şekil 2.4. Algılayıcı düğüm bileşenleri

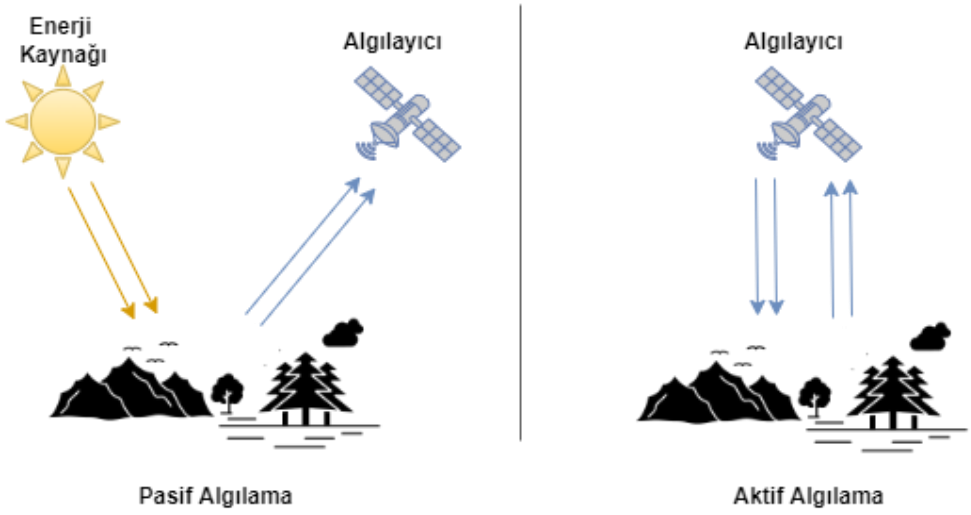
Algılama Birimi

Algılama birimi, bir veya daha fazla algılayıcı ile analog-dijital dönüştürücüden oluşmaktadır. Algılayıcılar, algılayıcı düğümün fiziki ortam ile etkileşimini gerçekleştiren bileşeni olup, belirli bir ortamda gelişen fiziksel olayları ve değişiklikleri tespit eden aygıtlardır. KAA'ların konuşlandırıldıkları ortamlarda sıcaklık, nem, basınç, hareket gibi fiziksel verilerin algılanması, algılayıcılar tarafından gerçekleştirilir. Her algılayıcı, kendi kapsama alanında gelişen söz konusu fiziksel koşulları algılamakla görevlidir. Algılayıcılar; küçük boyut, düşük enerji tüketimi, zorlu ortamlara adapte olabilme ve otonom çalışma gibi özelliklere sahip olmalıdır [60].

Algılayıcılar temel olarak pasif ve aktif olmak üzere iki kategoriye ayrılmaktadır.

1. **Pasif algılayıcılar:** Pasif algılayıcılar, fiziksel ortamları aktif araştırma ile fiilen manipüle etmeden ölçümler yapan ve ihtiyaç duydukları enerjiyi çevrelerinden elde eden algılayıcılardır. Bu tip algılayıcılarda enerjiye sadece analog sinyalleri yükseltmek için gereksinim duyulur. Bu tür algılayıcılara termometre, ışık algılayıcıları, titreşim, nem, duman detektörleri vb. örnek olarak verilebilir. Pasif algılayıcılarla yapılan ölçümlerde yön kavramının kullanılmadığı algılayıcılar, çok yönlü; yön kavramının kullanıldığı algılayıcılar ise dar ışınlı algılayıcılar olarak adlandırılır. Belirli bir yönde ölçüm yapabilen kameralar, dar ışınlı algılayıcılara örnek olarak verilebilir.
2. **Aktif algılayıcılar:** Fiziksel ortamı kendi ürettikleri sinyallerle aktif olarak araştıran algılayıcılardır. Sonar algılayıcılar, radyo algılayıcıları veya şok dalgaları oluşturan bazı sismik algılayıcılar örnek olarak verilebilir.

Aktif ve pasif algılama prensipleri Şekil 2.5'te karakterize edilmiştir.



Şekil 2.5. Aktif ve pasif algılama prensipleri

Kablosuz algılayıcı ağlar üzerine yapılan teorik çalışmaların çoğu pasif, çok yönlü algılayıcıları dikkate alır. Bazı pratik test ortamlarında kameralar gibi dar ışın tipi algılayıcılar kullanılır, ancak bu tür algılayıcıların hareketinin nasıl kontrol edileceği ve programlanacağı konusunda gerçek bir sistematik araştırma yoktur. Aktif algılayıcılar ise literatürde fark edilir ölçüde ele alınmamıştır [61].

Algılayıcıların elde ettikleri fiziksel veriler analog sinyaller şeklindedir. Verilerin işlenebilmesi ve çeşitli sonuçlar elde edilebilmesi için sayısallaştırılması gerekir. Analog sinyallerin sayısallaştırılması işlemi analog-dijital dönüştürücüler ile sağlanır.

İşlem Birimi

İşlem birimi, işlemci ve bellekten oluşmaktadır. Algılanan verileri işlemek, sonuçlar üretmek ve düğümün diğer bileşenlerini kontrol etmek için işlemci kullanılmaktadır. Bir kablosuz düğümde işlemci olarak; mikroişlemci (Microprocessor, µP), mikrodenetleyici (Microcontroller, µC), sayısal sinyal işlemciler (Digital Signal Processors, DSP), alanı programlanabilir kapı dizileri (Field-Programmable Gate Arrays) veya uygulamaya özgü tümleşik devreler (Application-Specific Integrated Circuits (ASICs) kullanılabilir.

Mikroişlemci veya mikrodenetleyici, nispeten benzer görevleri yerine getirmek için kullanılabilse de mimari bakımdan farklı özelliklere sahiptirler. Mikrodenetleyiciler, bilgi işlem bileşenlerinin (CPU, bellek, kesme kontrolleri, zamanlayıcı, seri portlar, veri yolu kontrolleri, G/Ç çevresel portları vb.) tamamını tek bir çip üzerinde birleştirirken, mikroişlemcilerde gerekli bileşenler birkaç yongadan oluşmaktadır. Söz konusu mimariden kaynaklı üç temel farktan söz edilebilir:

1. **Maliyet:** Genel olarak mikrodenetleyiciler, mikroişlemcilerden daha düşük maliyete sahiptirler. Zira mikroişlemciler, daha iyi bir performans sunabilmek için harici çevre birimlerinden yararlanacak daha pahalı cihazlarla kullanılmak üzere üretilirler. Nitekim mikroişlemciler, karmaşık hesaplama işlemlerini yerine getirebilmek için harici bellek kaynağına ihtiyaç duyarlar. Mikrodenetleyiciler ise genellikle özel bir işlevi yerine getirmek için tasarlanırlar. İcra edilecek tüm görevler, dahili bileşenlerce yerine getirilir. Mikrodenetleyiciler, amaca dönük özel uygulamalarda kullanıldığından, genellikle daha az bellek, daha az bilgi işlem gücü ve daha az karmaşıklık gerektirir. Bu faktörler nedeniyle de daha az maliyetlidirler.
2. **Hız:** Mikrodenetleyicilerin daha özel görevlere yönelik olmasına karşın mikroişlemciler daha genel, karmaşık ve öngörülemeyen görevleri ele alırlar. Başka bir deyişle, mikrodenetleyiciler, belirli bir görev için optimize edilen ve ilgili görevi yerine getirmek için doğru miktarda hız ve güce ihtiyaç duyan aygıtlar iken mikroişlemciler genel kullanım amacına sahiptirler. Doğal olarak mikroişlemciler, mikrodenetleyicilerden daha yüksek hıza sahiptirler. Birçok mikroişlemci 4 Ghz'e kadar saat hızı sunarken, mikrodenetleyiciler 200 Mhz veya daha düşük hızlar sunmaktadırlar. Bununla birlikte mikrodenetleyicide bulunan bileşenlerin fiziksel olarak birbirlerine yakınlıkları nedeniyle daha düşük saat hızına rağmen, işlemleri hızlı bir şekilde gerçekleştirebilirler. Mikroişlemcilerin ise harici çevresel birimlerle iletişim kurma gereksinimi, performans kaybına sebebiyet verebilmektedir.
3. **Güç Tüketimi:** Mikroişlemciler, daha genel ve hesaplama karmaşıklığı gerektiren işlerde daha yüksek performans sunarken, aynı zamanda daha fazla güç tüketir. Düşük hesaplama ve pil kapasitesine sahip uygulamalarda mikrodenetleyici kullanmak daha isabetli bir tercihtir.

Sonuç olarak mikrodenetleyicilerin programlanabilir olması, uyku moduna girebilmesi, daha düşük maliyetli olması ve düşük güç tüketimi gerektiren uygulamalar için optimize edilmiş olması gibi avantajlarından dolayı, algılayıcı düğümler için daha kullanışlıdır [62].

Mikroişlemci ve mikrodenetleyicilere alternatif olarak kullanılabilen DSP'ler, mimari ve komut kümesi bakımından büyük ölçekli vektörel verileri işlemek üzere tasarlanmıştır. Bu işlemciler, geniş bant kablosuz iletişim için uygun ve başarılı sonuçlar üretse de KAA'larda kullanılan kablosuz iletişim daha yalın olup, verilerin algılanmasıyla ilgili sinyal işleme görevleri aşırı karmaşık değildir. Dolayısıyla sayısal sinyal işlemcilerin avantajlarına algılayıcı düğümlerde pek gerek duyulmaz.

Diğer bir alternatif olan FPGA, sahada değişen gereksinimlere uyum sağlamak için yeniden programlanabilme ve yapılandırılabilme özelliklerine sahip olsa da bu işlemler zaman ve enerji tüketimine neden olduğundan, pek kullanılmaz.

ASIC'ler ise uygulamaya özgü tasarlanmış işlemcilerdir. Enerji verimliliği ve performans bakımından olumlu sonuçlar üretmesine karşın, esneklik bakımından kayıp söz konusudur. Öte taraftan, mikrodenetleyicilerin yazılımsal geliştirme gereksinimi duyduğu durumlarda, ASIC'lerde aynı işlevsellik donanımsal olarak sağlanmaktadır. Dolayısıyla daha maliyetli bir çözüm söz konusudur [63].

Algılayıcı düğümlerde işlem biriminin diğer bir önemli elemanı bellektir. Bir algılayıcı düğümde uygulamalar ve ara verileri saklamak için farklı türdeki bellek yapıları kullanılır. Kablosuz algılayıcı ağlarda bellek olarak genellikle flash bellek ve RAM kullanılmaktadır. Flash bellek, uygulama kodunu saklamak için; RAM ise uygulama programlarını, algılayıcının elde ettiği verileri, diğer düğümlerden gelen paketleri ve ara hesaplamaları depolamak için kullanılır. Flash bellek, RAM'in yetersiz olması veya RAM'in güç kaynağının bir süreliğine kapatılması gerektiğinde verilerin ara depolaması olarak da hizmet edebilir. Bununla birlikte flash belleğin okuma ve yazma hızındaki gecikmeler ile daha yüksek enerji gereksinimi de göz önünde bulundurulmalıdır. Üretim maliyetleri ve enerji tüketimi açısından, bellek boyutlarının optimum seçilmesi kritik öneme sahiptir [64].

İletişim Birimi

Algılayıcı düğümler arasında veri alışverişinin kablosuz olarak sağlanabilmesi için iletişim birimine ihtiyaç duyulmaktadır. İletişim biriminin en önemli elemanı kuşkusuz alıcı-verici (transceiver) cihazdır. Alıcı-verici, mikrodenetleyiciden gelen veri akışının radyo dalgalarına dönüştürülmesini sağlar. Bir alıcı-verici cihaz, radyo frekansı (Radio Frequency, RF) önucu ve temel bant işlemcisi olmak üzere iki bileşenden oluşmaktadır. Radyo frekansı önucu, anten sinyalinin ilk gittiği alıcı parçası olup, gerçek radyo frekansı bandında analog sinyal işlemeyi gerçekleştirir. Temel bant işlemcisi ise dijital alandaki tüm sinyal işlemlerini gerçekleştirir ve bir algılayıcı düğümün işlemcisi veya diğer dijital devreleriyle iletişim kurar [65].

Alıcı-verici cihazlar, veri iletişimine göre dört farklı durumda bulunabilirler.

1. **Gönderme:** Alıcı-verici cihazın verici kısmının aktif olduğunu ve antenin enerji yaydığı durumdur.
2. **Alma:** Cihazın, alıcı kısmının aktif olduğu durumdur.
3. **Bekleme (Boşta):** Bu durumda, alıcı-verici cihazı, veri almaya hazır durumdadır ancak şu an hiçbir şey almamıştır. Bekleme durumunda alma devresinin birçok parçası aktiftir, diğerleri kapatılabilir. Örneğin, senkronizasyon devresinde, alımla ilgili bazı unsurlar aktifken, izleme ile ilgili olanlar, yalnızca alım bir şey bulduğunda kapatılabilir ve etkinleştirilebilir. Myers vd. IEEE 802.11 alıcı-vericilerinde, edinme devresinin parçalarını kapatmak için teknikleri tartışır [66].

4. **Uyku:** Bir alıcı-verici cihaz, uyku durumuna geçtiğinde, önemli kısımları kapalı pozisyonda olur. Birkaç farklı uyku durumu sunan alıcı-vericiler vardır, IEEE 802.11 alıcı-vericileri için [66]'da uyku durumları tartışması yapılmıştır. Bu uyku durumları, kapatılan devre miktarında, kurtarma sürelerinde ve başlatma enerjisinde farklılık gösterir [67]. Örneğin, alıcı-verici tamamen kapatıldığında başlangıç maliyeti, cihazın konfigürasyonunun yanı sıra tam bir başlatmayı da içerir. Bununla birlikte daha hafif uyku modlarında, konfigürasyon ve çalışma durumu devam ederken, alıcı-vericinin yalnızca belli parçaları kapatılır.

Algılayıcı düğümünün protokol yığını ve işletim yazılımı, mevcut ve beklenen iletişim ihtiyaçlarına göre alıcı-vericinin hangi duruma geçeceğine karar vermelidir. Çalışma durumu değişiklikleri, bu kararı karmaşıklaştıran bir sorundur [68]. Örneğin, uyku modundan iletim moduna uyanan bir alıcı-verici, bir miktar başlatma süresi ve başlatma enerjisine gereksinim duyar. Bu başlatma süresi boyunca, veri iletimi veya alımı mümkün değildir [69]. Ortalama güç tüketimini en aza indirgemek için düğüm durumlarını programlama sorunu oldukça karmaşıktır. Konuyla ilgili literatürde çeşitli çalışmalar yapılmıştır [70, 71].

Alıcı-verici cihazlarda, iletim ortamı olarak çeşitli alternatifler kullanılabilir. Bazı durumlarda kablolu iletişim kullanılsa da kablosuz iletim ortamı için radyo frekansı tabanlı iletişim, optik iletişim (lazer), kızılötesi gibi seçenekler mevcuttur. Lazerler daha az enerji gereksinimine ihtiyaç duymakla birlikte, düğümler arasında iletişimin sağlanabilmesi için görüş hattına ihtiyaç duyar. Ayrıca atmosferik koşullara da duyarlıdır. Kızılötesi iletişimde, lazerler gibi anten ihtiyacı yoktur ancak yayın kapasitesi sınırlıdır. Radyo frekansı tabanlı iletişim ise nispeten uzun menzil ve yüksek veri hızı, makul enerji tüketimi, hat gerektirmemesi gibi avantajlarından dolayı KAA uygulamaları için en iyi alternatiftir [72].

Güç Kaynağı

Algılayıcı düğümler, dış ve zorlu ortamlara konuşlandırıldığından, enerji kaynağının düzenli olarak değiştirilmesi/yenilenmesi maliyetli ve zahmetli olabilir. Bununla birlikte ağın işlevlerinin kesintisiz sürdürülebilmesi için en önemli bileşen, enerjidir. Zira bir algılayıcı düğüm; algılama, iletişim ve veri işleme için güç tüketir. Kablosuz algılayıcı düğümleri, tipik olarak çok küçük elektronik cihazlar olduğundan, yalnızca 0,5-2 amper/saat ve 1,2-3,7 volttan daha az sınırlı bir güç kaynağı ile donatılabilirler [72]. Veri iletişimi için diğer işlemlerden daha fazla enerjiye gereksinim duyulur. Pottie ve Kaiser'in yaptıkları çalışmaya göre; 1 Kb verinin, 100 metrelik bir mesafeye iletilmesi, kabaca üç milyon talimatın hesaplanmasıyla aynı miktarda enerji tüketir [73].

Güç kaynağı, algılayıcı düğümlerin hayatta kalabilmeleri ve ağın kesintisiz çalışabilmesi için düğüme enerji sağlamaktır. Bir algılayıcı düğümün güç kaynağı ise geleneksel pillerdir. Geleneksel pillerin dışında da güç kaynakları mevcuttur. Güneş pilleri, sıcaklık farklılıklarının elektrik

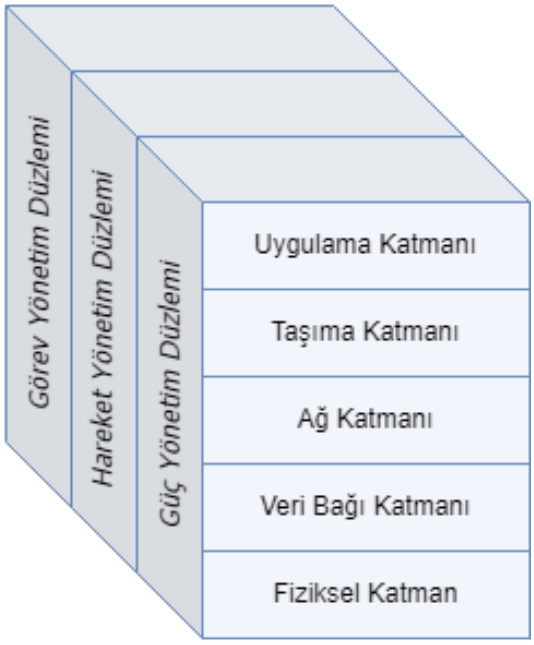
enerjisine dönüştürülme esasına göre çalışan sıcaklık gradyanları, titreşimleri elektrik enerjisine dönüştüren mekanizmalar, basınç değişimleri ve hava/sıvı akış mekanizmaları, alternatif güç kaynakları arasında sayılabilir [74].

2.2.2. Ağ ve Haberleşme Mimarisi

Kablosuz algılayıcı ağlarda, katmanlı ağ mimarisi ve kümelenmiş ağ mimarisi olmak üzere iki mimari kullanılmaktadır [75].

Katmanlı Ağ Mimarisi

Algılayıcı düğümlerde yaygın olarak Open Systems Interconnection (OSI) katmanlı mimarisi kullanılmaktadır. Bu mimaride uygulama, taşıma, ağ, veri bağı ve fiziksel katman olmak üzere beş katman bulunur. Ayrıca güç, hareket ve görev yönetim düzlemleri de çapraz katmanları oluşturur. Çapraz katmanlar, ağı yönetmeye ve algılayıcı düğümlerin beraber çalışmalarını sağlayarak ağın genel verimliliğini artırmaya olanak tanır. Algılayıcı düğümler arasındaki güç, hareket ve görev dağılımının izlenmesi, algılama görevinin koordine edilmesi ve toplam güç tüketiminin düşürülmesi gibi işlemler, çapraz katmanlar tarafından icra edilir [1]. Ağ mimarisine ait katmanlar Şekil 2.6'da gösterilmiştir.



Şekil 2.6. Katmanlı ağ mimarisi

Uygulama katmanında, ağ trafiğinin yönetimi gerçekleştirilir. Uygulama katmanı, verileri anlaşılır bir biçimde dönüştüren veya belirli verilerin elde edilmesi için sorgular gönderen farklı uygulamalar için yazılım sağlar [76]. Taşıma katmanı, ağ paketinin güvenli iletimini sağlamak, paket kaybını önlemek ve trafikte oluşabilecek tıkanıklıkları azaltmak veya önlemekten sorumludur [77]. Ağ katmanı, ağda uçtan uca bağlantı kurulması, sürdürülmesi ve ağ paketlerinin yönlendirilmesini sağlar. Bununla birlikte KAA'ların enerji, hafıza ve arabellek kısıtlamaları, yönlendirme işlemini zorlaştıran etkenlerdir. Ayrıca düğümlerin evrensel bir kimliğinin olmaması ve kendi kendilerine organize olmaları da diğer zorluklardandır [76]. Veri bağlantı katmanı, veri akışlarının çoğullanmasından, veri çerçevesi algılamasından, ortam erişiminden ve hata kontrolünden sorumludur. Fiziksel katman ise frekans seçimi, taşıyıcı frekans üretimi, sinyal algılama, modülasyon ve veri şifrelemeden sorumludur [1].

Çapraz katmanda bulunan güç yönetim düzlemi; algılayıcı düğümün güç seviyesinin yönetilmesinden sorumludur. Örneğin, algılayıcı düğüm, yinelenen iletileri almaktan kaçınmak için komşularından birinden bir mesaj aldıktan sonra alıcısını kapatabilir. Ayrıca bir düğümün güç seviyesinin düşük olması durumunda, komşu düğümlere güç seviyesinin düşük olduğunu ve yönlendirme mesajlarına katılmayacağını yayınlar. Hareket yönetim düzlemi, algılayıcı düğümlerin hareketini algılar ve kaydeder, böylece kullanıcıya giden bir rota her zaman korunur ve algılayıcı düğümler, komşu algılayıcı düğümlerin kim olduğunu takip edebilir. Görev yönetim düzlemi ise belirli bir bölgeye verilen algılama görevlerini dengeler ve programlar. Bir bölgedeki tüm algılayıcı düğümlerin aynı anda algılama görevini gerçekleştirmesi gerekmez. Sonuç olarak, bazı algılayıcı düğümler, güç seviyelerine bağlı olarak herhangi bir görevi diğerlerinden daha fazla gerçekleştirir [1].

Kümelenmiş Ağ Mimarisi

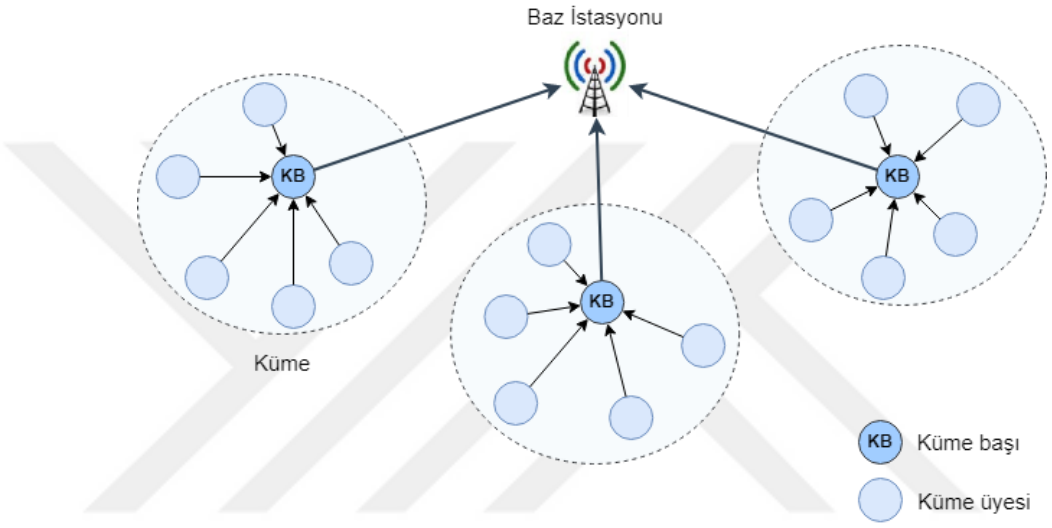
KAA'ların fiziki ortamlardan verileri doğru bir ölçümle elde etmesi, değerlendirmesi ve sonuçlar üretmesi kadar önemli olan diğer bir husus, ağın kesintisiz bir şekilde işlevini yerine getirebilmesi yani sürdürülebilir olmasıdır. KAA'larda ağ ömrünü doğrudan etkileyen en önemli parametre, enerjidir. Özellikle zorlu mekanlara konuşlandırılan algılayıcı düğümlerin güç kaynaklarının periyodik olarak değiştirilmesi istenen bir durum olmadığından, enerji tüketiminin optimize edilmesi gerekir. Kümelenmiş ağ mimarisinin, başta enerji tasarrufu olmak üzere birçok avantajı vardır. Bu avantajlar şu şekilde sıralanabilir:

- **Ölçeklenebilirlik:** Kümelenmiş bir KAA mimarisinde, ağın geneli daha küçük hiyerarşik birimlere ayrılarak kümeler oluşturulur. Kümeleme topolojisi, küme içinde kurulan rotayı yerelleştirerek, düğümlerde depolanan yönlendirme tablosunun boyutunu azaltabilir [78, 79]. Böylece ağ topolojisinin yönetimi kolaylaşır ve ortamdaki olaylara yanıt vermek için daha ölçeklenebilir bir yapı oluşturulmuş olur [80].

- **Veri toplama/birleştirme:** Algılayıcı ağlardaki yüksek düğüm yoğunluğu nedeniyle, aynı veriler birçok düğüm tarafından algılanır ve bu da veri fazlalığı/artıklığı ile sonuçlanır [81]. Fazla iletimi ortadan kaldırmak ve baz istasyonuna birleştirilmiş verileri göndermek için birden çok düğümden gelen verileri toplama/birleştirme yaklaşımı kullanılır. Bu yaklaşım, enerji tasarrufu için etkili bir tekniktir [82].
- **Yük tasarrufu:** Algılayıcı düğümlerin önemli miktarlarda fazla veri üretmesi ve belirli bir lokasyonda birden fazla düğümün aynı/benzer ölçümler yapması neticesinde veri fazlalığı/artıklığı oluşur ve bu sorun, veri toplama/birleştirme yaklaşımıyla giderilir. Kümeleme topolojisine sahip bir ağda, küme üyeleri yalnızca küme başı düğümlere veri gönderir. Küme başı düğümler algılanan verileri toplayarak, aktarım verilerini önemli ölçüde azaltmaya ve enerji tasarrufu sağlamaya yardımcı olur. Ayrıca kümeler için kurulan rotaların yerelleştirilmesi ile algılayıcı düğümlerde depolanan yönlendirme tablosunun boyutu azaltılır. Böylece algılayıcı ağ üzerindeki yük azaltılır [78, 79].
- **Enerji tasarrufu:** Kümeleme topolojisi kullanan bir ağda, veri toplama/birleştirme yaklaşımıyla aktarım verilerinin önemli ölçüde azaltılması, enerji tasarrufu sağlamaya yardımcı olur. Ayrıca küme içi ve kümeler arası iletişimde, uzun mesafeli iletişim görevini yerine getiren algılayıcı düğümlerin sayısı azaltılarak, ağın daha az enerji tüketimine izin verilir. Ek olarak, kümeleme yönlendirme şemasında veri iletimi görevi, yalnızca küme başı düğümler tarafından gerçekleştirir. Bu durum, yüksek miktarda enerji tasarrufu sağlayabilir [83].
- **Sağlamlık:** Kümelenmiş yönlendirme şeması; ağ topolojisi kontrolü, düğüm artışı, düğüm hareketliliği ve öngörülemeyen arızalar içeren ağ değişikliklerine yanıt verme için ağı daha uygun hale getirir. Kümeleme yönlendirme şeması, bu değişiklikleri kümeler bazında yaparak, tüm ağın sağlamlığını garanti altına alır ve yönetimini kolaylaştırır [83].
- **Çakışma ve gecikme azaltma:** Algılayıcı düğümler, ortamlardan elde ettikleri verileri iletmek için kablosuz ortamı paylaşmak ve yönetmek durumdadırlar. Geniş ölçekli bir ağda tüm düğümlerin ağı paylaşmaları, kaynak kullanımındaki verimliliği düşürebileceği gibi, çakışmalara da sebebiyet verecektir. Kümeleme modelinde ise kablosuz ortama ait kaynaklar, küme bazında paylaşılarak çakışmalar azaltılır ve kaynakların daha verimli kullanılmasına olanak tanınır [84]. Ayrıca kümelerden veri iletim görevi yalnızca küme başı düğümlere verildiğinden, gecikmeler de azaltılır. Zira küme başı düğümler ile veri iletimi, baz istasyonuna giden yolu kısaltır.
- **Hata toleransı:** Algılayıcı ağların savunmasız/zorlu ortamlara konuşlandırılmaları, kısıtlı pil ve donanımsal kaynaklar, donanımsal arızalar, iletim ortamı ve çevresel problemler gibi nedenlerden dolayı, algılayıcı düğümler devre dışı kalabilir [42, 43]. Hata toleransı, algılayıcı ağın sürdürülebilir olması için kritik öneme sahiptir. Kümelenmiş ağ

mimarisinde hata toleransı sağlamak için küme üyelerini izleyerek arızalı düğümleri tespit etme, küme başı düğümlerinin arızalanması veya enerjilerinin tükenmesi durumunda yeni küme başı düğümü seçme, düğümler arasında yük dengeleme gibi yöntemler bulunmaktadır [49-55].

Kümeleme süreci, algılayıcı düğümlerin kümeler halinde gruplandırılmasını ve her küme için bir küme başı düğümü seçilmesini kapsar. Kümelenmiş bir KAA mimarisi Şekil 2.7'de gösterilmiştir.



Şekil 2.7. Kümelenmiş KAA mimarisi

Kümelenmiş bir KAA mimarisinde; algılayıcı düğüm, küme başı düğüm, düğümlerden oluşan kümeler ve baz istasyonu bulunur. Algılayıcı düğüm; ortam koşullarının algılanması, algılanan verilerin işlenmesi ve yönlendirilmesi gibi görevleri yürütür. Küme başı düğümü ise küme üyeleri arasındaki iletişimi organize etme, üyelerden alınan verileri birleştirme ve baz istasyonuna iletme gibi önemli görevleri icra eder. Kümeler, algılayıcı ağın daha küçük birimlere ayrılmasıyla elde edilen, küme üyeleri ve küme başı düğümlerden oluşan birimlerdir. Baz istasyonu ise ağdan gelen verilerin toplandığı ve son kullanıcıya iletildiği bileşendir.

Kümeleme sürecinde, küme başı seçimi kritik bir görevdir. Zira küme başı, küme üyeleri tarafından elde edilen verileri birleştirme ve baz istasyonuna iletme gibi önemli görevleri yürütmektedir. Dolayısıyla küme başı seçiminde şu faktörler göz önünde bulundurulmalıdır:

- Enerji tasarrufu için küme başı düğümlerin konumlandırılacağı lokasyon ile baz istasyonu arasındaki mesafe uzak olmamalıdır. Aksi durumda iletim maliyeti artacağından, daha fazla enerjinin tükenmesine ve ağ ömrünün bitmesine sebebiyet verecektir. Literatürde bu

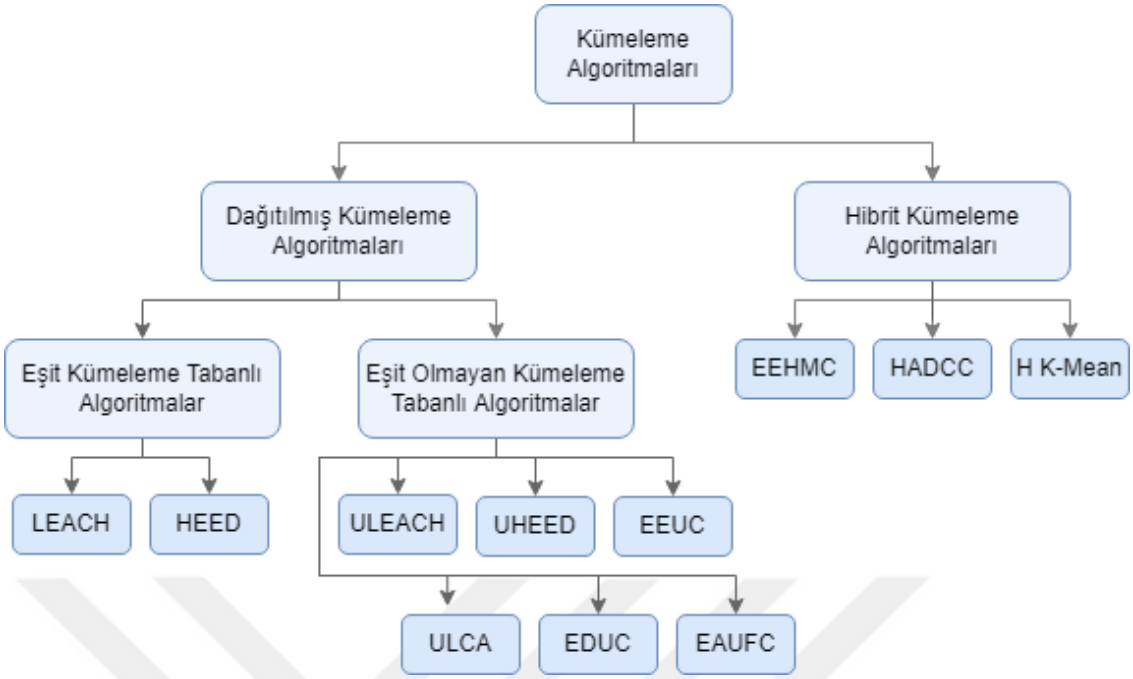
konuyla ilgili çeşitli çalışmalar olup, Sharma vd. enerji verimli mesafe tabanlı küme başı seçim algoritması önermişlerdir [85].

- İletim maliyetinin düşürülmesi için küme başı düğümlerin, üye düğümler ile mesafesi de önemli bir parametredir [86]. Üye ve küme başı düğümler arasındaki mesafenin azalması ile iletim maliyetinin düşmesi paralellik göstermektedir.
- Bir algılayıcı ağda küme başı düğümler, küme üyelerinin algıladıkları verileri toplama, birleştirme ve baz istasyonuna iletmekle sorumludur. Küme üyeleri, işlem yapmadıkları zamanlarda enerji tasarrufu için uyku moduna geçebilirken, küme başı düğümler aktif durumda kalmalıdırlar [87]. Küme başı düğümlerin fazladan enerji gerektiren işleri yapmaları ve sürekli aktif halde bulunmaları nedeniyle, daha fazla enerji tüketirler. Bununla birlikte bir küme başı düğümün enerjisinin tükenmesi, algılanan verilerin baz istasyonuna iletilmemesi anlamına geldiğinden, küme başı seçilecek düğümün yüksek enerjili olması ve gerektiğinde yeniden kümeleme işleminin yapılması gerekir.

Literatürde küme başı seçimi ve kümelerin düzenlenmesi sürecini oluşturan kümeleme işlemiyle alakalı birçok farklı çalışma mevcuttur. Bununla birlikte KAA'lar için homojen ve heterojen kümeleme olmak üzere iki farklı kümeleme modelinden söz edilebilir. Homojen kümelemede, küme üyesi düğümlerin enerji, iletişim ve hesaplama yetenekleri eşittir [88]. Heterojen kümelemede ise tersi bir durum söz konusudur. Kümeleme algoritmalarını farklı şekillerde sınıflandıran literatür çalışmaları mevcut olmakla birlikte, algoritmaları sınıflandırmak ve karşılaştırmak için ağdaki kümelerin boyutu (düğüm sayısının eşit olup, olmaması), düğüm mesafesi, paket iletim türü (tek sekmeli, çok sekmeli) gibi öznitelikler kullanılabilir. Şekil 2.8'de kümeleme algoritmaları; merkezi, dağıtılmış ve hibrit kümeleme temelinde sınıflandırılmıştır [89].

Dağıtılmış kümeleme algoritmalarında, küme başı seçimi için merkezi bir kontrol olmayıp, düğümler, küme başını seçmek için kendi aralarında bilgi alışverişi yaparlar. Ağdaki tüm düğümler arasında enerji tüketimini dinamik olarak dengelemek için küme başı düğümler, çeşitli parametreler referans alınarak değiştirilir [90]. Dağıtılmış kümeleme algoritmaları küme boyutlarına göre alt kategorilere ayrılır. Bir kümedeki düğüm sayısı, o kümedeki enerji yoğunluğunu temsil ettiğinden, küme boyutu, kümelemede önemli bir konudur [91]. Küme boyutlarına dayalı dağıtılmış kümeleme algoritmaları, eşit veya eşit olmayan kümeleme tabanlı algoritmalar olmak üzere ikiye ayrılır.

Eşit kümeleme tabanlı algoritmalarda, ağdaki kümelerin boyutu aynıdır. Eşit kümeleme tabanlı algoritmalardan olan düşük enerjili uyarlanabilir kümeleme hiyerarşisi (Low-Energy Adaptive Clustering Hierarchy, LEACH), ağdaki yükü ve enerji tüketimini dengelemek için küme başı görevini düğümler arasında döndürür [92].



Şekil 2.8. Kümeleme algoritmalarının sınıflandırılması

LEACH algoritması, küme başı seçimi için herhangi bir merkezi kontrol olmaksızın düğümler tarafından kendi kendini yöneten kararların alındığı dağıtılmış bir algoritma kullanarak kümeler oluşturur. Bir düğümün küme başı olarak görevlendirilmesi, belirli periyotlarla dinamik olarak belirlenir. Bir küme başı olarak çalışma kararı, n düğümü tarafından p olasılıkla 0 ile 1 arasında rastgele bir sayı seçilerek verilir. Eğer sayı $T(n)$ eşiğinden küçükse, düğüm mevcut tur için küme başı olur. Eşik, Denklem 2.3'e göre belirlenir.

$$T(n) = \begin{cases} \dfrac{p}{1 - P * \left(rmod \dfrac{1}{p}\right)} & eğer\ n\ \in G \\ 0 & değilse \end{cases} \tag{2.3}$$

Denklemde gösterilen p, küme başlarının istenen yüzdesi; G, $\frac{1}{p}$ turlarında küme başı olmayan düğümler kümesidir. r ise mevcut tur sayısı olup, r = 0'da her düğümün küme başı olma olasılığı p kadardır. r değeri arttıkça, küme başı olmaya uygun daha az sayıda düğüm olduğundan, kalan düğümlerin küme başları olma olasılığı artırılmalıdır [89].

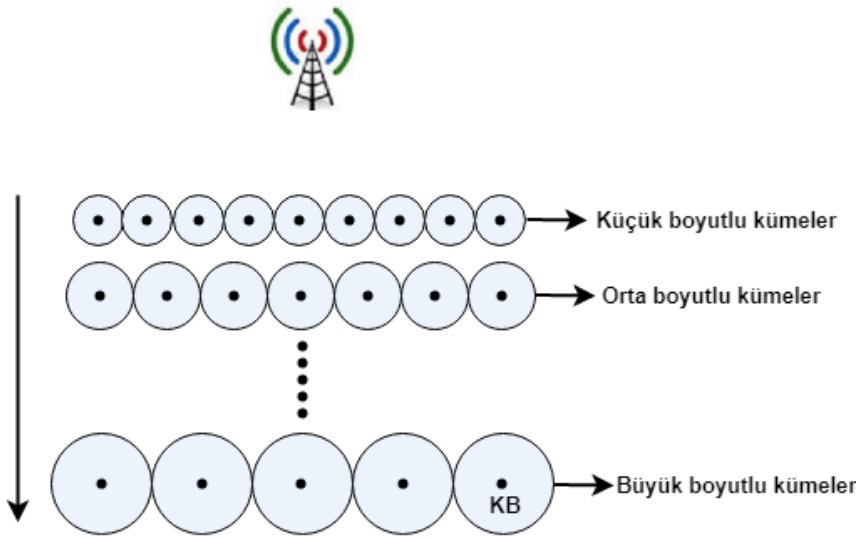
Hibrit enerji verimli dağıtılmış kümeleme (Hybrid Energy Efficient Distributed Clustering, HEED) algoritması, ağda güç dengelemesini sağlamak için küme başı seçiminde düğümün kalan enerjisini ve küme içi iletişim maliyetini kullanmaktadır. Küme içi iletişim maliyeti, bir düğümün birden fazla küme başının kapsama alanına girmesi durumunda kritik değer taşır. HEED algoritması başlatma, tekrarlama ve sonlandırma aşamalarından oluşur. Başlatma aşamasında her

düğüm, kalan enerjisine ve olasılık parametresine dayalı olarak küme başı olma olasılığını belirler. Tekrarlama aşamasında her düğüm en düşük maliyetli küme başını bulana kadar birkaç yinelemeden geçer. Sonlandırma aşamasında ise her bir düğüm, mevcut turda küme başı olma veya bir kümeye katılma konusunda nihai bir karar verir. HEED algoritmasında enerji tüketimini dağıtarak ağ ömrünü uzatma, belirli adımlarda kümeleme sürecini sonlandırma ve küme başlarını düzgün dağıtarak yük dengelemesini sağlama hedeflenmektedir [93]. Bir düğümün küme başı olma olasılığı denklem 2.4'te gösterilmiştir.

$$CH_{prob} = C_{prob} * \frac{E_{res}}{E_{max}} \tag{2.4}$$

CH_{prob}, bir düğümün küme başı olma olasılığını; C_{prob} , tüm düğümler arasında küme başı yüzdesini gösterir. E_{res} düğümdeki kalan enerjiyi, E_{max} ise tipik olarak tüm düğümler için aynı olan maksimum enerjiyi (tam şarjlı bir pil) gösterir.

Eşit kümeleme mimarisi, ağ trafiğini azaltarak enerji verimliliğini sağlamakla birlikte, bu mimaride baz istasyonuna yakın küme başı düğümler, baz istasyonuna uzak konumdaki küme başı düğümlerden daha fazla enerji tüketir. Zira baz istasyonuna yakın küme başı düğümler hem kendi üyelerinden hem de diğer küme başı düğümlerden gelen trafiği baz istasyonuna iletmekle görevlidir. Baz istasyonuna yakın küme başı düğümlerde dengesiz enerji tüketimine neden olan bu sorun, sıcak nokta sorunu olarak adlandırılır [94]. Algılayıcı ağın sıcak nokta sorununu önlemek için, küme başı düğümler arasında yük dengeleme esasına dayanan eşit olmayan kümeleme teknikleri kullanılabilir [95]. Eşit olmayan kümeleme prensibi Şekil 2.9'da gösterilmiştir.



Şekil 2.9. Eşit olmayan kümeleme mimarisi

Eşit olmayan kümeleme mimarisi, baz istasyonuna yakın kümelerin boyutunu azaltmaya, uzak kümelerin ise boyutunu arttırmaya dayanır. Yani baz istasyonuna olan mesafe nispetince küme boyutu artırılır. Baz istasyonu yakınındaki küme daha küçük, daha az üyeye sahip, dolayısıyla küme içi trafik daha azdır. Böylece daha küçük kümeler, küme içi trafik için daha az enerji tüketir ve kümeler arası trafiğe daha fazla odaklanır. Benzer şekilde, baz istasyonuna daha uzak olan daha büyük kümeler, daha fazla küme üyesine işaret eder ve küme içi trafik için daha fazla enerji harcar. Eşit olmayan kümeleme, tüm küme başı düğümlerin aynı miktarda enerji harcamasına izin verir, böylece yükü verimli bir şekilde dengeleyerek sıcak nokta sorununu ortadan kaldırır. Enerji verimli eşit olmayan kümeleme algoritması (Energy Efficient Unequal Clustering, EEUC), eşit olmayan kümeleme tabanlı HEED algoritması (Unequal Hybrid Energy Efficient Distributed Clustering, UHEED) ve eşit olmayan katmanlı kümeleme yaklaşımı (Unequal Layered Clustering Approach, ULCA), baz istasyonundan küme başı düğümlere olan mesafe ile orantılı olarak küme boyutu ayarlama mantığına göre çalışmaktadır [96-98].

LEACH algoritması, küme başı düğümünü belirli olasılık temelinde seçer ve küme başı olma görevi düğümler arasında döndürülür. Eşit olmayan kümeleme tabanlı LEACH (Unequal LEACH, ULEACH) algoritmasında ise küme başı seçimi aşamasında, düğümlerin enerji oranları ve baz istasyonuna olan mesafesi de hesaplanır. Ağın başlatılması sırasında, baz istasyonu belirli bir güç seviyesinde tüm düğümlere bir "merhaba" mesajı yayınlar. Bu şekilde, her bir düğüm alınan sinyal gücüne göre baz istasyonuna olan yaklaşık mesafeyi hesaplayabilir ve ardından baz istasyonuna bir rapor mesajı (ilk enerji ve konum) gönderebilir. Baz istasyonu, mesafe ve kalan enerjinin matrislerini oluşturur, ardından mesafe matrisini ağdaki her bir düğüme yayınlar. Küme başı düğüm rastgele bir sayı üretilerek tanımlanır ve Denklem 2.3'teki hesaplamaya göre küme başı seçimi yapılır [99].

Enerjiye dayalı eşit olmayan kümeleme (Energy-Driven Unequal Clustering, EDUC) algoritması, küme içindeki düğümlerin enerji tüketimini etkin bir şekilde yöneterek, enerji tasarrufu sağlar. Eşit olmayan kümeleme yapısına dayalı olarak, küme başı görevini döndürmek ve enerji tüketimini dengelemek için enerji odaklı bir küme başı rotasyon stratejisi benimsenmiştir. Her düğüm, tüm ağ ömrü boyunca yalnızca bir kez küme başı olarak görev yapar. Bu nedenle, küme başı dönüşünde tüketilen enerji en aza indirilir. EDUC algoritması, küme oluşturma ve veri toplama aşamalarından oluşur. Ağ kurulum aşamasında, baz istasyonu belirli bir güç seviyesinde bir sinyal yayınlar. Her düğüm, alınan sinyal gücüne dayalı olarak baz istasyonuna olan yaklaşık mesafesini hesaplayabilir. Bir sonraki aşama küme oluşturma aşamasıdır. T_1 zamanı, küme başı rekabet aşaması olarak adlandırılır. Bu aşamada, her düğüm, kalan enerjisine dayalı olarak bekleme süresini hesaplar. Herhangi bir i düğümü için t_{wi} bekleme süresi Denklem 2.5'teki gibi hesaplanabilir:

$$t_{wi} = \left(1 - \frac{E_{\mathrm{cur}i}}{E_{max}}\right) T_1 V_r \tag{2.5}$$

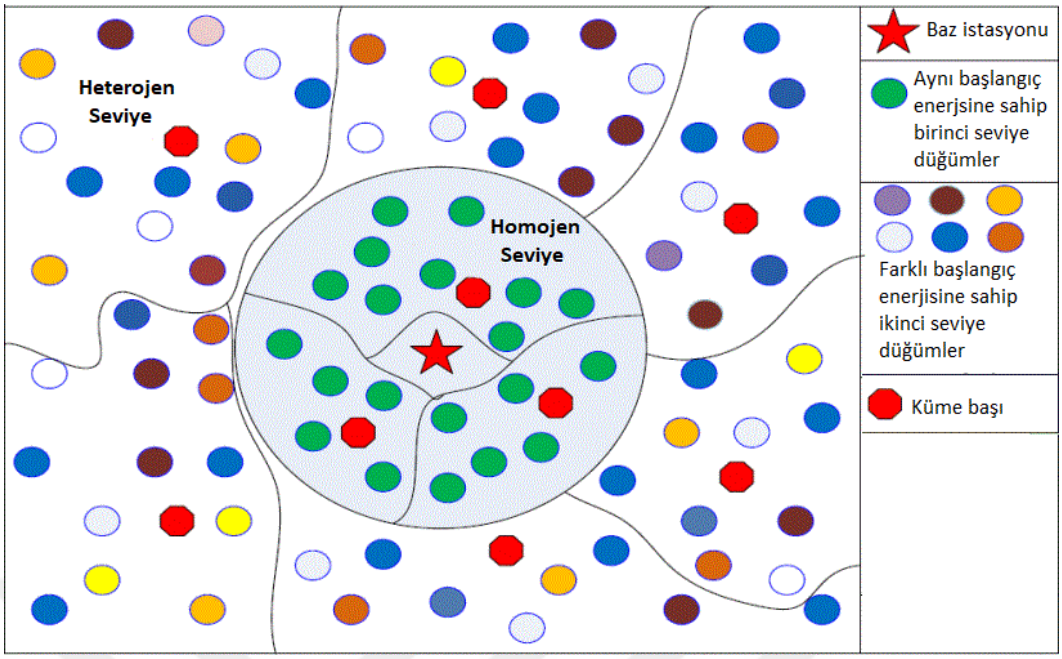
Denklemdeki $E_{\mathrm{cur}i}$, i düğümünün kalan enerjisidir ve E_{max}, ağdaki maksimum kalan enerjidir. Küme oluşturma aşaması tüm ağın ilk aşaması olduğundan, E_{max} ağdaki maksimum başlangıç enerjisi olarak kabul edilebilir. Bu nedenle, E_{max} değeri önceden belirlenir. V_r iki düğümün aynı anda mesaj gönderme olasılığını azaltmak için belirlenen rastgele bir değerdir [100].

Bulanık eşitsiz kümeleme algoritması (Energy Aware Unequal Fuzzy Clustering, EAUCF), düğümlerin kalan enerjilerini ve baz istasyonuna olan mesafelerini dikkate alarak küme başı yarıçapını ayarlar. Bu işlem, baz istasyonuna daha yakın olan veya daha düşük pil seviyesine sahip algılayıcı düğümlerin küme içi çalışmasının azaltılmasına ve sıcak nokta sorununun önlenmesine yardımcı olur. Küme başı yarıçap tahminindeki belirsizlikleri ele almak için bulanık mantık kullanılmıştır. EAUCF, literatürdeki LEACH, CHEF ve EEUC gibi popüler algoritmalara göre çoğu durumda daha iyi performans göstermektedir [101].

Dağıtılmış kümeleme algoritmalarına alternatif olarak kullanılan diğer bir yöntem ise hibrit kümeleme algoritmalarıdır. Son zamanlarda araştırmacılar, hibrit kümeleme teknikleri üzerine çalışmalar yapmaktadırlar. Hibrit kümeleme, birden fazla algoritmanın özelliklerini tek bir algoritmada birleştirme esasına dayanır [89].

Enerji verimli hibrit çok atlamalı kümeleme (Energy Efficient Hybrid Multi Hop Clustering, EEHMC) şemasında, küme başı kurulum kararları baz istasyonu tarafından (merkezi yaklaşım) yürütülür ve küme oluşumu, röle düğüm seçimi ve veri iletim kararları, algılayıcı düğümler tarafından (dağıtılmış yaklaşım) alınır. Baz istasyonu, küme başı seçimi için karar verici parametreler olarak düğümlerin kalan enerjisini, verici aralığındaki komşu sayısını ve küme başı düğümler arasındaki minimum ayırma mesafesini kullanır. Küme oluşturma sürecinde ise baz istasyonu, tüm algılayıcı düğümlere bir küme başı duyuru mesajı gönderir. Mesajı alan her düğüm, aday bir küme başı veya üye düğüm olup olmadığını kontrol eder. Eğer bir küme başı ise tüm komşularına bir reklam mesajı yayınlar. Alınan sinyal gücüne göre her üye düğüm, hangi küme başına ait olduğunu seçer ve en yakın küme başına üye olarak bir katılma talep mesajı gönderir. Benzetim sonuçlarına göre EEHMC, ağ ömrünü LEACH-C'ye göre %27,63'e kadar artırmaktadır [102].

Hibrit gelişmiş dağıtılmış ve merkezileştirilmiş kümeleme (Hybrid Advanced Distributed and Centralized Clustering, HADCC) algoritması; merkezi, dağıtılmış, homojenliğe duyarlı ve heterojenliğe duyarlı algoritmaların avantajlarını birleştirir. Bu yaklaşımda, düğümün konumu ve kalan enerjisine göre küme başı seçimi yapılır. Algoritmayı yürütmek için, tüm ağ bölgesinin homojen ve heterojen olmak üzere iki fiziksel seviyeye ayrıldığı gelişmiş bir ağ topolojisi önerilmiştir. Önerilen topoloji Şekil 2.10'da gösterilmiştir [103].



Şekil 2.10. HADCC ağ topoloji modeli

Ağın homojen kısmında, sadece normal düğümler bulunur, bu nedenle ağ topolojisinde sadece yeşil renkli düğümler gösterilir. Heterojen ağ bölümünde farklı renklerle gösterilen farklı enerjilere sahip düğümler bulur. Baz istasyonu ise ağın merkezinde yer alır.

HADCC algoritmasında küme başı seçim aşamasında her bir düğümün uygunluğu hesaplanır. Uygunluk hesaplamada başlangıç enerjisi, kalan enerji, enerji tüketim oranı (Energy Consumption Ratio, ECR) ve düğümlerin baz istasyonuna olan mesafesi kilit rol oynar. Uygunluk hesabından önce her bir düğümün ECR'sinin hesaplanması gerekir. ECR 2.6'daki denkleme göre hesaplanabilir.

$$ECR(m) = \frac{E_0}{E_0 - E_r} \tag{2.6}$$

E_0 başlangıç enerjisini, E_r ise ilk seviyedeki her düğümün kalan enerjisini gösterir. Her düğümün ECR'si hesaplandıktan sonra, baz istasyonu düğümlerin uygunluğunu 2.7'deki denklemle hesaplar.

$$Uygunluk(m) = \frac{E_r}{\frac{E_0}{E_0 - E_r} * d_{toBS}} \tag{2.7}$$

d_{toBS}, m düğümünün baz istasyonuna olan mesafesidir. Uygunluk değeri en yüksek olan düğüm, küme başı olarak seçilir [103].

Hiyerarşik k-Ortalama algoritması, hiyerarşik ve k-ortalama algoritmasını birleştiren kümeleme algoritmasıdır. Hiyerarşik yaklaşımda, en yakın iki küme, tek küme gelene kadar özyinelemeli olarak gruplandırılır. Kümeler arasındaki mesafe benzerliklerine göre belirlenir. Farklı mesafelerde, farklı kümeler oluşturulur ve bir dendogram ile temsil edilir. Hiyerarşik kümeleme, farklı veri parçalarının diğer verilerden ne kadar farklı olduğunu göstermede etkili olsa da bu kümeleme biçiminin birkaç dezavantajı vardır. Birincil dezavantaj, hiyerarşik kümelemenin yalnızca küçük miktarlardaki verileri bölmede etkili olmasıdır. Veri büyüdükçe dendogramda bilgi kaybına neden olur. K-Ortalama kümeleme algoritmasında ise belirli sayıda ayrık ve hiyerarşik olmayan küme oluşturulur. K-Ortalama yöntemi sayısal, denetimsiz, deterministik olmayan, yinelemeli bir yöntemdir. Bu algoritmaya göre, her kümede her zaman en az bir düğümü olan 'k' kümeleri vardır. Bu algoritmanın en büyük dezavantajı küme sayısının (k) önceden belirtilmesidir. Algoritma küme sınırlarını değil küme merkezlerini optimize ettiğinden, genellikle kümeler arasında yanlış kesme sınırlarına yol açar. k-ortalama algoritması, büyük ve çoklu veri kümelerinde, hiyerarşik kümelemeden hesaplama açısından daha hızlıdır. Ayrıca, özellikle kümeler küresel ise hiyerarşik kümelemeye göre daha sıkı kümeler üretir. Ancak üretilen kümelerin kalitesi 'k' seçimine bağlıdır.

Geliştirilen hibrit algoritmanın hedefi, verilen algılayıcı düğüm kümesi için optimal sayıda kümeye ulaşmak ve bu kümeler için küme başı düğümleri seçmektir. Hem hiyerarşik hem de k-Ortalama kümelemenin kendi sınırlamaları olduğundan, iki yaklaşımın özelliklerinden yararlanılır. K-Ortalama kümeleme kullanılarak, küme konfigürasyonu ve ağırlık merkezi elde edilir. Her küme için merkeze en yakın düğüm, küme başı olarak seçilir. Oluşturulan kümelerin sayısı neredeyse optimal olduğu için bu tür kümelemenin verimli olması beklenir [104].

Kablosuz algılayıcı ağlarda; enerji verimliliği, ölçeklenebilirlik, yük dengeleme ve ağ ömrünü uzatma gibi birçok kritik işlevi gerçekleştirebilmek için kümeleme mimarisi kullanılmaktadır. Birçok araştırmacı, optimal kümeleri elde etmek ve ağ ömrünü uzatmak için eşit olmayan kümeleme, hibrit kümeleme gibi farklı kümeleme teknikleri önermişlerdir. Bununla birlikte kümeleme sürecini yürütme ve yönetmenin de maliyetinin olduğu unutulmamalıdır. Ayrıca yanlış kümeleme ve küme başı seçme stratejileri, ağın işlevselliğini olumsuz yönde etkileyecektir. Dolayısıyla kümeleme sürecinde istenen sonuçları elde edebilmek için kullanılacak algoritmanın ve söz konusu faktörlerin göz önünde bulundurulmaları gerekir.

Bu bölümde incelenen kümeleme algoritmalarının; ağ modeli, kümeleme hedefi, kümeleme türü ve küme başı seçim parametreleri Tablo 2.2'de gösterilmiştir.

Tablo 2.2. Kümeleme algoritmalarının karşılaştırılması

Kümeleme Algoritması	Ağ Modeli	Kümeleme Hedefleri	Kümeleme Türü	Küme Başı Seçim Parametreleri
LEACH	Homojen	Enerji tasarrufu	Eşit kümeleme	Kalan enerji Rasgele yaklaşım
HEED	Homojen	Enerji tasarrufu	Eşit kümeleme	Kalan enerji
ULEACH	Homojen	Enerji tasarrufu	Eşit olmayan kümeleme	Enerji oranı Rekabet mesafesi
UHEED	Homojen	Enerji tasarrufu	Eşit olmayan kümeleme	Kalan enerji Mesafe
EEUC	Homojen	Enerji tasarrufu	Eşit olmayan kümeleme	Yerelleştirilmiş rekabet mesafesi
ULCA	Homojen	Daha uzun ağ ömrü	Eşit olmayan kümeleme	Kalan enerji Mesafe
EDUC	Heterojen	Enerji tasarrufu	Eşit olmayan kümeleme	Kalan enerji Mesafe
EAUFC	Homojen	Enerji tasarrufu	Eşit olmayan kümeleme	Kalan enerji Mesafe
EEHMC	Homojen	Enerji verimliliğini artırmak	Hibrit kümeleme	Kalan enerji Komşu sayısı Mesafe
HADCC	Homojen Heterojen	Enerji tasarrufu	Hibrit kümeleme	Kalan enerji Mesafe
H k-Mean	Heterojen	Enerji tasarrufu Optimum kümeleme	Hibrit kümeleme	Ağırlıklı kalan enerji

3. KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK

Algılayıcı düğüm ve kablosuz iletişimdeki teknolojik gelişmeler ve donanım maliyetlerinin düşmesine paralel olarak, KAA'lar yaygın bir kullanım alanına ulaşmıştır. Söz konusu kullanım alanları arasında sağlık hizmetleri, felaket algılama, askeri ve istihbari faaliyetler gibi verinin güvenli bir şekilde elde edilmesinin ve iletilmesinin kritik öneme sahip olduğu alanlar da bulunmaktadır.

KAA'ların donanımsal kısıtları, mimari özelliklerinin geleneksel ağlardan farklı olması ve zorlu/savunmasız ortamlara konuşlandırılmaları gibi etkenler nedeniyle KAA'lara özgü güvenlik çözümleri geliştirilmelidir. Bununla birlikte KAA'larda güvenliğin sağlanması birtakım zorlukları barındırır. Bu zorluklardan bazıları şu şekilde sıralanabilir [105]:

- Algılayıcı düğümler geniş coğrafi mekanlara konuşlandırılacakları için toplam düğüm maliyetinin mümkün olduğunca düşük olması gerekir. Dolayısıyla geliştirilen her güvenlik çözümü gerek maddi açıdan gerekse de donanımsal açıdan ek maliyet gerektirir.
- Algılayıcı düğümler savunmasız ortamlara yerleştirildiklerinden fiziksel olarak ele geçirilme veya kurcalamaya açıktır.
- KAA'lar, donanım kısıtları nedeniyle bir taraftan kaynak tüketiminin minimizasyonunu gerektirirken, öte taraftan veri gizliliği için güvenlik seviyesinin maksimize edilmesini gerektirir. Bu durum, etkili ve verimli bir güvenlik mekanizmasının geliştirilmesini zorlaştırır.
- Algılayıcı düğümler genellikle ciddi şekilde kısıtlandığından, asimetrik kriptografi çoğu uygulama için genellikle çok pahalıdır. Bunun yerine, çoğu güvenlik şeması simetrik anahtar şifrelemesini kullanır. Her iki durumda da güvenli iletişim için anahtarlar kullanılır. Anahtar dağıtımını yönetmek, KAA'lara özgü değildir, ancak düşük bellek kapasitesi gibi kısıtlamalar, merkezi anahtarlama tekniklerini imkânsız hale getirir.
- Algılayıcı ağ, dinlenmesi kolay kablosuz iletim ortamını kullanır. Bu durum kötü niyetli kullanıcılara ağa dışarıdan müdahale etme imkânı tanır.
- Daha fazla tasarım karmaşıklığı ve daha yüksek enerji gereksinimi edeniyle, KAA'larda frekans atlamalı yayılma spektrumu ve düğümlerin fiziksel kurcalamaya karşı koruması gibi gelişmiş parazit önleme teknikleri genellikle zor veya imkansızdır.
- Küçük boyut, düşük maliyet ve sınırlı enerji kısıtlamaları ile birlikte radyo iletiminin kullanılması, KAA'ları hizmet reddi saldırılarına karşı daha duyarlı hale getirir.
- KAA'ların geçici ağ oluşturma topolojisi, pasif gizli dinlemeden aktif müdahaleye kadar çeşitli saldırılar yapılmasını kolaylaştırır.

- KAA'ların ölçeklenebilir yapıları nedeniyle, oluşturulacak güvenlik mekanizmasının geniş alanlara ölçeklendirilmesi gerekebilir. Ancak mevcut standart güvenlik protokollerinin çoğu, iki taraf için tasarlanmış olup, çok sayıda katılımcıya ölçeklenmez.

Geleneksel ağlara uygulanan güvenlik çözümlerinin, KAA'lara uygulanması zor hatta bazı durumlarda imkânsız olsa da kullanım alanı giderek yaygınlaşan algılayıcı ağlara yönelik etkili ve verimli güvenlik mekanizmalarının geliştirilmesi zaruridir. Bu bölümde KAA'ların güvenlik ilkeleri ile KAA'lara yönelik saldırılar ve geliştirilen güvenlik mekanizmaları incelenmiştir.

3.1. Kablosuz Algılayıcı Ağlarda Güvenlik İlkeleri

Kablosuz algılayıcı ağlarda güvenlik hizmetlerinin nihai hedefi, algılanan verileri ve ağ kaynaklarını saldırılara ve hatalı davranışlara karşı korumaktadır [35]. Güvenliği sağlanan bir algılayıcı ağ, konuşlandırıldığı ortamdan güvenli bir şekilde veri toplayabilmeli, elde edilen verilerin içeriğinin değiştirilmediğini garanti altına alabilmeli ve verileri güvenli bir şekilde hedef alıcılara ulaştırabilmelidir. Söz konusu prensiplerin sağlanabilmesi için veri gizliliği, kimlik doğrulama, veri bütünlüğü ve ağın sürdürülebilirliği gibi güvenlik ilkeleri yerine getirilmelidir.

3.1.1. Veri Gizliliği

Veri gizliliği, algılayıcı düğümler tarafından elde edilen verilerin yalnızca istenen alıcılara ulaştırılmasını ve komşu düğümler de dahil olmak üzere yetkisiz kişilerce erişiminin engellenmesini sağlayan mekanizmadır. Veri gizliliği bazı durumlarda kritik olabilir. Algılayıcı ağlarda hassas verileri gizli tutmak için kullanılan standart yaklaşım, verileri yalnızca hedeflenen alıcıların sahip olduğu gizli bir anahtarla şifrelemektir [106].

3.1.2. Kimlik Doğrulama

Algılayıcı düğümlerin haberleşmek için kablosuz iletim mimarisini kullanması, ağa sahte paketlerin enjekte edilmesine olanak tanır [107]. Algılayıcı düğümlerin gerek veri iletim gerekse de karar verme sürecinde verilerin doğru kaynaktan geldiğinden emin olması gerekir [106]. Kimlik doğrulama, gönderen ve alıcı düğümlerin gizli anahtarları paylaştığı simetrik veya asimetrik mekanizmalar aracılığıyla sağlanır. Kablosuz iletim ortamı ve algılayıcı ağların gözetimsiz yapısı nedeniyle, kimlik doğrulamasını sağlamak zordur [108].

3.1.3. Veri Bütünlüğü

Veri gizliliğini sağlamaya yönelik mekanizmalar, bilgilerin sızdırılmasını engellese de verinin güvenliğini tek başına sağlamada yeterli olmaz. Zira kötü niyetli bir düğüm, ağa sahte paket

ekleyebilir veya paket içerisindeki verileri değiştirebilir. Dahası iletişim ortamından kaynaklı zorluklar nedeniyle bir saldırı olmaksızın bile veri kaybı/hasarı meydana gelebilir. Veri bütünlüğü ise verinin gönderici düğümden, alıcı düğüme aktarımı esnasında değiştirilmemesini garanti altına alır [109]. Veri bütünlüğünü sağlamak için, mesaj doğrulama kodları (Message Authentication Code, MAC) veya dairesel kodlar (cyclic codes) kullanılabilir [110].

3.1.4. Kullanılabilirlik

Kullanılabilirlik, bir algılayıcı ağın işlevlerini kesintisiz olarak sürdürebilmesini sağlar. Ağın sürdürülebilir olması, algılayıcı ve küme başı düğümler ile baz istasyonu da dahil olmak üzere ağın tüm kaynaklarının iletişim için hazır olmasını gerektirir. Ağın kullanılabilirliği gerek hizmet reddi saldırıları gibi harici müdahaleler ile gerekse de kaynakların tükenmesi gibi dahili sebeplerle sekteye uğrayabilir. Bu durum, sağlık, felaket izleme veya askeri uygulamalar gibi kritik alanlarda ciddi kayıplara sebebiyet verebilir. Örneğin; felaket izleme uygulamalarında olası bir afetin tespit edilememesinden kaynaklı büyük kayıplar yaşanabilir veya askeri bir uygulamada düşman istilası için bir arka kapı açılabilir [111].

Ağın kullanılabilirliğine yönelik olarak, düğümler arası ek iletişim veya mesajların başarılı bir şekilde iletilmesi için merkezi bir erişim kontrol sistemi önerilmiştir [112]. Ancak söz konusu yaklaşımlar ek hesaplama, dolayısıyla ek enerji tüketimini gerektirir.

3.1.5. Veri Tazeliği

Verinin gizliliği ve bütünlüğünü sağlamakla birlikte, verinin tazeliğinin de sağlanması esastır. Veri tazeliği, verinin yeni olduğunu gösterir ve eski mesajların yeniden iletilmemesini sağlar. Bu gereksinim, özellikle anahtar kullanımında önem kazanır. İdeal olarak bir anahtar oluşturma süreci, katılımcılarla paylaşılan her anahtarın (oturum anahtarı) yeni olduğunu garanti etmelidir [106]. Aksi durumda eski anahtar kullanılarak bir yeniden yürütme (replay) saldırısı başlatılabilir. Veri tazeliğini sağlamak için pakete nonce veya zamanla ilgili başka bir sayaç eklenebilir [109, 112].

3.1.6. Kendi Kendine Organizasyon

KAA mimarisinde, geleneksel ağlardan farklı olarak, ağ yönetimi için sabit bir altyapı yoktur. Algılayıcı düğümler, haberleşme ve hata toleransı amacıyla farklı durumlara göre kendi kendini organize edebilecek düzeyde esnek olmalıdır. Aksi durumda ağa yönelik herhangi bir saldırı veya hata durumunda yıkıcı sonuçların ortaya çıkması muhtemeldir. Algılayıcı ağın sürdürülebilirliği açısından kritik öneme sahip olan bu özellik, aynı zamanda ağ güvenliğini sağlama açısından ciddi zorluklar getirmektedir [106].

3.1.7. Güvenli Konumlandırma

Algılayıcı düğümlerin doğru olarak konumlandırılması ve otomatik olarak bulunabilir durumda olması gerekir. Zira birçok KAA uygulaması, düğümlerin doğru konum bilgilerine ihtiyaç duyar. Örneğin; felaket izleme uygulamalarında, olası bir felaketin yerini tam olarak belirlemek için doğru konum bilgisine ihtiyaç duyulacaktır. Ancak saldırganlar, yanlış sinyal gücü bildirerek veya sinyal tekrarlayarak konum bilgilerini manipüle edebilir. Araştırmacılar, güvenli konumlandırma ile ilgili çeşitli çalışmalar yapmışlardır. Menzil ve mesafe sınırlamalarına dayalı doğrulanabilir çoklu kullanım (Verifiable Multilateration, VM) mekanizması ile konum işaretçilerinin kullanıldığı aralıktan bağımsız güvenli konumlandırma (Secure Range-Independent Localization, SERLOC) mekanizması, bu çalışmalardan bazılarıdır [113, 114].

Algılayıcı ağ trafiğini güvenli hale getirmek için açıklanan güvenlik ilkeleri, birincil ve ikincil derecede öneme sahiptir. Birincil hedef kapsamında değerlendirilebilecek ilkeler; veri gizliliği, kimlik doğrulama, veri bütünlüğü ve kullanılabilirlik ilkeleridir. Veri tazeliği, kendi kendine organizasyon ve güvenli konumlandırma ise ikincil hedef olarak değerlendirilebilir. Birincil ve ikincil hedefler Şekil 3.1'de gösterilmiştir.

Şekil 3.1. Birincil ve ikincil güvenlik hedefleri

3.2. Kablosuz Algılayıcı Ağlara Yönelik Saldırılar

Kablosuz algılayıcı ağlar, kullandıkları iletim ortamının yayın doğası gereği saldırılara açıktır [108]. Bununla birlikte algılayıcı düğümlerin donanımsal kısıt1arı ve geleneksel ağlardan farklı altyapı mimarisi, etkili ve verimli bir güvenlik mekanizmasının geliştirilmesini zorlaştırır. Ayrıca düğümlerin savunmasız/zorlu ortamlara yerleştirilmeleri, kurcalamaya ve fiziksel müdahalelere sebebiyet verebilir. Kablosuz algılayıcı ağlara yönelik saldırılar üç sınıf halinde incelenebilir [111].

1. **Gizlilik ve kimlik doğrulamaya yönelik saldırılar:** Algılayıcı ağın, kablosuz iletişim altyapısını kullanması, ağa sahte veya kötü niyetli paketlerin enjekte edilmesine ve

algılayıcılar tarafından elde edilen hassas verilerin gizlice izlenmesine olanak tanır. Veri gizliliği, algılayıcı düğümler tarafından elde edilen verilerin yalnızca istenen alıcılara ulaştırılmasını ve komşu düğümler de dahil olmak üzere yetkisiz kişilerce erişiminin engellenmesini sağlar. Veri gizliliğini sağlamak için temel yaklaşım, standart şifreleme tekniklerinin kullanılmasıdır. Kimlik doğrulama süreci ise iletilen paketlerin doğru kaynaktan geldiğini garanti altına alır. Bununla birlikte güvenliği ihlal edilmiş bir düğüm, meşru bir düğümün gizli anahtarlarına sahip olduğundan, kendisini ağda doğrulayabilme kabiliyetine sahiptir. Güvenliği ihlal edilmiş düğümleri tespit etmek ve olası saldırıların önüne geçmek için saldırı tespit sistemleri kullanılabilir.

2. **Ağın kullanılabilirliğine yönelik saldırılar:** Kullanılabilirlik, bir algılayıcı ağın işlevlerini kesintisiz olarak sürdürebilmesini sağlar. Algılayıcı ağa yönelik gerçekleştirilen hizmet reddi saldırıları (DoS), ağın kullanılabilirliğini sekteye uğratabilir. Ağın kesintiye uğraması özellikle kritik uygulamalarda ciddi kayıplara sebebiyet verebilir. Ağın kullanılabilirliğine yönelik olarak, düğümler arası ek iletişim veya mesajların başarılı bir şekilde iletilmesi için merkezi bir erişim kontrol sistemi önerilmiştir [112]. Ancak söz konusu yaklaşımlar ek hesaplama, dolayısıyla ek enerji tüketimini gerektirir.
3. **Hizmet bütünlüğüne yönelik saldırılar:** Algılayıcı ağa sahte paketler enjekte etme veya mevcut paket içerisindeki verileri değiştirme, ağın hatalı sonuçlar üretmesine sebebiyet verir. Veri bütünlüğünü sağlamak için, MAC veya dairesel kodlar kullanılabilir [110].

Kablosuz algılayıcı ağlara yönelik olarak gerçekleştirilen saldırılar, niteliğine göre pasif veya aktif olarak sınıflandırılabilir. Algılayıcı ağ, kablosuz bir kanal üzerinden iletişim kurarken, pasif bir saldırgan, özel veya hassas bilgileri çalmak amacıyla ağın radyo frekans aralığını kolayca dinleyebilir [107]. Esasında algılayıcı ağdan gelen birçok bilgi, muhtemelen doğrudan saha gözetimi yoluyla toplanabilir. Ancak pasif saldırılarda, izleme ve gözetleme faaliyetleri için fiziksel olarak sahada bulunmaya gerek olmayıp, anonim bir şekilde, düşük riskle bilgi toplanabilmektedir [115].

Temelde veri gizliliğine yönelik olarak gerçekleştirilen pasif saldırılarda, saldırgan, şifrelenmemiş trafiği izler ve diğer saldırı türlerinde kullanılabilecek hassas bilgileri arar. Pasif saldırılar, ağ trafiğini izlemeyi ve analiz etmeyi, zayıf şifrelenmiş trafiğin şifresini çözmeyi ve kimlik doğrulama bilgilerini yakalamayı içerir. Bu tür saldırılar, kullanıcının izni veya bilgisi olmadan, bilgilerinin veya veri dosyalarının ele geçirilmesiyle sonuçlanır [116]. Ağın gizliliğine yönelik olarak gerçekleştirilen pasif saldırılardan bazıları şunlardır [108]:

- **İzleme ve dinleme:** Güçlü bir alıcıya ve iyi tasarlanmış bir antene sahip bir saldırgan, veri akışını yakalayarak, algılayıcı düğümlerin fiziksel konumlarını öğrenebilir ve onları yok edebilir. Saldırgan, algılayıcı düğümlerin konumlarının yanı sıra, mesaj kimlikleri, zaman

damgaları ve diğer alanlar dahil olmak üzere uygulamaya özel mesajların içeriğini gözlemleyebilir [117].

- **Trafik analizi:** Algılayıcı düğümlerin izlenmesi ve analiz edilerek paketlerin içeriğinin açığa çıkarılması, ağa zarar verebilir.
- **Kamuflaj:** Ağ trafiğindeki paketleri çekmek veya yanlış yönlendirmek için algılayıcı ağa düğüm eklenebilir veya mevcut düğümler ele geçirilebilir.

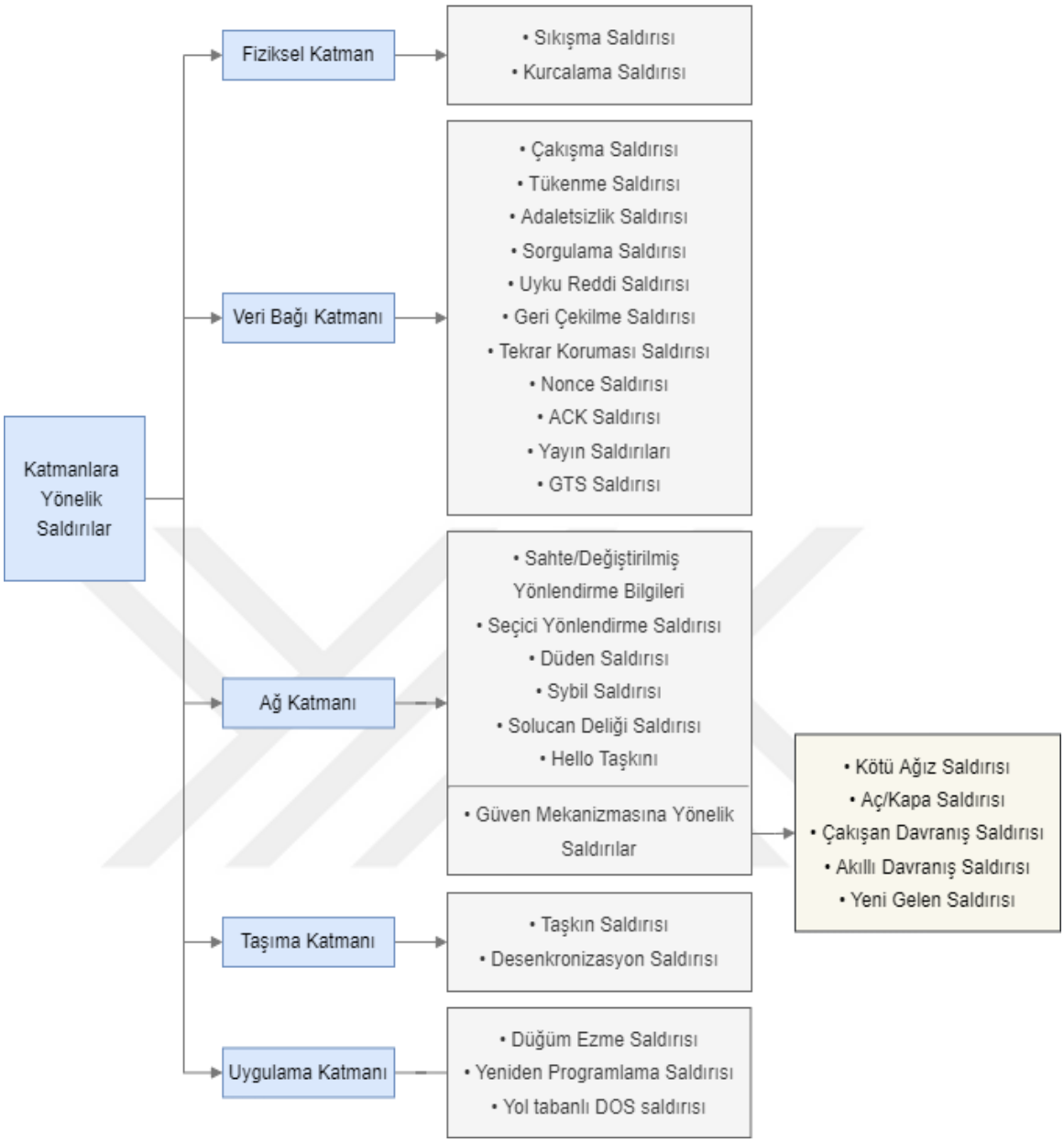
Aktif saldırılarda ise saldırgan pasif durumundan çıkıp, ağdaki kontrolü sağlamak için aktif duruma geçmektedir. Aktif saldırılarda veri akışı izlenir, analiz edilir ve verilerde değişiklik yapılabilir.

Güvenliği ihlal edilmiş düğümler, ağa içeriden saldırı yapmak, veri akışını bozmak veya gizli verileri çalmak için kullanılabilir. Güvenliği ihlal edilmiş düğüm, aktif saldırılarla ele geçirilmiş/yeniden programlanmış bir düğüm olabileceği gibi daha güçlü donanım ve radyo kaynağına sahip (dizüstü bilgisayar gibi) güçlü bir cihaz olabilir. Güvenliği ihlal edilmiş bir düğüm, meşru düğümlerde çalışan kodların aksine bazı kötü amaçlı kodlar çalıştırarak, ağın işleyişini bozmaya veya gizli verileri çalmaya meyillidir. Bu düğümlerin, algılayıcı ağ ile iletişim kurabilmek için meşru düğümlerle uyumlu telsizi vardır. Ayrıca ağ içi iletişimde gizlilik için bazı kriptografik teknikler kullanılsa bile güvenliği ihlal edilmiş düğüm, ağda meşru bir görünümdedir. Bu durumda meşru bir düğümün gizli anahtarlarına sahip olması gerekir [107].

Kablosuz algılayıcı ağlar, katmanlı bir mimari kullanır ve her katmana yönelik ayrı saldırılar gerçekleştirilebilir. KAA katmanlarına yönelik saldırılar Şekil 3.2'de kategorize edilmiştir.

3.2.1. Fiziksel Katman Saldırıları

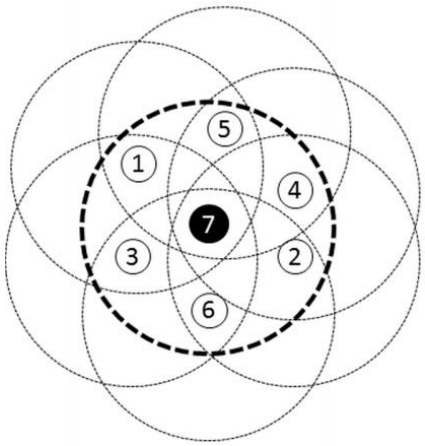
Fiziksel katman frekans seçimi, taşıyıcı frekans üretimi, sinyal algılama, modülasyon ve veri şifrelemeden sorumludur [1]. Kablosuz algılayıcı ağlar, radyo tabanlı iletim altyapısını kullandıklarından, iletim ortamında sıkışma olasılığı vardır. Bu olasılık, algılayıcı ağların fiziksel katmanlarına yönelik sıkışma saldırıları yapılmasına olanak tanır. Ayrıca algılayıcı düğümlerin savunmasız/zorlu ortamlara konuşlandırılmaları, saldırganların fiziksel müdahalelerine imkân verir. Fiziksel katman saldırıları, temel olarak sıkışma ve kurcalama saldırıları olarak ikiye ayrılır [35].



Şekil 3.2. KAA katmanlarına yönelik saldırılar

Sıkışma Saldırısı

Sıkışma, saldırganın yüksek enerjili sinyaller yayarak, ağın işleyişini bozmaya çalıştığı bir saldırı türüdür [105]. Bu saldırıda amaç, iletişime müdahale etmektir [118]. Sıkışmaya sebep olan kaynak, tüm ağın veya ağın bir bölümünün işleyişini bozabilecek kadar güçlü olabilir. Bununla birlikte güvenliği ihlal edilmiş bazı düğümlerin, ağda rastgele dağıtılması ve bu düğümlerin sıkışma kaynağı olarak kullanılmasıyla da tüm ağ iletişimi bozulabilir [35]. Dolayısıyla sıkışma kaynağının ağdaki pozisyonu, kritik bir öneme sahiptir. Güvenliği ihlal edilmiş bir düğümün, iletim menzilindeki diğer düğümler ile olan ilişkisi Şekil 3.3'te gösterilmiştir [119].



Şekil 3.3. Kritik bir konumda bulunan sıkışma kaynağı

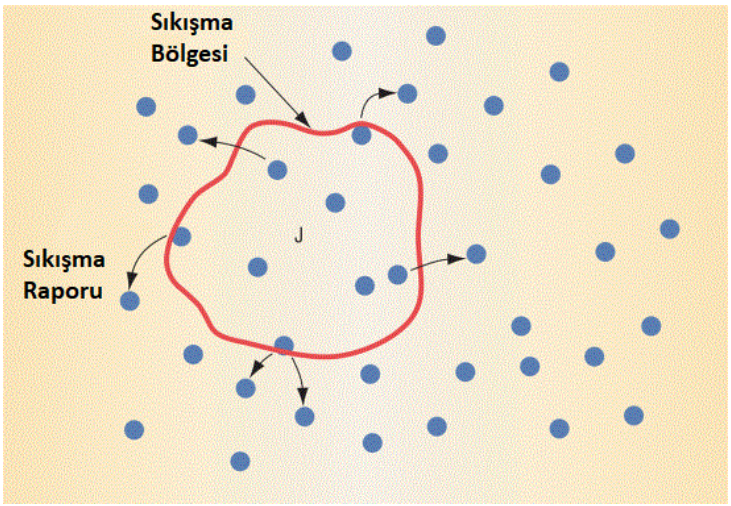
Şekil 3.3'de her düğümün iletim menzili, kesikli dairelerle gösterilmiştir. Sıkışma kaynağı olarak kullanılan düğüm ise merkezi konumda bulunan 7 numaralı düğümdür. Şekilden de anlaşılacağı üzere sıkışma düğümünün iletim menzili, diğer düğümleri de kapsadığından, diğer düğümlerin iletişimlerini bozabilecek kapasiteye sahiptir. Şöyle ki, herhangi bir düğüm veri iletmeye çalıştığında, sıkışma düğümü sinyal yayabilir. Bu sinyaller, iletilen verinin bozulmasına ve yeniden iletilmesine neden olarak ek enerji tüketimine neden olur. Dolayısıyla merkezi veya ağın işleyişini önemli ölçüde etkileyebilecek bir pozisyona yerleştirilecek sıkışma kaynakları, tüm ağı etkileyebilecek potansiyele sahiptir. Xu vd. sıkışma saldırılarını dört kategori altında inceler [120].

1. **Sürekli sıkışma:** Ağ trafiğine sürekli olarak radyo sinyali yayınlanarak, düğümlerin ilettikleri verilerin bozulmasına sebep olan saldırı tipidir. Sürekli sıkışma saldırısında, veri iletiminden önce iletim kanalının boşta kalması beklenmez. Bu saldırı tipi önemli miktarda enerji gerektirir. Bu nedenle saldırgan, hedef ağ ile benzer güç kısıtlamaları altındaysa, saldırı başarısızlıkla sonuçlanabilir [118].
2. **Aldatıcı sıkışma:** Bu saldırı tipinde, ağa rastgele bitler göndermek yerine, yasal bir trafik gibi görünmesi için ağa sabit bir bayt akışı gönderilir. Neticede diğer düğümler, bu paketlerin meşru bir paket olduğuna inandırılacak ve sürekli alma modunda kalması için aldatılacaktır. Örneğin, TinyOS'ta bir giriş dizisi (0xAA) algılanırsa, diğer düğümlerin gönderilecek paketi olup olmadığına bakılmaksızın, düğümler alma modunda kalır. Dolayısıyla düğümler, gönderecekleri paketleri olsa bile gönderme durumuna geçemez.
3. **Rastgele sıkışma:** Sürekli olan radyo yayını yapmak yerine, uyku ve sıkışma arasında geçiş yapılan saldırı tipidir. T_j birimlik süre boyunca sıkışma yaptıktan sonra telsiz kapatılır ve uyku moduna geçilir. T_s zamanı kadar uykuda kaldıktan sonra tekrardan sıkışma yapmaya devam edilir. T_j ve T_s rastgele veya sabit değerler olabilir. Rastgele sıkışma

saldırısında, sürekli veya aldatıcı sıkışma gibi davranılabilir. Özellikle sınırsız güç kaynağına sahip olmayan sıkışma kaynakları, enerji tasarrufu yapabilmek için rastgele sıkışma saldırısı yapmaktadır.

4. **Reaktif sıkışma:** Reaktif sıkışma modeli, kanalı sürekli meşgul etmek yerine, sadece iletişim esnasında sıkıştırmaya dayanır. Yani iletim kanalı kullanılmadığında sessiz kalınır, kanalda aktivite algılandığında ise radyo sinyali iletmeye başlanır. Kanalın aktif olarak kullanılıp kullanılmadığını algılamak için sıkışma kaynağının radyosunun sürekli açık olması gerektiğinden, enerji tasarrufu yapılamaz. Bununla birlikte reaktif sıkışma saldırılarının tespit edilmesi zordur.

Sıkışma saldırılarını tespit etmek için; alınan sinyal gücü göstergesi (RSSI) değerlerinin istatistiksel olarak analiz edilmesi, boş bir kanalı algılamak için gereken ortalama süre (taşıyıcı algılama süresi) ve paket teslim oranı (Packet Delivery Ratio, PDR) tekniklerini birleştiren algoritmalar kullanılabilir [120]. Başka bir yöntem ise radyo durumunun açık ve kapalı arasında geçiş yapılarak uyku zamanını belirlemektir. Söz konusu ayarlama işlemi, uyku ve uyanma sürelerini bildiren protokol paketlerini şifreleyerek de gerçekleştirilebilir. Örneğin, IEEE 802.15.4'teki işaret paketleri, algılayıcı düğümleri senkronize etmek için uyku/uyanma aralıklarını içerir. Böylece bu işaret mesajları, olası sıkışma kaynaklarını uyku/uyanma aralıkları hakkında bilgilendirmemek için şifrelenebilir. Bu eylem, sıkışma sinyallerinin alınmamasını ve veri paketlerinin korunmasını sağlar. Ayrıca düşman, sıradan düğümler uyurken, sinyaller yayarak enerjisini gereksiz yere tüketir [119]. Wood ve Stankovic, sıkışma sinyallerinin kesintili olması durumunda, algılayıcı düğümlerin, birkaç yüksek güçlü ve öncelikli mesajı baz istasyonuna göndermesini önermişlerdir [121]. Algılayıcı düğümler, bu tür mesajları başarıyla iletme olasılığını en üst düzeye çıkarmak için Şekil 3.4'te gösterildiği gibi iş birliği yapmalıdırlar.



Şekil 3.4. Sıkışma bölgesindeki düğümlerin, saldırıyı komşu düğümlere bildirmesi

Önerilen yaklaşımdaki iş birliği çerçevesinde, sıkışma bölgesindeki düğümler, saldırıyı komşularına bildirir. Düğümler ayrıca yüksek öncelikli mesajları süresiz olarak arabelleğe alabilir, bu da sıkışmada bir boşluk oluştuğunda bunları aktarmalarını sağlar.

Sıkışmaya karşı önerilen diğer bir yöntem ise frekans atlamalı yayılı spektrum (Frequency Hopping Spread Spectrum, FHSS) kullanımıdır. FHSS, veri paketlerinin üçüncü taraflarca dinlenmesini engellemek için, taşıyıcı frekansın sürekli değiştirilmesi esasına dayanır. Verici ve alıcı, iletişim öncesi taşıyıcı frekanslar için ayarlanmıştır yani hangi zamanda hangi frekansın kullanılacağı önceden belirlenmiştir. Bu bilgiye sahip olmayan saldırganın, paketi dinlemesi engellenmiş olur [122]. Bununla birlikte olası frekans aralığı sınırlı olduğundan, saldırgan frekans bandının geniş bir bölümünü karıştırmaya odaklanabilir. Genel olarak, düşük maliyet ve düşük güç gereksinimlerini korumak için, algılayıcı cihazları tek frekanslı kullanımla sınırlıdır. Bu nedenle KAA'lar, sıkışma saldırılarına karşı oldukça hassastır [35].

Kurcalama Saldırısı

Kablosuz algılayıcı ağların savunmasız/zorlu bölgelere konuşlandırılmaları, onları fiziksel müdahalelere açık hale getirir. Fiziksel olarak ele geçirilen bir düğümün, kriptografik anahtarları ele geçirilebilir, devresi ve program kodları değiştirilebilir. Hatta saldırgan tarafından kontrol edilen kötü niyetli bir düğümle değiştirilebilir [123]. Nitekim algılayıcı düğümlerin bir dakikadan daha kısa sürede manipüle edilebileceği MICA2 algılayıcısı üzerinde gösterilmiştir [124]. Kurcalamaya karşı savunmalar arasında düğümlerin gizlenmesi, kamufle edilmesi veya kurcalamaya karşı korumalı paketler önerilmiştir [121]. Ayrıca düğümlere fiziksel erişim sağlandığında, algılayıcı çipindeki veriyi ve bellek içeriğini, saldırganlar tarafından erişilemez hale getirmek için kurcalamaya dayanıklı donanımlar üzerinde çalışılmıştır [125]. Kurcalamaya karşı önerilen diğer bir yaklaşım ise düğümlerin ele geçirilme ihtimalinin tasarım aşamasında hesaplanarak, hata toleranslı bir yapı oluşturulmasıdır [105].

3.2.2. Veri Bağı Katmanı Saldırıları

Veri bağlantı katmanı, veri akışlarının çoğullanmasından, veri çerçevesi algılamasından, ortam erişiminden ve hata kontrolünden sorumludur [1]. Bağlantı katmanına yönelik saldırılar arasında kasıtlı çakışmalar, kaynakların tüketilmesi, adaletsizlik, sorgulama, uyku reddi, geri çekilme saldırıları ve yeniden oynatma mekanizmasının manipüle edilmesi bulunmaktadır.

Çakışma Saldırısı

Birden fazla düğümün aynı zaman aralığında, aynı frekansta iletim yapmaya çalışması, iletim kanalında çakışmaya neden olur [121]. Saldırgan, hedef düğümlerin veri iletim zamanında, bağlantı katmanı paketleri göndererek, düğümlerin iletim yapmasını engeller. Sıkışma saldırılarının aksine,

sürekli olarak değil, belirli zaman aralıklarında ağa saldırı yapılarak, enerji tasarrufu yapılır [119]. Paketlerin iletim kanalında çakışması, paketlerin bozularak atılmasına, yeniden iletilmesine ve ek maliyete neden olur.

Bağlantı katmanı protokollerinin çoğunda, zamanlama bilgileri, senkron veri iletimine başlamadan önce düğümler tarafından paylaşılır. Bu, veri iletiminde yer alan düğümler için ortak bir program sağlar. İletişim için faydalı gibi görünse de zamanlama bilgilerinin saldırgan düğümlere sızdırılmasına da neden olabilir. Dolayısıyla çakışmalara karşı ilk savunma mekanizması, zamanlama bilgilerini bulunduran paketlerin şifrelenmesidir. Tek anahtarlı bir şifrelemede, anahtar çalınmaya karşı savunmasız olabilir. Buna karşın anahtarların düğümler arasında üretilmesi halinde, enerji tüketimi olumsuz etkilenebilir [119]. Çakışmalara karşı önerilen diğer bir savunma yöntemi, hata düzeltme kodlarının kullanılmasıdır [121]. Hata düzeltme kodları düşük düzeydeki çakışmalara karşı iyi sonuçlar üretebilse de ağa ek işlem ve hesaplama maliyeti yükler. Law vd. tarafından önerilen savunma mekanizmasında ise bir düğüm, hedefinden ACK paketini alamadığında iletişim programını değiştirmesi ve duyuru yapması önerilmiştir [126]. Law, bu saldırıyı önerdikleri güvenlik mekanizmasıyla birlikte OMNeT++ platformunda simüle etmiştir.

Tükenme Saldırısı

Aynı iletim ortamını aynı anda kullanmak isteyen düğümler, iletim ortamında çakışmaya neden olur. Çakışan paketler bozulur ve yeniden iletilir. Kötü niyetli bir saldırgan, bu çalışma mekanizmasını suistimal ederek, paketlerin tekrar tekrar çakışmasına ve düğümlerin kaynaklarının tükenmesine neden olabilir. Bu saldırıya olası bir çözüm; ağa, aşırı istekleri görmezden gelebileceği ve böylece tekrarlanan iletimlerin neden olduğu enerji boşalmasını önleyebileceği şekilde hız limitleri uygulamaktır. Diğer bir teknik ise her düğüme iletim için belirli zaman dilimlerini tahsis etmektir [121].

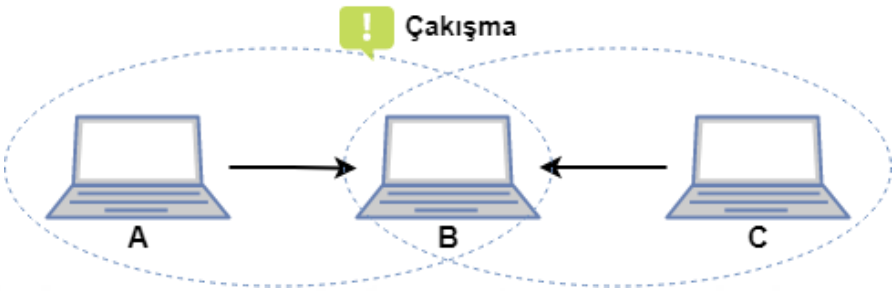
Adaletsizlik Saldırısı

İletim kanalında aralıklı olarak çakışmalara sebebiyet vermek, düğümlerin bir kısmının iletim yapamamalarına neden olacağından, adaletsizliğe neden olur. Küçük çerçevelerin kullanılması, saldırganın iletim kanalını ele geçirebileceği süreyi azaltarak, bu tür saldırıların etkisini azaltır. Bununla birlikte, bu teknik genellikle verimliliği azaltır ve bazı durumlarda daha fazla adaletsizliğe sebebiyet verebilir [127].

Sorgulama Saldırısı

Sorgulama saldırıları, birçok MAC protokolü tarafından kullanılan gönderme/göndermeyi temizle (Request to Send, RTS/Clear to Send, CTS) mekanizmasını manipüle etmeye dayanır. RTS/CTS mekanizmasının gizli düğüm problemine karşı ağın performansını artırdığı görülmüştür [128-134]. Gizli düğüm sorunu, kablosuz ağlarda bir engel veya kapsama alanı probleminden

dolayı, düğümlerin birbirlerini görememelerine rağmen, ortak bir düğüme veri göndermeye çalışmaları sonucu ortaya çıkan çakışma durumudur. Neticede birbirinden habersiz iki ayrı düğüm, birbirlerinin veri paketlerini bozarlar [135]. Gizli düğüm problemi Şekil 3.5'te karakterize edilmiştir.



Şekil 3.5. Gizli düğüm

Sorgulama saldırılarında saldırgan, hedeflenen bir düğümün kaynaklarını tüketmek için art arda RTS mesajları göndererek, CTS yanıtı alır. Sorgulama saldırılarına karşı koymak için bir düğüm, aynı kimlikten gelen bağlantıları kabul etmede kendisini sınırlayabilir, güçlü kimlik doğrulama protokolleri kullanabilir veya tekrarlama koruması uygulayabilir [136, 118].

Uyku Reddi Saldırısı

Kablosuz algılayıcı ağların donanımsal kısıtları ve sınırlı enerji kaynakları, birçok güvenlik tehdidine maruz kalmalarına neden olmaktadır. Kablolu ve kablosuz ağların işlevselliğini kesintiye uğratmak amacıyla yapılan hizmet reddi saldırıları, KAA'ların enerji seviyelerini tüketmeyi hedefler. KAA'larda enerji tasarrufu sağlamak amacıyla iletim kanalını aktif olarak kullanmayan düğümler uyku moduna alınır. Uyku reddi saldırıları, algılayıcı düğümün uyku moduna girmesini engellemek için iletim kanalını meşgul ederek, düğümleri sürekli alma modunda bekletir. Böylece algılayıcı düğümlerin enerjisini tüketir ve ağın kullanılabilirliğini kesintiye uğratır. Stejano ve Anderson, uyku yoksunluğu işkencesi olarak tanımladıkları bu saldırının pille çalışan mobil cihazlar üzerindeki etkisini araştırarak, bu saldırı kavramını ilk kez ortaya koymuştur [137].

Sıkışma saldırılarının bir algılayıcı ağı kalıcı olarak devre dışı bırakabilmesi için hedef cihazların pillerini tüketmesi ayları alabilir. Bununla birlikte algılayıcı düğümlerin telsizlerini açık tutan akıllı bir uyku reddi saldırısı, pilleri yalnızca birkaç gün içinde tüketebilir (bazı cihazlar için). Örneğin Crossbow Mica2 düğümü, alma modunda 36,81 mW ve uyku modunda 0,048 mW enerji tüketir. İki standart 3.000 mAh AA pil, uyku modundaki bir cihaz için 4.000 günden fazla, alma modundaki bir cihaz için ise yalnızca 10 gün dayanır [118].

Algılayıcı düğümlerin uyku moduna geçişlerinin kontrolü MAC protokolleri tarafından yapıldığı için, uyku reddi saldırıları MAC protokollerine odaklanır. Üstelik bir saldırgan, ağ trafiğini analiz ederek, algılayıcı ağın hangi MAC protokolünü kullandığını belirleyebilir. Araştırmalar, bir saldırganın protokolü bilmesi halinde, bağlantı katmanı şifrelemesine rağmen, uyku reddi saldırıları gerçekleştirebileceğini göstermektedir. Saldırganın şifreleme algoritmasını delmesi durumunda daha etkili saldırılar mümkün olup, ağın ömrünü birkaç aydan birkaç güne indirebilir. Üstelik uyku reddi saldırılarının çoğunun sabit bir sinyal gerektirmemesi, trafiği kötü amaçlı tanımlamayı ve saldıran düğümleri bulmayı zorlaştırır [118]. Uyku reddi tehditlerini azaltmak için güçlü bir bağlantı katmanı kimlik doğrulaması, yeniden oynatma saldırılarına karşı koruma, sıkışma tanımlama ve önleme mekanizması, yayın saldırısı koruması ve kurcalamaya karşı dirençli yapılar önerilmiştir [138].

Geri Çekilme Saldırısı

Veri bağı katmanında kullanılan CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance) protokolü, iletim kanalındaki çakışmaları önlemek için geri çekilme mekanizması kullanarak, düğümlerin kanala erişimini yönetir. Geri çekilme mekanizması, belirli bir zaman periyodunda, birden fazla düğümün aynı anda iletim yapması ile oluşacak çakışma riskini en aza indirir [139]. Geri çekilme zamanlayıcıları, rastgele seçilen zamanlarda uyumak üzere tasarlanmıştır. Kötü niyetli bir düğüm, diğer düğümlerden daha az uyumak ve iletim kanalına haksız bir şekilde daha fazla erişim sağlamak için küçük bir geri çekilme değeri belirleyebilir [140]. Böylece iletim kanalı büyük oranda saldırgan düğüme tahsis edilmiş olur. Günümüzde ağ bağdaştırıcılarının son derece programlanabilir olması, algılayıcıların geri çekilme parametrelerini değiştirebilmelerine izin verir [141]. Ayrıca KAA'lar için önerilen birçok MAC katmanı protokolünün CSMA'yı kullanması, geri çekilme saldırılarının yoğunluğunu artırır. MAC katmanı protokolleri üzerine yapılan araştırmalarda, CSMA'nın en yaygın erişim mekanizması olduğu gösterilmiştir [142, 143].

Geri çekilme saldırılarının tespiti zordur. Zira bir düğümün tesadüfen küçük geri çekilme değerleri mi seçtiğine veya küçük geri çekilme değerlerinin kasıtlı bir stratejisinin parçası olup olmadığına karar vermek zordur. Raya vd. geri çekilme saldırılarını da içeren bir kısım saldırıları tespit etmek ve önlemek için DOMINO uygulamasını geliştirmiş ve simüle etmişlerdir [144]. Kyasanur ve Vaidya, geri çekilme saldırılarına sebep olan düğümlerin tespiti için IEEE 802.11 protokolünde bir değişiklik önermektedir [145]. Önerdikleri şemada, alıcı düğüm (güvenilir bir ana bilgisayar/bir baz istasyonu) gönderici tarafından kullanılacak geri çekilme değerini atar. Bu nedenle alıcı, gönderenin herhangi bir yanlış davranışını tespit edebilir ve bir sonraki iletim için geri çekilme değerlerini artırarak cezalandırabilir. Gönderici düğümün hatalı davranışının, belirlenen eşik değerinden yüksek olması durumunda, söz konusu düğüm etiketlenir ve gönderdiği

tüm paketler bırakılır. Bu yaklaşımın temel problemi, alıcı düğümün ele geçirilme ihtimali bulunan ağlarda uygulama sorunudur. Diğer bir savunma yaklaşımı, düğümlerin gerçekten rastgele sayılar kullanıp kullanmadığını kontrol etmektir [140]. Başka bir savunma stratejisi ise geri çekilme mekanizmasıyla ilgili protokol paketlerinin şifrelenmesi, böylece saldırganın küçük geri çekilme aralıkları seçmesine izin verilmemesi olabilir [119].

Tekrar Koruması Saldırısı

IEEE 802.15.4 protokolünde, gönderici bir düğümün aynı mesajı tekrar göndermesini engellemek için tazelik mekanizması kullanılır. Bu mekanizma, tekrarlanan mesajın alıcı tarafından kabul edilmesini önler ve gelen çerçevenin tekrar değil, en son çerçeve olmasını sağlar. Bunun için de her pakete bir sıra numarası atanır. Alıcı en son sayacı kontrol eder ve bir önceki sayaç değerine eşit veya bundan daha düşük sayaç değerine sahip çerçeveyi reddeder. Bu mekanizma, tekrar saldırılarını engellemek için bir tedbir olsa da tekrar koruma saldırılarına sebebiyet vermektedir. Şöyle ki, saldırgan bir düğüm, gönderdiği paketlerin sayaç numaralarına büyük değerler atayarak alıcıya göndermesi halinde, tekrar sayacının değeri yükselecektir. Meşru düğümler, alıcıda tutulan tekrar sayacından daha küçük olan makul boyuttaki çerçeve sayacına sahip bir çerçeve gönderdiğinde, ilgili çerçeve, tazelik mekanizması tarafından atılacaktır. Bu saldırı, tazelik mekanizmasını manipüle ettiğinden, tazelik ölçütü olarak çerçeve sayacı yerine zaman damgası önerilmiştir. Bu yaklaşımda alıcı düğüm, göndericiden aldığı en son zaman damgasını kontrol eder ve zaman damgası önceki zaman damgasına eşit veya bundan daha az olan çerçeveyi reddeder. Bu yaklaşımın dezavantajı artan mesaj boyutudur [146].

Nonce Saldırısı

Nonce, kriptografik iletişimde yalnızca bir kez kullanılabilen bir sayıdır [147]. Algılayıcı düğümler, iletişimde kullanmak üzere düğümlerin listesini içeren bir erişim kontrol listesi (Access Control List, ACL) depolayabilir. ACL içerisinde hedef adres, anahtar, nonce ve seçenek alanları bulunmaktadır. Bu alanlar şifreli mesaj iletişiminde kullanılır. İki iletimde, aynı anahtar ve nonce çiftinin kullanılması, şifreli metinleri elde eden saldırganlar için faydalı olabilir [146]. Uyku modu, elektrik kesintisi, donanım arızası vb. birçok durumda aynı nonce oluşabilmektedir.

Nonce saldırılarına karşı, pakete nonce alanını çerçeve sayacından ayıracak şekilde yeni alanlar eklenebilir. Ayrıca literatürde birçok çalışma, çerçeve sayacı yerine zaman damgası kullanılmasını önermektedir. Zaman damgası, diğer bazı savunma türlerine karşı da güvenlik sağlamaktadır [146].

ACK Saldırısı

Bir düğümün gönderdiği veri paketinin, alıcı düğüm tarafından başarıyla alınması halinde, alıcı düğüm bir ACK paketi ile yanıt verir. ACK saldırılarında, saldırgan, ağ trafiğini dinler ve

gönderici düğümün başarılı gönderim yapmasını engeller. Ardından sahte bir ACK paketi oluşturarak düğüme gönderir. Xiao vd. savunma mekanizması olarak, ACK çerçevesinin sonuna mesaj bütünlük kodu (MIC) eklenebileceğini önermişlerdir [146].

Yayın Saldırıları

Yayın saldırıları, saldırgan bir düğümün, ağın enerjisini tüketmek için iletim kanalına yayın yaptığı saldırılardır. Yayın saldırıları kimliği doğrulanmış veya doğrulanmamış olmak üzere iki şekilde yapılabilir.

Kimliği doğrulanmamış yayın saldırısında, saldırgan MAC kurallarını bilir fakat ağa giremez [148]. Ağa, kimliği doğrulanmamış trafik yayınlar. Neticede hem radyo iletiminden hem de azalan uyku sürelerinden kaynaklı olarak enerji tüketimine neden olur. Kimliği doğrulanmış yayın saldırısında ise saldırgan, MAC kurallarını bilir ve ağa nüfuz edebilir [148]. Ağa, güvenilir trafik yayınlayarak, enerji tüketir.

Yayın saldırılarına karşı yayılmış spektrum iletişimi kullanılabilir. Program bilgilerinin meşru düğümlerden sızmasını önlemek için protokol paketleri şifrelenebilir. Ancak tüm paketleri şifrelemek, tüm sisteme çok fazla ek maliyet getirir. Bu nedenle yalnızca yayın mesajlarında kimlik doğrulama kullanılabilir [119].

Garantilenmiş Zaman Slotu Saldırısı

IEEE 802.15.4 standardında, ağ cihazlarına özel yuvalar (slot) atamak için PAN (Personal Area Network) koordinatörü kullanılır. PAN koordinatörü, iletim esnasında paketlerin çakışmasını engellemek için her ağ cihazına garantilenmiş zaman slotu (Guaranteed Time Slot, GTS) atar. GTS saldırıları, ağ cihazı ile onun PAN koordinatörü arasındaki iletişimi bozmaya dayanır [149]. Saldırgan önce beacon mesajlarını alarak PAN koordinatörü ile senkronize olur. Meşru bir düğüm, GTS yuvası için PAN koordinatörüne talepte bulunduğunda, PAN koordinatörü olumlu yanıt verirse, bu yanıt tüm düğümlere bildirilir. Böylece saldırgan, meşru düğümlerin GTS sürelerini öğrenebilir. Saldırgan, GTS anlarında veri paketi göndererek, meşru düğümler ile PAN koordinatörü arasındaki verilerin çakışmasına ve bozulmasına neden olur.

GTS saldırıları, iki meşru düğüm arasındaki iletişimin akıllı ve senkronize bir şekilde bozulmasına dayanır. Bu durumda sıkışma/çakışma saldırılarına karşı önerilen savunma mekanizmaları kullanılabilir. Örneğin, GTS iletimi için PAN koordinatörü tarafından her bir düğüme farklı frekanslar atanabilir. Bu durumda, saldırgan, her bir iletimin frekansını öğrenmelidir. Bunun yanı sıra, protokol kuralları yeniden düzenlenerek, beacon mesajındaki GTS alanları, düşmana bilgi sızdırmamak için kaldırılabilir. Ayrıca GTS istek mesajları şifrelenebilir [119]. Perrig vd. tarafından geliştirilen SPINS; veri gizliliği, veri bütünlüğü, iki taraflı kimlik doğrulama gibi özellikleri de barındırdığı için şifrelemede kullanılabilir [151].

3.2.3. Ağ Katmanı Saldırıları

Ağ katmanı, ağda uçtan uca bağlantı kurulması, sürdürülmesi ve ağ paketlerinin yönlendirilmesini sağlar [76]. Ağ katmanı saldırıları, ağın işlevselliğini kesintiye uğratacak ve hassas bilgilerin kaybı veya çalınmasıyla sonuçlanabilecek bazı saldırılara açıktır. Bu saldırılar şu şekilde sıralanabilir.

Sahte/Değiştirilmiş Yönlendirme Bilgileri

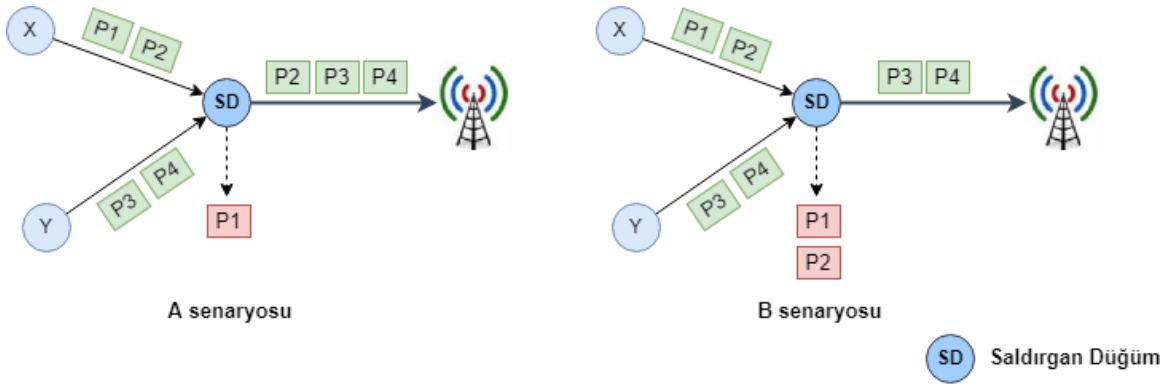
Ağ ve yönlendirme katmanına yapılan en temel saldırı, algılayıcı düğümlerin birbirleriyle ve baz istasyonuyla haberleşebilmeleri için kullandıkları yönlendirme bilgilerini hedeflemektir. Yönlendirme bilgilerinin değiştirilmesi, yeniden oynatılması veya sahte yönlendirme bilgilerinin kullanılması, ağ trafiğini saldırgan düğüme çekebilir veya kesintiye uğratabilir. Bununla birlikte kaynak ve hedef düğüm arasındaki rotanın uzamasına veya kısalmasına sebebiyet verebilir. Veri bağı katmanı şifrelemesi ve global olarak paylaşılan bir anahtar kullanılarak kimlik doğrulaması yapılması, bu saldırılara karşı güvenlik sağlamaktadır [150]. Diğer bir teknik ise paketlere MAC kodu eklemektir. Böylece mesajların sahte olup olmadığı veya değiştirilip değiştirilmediği garanti altına alınır. Tekrarlanan bilgilere karşı, mesajlara sayaçlar veya zaman damgaları da eklenebilir [151].

Seçici Yönlendirme Saldırısı

Algılayıcı düğümlerin her ne kadar kendilerine gelen mesajları güvenilir bir şekilde iletmesi varsayılsa da kötü niyetli bir düğüm, kara delik gibi davranarak, kendisine ulaşan paketleri ağdan düşürebilir. Böyle bir durumda, komşu düğümlerin, saldırgan düğümün başarısız olduğu sonucuna varması ve alternatif yol aramaya karar vermesi muhtemeldir. Bu nedenle saldırgan bir düğüm, sadece belirli paketleri seçici olarak iletmeyebilir veya değiştirebilir. Böylece saldırıya dair şüphe sınırlandırılmış olur [150].

Seçici yönlendirme saldırısı başlatan bir düğüm, komşu düğümleri daha kısa bir rotada oldukları konusunda aldatır. Dolayısıyla saldırgan düğümün, baz istasyonuna olan mesafesi ne kadar az olursa, çekeceği trafik o kadar fazla olur [152].

Şekil 3.6'da saldırgan düğüm; A senaryosunda, X düğümünden gelen P1 paketini iletmeyerek düşürmüş (seçici yönlendirme), B senaryosunda ise X düğümünden gelen tüm paketleri düşürmüştür (kara delik).

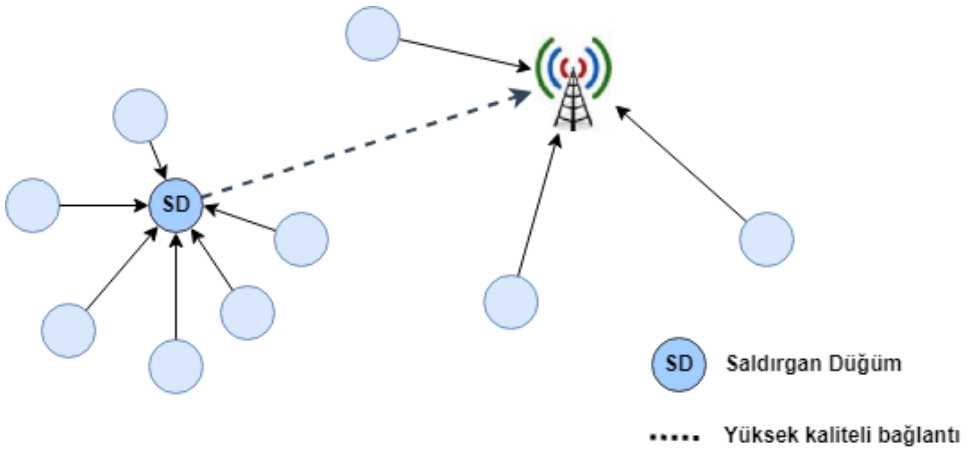


Şekil 3.6. Seçici yönlendirme saldırısı

Karlof ve Wagner'a göre, güvenliği ihlal edilmiş bir düğüm, bir baz istasyonunun yakınında bulunuyorsa, seçici bir yönlendirme saldırısı başlatmak için kendisini bir veri akışına dahil etme olasılığı yüksektir. Bu tür seçici yönlendirme saldırılarına karşı koymak için çok yollu yönlendirme kullanılabilir [150].

Düden Saldırısı

Düden saldırılarında, saldırgan düğüm, kendisini baz istasyonuna giden en kısa rotaya sahip düğüm olarak tanıtarak, diğer düğümler için cazip bir hale getirir. Bu tür saldırılarda, diğer düğümlerden çok daha yüksek hesaplama ve iletişim gücüne sahip cihazlar (dizüstü bilgisayar gibi) kullanılabilir. Böylece baz istasyonuna tek atlamalı (single-hop) bir bağlantıya sahip olabilir. Ardından, ağın geniş bir alanına ulaşmak için yeterli güçle iletim yaparak, yüksek kaliteli bir rota olduğu konusunda çevredeki düğümleri aldatabilir. Baz istasyonuna yüksek kaliteli bir rota sağlayan tek bir güvenliği ihlal edilmiş düğüm bile çevredeki birçok düğümü etkileyebilecek potansiyele sahiptir. Şekil 3.7'de ağ trafiğini çeken saldırgan bir düğüm karakterize edilmiştir.

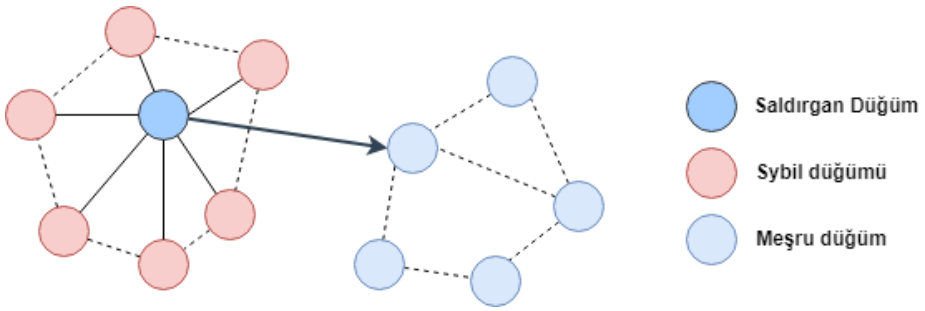


Şekil 3.7. Düden saldırısı

Düden saldırılarına karşı coğrafi yönlendirme protokolleri kullanılabilir. Böylece trafik, baz istasyonunun fiziksel konumu aracılığıyla yönlendirileceği için, saldırgan düğümün diğer düğümleri cezbetmesini ve düden oluşturmasını zorlaştırır [150]. Bir başka savunma tekniği ise Krontiris vd. [7] tarafından önerilmiştir. Önerdikleri yaklaşım, her düğüme saldırı tespit sistemi kurulmasına ve düğümün belirlenen kurallara uyup uymadığının kooperatif olarak kontrol edilmesine dayanır. Düğümlerin çoğu, bir düğümün kurallara uymadığını doğrularsa, bir uyarı oluşturulur. Ngai vd. [153] şüpheli düğümleri listeleme ve ağ trafiğini analiz ederek, saldırgan düğümü tespit etmeye odaklı bir algoritma sunarlar.

Sybil Saldırısı

Sybil saldırısı, kötü niyetli bir düğümün, gayri meşru bir şekilde birden fazla kimliği ele geçirmesi olarak adlandırılır. Kötü amaçlı bir cihazın ek kimlikleri sybil düğümleri olarak tanımlanır [154]. Sybil saldırısında amaç, güvenliği ihlal edilmiş düğümün birçok rotada seçilme olasılığını arttırmaktır [119]. Bir sybil düğümü iki şekilde kimlik alabilir: İlki rastgele yeni sybil kimliği oluşturarak, ikincisi ise meşru düğümlerin kimliklerini çalarak. Özellikle düğüm kimliği tanımlamanın sınırlandırıldığı durumlarda, saldırgan meşru düğümleri devre dışı bırakarak, onların kimliklerini almaya yönelecektir [154]. Neticede sybil düğümü, ağdaki diğer düğümlere birden fazla kimlik sunar. Bu saldırı, özellikle dağıtılmış depolama, çok yollu yönlendirme ve topoloji bakımı gibi hataya dayanıklı şemaları hedefler. Sybil saldırıları Şekil 3.8'de karakterize edilmiştir.



Şekil 3.8. Sybil saldırısı

Sybil saldırılarına karşı önerilen çözümlerden biri, her düğümün güvenilir bir baz istasyonuyla benzersiz bir simetrik anahtarı paylaşmasıdır [150]. İki düğüm daha sonra birbirlerinin kimliğini doğrulamak ve paylaşılan bir anahtar oluşturmak için Needham-Schroeder benzeri bir protokol kullanabilir [155]. Baz istasyonu, bir düğümün sahip olmasına izin verilen komşu sayısını makul bir şekilde sınırlayabilir ve bir düğüm onu aştığında bir hata mesajı gönderebilir. Bir düğümün komşu sayısını sınırlamak, düğümün tehlikeye girmesi durumunda yalnızca doğrulanmış komşularıyla iletişim kurabilmesini sağlar. Bu, düğümlerin birkaç atlama uzaktaki baz

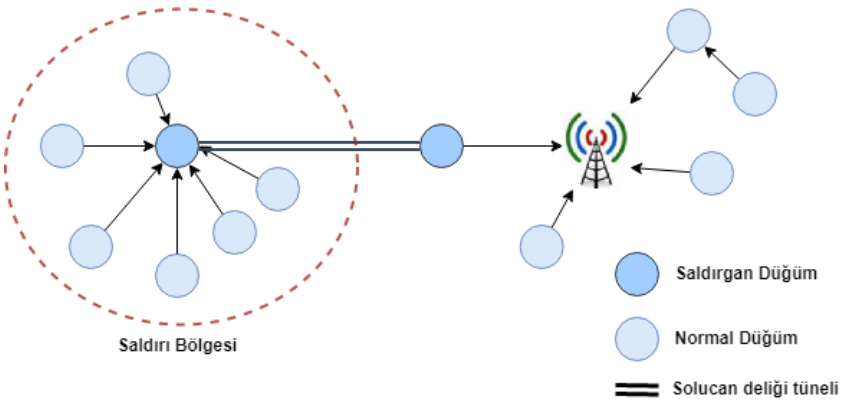
istasyonlarına mesaj göndermesinin yasak olduğu anlamına gelmez, ancak bunu yapmak için doğrulanmış komşuları dışında herhangi bir düğümü kullanmaları kısıtlanır [150]. Sybil saldırılarına karşı önerilen diğer bir yöntem ise konum doğrulamadır. Bu yaklaşımda, algılayıcı düğümlerin hareketsiz oldukları varsayılır. Temel mekanizma, her bir düğümün fiziksel konumunun doğrulanmasına dayanır. Bununla birlikte düğümlerin konumlarının tam olarak güvenli bir şekilde belirlenmesi problemi ortaya çıkmaktadır [154]. Newsome vd. algılayıcı ağdaki, sybil düğümlerini tespit etmek için radyo kaynağı testini kullanmıştır [154]. Bu yaklaşım, herhangi bir fiziksel cihazın yalnızca bir radyoya sahip olduğu varsayımına dayanır. Önerilen mekanizmaya göre bir sybil düğümünü tespit etme olasılığı Denklem 3.1'de gösterilmiştir:

$$\Pr(detection) = 1 - \left(1 - \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{C}} \frac{S-(m-M)}{c}\right)^{r} \tag{3.1}$$

Bir düğümün n komşu kümesinde, s sybil düğümlerinin sayısı, m kötü niyetli düğümlerin sayısı, g ise iyi (doğru) düğümlerin sayısıdır. Bunlardan bir düğüm aynı anda yalnızca c komşuyu test edebilir. Bu c komşulardan S sybil düğümü, M kötü niyetli düğümü ve G iyi (doğru) düğümü vardır. r testi yinelemek için tur sayısıdır.

Solucan Deliği Saldırısı

Solucan deliği saldırılarında, saldırgan, algılayıcı ağın bir bölümünden alınan paketleri, düşük gecikmeli bir bağlantı üzerinden tüneller ve ağın farklı bir bölümünde yeniden oynatır [156]. Bir baz istasyonunun yakınında bulunan bir saldırgan, iyi yerleştirilmiş bir solucan deliği oluşturarak yönlendirmeyi tamamen bozabilir. Bir saldırgan, çok sekmeli düğümleri, baz istasyonuna daha yakın olduklarına ikna edebilir. Solucan deliğinin diğer tarafındaki saldırgan, baz istasyonuna yüksek kaliteli bir rota sağlayacağından, bir düden oluşturabilir ve çevredeki tüm trafiği kendi üzerine çekebilir [157]. Şekil 3.9'da solucan deliği saldırısı karakterize edilmiştir.



Şekil 3.9. Solucan deliği saldırısı

Solucan deliği saldırılarına karşı coğrafi yönlendirme protokolleri önerilmiştir [150]. "Komşu düğümler", aralarındaki mesafenin normal radyo aralığının çok ötesinde olduğunu fark edecekleri için, yapay bağlantılar, coğrafi yönlendirme protokollerinde kolayca algılanır. Solucan deliği saldırılarını önlemek için bir diğer teknik, paket yayılma gecikmesini ölçmek ve çok uzağa giden paketleri atmaktır [156]. Paket yayılma gecikmesi, bir düğümün paketi göndermesinden, alıcının paketi almasına kadar geçen süredir. Ancak bu yaklaşım, sıkı zaman senkronizasyonu gerektirir.

Hello Taşkını

Hello paketi, düğümlerin kendilerini komşu düğümlere tanıtabilmek için gönderdikleri bir pakettir. Paketi alan düğüm, gönderici düğümün radyo menzilinde olduğunu varsayabilir. Karlof ve Wagner [150], bu varsayımın bir saldırgan tarafından manipüle edilebileceğini belirtmiştir. Zira yeterince güçlü yayın yapabilme kapasitesine sahip bir saldırgan, ağdaki düğümleri kendi komşusu olduğuna ikna edebilir. Örneğin, bir saldırganın, ağdaki her düğüme, baz istasyonuna giden çok yüksek kaliteli bir rotanın duyurusunu yapması, çok sayıda düğümün bu rotayı kullanmaya çalışmasına neden olabilir. Üstelik bu düğümler, saldırgan düğümden yeterince uzakta olsa bile ilgili rotayı kullanacaktır. Ağdaki tüm düğümlerin, güçlü yayın kapasitesine sahip saldırganın HELLO paketini cevaplaması, aşırı enerji tüketimine sebep olur [158].

Düğümlerin rota oluşturmadan önce çift yönlü bağlantıları doğrulamasını sağlayan ikili kimlik doğrulama, bu saldırıya karşı kullanılabilir. Diğer bir metot ise düğümlerin iletişim aralığında olmayan düğümlerden gelen Hello mesajlarını azaltmasını sağlayan coğrafi ve enerji duyarlı yönlendirme protokolleridir [159]. Coğrafi protokoller, her düğümün konumunu bilmesini ve bu konumu diğer düğümlere iletebilmesini gerektirir [118]. Saghar vd. [158] Hello taşkınlarına karşı RAEED (Robust formally Analysed protocol for wirEless sEnsor networks Deployment) protokolünü önermişlerdir. RAEED, geliştirilmiş çift yönlü doğrulamayı ve INSENS ile LEAP'ın anahtar değişim özelliklerini kullanır [160, 161].

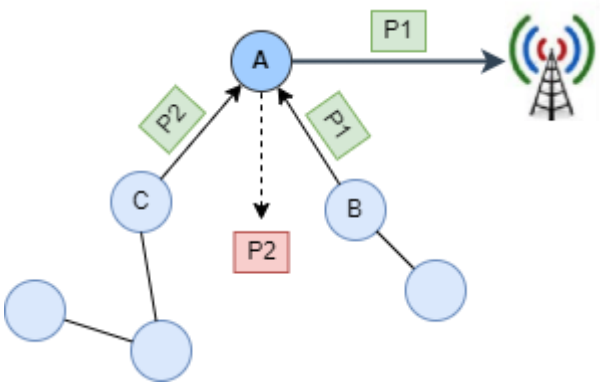
Güven Mekanizmasına Yönelik Saldırılar

Algılayıcı ağlarda, düğümlerin güven/itibar değerleri, diğer düğümlerle iletişimleri için önemlidir. Yüksek itibar değerine sahip düğümler güvenilir kabul edilir. Algılayıcı düğümlerin başlangıçtaki güven değerleri ile ilgili üç seçenek söz konusudur. İlki, başlangıçta tüm düğümlerin güvenilir kabul edildiği ve birbirlerine güvendiği durumdur. Süreç içerisinde, düğümlerin davranışlarına göre güven değerleri azalır veya güvenilmez hale gelebilir. İkincisi, başlangıçta her düğümün güvenilmez kabul edildiği ve birbirlerine güvenmediği durumdur. Zaman içerisinde olumlu davrandıkça güven değerleri artacaktır. Üçüncüsü ise tüm düğümlerin tarafsız olduğu ve etkileşimlerine göre güven değerlerinin artıp, azaldığı durumdur [162]. Algılayıcı düğümler,

doğrudan veya dolaylı olarak itibar değerlerini güncelleyebilirler. Doğrudan güncelleme, dış etki olmaksızın, bir düğümün komşu düğümle olan etkileşimleriyle; dolaylı güncelleme ise komşu düğümlerin, üçüncü bir düğüm hakkındaki tavsiyeleriyle yapılır. Bununla birlikte tavsiye güveni adı verilen güven değeri, doğrudan güvenin özel bir türü olup, doğrudan güven ile komşulardan gelen önerilerin karşılaştırılması ile elde edilir [163].

Algılayıcı düğümlerin güven mekanizmaları, düğümlerin birbirleriyle güvenli iletişimi için kritik bir konudur. Bununla birlikte, söz konusu mekanizmayı manipüle ederek, trafiği bozmaya çalışan bazı saldırılar da mevcuttur. Bu saldırılar şunlardır:

- **Kötü ağız saldırısı:** Güvenliği ihlal edilmiş bir düğümün, komşu düğümler hakkında gerçek olmayan, aldatıcı bildirimlerde bulunması yani "kötü ağızdan" tavsiyelerde bulunması olarak tanımlanabilir [164]. Saldırgan, meşru düğümleri kötü gösterebileceği gibi güvenliği ihlal edilmiş düğümleri ise olumlu bir şekilde iletebilir [165]. Sun vd. bu saldırılara karşı kötü niyetli düğüm algılama performans metriği kullanılmasını önermişlerdir. Bu metoda göre her düğüm, ortalama algılama oranı (Average Detection Rate, AVD) ve yanlış alarm oranı parametrelerini kullanarak kötü niyetli düğümü yerel olarak algılar. AVD, kötü niyetli düğümleri tespit eden iyi davranıştaki toplam düğüm sayısının, kötü niyetli düğüm kümesine bölünmesiyle hesaplanır [163].
- **Aç/kapa saldırısı:** Saldırgan, diğer düğümler tarafından algılanmamak için bir süre iyi, daha sonra kötü davranır. Dolayısıyla güven değeri dinamik olarak değişir ve tespit edilmesi zorlaşır. Bu saldırıya karşı unutma faktörü adı verilen bir parametre önerilmiştir [163]. Unutma faktörü, farklı zaman dilimlerindeki iyi davranışların gözlemlenmesine dayanır. Tıpkı gerçek hayattaki gibi güvenilir biri olmak uzun zaman alırken, güvenilirliğin azalması kısa sürede gerçekleşir. Bu nedenle unutma faktörü, iyi ve kötü davranış dönemleri için uyumlu olarak tanımlanmalıdır.
- **Çakışan davranış saldırısı:** Saldırganın, farklı düğüm gruplarına, farklı davrandığı saldırı tipidir. Bu saldırıda güvenliği ihlal edilmiş bir düğüm, bir grup düğüme iyi davranırken, diğer grup düğüme ise kötü davranabilir. Bu saldırı tipi, meşru düğümlerin saldırgan düğüm hakkında farklı itibar değerleri üretmesine ve düğümler arasında tutarsız güven değerleri oluşmasına neden olur. Şekil 3.10'da saldırgan A düğümünün, meşru B ve C düğümlerine yönelik çelişkili davranışları karakterize edilmiştir. A düğümü, B düğümünden gelen paketleri iletirken, C düğümünden gelen paketleri iletmeyi reddeder. Neticede B ve C düğümleri, A düğümü ile ilgili itibar değerini paylaştıklarında, bir tutarsızlık meydana gelir ve birbirlerine olan güvenleri azalır.



Şekil 3.10. Çakışan davranış saldırısı

Çakışan davranış saldırısına yönelik tespit mekanizması olarak, savunma yüzdesinin hesaplanması önerilmiştir [163]. Saldırgan düğüm, bir grup düğümün (G1) paketlerini iletirken, diğer grubun (G2) paketlerini reddeder. Saldırı yüzdesi ise G2'deki düğüm sayısının, toplam düğüm sayısına bölünmesiyle elde edilir. Saldırı yüzdesi düşükse, saldırganın dürüst tavsiyeleri, onu güvenilir bir düğüm yapar. Bu durum, saldırının tespitini zorlaştırır. Eğer saldırı yüzdesi yüksekse ve saldırgan düğüm, paketleri düşürmeye devam ederse saldırı kolayca tespit edilebilir.

- **Akıllı davranış saldırısı:** Saldırganın, itibar değeri veya güven oylaması gibi önemli bilgileri tespit etmeye çalıştığı saldırı tipidir. Saldırgan, elde edeceği güven değerlerine göre kendi davranışlarını uyarlayacaktır [166]. Bu saldırıya karşı savunma mekanizması olarak mesajların şifrelenmesi önerilmiştir [119].
- **Yeni gelen saldırısı:** Algılayıcı düğümlerin başlangıçtaki güven değerlerinin olumlu veya tarafsız olduğu durumlarda, düğümlerin kötü niyetli davranışları, onların güven değerlerini düşürür. Kötü niyetli davranışların belirli bir eşiği geçmesi durumunda ise ilgili düğüm, ağdan dışlanır. Saldırgan bir düğüm, kötü itibarını silmek için ağa yeni gelen biri olarak katılabilir ve ilk itibar değeri ile çalışmaya başlayabilir. Bu durum saldırgan düğümlerin tespitini anlamsız kılar. Bu saldırıya karşı kimlik doğrulama ve erişim kontrolü önerilmiştir. Böylece yeni kimlikler alarak ağa girmeleri engellenmiş olur. Başka bir yaklaşım ise, ağa yeni katılan düğümlere olumsuz itibar değeri vermektir. Böylece ilgili düğüm uzun bir süre olumlu davranmak durumunda kalacaktır. Hoffman vd. [167] tarafından önerilen "aidat ödeme" yaklaşımı, düğümlerin ağ içerisinde kalabilmeleri için güven değerlerini yüksek tutmalarına ve sürekli olumlu davranmalarına dayanır. Misaghi vd. [168] tarafından önerilen yaklaşımda ise kendi kendini organize eden bir sanal güven ağına dayalı güven değerlendirme şeması önerilmiştir. Düğümler, diğer düğümlerin güvenilirliğini tahmin etmek için güven ağı içinde tutulan davranışlara dayalı olarak güven zincirleri oluşturur. Düğümler, güven ağlarını komşularla periyodik olarak değiş tokuş

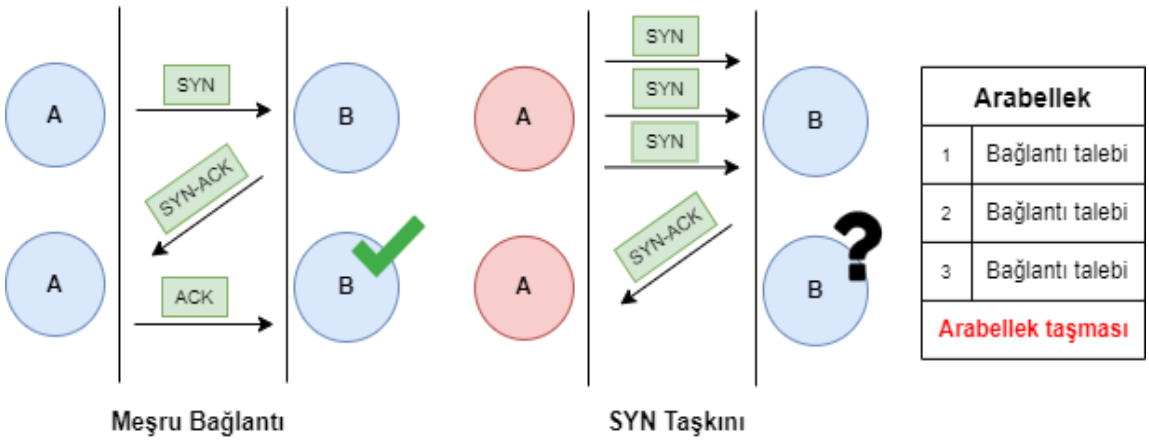
ederek ağ boyunca güven bilgilerini yaymak için verimli bir yöntem sağlar. Yöntem, tamamen dağıtılmış ve kendi kendine organize edilmiştir, herhangi bir güvenilir üçüncü taraf gerektirmez. Benzetim sonuçları, önerilen yaklaşımın etkili olduğunu ve düşük bir ek yük getirdiğini göstermektedir.

3.2.4. Taşıma Katmanı Saldırıları

Taşıma katmanı, ağ paketinin güvenli iletimini sağlamak, paket kaybını önlemek ve trafikte oluşabilecek tıkanıklıkları azaltmak veya önlemekle sorumludur [77]. Taşıma katmanına yönelik yapılan saldırılar şunlardır:

Taşkın Saldırısı

Düğümler arasında iletişim başlaması için, üçlü el sıkışmanın gerçekleşmesi gerekir [169]. Saldırgan, bu mekanizmayı manipüle ederek hedef düğümü, meşru trafiğe yanıt veremeyecek duruma getirir: Saldırgan, hedef düğüme bağlantı talebinde bulunmak için bir SYN (synchronize) paketi gönderir. Hedef düğüm, talebi aldığını belirtmek için SYN/ACK paketi ile cevap verir. Bağlantının kurulması için saldırganın ACK (acknowledgement) mesajı ile yanıt vermesi gerekir ancak yanıt vermez ve yarı açık bir bağlantı kalmasına sebebiyet verir. Hedef düğüm, ACK paketi beklerken, saldırgan daha fazla SYN paketi gönderir. Düğümler, bağlantı isteklerini sınırlı boyuttaki bir arabellekte depolar ve arabellek, birkaç başarısız bağlantı girişiminden sonra taşar [119]. Neticede hedeflenen düğüm, meşru bağlantı taleplerine cevap veremez duruma gelir. Şekil 3.11'de SYN taşkınları karakterize edilmiştir.



Şekil 3.11. SYN taşkını

SYN taşkınlarına güvenlik çözümü olarak, SYN çerezleri önerilmiştir [118]. Bu teknik ile bağlantı talepleri, hedef tarafta tutulmaz. Dolayısıyla hedef düğümün arabellek taşması

engellenebilir. Başka bir yöntem ise, belirli bir düğümden gelen bağlantıların sayısını sınırlamaktır [127]. Ancak bu durum meşru düğümlerin de bağlantılarını sınırlayacaktır. Diğer bir yaklaşım ise bağlantı talebi gönderen her düğüme bulmaca dağıtılmasıdır [170]. Böylece talep gönderen düğüm, hedef düğümün kaynaklarını tüketecek kadar hızlı bağlantı gönderemeyecektir.

Desenkronizasyon Saldırısı

Desenkronizasyon saldırısı, saldırganın, aktif bir bağlantıyı kesintiye uğratmasına ve bağlantının iki ucundaki düğümlere defalarca mesajlar göndermesine dayanır. Bu mesajlar, düğümlerin, kaçırılan çerçevelerin yeniden iletilmesini talep etmesine neden olan sahte sıra numaraları veya kontrol bayraklarını taşır. Bu durumda düğümler tekrar iletimde bulunarak, enerjilerini boşa harcar. Bu saldırılar, kimlik doğrulaması ile engellenebilir [121].

3.2.5. Uygulama Katmanı Saldırıları

Ağ trafiğinin yönetimi uygulama katmanında gerçekleştirilir. Uygulama katmanı, verileri anlaşılır bir biçimde dönüştüren veya belirli verilerin elde edilmesi için sorgular gönderen farklı uygulamalar için yazılım sağlar [76]. Uygulama katmanına yönelik saldırılar arasında düğümlerin algılanan verilerle boğulması, düğümlerin yeniden programlanması ve ağa tekrar tekrar mesajlar gönderilmesi bulunmaktadır.

Düğüm Ezme Saldırısı

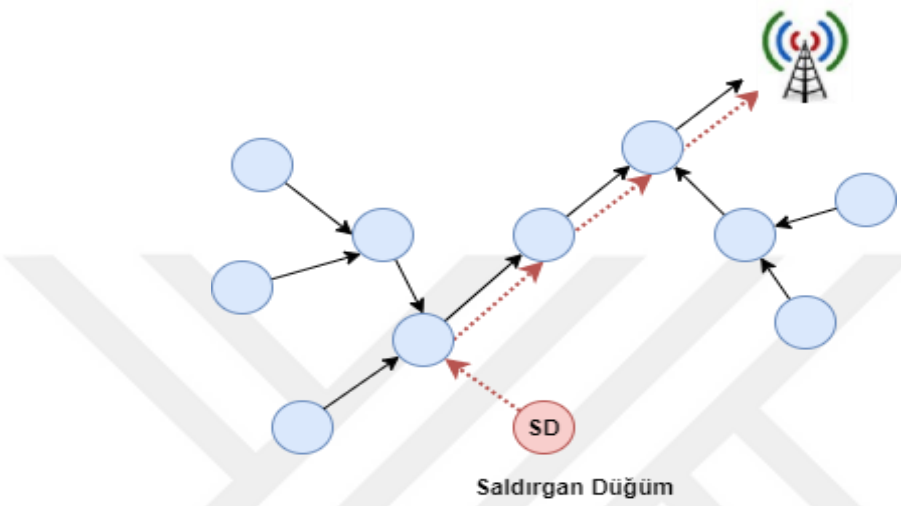
Ağın bant genişliğini ve enerjisini hedef alan bu saldırı; ağda bulunan düğümleri, algılayıcı uyaranlarıyla boğmaya çalışarak, ağın büyük hacimli trafiği bir baz istasyonuna iletmesine neden olabilir. Bu saldırı, uygulamanın dinamik olarak ortamdan veri topladığı durumlarda geçerli olur. Örneğin, bir hareket algılama uygulaması dinamik bir uygulamadır. Hız sınırlayıcı ve verimli veri toplama algoritmaları bu saldırıların etkilerini azaltabilir [118].

Yeniden Programlama Saldırısı

TinyOS Deluge ağ programlama sistemi gibi protokoller, algılayıcı düğümlerin uzaktan yeniden programlanabilmesine olanak tanır [171]. Algılayıcı düğümlerin zorlu ortamlara konuşlandırıldığı varsayıldığında, uzaktan yeniden programlama yapmak mantıklı bir durumdur. Bununla birlikte yeterince korunmayan bir sistem, saldırganların hedefi haline gelir ve tıpkı meşru kullanıcı gibi saldırganlar da düğümleri uzaktan programlayabilir. Kimlik doğrulama ve düğüm kurcalamaya yönelik savunma mekanizmaları, yeniden programlamaya karşı önlem olarak kullanılabilir [172, 118].

Yol tabanlı DOS saldırısı

Bu saldırı, bir algılayıcı ağın hiyerarşik olarak en alttaki düğümünden, ağa sahte veya yeniden oynatılan paketler gönderilmesi ile oluşur. Paketler, alt düğümden, baz istasyonuna kadar giden yol boyunca iletilir. Bu durum, bant genişliğinin ve düğümlerin enerjilerinin tükenmesine sebebiyet verir [173]. Yol tabanlı DOS saldırısı Şekil 3.12'de karakterize edilmiştir.



Şekil 3.12. Yol tabanlı DOS saldırısı

Kimlik doğrulama ve yeniden oynatmayı önleme metotları, bu saldırıya karşı güvenliği sağlayabilir [118].

Algılayıcı ağlara yönelik saldırılar ve savunma mekanizmaları Tablo 3.1'de gösterilmiştir.

Tablo 3.1. Katmanlara yönelik saldırılar ve savunma mekanizmaları

Katman	Saldırı Tipi	Savunma Mekanizması
Fiziksel katman	Sıkışma saldırısı	RSSI değerlerinin analizi, taşıyıcı algılama süresi ve PDR tekniklerini birleştiren algoritmalar, radyo açık/radyo uyku değişimi, istasyonu öncelikli mesaj bildirimi, FHSS kullanımı
	Kurcalama saldırısı	Düğümlerin gizlenmesi, kurcalamaya karşı paketler, kendini imha eden kurcalamaya karşı donanımlar, hata toleranslı yapı
Veri bağı katmanı	Çakışma saldırısı	Paket şifreleme, hata düzeltme kodları, program değiştirme
	Tükenme saldırısı	Hız limiti, zaman dilimi tahsisi
	Adaletsizlik saldırısı	Küçük çerçeve
	Sorgulama saldırısı	Kimlik doğrulama, tekrarlama koruması
	Uyku reddi saldırısı	Kimlik doğrulama, tekrarlama koruması, sıkışma tanımlama ve önleme, yayın saldırısı koruması, kurcalamaya karşı dirençli yapılar
	Geri çekilme saldırısı	DOMINO, güvenilir alıcının geri çekilme değeri ataması, rastgele sayı kullanılıp kullanılmadığının tespiti, paket şifreleme
	Tekrar koruması saldırısı	Zaman damgası
	Nonce saldırısı	Pakete yeni alan ekleme, zaman damgası
	ACK saldırısı	Mesaj bütünlük kodu
	Yayın saldırıları	Yayılmış spektrum, paket şifreleme, kimlik doğrulama
	GTS saldırısı	Sıkışma/çakışma savunma mekanizmaları, paketten GTS bilgilerini kaldırma, GTS istek mesajlarını şifreleme
Ağ katmanı	Sahte/değiştirilmiş yönlendirme bilgileri	Veri bağı katmanı şifrelemesi, kimlik doğrulaması, MAC kodu, sayaç veya zaman damgası
	Seçici yönlendirme saldırısı	Çok yollu yönlendirme
	Düden saldırısı	Coğrafi yönlendirme protokolleri, saldırı tespit sistemi, şüpheli düğümleri listeleme, trafik analizi
	Sybil saldırısı	Kimlik doğrulama, komşu sınırlandırma, konum doğrulama, radyo kaynağı testi,
	Solucan deliği saldırısı	Coğrafi yönlendirme protokolleri, paket yayılma gecikmesi
	Hello taşkını	İkili kimlik doğrulama, coğrafi yönlendirme protokolleri, RAEED
	Kötü ağız saldırısı	Kötü niyetli düğüm algılama performans metriği
	Aç/kapa saldırısı	Unutma faktörü
	Çakışan davranış saldırısı	Savunma yüzdesi
	Akıllı davranış saldırısı	Paket şifreleme
	Yeni gelen saldırısı	Kimlik doğrulama, erişim kontrolü, başlangıçta olumsuz itibar değeri, aidat ödeme, güven değerlendirme şeması
Taşıma katmanı	Taşkın saldırısı	SYN çerezleri, sınırlı bağlantı sayısı, bulmaca
	Desenkronizasyon saldırısı	Kimlik doğrulama
Uygulama katmanı	Düğüm ezme saldırısı	Hız sınırlayıcı, verimli veri toplama algoritmaları
	Yeniden programlama saldırısı	Kimlik doğrulama, kurcalama savunma mekanizmaları
	Yol tabanlı DOS saldırısı	Kimlik doğrulama, tekrarlama koruması

3.3. Kablosuz Algılayıcı Ağlarda Güvenlik Mekanizmaları

Güvenlik mekanizmaları, algılayıcı ağın güvenilir bir şekilde veri toplamasını, değerlendirmesini ve iletmesini sağlar. Ağa yönelik tehdit unsurlarının tespit edilmesi ve olası veri kayıplarının önüne geçilmesi için güvenlik mekanizmaları elzemdir. KAA'lara yönelik güvenlik mekanizmaları arasında güvenli grup yönetimi, güvenli veri toplama ve saldırı tespit sistemi bulunur.

3.3.1. Güvenli Grup Yönetimi

Özelikle geniş ölçekli coğrafi alanlara konuşlandırılan algılayıcı ağlar, enerji/yük tasarrufu, tekrarlı verileri ve çakışmaları engelleme, hata toleransı ve sağlamlık gibi birçok gerekçeyle daha küçük gruplara bölünerek yönetilir. Algılanan ham verilerin ağ içinde toplanması, birleştirilmesi ve analiz için baz istasyonuna gönderilmesi grup liderleri tarafından yürütülür. Veri kaybının önlenmesi ve tutarlı verilerin elde edilmesi için, grup lideri, grup üyesi olan düğümlerden aldığı verilerin kimliğini doğrulamalıdır. Yani grup anahtar yönetimine gereksinim duyulur. Bununla birlikte algılayıcı ağlar kendi kendine organize olabilme kabiliyetine sahip olduklarından, ağa yeni bir düğümün eklenmesi veya çıkarılması işleri zorlaştırır. Dolayısıyla güvenli bir grup yönetimi için güvenli protokoller de gereklidir. Bu protokollerin; KAA'ların iletişim ve hesaplama kapasitelerini, sınırlı enerji kaynaklarını ve iletim ortamı gibi zorluklarını göz önünde bulunduran, etkili aynı zamanda kaynak tüketimi açısından verimli olması zaruridir [127].

3.3.2. Güvenli Veri Toplama

Kablosuz algılayıcı ağlar, geniş bir fiziki alanda, yoğun bir algılama kapasitesine sahiptir. Bununla birlikte algılayıcı ağı oluşturan düğümlerin donanımsal kısıtları, mimarileri ve iletim ortamı, enerji tüketimini önemli bir kriter haline getirir. Veri iletişimi, bir algılayıcı ağın toplam enerji tüketiminin önemli bir kısmını oluşturur. Nitekim [151]'de SNEP protokolü için hesaplama ve iletişimin enerji maliyetleri listelenmiş, veri iletiminin söz konusu maliyetin %71'ini oluşturduğu gösterilmiştir. Bu nedenle algılayıcı ağın sürdürülebilir olması için gereksiz verilerin ortadan kaldırılması ve veri iletim maliyetlerinin düşürülmesi gerekir.

Algılayıcı ağların yüksek düğüm yoğunluğu nedeniyle aynı veriler, birçok düğüm tarafından algılanır ve bu da veri fazlalığı/artıklığı ile sonuçlanır [81]. Fazla iletimi ortadan kaldırmak ve baz istasyonuna birleştirilmiş verileri göndermek için birden çok düğümden gelen verileri toplama/birleştirme yaklaşımı kullanılır. Bu yaklaşım, enerji tasarrufu için etkili ve gerekli bir tekniktir [82].

Geleneksel veri toplama teknikleri, verileri birleştirmek için SUM, COUNT, AVERAGE, MIN/MAX gibi basit sorguları içerir. Bazı araştırmacılar; medyan, en sıkı veri değeri, veri dağılımının histogramı gibi parametreleri de veri toplama için önermişlerdir [174].

Bir algılayıcı ağda veri toplama, verileri algılama ve birleştirme adımlarından oluşur. Veri toplama, alana konuşlandırılan toplayıcı düğümler tarafından gerçekleştirilir. Bu düğümlerin güvenliğinin ihlal edilmesi, veri kaybına veya sahte verilerin ağ trafiğine girmesine neden olabilir. Dolayısıyla güvenli veri toplama; kimlik doğrulama, gizlilik ve bütünlük gerektirir. Bununla birlikte güvenliği ihlal edilmiş düğümlerin tespiti için düğümlerin iş birliği içerisinde olmaları da gereklidir [35].

3.3.3. Saldırı Tespit Sistemi

Algılayıcı ağların güvenliği için önerilen güvenlik ilkeleri ve mekanizmaları, ağ güvenliğini sağlamak için önceden yapılandırılır. Söz konusu yapılandırmalar güvenlik için kritik olsa da güvenliği tamamen sağlama konusunda yeterli değildir. Güvenliği ihlal edilmiş düğümlerin algılanması ve önlenmesi, tüm ağın güvenilir sonuçlar üretmesi için elzemdir. Marti vd. [175] yaptıkları çalışmada, hatalı davranan düğümlerin, tüm ağın verimini ciddi manada düşürebildiği gösterilmiştir. İlgili çalışmanın benzetim sonuçları, ağdaki düğümlerin %10-%40'ı hatalı davranırsa, ortalama verimin %16-%32 oranında düştüğünü göstermektedir. Dolayısıyla güvenilir bir ağ hem güvenlik ilkeleri ve mekanizmaları ile yapılandırılmış olmalı hem de güvenliği ihlal edilmiş düğümleri tespit etme ve önleme kabiliyetine sahip olmalıdır.

Saldırı tespit sistemleri (STS), bir ağa veya sisteme yönelik kötü niyetli aktiviteleri izleyen, olası ihlal durumlarını sistem yöneticisine bildiren veya uyarı üreten cihaz veya yazılımlardır [176]. Algılayıcı ağlara yönelik güvenlik mekanizmaları, spesifik saldırılara karşı koymak için tasarlanmıştır. STS'ler ise algılayıcı ağın katmanlarını ve kullanıcı faaliyetlerini izleyerek, kötü niyetli her türlü faaliyeti tespit etmeye yönelik bir mekanizmadır [177]. STS mekanizmasının güvenilirliği, ürettiği yanlış pozitifler (yanlış alarmlar) ve yanlış negatifler (algılanamayan saldırılar) ile ölçülür. Etkili ve verimli bir STS, bu iki kavramı minimize etmeye çalışır [178].

Algılayıcı ağlara kurulu saldırı tespit sistemleri şu görevleri yerine getirebilir:

- Çeşitli güvenlik mekanizmaları sadece belirli saldırı türlerine karşı güvenliği sağlarken, saldırı tespit sistemleri, algılayıcı ağın katmanlarını olası tüm saldırılara karşı etkili ve verimli bir şekilde koruyabilir.
- Algılayıcı ağı etkili ve verimli bir şekilde korumaya aldığından, ağın sürdürülebilir olmasını sağlar.
- Algılama metotlarının hibrit olarak kullanılması halinde yeni ve güncel saldırılara karşı etkili bir güvenlik elde edilebilir.

- Algılayıcı düğümlerin veri toplama, değerlendirme ve baz istasyonuna güvenli iletimi gibi süreçlerin güvenli bir şekilde yürütülmesini sağlar.
- Algılanan verilerin gizliliğini sağlamakla birlikte verilerin iletim boyunca bütünlüğünü korumaya olanak tanır.
- Verilerin yeniden iletimini denetleyebileceği gibi verilerin güncelliğini/tazeliğini de garanti altına alır.
- Ağa dahil olan kullanıcıların sisteme giriş-çıkışları da dahil olmak üzere her türlü normal veya şüpheli aktivitesini takip edebilir [179].

Saldırı tespit sistemleri, ağın güvenliğini sağlamak için kritik görevler yürütebilmesine rağmen birtakım işlemleri ise gerçekleştiremez. Söz konusu işlemler şunlardır:

- Kullanılan ağ topolojisinden kaynaklı düğüm arızalarını/hatalarını gideremez.
- Algılayıcı ağın konuşlandırıldığı zorlu ve savunmasız ortamdan kaynaklı fiziki müdahalelere karşı çözüm geliştiremez. Zira söz konusu müdahaleler neticesinde düğümün kriptografik anahtarları ele geçirilebileceği gibi düğümün program kodları da değiştirilebilir.
- Yönlendirme algoritmalarına ait zayıflıkları ve güvenlik açıklarını telafi edemezler.
- Sıkışma ve diğer kaynak tüketim saldırılarına yoğun maruz kalan ağlarda, STS'ler verimli bir şekilde çalışamayabilir.

Saldırı tespit sistemleri mimarilerine göre ağ tabanlı veya host tabanlı sistemler olmak üzere ikiye ayrılır.

1. **Ağ tabanlı sistemler:** Ağdaki tüm cihazlardan gelen trafiği incelemek için ağ içinde planlı bir noktada kurulur. Tüm alt ağda geçen trafiği gözlemler ve alt ağlarda geçen trafiği bilinen saldırıların koleksiyonuyla eşleştirir. Bir saldırı tespit edildiğinde veya anormal davranış gözlemlendiğinde, uyarı yöneticiye gönderilebilir [180]. Ağ tabanlı STS'lerin, geniş ölçekli ağları izleyebilme ve saldırganlara karşı gizlilik gibi avantajlarının yanı sıra yoğun trafik altında başarısızlık ihtimali, şifrelenmiş veya parçalanmış paketleri analiz edememe gibi dezavantajları vardır [179].
2. **Host tabanlı sistemler:** İşletim sistemlerini ve sistemin günlük dosyalarını izleyerek saldırı tespiti yapan sitemlerdir. Host tabanlı sistemler, yerel makineleri izleyerek ağ tabanlı sistemlerin tespit edemediği saldırıları da yakalayabilirler. Ayrıca şifrelenmiş ağ trafiğine de çalışabilir. Ancak sunucu tabanlı sistemlerin yönetimi zordur. Bununla birlikte sadece üzerinde çalıştığı sistemi koruma altına alır. Ayrıca işletim sistemini izleme neticesinde büyük miktarlardaki verilerle uğraşma zorluğu ve sistem kaynaklarına ek yük sorunu ortaya çıkabilir. Sisteme yönelik saldırılar sonucunda devre dışı kalma olasılığı da vardır [179].

Saldırı tespit sistemleri, veri kaynaklarından bağımsız olarak; istemciye, sunucuya veya her ikisine de kurulan ve ağ davranışını izleyerek, değerlendiren ve gerektiğinde uyarı üreten birimine STS ajanı adı verilir. STS ajanı üç aşamada işlem yapar:

1. **İzleme ünitesi:** Gerek yerel olayların gerekse de komşu düğümlerin izlenmesi görevlerini icra eder.
2. **Analiz ve tespit ünitesi**: Saldırı tespit sisteminin mimarisine ve kullanılan algoritmaya bağlı olarak, ağ trafiğini ve düğümlerin davranışlarını analiz etme ve olası ihlalleri tespit etme faaliyetlerinden sorumludur.
3. **Uyarı ünitesi:** Ağ trafiğinde tespit edilen güvenlik ihlallerini, mekanizmaya bağlı olarak, sistem yöneticisine bildiren ve uyarı üreten birimdir. STS bileşenleri, Şekil 3.13'te şematik olarak gösterilmiştir.

Şekil 3.13. STS bileşenleri

STS ajanı, ağı güvenlik ihlallerinden korumak için önemli görevler yerine getirir. STS ajanının, algılayıcı ağa kurulumu için üç farklı kurulum mekanizması önerilmiştir [181]:

1. **Merkezi mekanizma:** Düğümler, ortamdan algıladıkları verileri havuza veya baz istasyonuna gönderirler. Merkezi kurulum mekanizmasında, STS ajanı havuz veya baz istasyonuna kurulur. Dolayısıyla ağ trafiğinin izlenmesi ve olası ihlallerin tespit edilerek uyarı üretilmesi sorumluluğu havuz veya baz istasyonuna aittir. Bu yaklaşım, algılayıcı düğümlerin davranışını toplu olarak analiz etmek için düğümlerden bilgi toplayan ek bir özel yönlendirme protokolü gerektirir.
2. **Dağıtık mekanizma:** Algılayıcı düğümlerin kendi STS mekanizmasına sahip olduğu yaklaşımdır, yani STS ajanı her düğüme kurulur. Dağıtık mekanizmada düğümler hem yerel olayları hem de radyo aralığındaki düğümlerden aldıkları verileri analiz eder, anormal aktiviteler için uyarı üretir. Bir düğümün karar verme süreci, bireysel veya iş birliğe dayalı olmak üzere iki farklı şekilde gerçekleştirilir. Bireysel karar mekanizmasında, diğer düğümlerin anormal davranışlarını tespit eden düğüm, bu bilgiyi doğrudan havuza veya baz istasyonuna gönderir. İş birliğe dayalı karar mekanizmasında ise herhangi bir düğümün anormal davranışını tespit eden düğüm, diğer düğümlerle iletişim kurar ve düğümlerin

oylaması sonucu ortak bir karar verilir. Düğümlerin çoğunluğu, söz konusu düğümü, güvenliği ihlal edilmiş düğüm olarak oylarsa, uyarı üretilir ve ağ yeniden yapılandırılır.

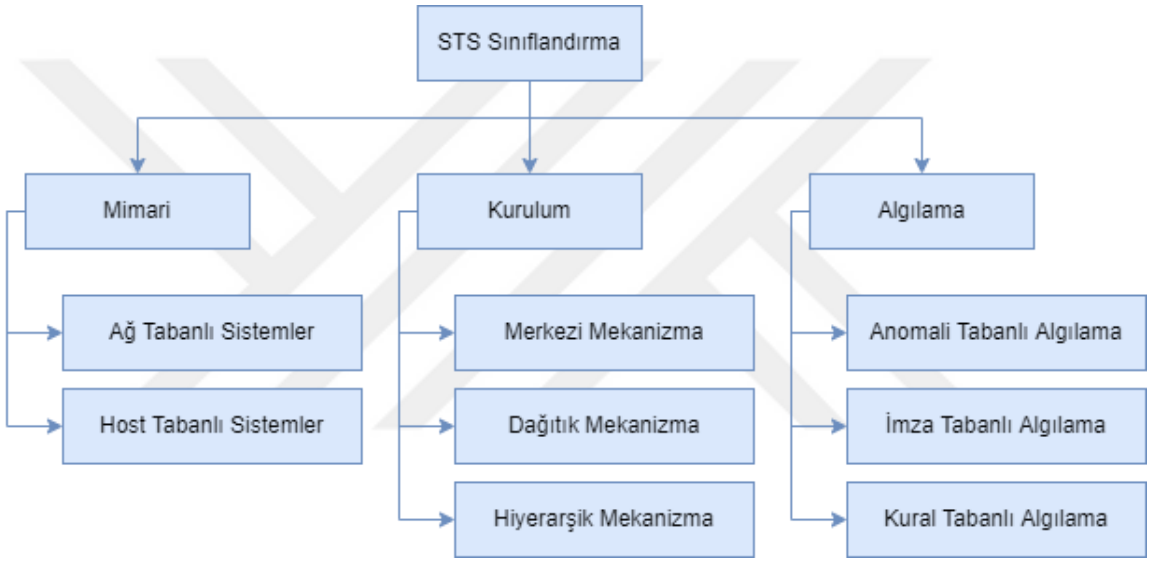
3. **Hiyerarşik mekanizma:** KAA'lar, enerji/yük tasarrufu, veri trafiğini azaltma, hata toleransı ve sağlamlık gibi birçok avantajından dolayı daha küçük hiyerarşik birimlere yani kümelere ayrılırlar. Algılanan verilerin toplanması ve yönlendirilmesi görevi ise küme başı düğümler tarafından yerine getirilir. Küme başı düğümlerin, diğer düğümlerden daha fazla yeteneğe sahip olduğu varsayılır. Hiyerarşik mekanizmada STS ajanı, küme başı düğümlere kurulur. Bu düğümler hem kendi görevlerini hem de ağ güvenliğini sağlama görevini yerine getirir. Bu yaklaşımda, dağıtık mekanizmada ortaya çıkan algılama yükü minimize edilmiştir.

Kablosuz algılayıcı ağlara yönelik saldırı tespit sistemlerinde çeşitli algılama yöntemleri kullanılmaktadır. Söz konusu yöntemler arasında ağın normal davranışından sapan trafiği analiz etmek için anomali tabanlı algılama, daha önce tanımlanan imza veya dizilere göre algılama yapan imza tabanlı algılama ve çeşitli kurallara göre saldırı tespiti yapan kural tabanlı algılama bulunmaktadır.

- **Anomali tabanlı algılama:** Ağ trafiğini izleyerek, normal veya kötü niyetli olarak sınıflandıran bir metottur. Bu yaklaşımda ağın normal davranışı belirlenir ve normalden sapan herhangi bir trafik, izinsiz giriş olarak algılanır. Anomali tabanlı algılama metoduna dayanan STS'lerin çoğunda, izinsiz girişler, belirli eşik değerleriyle tanımlanır; yani, eşiğin altındaki herhangi bir faaliyet normal, eşiğin üzerindeki faaliyetler ise izinsiz giriş olarak algılanır [182]. Anomali tabanlı algılama metodunun, yeni ve bilinmeyen saldırıları tespit etme yeteneği yüksektir. Bununla birlikte yanlış pozitif oranı yüksektir [183].
- **İmza tabanlı algılama:** Önceden bilinen güvenlik ihlallerinin imzaları/kalıpları üretilir ve gelecekteki ihlallerin tespiti için söz konusu imzalar/kalıplar referans olarak kullanılır [183]. Bu yöntem, model eşleştirme esasına dayanır ve yalnızca bilinen saldırılar için doğru ve verimli bir şekilde çalışmaktadır. Yeni ve bilinmeyen saldırılar için yeterli güvenliği sağlayamaz. Ayrıca bu yöntemin etkili bir şekilde kullanılabilmesi için güvenlik ihlallerinin tanımlanması gerekir. Örneğin, bilinen saldırıların imzalarının bir günlük dosyasında oluşturulması gibi. Saldırı senaryosunu tespit etmek için her örnek, günlük dosyasının girişleriyle eşleştirilir. Dolayısıyla KAA'lar için pahalı bir yöntemdir [184].
- **Kural tabanlı algılama:** Bu yöntemde, algılayıcı ağın doğru ve verimli bir şekilde çalışabilmesi ve olası güvenlik ihlallerinin tespit edilebilmesi için bir dizi kısıtlamalar ve kurallar tanımlanır [185]. Algılayıcı düğümlerin davranışları, sırayla her bir kurala göre kontrol edilir. Her düğüm ile ilişkilendirilen hata değeri vardır. Düğümlerin herhangi bir kuralı ihlal etmesi durumunda, hata değeri artırılır. Düğümün hata sayısı, belirli bir *t* zaman aralığında, eşik değerinden fazla olursa, o düğüm hakkında uyarı oluşturulur [184]. Bu

yöntem, düşük bir yanlış pozitif oranına sahip olmakla birlikte önceden bilinmeyen saldırıları tespit etme yeteneğine de sahiptir [185]. Ancak saldırı tespiti için kural tanımlama, zaman alıcı bir süreçtir [183].

Algılama metotları ile tespit edilen saldırılara karşı sistem aktif veya pasif yanıtlar verebilir. Aktif yanıtlar, saldırı tespitinin gerçekleşmesiyle otomatik olarak yerine getirilen süreçleri kapsar. Bu çerçevede, saldırı hakkında ek bilgi toplama veya saldırgan ile hedef ağ arasındaki iletişimi kesme gibi yanıtlar verilebilir. Pasif yanıtlar ise daha çok saldırı tespiti ile ilgili alarm oluşturma ve sistem yöneticisine bildirme şeklinde çalışır [179]. Şekil 3.14'te STS'ler çeşitli kriterlere göre sınıflandırılmıştır.



Şekil 3.14. STS sınıflandırma

Etkili bir STS tasarımı için, algılayıcı ağın konuşlandırıldığı fiziki ortam, ağın ölçeği ve donanımsal kısıtları göz önünde bulundurulmalıdır. Zira tasarlanan bir STS, güvenlik tehditlerine karşı etkili olabilir ancak enerji verimli de olması esastır. Dolayısıyla hedef ağa özgü modeller seçilmelidir. Trafik düzeninin çoğunlukla aynı olduğu küçük ölçekli ağlarda anomali tabanlı algılama metodu kullanılabilir. Zira bu tür ağlarda olağan dışı trafik düzeni veya değişen davranış, kolay bir şekilde izinsiz giriş olarak algılanabilir. İmza tabanlı STS'ler, daha fazla güvenlik tehdidinin ve saldırıların hedefi konumunda olan geniş ölçekli ağlar için daha uygundur. Bununla birlikte imza tabanlı yaklaşım, anomali tabanlı yaklaşıma göre daha fazla kaynak ve hesaplamaya ihtiyaç duyar. Ayrıca veri tabanına güncel saldırı imzalarının eklenmesi, önemli ve karmaşık bir süreçtir [182]. Dolayısıyla etkili ve verimli bir STS tasarımı için ağın donanımsal ve enerji kısıtları göz önünde bulundurulmalı ve ağın ölçeğine/ihtiyaçlarına uygun modeller belirlenmelidir.

4. MATERYAL VE METOT

Bu tez çalışmasında, kullanımı gittikçe yaygınlaşan kablosuz algılayıcı ağlarda, güvenliği ihlal edilmiş düğümlerin algılanması ve önlenmesi için kapsamlı bir saldırı tespit sistemi modellenmiştir. Saldırı tespit sistemleri için önerilen algılama metotlarının, günümüz şartlarında yeterli güvenliği sağlamada yetersiz olduğu görüldüğünden, algılama metotlarını birlikte ihtiva eden hibrit bir algılama modeli ortaya konmuştur. Modellenen STS'nin çeşitli kriterlere göre performans analizi 5. bölümde sunulmuştur.

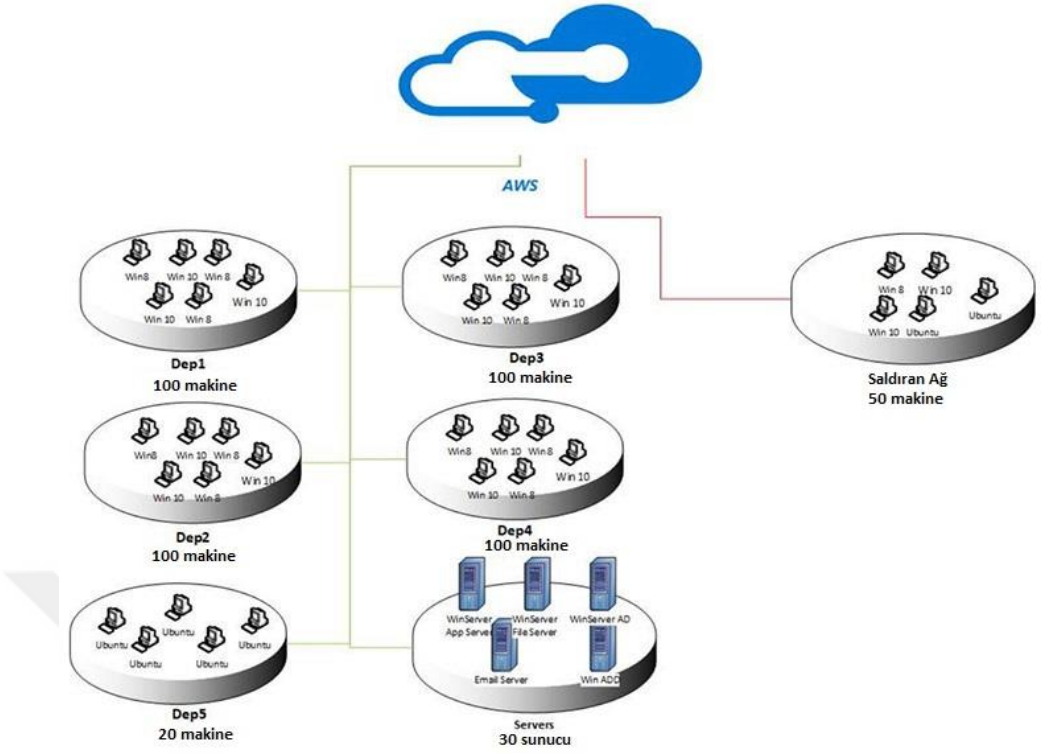
4.1. Veri Kümesi

Saldırı tespit sistemleri, bir ağa veya sisteme yönelik güvenlik ihlallerini tespit etme ve önleme bakımından kritik öneme sahip olmakla birlikte, güvenilirliğinin kanıtlanması için önemli ölçüde değerlendirmeye tabi tutulmalıdır. Özellikle ağ trafiğinden elde edilen gerçek verilerin normal veya saldırı olarak sınıflandırılması ve STS'nin başarı oranının net bir şekilde belirlenmesi gerekir. Bununla birlikte gerçek bir ağ trafiğinden verileri elde etmek, ancak ağın belirli bir süre gözlenmesi ile gerçekleştirilebilir -ki bu yöntem, maliyetlidir. Bu ihtiyacı karşılamak için çeşitli veri setleri oluşturulmuştur.

Saldırı tespiti için oluşturulmuş veri setleri, belirli saldırı örneklerini içerebileceği gibi birçok saldırı örneğini de kapsayabilir. Ancak güvenilir veri setlerinin mevcudiyeti maalesef nadirdir. Zira güvenilir birçok veri kümesi, gizlilik gerekçesiyle paylaşılmaz; öte taraftan diğer veri kümeleri güvenilirlik probleminin yanı sıra büyük ölçüde güncelliğini yitirmiştir. Ağ davranışları ve saldırı tipleri değiştikçe/geliştikçe, söz konusu veri kümelerinin güvenilirliği azalmaktadır.

Güncel ve güvenilir veri kümesi ihtiyacına binaen, İletişim Güvenliği Kurumu (CSE) ve Kanada Siber Güvenlik Enstitüsü (CIC) tarafından IDS2018 veri kümesi geliştirilmiştir. IDS2018 veri kümesi, hizmet reddi ve ağ tabanlı saldırılar da dahil olmak üzere 7 farklı saldırı senaryosu içerir. Veri kümesini oluşturmak için saldıran altyapı 50 makine, hedef altyapı ise 420 makine ve 30 sunucudan oluşan 5 departman içerir. Veri kümesi, CICFlowMeter-V3 uygulaması kullanılarak yakalanan trafikten çıkarılan 80 özelliğin yanı sıra her makinenin ağ trafiğini ve sistem günlüklerini içerir [186].

IDS 2018 için birbirine bağlı Windows ve Linux tabanlı iş istasyonlarından oluşan test ortamı tercih edilmiştir. Windows makineleri için farklı hizmet paketleri kullanılmıştır, zira her paketin bilinen farklı güvenlik açıkları vardır. Linux makineleri için yeni penetrasyon test cihazları tarafından saldırıya uğramak üzere geliştirilmiş Metasploit uyumlu dağıtım kullanılmıştır. Şekil 4.1'de IDS2018 veri kümesini oluşturmak için kullanılan ağ topolojisi gösterilmektedir [187].



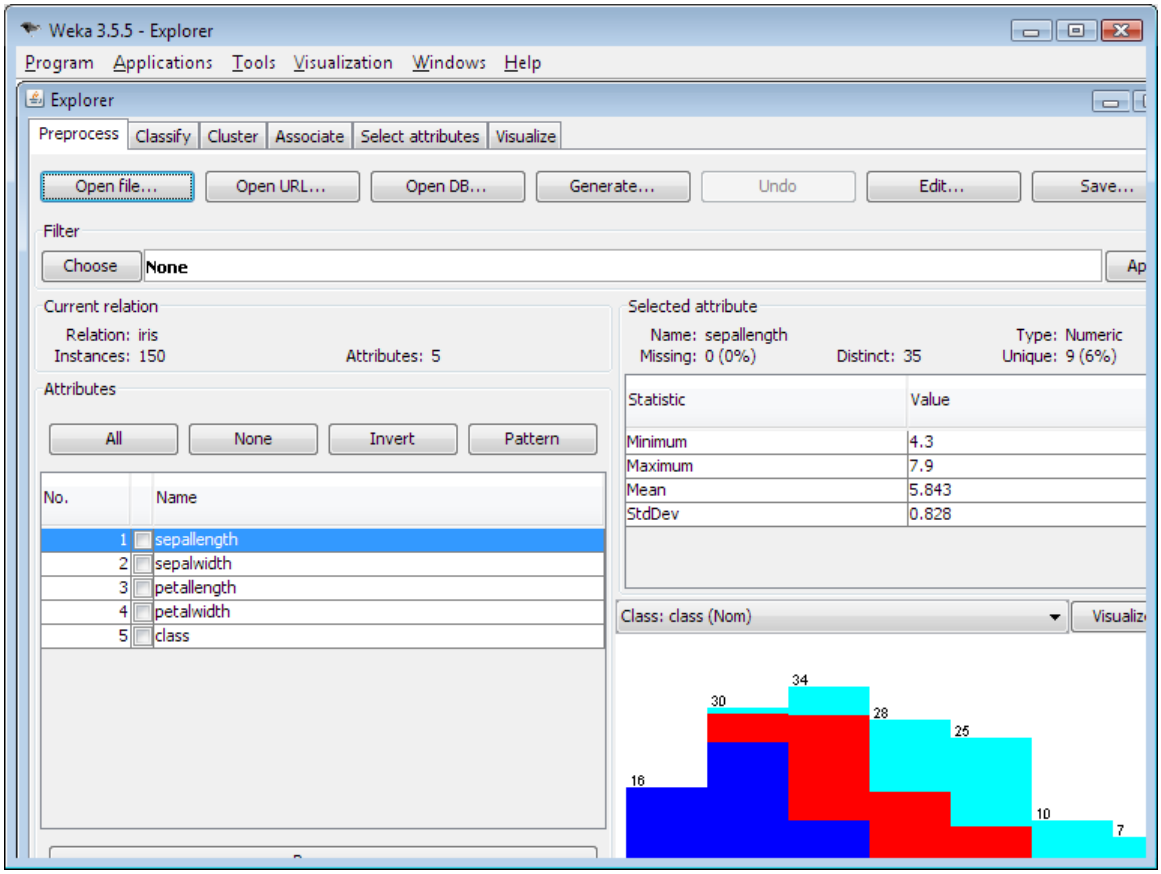
Şekil 4.1. IDS2018 ağ topolojisi

Saldırı senaryoları, Şekil 4.1'deki ağ topolojisine, ağ dışındaki makineler kullanılarak uygulanmıştır. Gerçek dünya ağlarına benzer makine çeşitliliğine sahip olmak için; ar-ge departmanı (Dep1), yönetim departmanı (Dep2), teknisyen departmanı (Dep3), sekreter ve operasyon departmanı (Dep4), BT departmanı (Dep5) olmak üzere 5 alt ağ ve sunucu odaları kurulmuştur. BT departmanı dışındaki tüm departmanlar için farklı MS Windows işletim sistemleri (Windows 8.1 ve Windows 10), BT departmanındaki tüm bilgisayarlar için Ubuntu kullanılmıştır. Sunucu odası için MS Windows 2012 ve 2016 gibi farklı sunucular kullanılmıştır. Toplamda 10 gün boyunca yapılan çalışma neticesinde yaklaşık 16 milyon örnekten oluşan IDS2018 veri kümesi elde edilmiştir. Bu yönüyle IDS2018, genel kullanıma açık ve çok çeşitli saldırı türlerini kapsayan en geniş ve güncel veri kümesidir. Bu tez çalışmasında modellenen hibrit saldırı tespit sistemini eğitmek için IDS2018 kullanılmıştır.

4.2. Veri Madenciliği Aracı: WEKA

WEKA (Waikato Environment for Knowledge Analysis), veri madenciliği için makine öğrenme algoritmalarını bünyesinde barındıran kapsamlı bir araçtır. Günümüzde yaygın olarak kullanılan birçok makine öğrenme algoritmasını ve metotlarını kapsamaktadır. WEKA; veri hazırlama, sınıflandırma, regresyon, kümeleme, birliktelik kuralları madenciliği ve görselleştirme

için araçlar içerir [188]. WEKA, Java dili ile programlanmış, açık kaynak kodlu ve ücretsiz bir araçtır. Şekil 4.2'de WEKA uygulamasının ekran görüntüsü bulunmaktadır.



Şekil 4.2. WEKA uygulamasının ekran görüntüsü

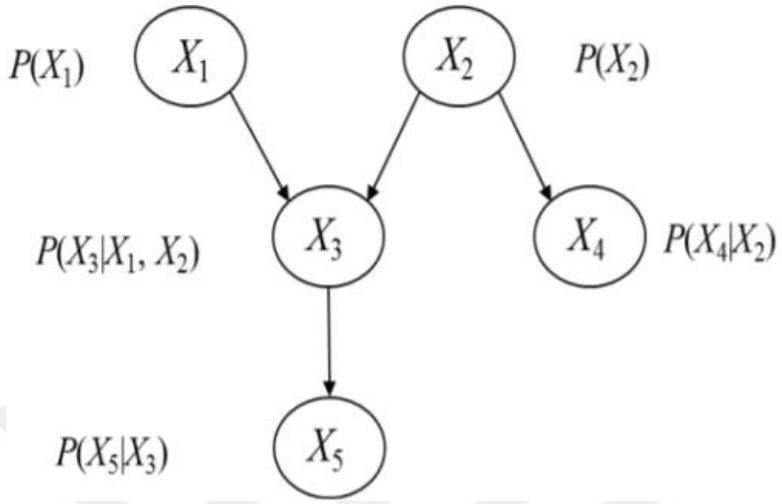
4.3. Makine Öğrenme Algoritmaları

Bu tez çalışmasında modellenen hibrit saldırı tespit sisteminin imza tabanlı algılama metodu, çeşitli makine öğrenme algoritmalarını kullanmaktadır. Bu algoritmalar ile ağ trafiğindeki anormal paketler tespit edilmekte ve saldırı olarak sınıflandırılmaktadır. Bu çalışmada BayesNet, Random Forest, J48, JRip ve PART algoritmaları kullanılmıştır.

4.3.1. BayesNet Algoritması

Bayes ağı, değişkenler arasındaki ilişkileri grafiksel olarak açıklamak için kullanılan modelleme yöntemlerinden birisidir. Bayes ağları, değişkenler arasındaki ilişkileri ifade etmek için olasılık teorisi ve çizge teorisi kavramının birleştirilmesiyle ortaya çıkmıştır [189]. Bayes ağında düğümler, rastgele değişkenlerle; düğümler arası ilişkiler ise yönlü oklar aracılığıyla gösterilir. Okun başlangıcı, ebeveyn düğümü; bitişi ise çocuk düğümü gösterir [190]. Bayes ağları,

bağımlılıklar ve koşullu olasılıklar nedeniyle döngüye veya kendi kendine bağlantıya izin vermez [191]. Şekil 4.3'te beş değişkenden oluşan örnek bir bayes ağı gösterilmiştir [190].



Şekil 4.3. Bayes ağı örneği

Şekil 4.3'te X_1, X_2, X_3, X_4 ve X_5 değişkenleri, bu değişkenlerin birbirleriyle hiyerarşik ilişkileri ve değişkenlerin koşullu olasılık dağılımları gösterilmiştir. Aralarında yönlü ok bulunmayan değişkenlerin, birbirleriyle hiyerarşik veya olasılıksal bir ilişkisi yoktur.

Bayes ağları, matematiksel olarak Bayes teoremine dayanır. Bayes teoremi, stokastik süreç [192] esnasında ortaya çıkan iki rastgele olay arasındaki koşullu ve önsel olasılıklar arasındaki ilişkiyi tanımlar [193]. Bayes teoremi Denklem 4.1 ile formülize edilebilir:

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} \tag{4.1}$$

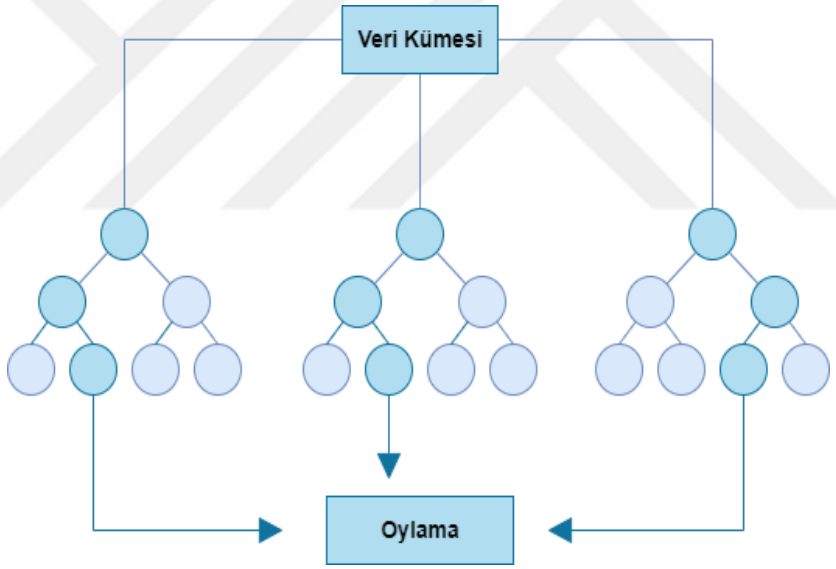
$P(A|B)$, B için A'nın koşullu olasılığını; $P(B|A)$ ise A için B'nin koşullu olasılığını tanımlar. $P(A)$, A olayı için önsel olasılıktır; zira B olayı için önceden bilgi içermemektedir. $P(B)$ ise B için önsel olasılıktır.

Bayes ağları; küçük ve eksik veri kümelerine uygunluğu, yapısal öğrenmenin mümkün olması, farklı veri kaynaklarını birleştirebilmesi, belirsizlikleri giderme ve karar analizi için destek sunması ve hızlı yanıt vermesi gibi birçok avantaja sahiptir [194]. Ayrıca karmaşık olasılık problemlerini verimli bir şekilde hesaplar ve diğer öğrenme yöntemlerine göre daha genişletilebilir bir yapıya sahiptir. Bu gibi avantajlarından dolayı özellikle karar destek sistemlerinde olmak üzere; deprem ve afetler için risk analizi, tıbbi teşhis, bilimsel kanıtların değerlendirilmesi, çevresel modelleme ve yönetim gibi birçok farklı alanda kullanılmaktadır [195-198]. Söz konusu avantajlarına karşın, sürekli değişkenlerin ayrıklaştırılması problemi, uzman bilgisinin toplanması

ve yapılandırılması zorluğu, yüksek boyutlu verilerdeki kötü performansı ve ağ tasarımının zorluğu gibi dezavantajları vardır [194, 199].

4.3.2. Random Forest Algoritması

Temelde, karar ağaçlarına dayanan ve tahmin modelleri oluşturabilmek için birden fazla karar ağacı kullanan, denetimli bir öğrenme algoritmasıdır [200]. Karar ağaçları, kullandıkları eğitim verilerini analiz ederek, test verilerinin hangi sınıfa ait olduğunu belirler [201]. Random Forest algoritmasını, karar ağacı algoritmalarından ayıran en önemli fark, kök düğümü bulma ve bölme işlemlerinin rastgele yapılmasıdır [202]. Random Forest algoritmasında düğümleri dallara ayırmak için en iyi dalı kullanmak yerine, her düğümde rastgele seçilen değişkenlerden en iyisi kullanılır. Her bir düğümdeki bu rastgele özellik seçimi, ağaçlar arasındaki korelasyonu ve hata oranını azaltır. Kullanılan her veri seti, orijinal veri setinden üretilir ve oluşturulan ağaçlar budanmaz [203]. Random Forest algoritmasının çalışma mantığı Şekil 4.4'te gösterilmiştir.



Şekil 4.4. Random Forest algoritmasının çalışma mantığı

Random Forest algoritması, rastgele orman oluşturma ve tahminde bulunma adımlarından oluşur. Rastgele orman oluşturma adımları Tablo 4.1'de gösterilmiştir [204]:

Tablo 4.1. Rastgele ağaç oluşturma işleminin sözde kodu

1: Özellik kümesinde bulunan toplam M özellikten rastgele x özellik seç.
2: M'deki her x özelliği için;
3: a. Bilgi kazancını (information gain) hesapla.
4: (En iyi dallanmayı belirlemek için GINI indeksi de kullanılabilir.)
5: $\mathbf{Gain(t, x) = E(t) - E(t, x)}$ (4.2)
6: $\mathbf{E(t) = \sum_{i=1}^{c} - P_i log_2 p_i}$ (4.3)
7: $\mathbf{E(t, x) = \sum_{c \in X} P(c) E(c)}$ (4.4)
8: b. En yüksek bilgi kazancına sahip d düğümünü seç.
9: c. Düğümleri çocuk düğümlerine böl.
10: d. Bölünme için minimum örnek sayısına ulaşana kadar a, b ve c adımlarını tekrarla.
11: N ağaçtan oluşan bir orman oluşturmak için 1. ve 2. adımları N kez tekrarla.

$E(t)$ iki sınıfın entropisi, $E(t, x)$ ise x özelliğinin entropisidir. Entropi farkları, bilgi kazancını yani $Gain(t, x)$ değerini verir. Bir sonraki aşamada ise elde edilen tahminler için oylama yapılır. Algoritma, en yüksek oy alan tahmini seçer.

Random Forest algoritmasının çalışma prensibi; yüksek doğruluk, büyük verilerle verimli çalışma, düşük hata oranı ve hata dengeleme, eksik verileri tahmin etme, hız ve uyum konusunda çok iyi performans göstermesini sağlar [205]. Söz konusu avantajlarından dolayı; bankacılık, tıp, e-ticaret gibi birçok alanda kullanılmaktadır [202]. Random Forest algoritması, büyük veri kümelerini işleyebildiğinden, daha doğru tahminler sağlayabilir ancak her bir karar ağacı için veri hesapladığından yavaş çalışabilir. Ayrıca daha büyük veri kümelerini işlemesi, bu verileri depolamak için daha fazla kaynağa gereksinim duymasına neden olur. Bununla birlikte tek bir karar ağacının tahminini yorumlamak, bir ormana kıyasla daha kolaydır [206].

4.3.3. J48 Algoritması

J48 algoritması, C4.5 karar ağacı algoritmasının açık kaynaklı bir Java uygulamasıdır [207]. Verileri kategorik ve sürekli olarak incelemek için kullanılan önemli makine algoritmalarından biridir [208]. J48, karar ağaçlarını optimize etmek için Shannon tarafından geliştirilen bilgi kuramından yararlanır [209]. Bunun için de bilginin önemli bir ölçütü olan entropi değerlerini kullanır. Entropi, bir değişkenin belirsizlik ölçüsüdür; yüksek entropi, yüksek belirsizliği gösterir. J48 algoritması şu şekilde çalışır [210]:

1. Hedef değişken için entropi değerleri, Denklem 4.5'e göre hesaplanır.

$$E(D) = -\sum_{i=1}^{m} (p_i log_2 p_i) \quad (4.5)$$

2. Her tahmin edici değişken için bilgi değeri, Denklem 4.6'ya göre hesaplanır.

$$E_A(D) = -\sum_{j=1}^{v} \frac{|D_j|}{|D|} * Info(D_j) \quad (4.6)$$

3. Her değişken için bilgi kazanımı, Denklem 4.7'e göre hesaplanır.

$$Gain(A) = E(D) - E_A(D) \quad (4.7)$$

Denklemlerde bulunan A, tahmin edici değişkeni, D ise hedef değişkeni gösterir. m, hedef değişkenin alabileceği değerlerin adedini; v ise tahmin edici değişkenin alabileceği değerlerin adedini gösterir.

J48 algoritmasında, en yüksek bilgi kazanımına sahip değişken belirlenir ve dallanma bu değişkenden itibaren başlatılır. Bu sayede veriler, dalların altında dengeli dağıtılır. Sonraki adımlarda toplam entropi yerine, belirlenen tahmin edici değişkenin bilgi değeri kullanılır. Geride bırakılan tahmin edici değişkenlerden hangisinin belirlenen değişken ile bölümlenmesinin daha fazla bilgi kazancı sağlayacağı hesaplanır. Bu işlem tüm değişkenler ağaçta konumlandırılıncaya kadar devam eder [210].

J48 algoritmasının, başarılı sınıflandırma sonuçları üretmesine rağmen, sınıflandırmada faydası olmayan boş değerlere sahip düğümlerin ve önemsiz dalların ortaya çıkması ile bazı durumlarda ağaç yapısının fazla büyümesi gibi istenmeyen durumları da vardır [208].

4.3.4. JRip Algoritması

JRip (RIPPER) algoritması, REP (Reduced Error Pruning) ve IREP (Incremental Reduced Error Pruning) algoritmalarının optimize edilmiş versiyonudur.

REP algoritması, başlangıçta büyük bir kural kümesi oluşturur ve ardından kabul edilebilir bir doğruluk düzeyine ulaşılana kadar kural kümesini budar. Böl ve yönet prensibine göre çalışır. Eğitim verileri büyüme ve budama kümelerine bölünür. Budamanın amacı, eğitim verilerine aşırı genelleme yapan kuralların yönlerini ortadan kaldırmaktır. Genel olarak budama, özellikle veriler gürültülü olduğunda, görünmeyen verilerdeki hata oranlarını iyileştirir. Ancak büyük gürültülü veri kümelerinde hesaplama açısından maliyetli bir algoritmadır.

IREP algoritması, temel REP konseptini değiştirilmiş bir böl ve yönet stratejisi ve yeni bir budama tekniği ile kullanmaktadır. IREP'in en önemli değişikliği hem budama öncesi hem de budama sonrası entegrasyon adımlarıdır. IREP'te açgözlü yaklaşımla bir kural seti oluşturulur ve sonrasında budanır. Budama işlemi sonrasında eğitim setindeki ilgili örnekler silinir. REP'den farklı olarak, kötü bir bölümlemenin neden olduğu sorunları dengelemek için, kalan eğitim verileri, her kural öğrenildikten sonra yeniden bölümlenir. İşlem, hiçbir olumlu örnek kalmayana veya bulunan son kural kabul edilemez derecede yüksek bir hata oranına sahip olana kadar tekrarlanır. Bu çalışma mekanizması, ciddi performans artışına neden olur [211].

IREP algoritmasının yaptığı iyileştirmeler, özellikle büyük veri kümelerinde oldukça iyi performans gösteriyor gibi görünmektedir. Bununla birlikte, kurallar kümesi üzerinde global bir optimizasyon adımı gerçekleştirerek, kayda değer bir performans avantajının elde edilebileceği bulunmuştur. Bireysel kurallar gözden geçirilerek veya değiştirilerek kuralın doğruluğunu artırılmaktadır. Deneyler, kural kümelerinin hem boyutunun hem de performansının, tümevarım sonrası optimizasyon ile önemli ölçüde iyileştirildiğini göstermektedir. Öte yandan, sürecin kendisi oldukça karmaşıktır.

RIPPER algoritmasında sınıflar artan boyutta incelenir ve artımlı azaltılmış hata budama kullanılarak sınıf için başlangıç kuralları seti oluşturulur. Örneklerin ve kural setinin açıklama uzunluğuna bağlı olarak ekstra bir durma koşulu getirilir. (Minimum açıklama uzunluğu, bilgileri bir uçtan diğer uca aktarmak için gereken minimum sayıda biti temsil eder [215].) Yeni kural, kural kümesinin toplam açıklama uzunluğunu d bit (varsayılan olarak d, 64 bittir) kadar artırırsa veya öğrenilen kuralın hata oranı %50'den fazla olduğunda kural eklemeyi durdurur. Sınıf için bir kural seti ürettikten sonra, her kural yeniden ele alınır ve yine azaltılmış hata budama kullanılarak iki varyant üretilir. Ancak bu aşamada, sınıf için diğer kuralların kapsadığı örnekler, budama setinden çıkarılır ve kalan örneklerin başarı oranı, budama kriteri olarak kullanılır. İki değişkenden biri daha iyi bir açıklama uzunluğu verirse, kuralın yerini alır. Ardından, sınıfın yeni ortaya çıkarılan tüm örneklerini temizlemek için orijinal oluşturma aşaması yeniden etkinleştirilir. Bir sonraki sınıf için kural oluşturmaya devam etmeden önce, her kuralın, açıklama uzunluğunun azaltılmasına katkıda bulunduğundan emin olmak için son bir kontrol yapılır [212].

Algoritmanın adımları şu şekildedir [213]:

1. **Yapı Aşaması:** Kural kümesinin ve örneklerin açıklama uzunluğu, o ana kadar karşılaşılan en küçük açıklama uzunluğundan 64 bit daha büyük olana veya hiçbir olumlu örnek kalmayana ya da hata oranı %50'ye büyük veya eşit olana kadar büyüme ve budama aşamaları tekrarlanır.
   i. **Büyüme:** Kural mükemmel olana kadar (%100 doğru) kurala açgözlülükle öncüller (veya koşullar) eklenerek bir kural geliştirilir. Prosedür, her özelliğin olası her değerini dener ve en yüksek bilgi kazancına sahip koşulu seçer.
   ii. **Budama:** Bir kuralın özgüllüğünü artırmak artık entropiyi azaltmadığında, kural hemen budanır [214].
2. **Optimizasyon:** Durdurma kriterine ulaşana kadar büyüme ve budama adımları tekrarlanır, bu noktada tüm kurallar dizisi çeşitli buluşsal yöntemler kullanılarak optimize edilir [214].

Algoritmanın sözde kodu Tablo 4.2'de gösterildiği gibidir [212]:

Tablo 4.2. RIPPER algoritmasının sözde kodu

1: Örnek kümesi için E'yi başlat
2: Her C sınıfı için küçükten büyüğe yapıyı oluştur:
3: YAPI:
4: E'yi, Yetiştirme ve Budama kümelerine 2:1 oranında ayır.
5: (a) C ile ilgili daha fazla keşfedilmemiş örnek kalmayana kadar tekrarla veya
6: (b) kural kümesinin ve örneklerin açıklama uzunluğu, şu ana kadar bulunan en küçük açıklama
7: uzunluğundan 64 bit daha büyük veya
8: (c) hata oranı %50'yi aşıyor.
9: **BÜYÜME**: Her özelliğin olası her değerini test ederek ve en büyük bilgi kazancı (G) olan koşulu
10: seçerek, kural %100 doğru olana kadar, açgözlülükle koşullar ekleyerek bir kuralı büyüt.
11: **BUDAMA**: Koşulları sondan ilk sıraya kadar buda. Kuralın değeri (W) arttığı sürece devam et.
12: OPTİMİZASYON:
13: *OLUŞTURMA ÇEŞİTLERİ:*
14: C sınıfı için her R kuralında,
15: E'yi yeniden Yetiştirme ve Budama setlerine ayır.
16: C için diğer kuralların kapsadığı tüm örnekleri Budama kümesinden kaldır.
17: Yeni bölünmüş verilerden iki rakip kural oluşturmak ve budamak için BÜYÜME ve
18: BUDAMA aşamasına geç:
19: R1, sıfırdan yeniden oluşturulmuş yeni bir kuraldır.
20: R2, R'ye açgözlü bir şekilde öncüller eklenerek oluşturulur.
21: Azaltılmış veri üzerinde A metriğini (W yerine) kullanarak budama yap.
22: TEMSİLCİ SEÇİMİ:
23: R, R1 ve R2'den hangisi en küçük açıklama uzunluğuna sahipse R'yi değiştir.
24: TEMİZLEME:
25: C sınıfının ele alınmamış örnekleri varsa, bu örneklere dayalı daha fazla kural oluşturmak için
26: YAPI aşamasına dön.
27: Tüm kural kümesi için açıklama uzunluğunu hesapla. Açıklama uzunluğunu artıran herhangi bir
28: kuralı sil.
29: Devam et

Büyüme aşamasında kullanılan bilgi kazancı (G), kural değeri (W) ve A metriği sırasıyla Denklem 4.8, Denklem 4.9 ve Denklem 4.10'a göre hesaplanır:

$$G = p[\log(p|t) - \log(P|T)] \tag{4.8}$$

$$W = \frac{p+1}{t+2} \tag{4.9}$$

$$A = \frac{p + n'}{T} \tag{4.10}$$

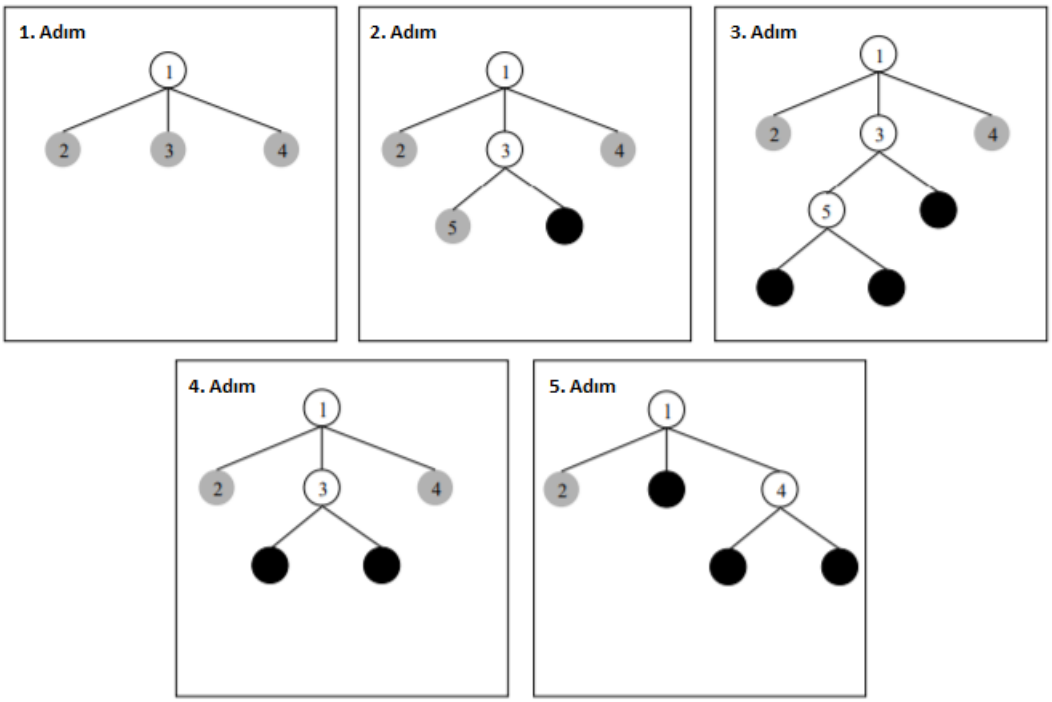
Denklemlerde bulunan p, kuralın kapsadığı pozitif örneklerin sayısını (gerçek pozitifler); n, kuralın kapsadığı olumsuz örneklerin sayısını (yanlış negatifler); t, kuralın kapsadığı toplam örnek sayısını $(p + n)$; n', kuralın kapsadığı olumsuz örneklerin sayısını (gerçek olumsuzlar, $N - n$); P, ilgili sınıfın olumlu örneklerinin sayısını; N, ilgili sınıfın olumsuz örneklerinin sayısını; T ise ilgili sınıfın toplam örnek sayısını $(P + N)$ gösterir [212].

4.3.5. PART Algoritması

PART algoritması, C4.5 ve RIPPER algoritmalarının optimize edilmiş bir versiyonu olup, kural üretmek için C4.5 ve RIPPER algoritmalarının aksine kural kümesi üzerinde global bir optimizasyon gerçekleştirmez. C4.5 algoritmasında, bir karar ağacından oluşturulan ilk kural kümesi, gereğinden fazla büyük ve gereksizdir. Kural kümesindeki hata oranını en aza indirmek için koşullar açgözlü yaklaşımla silinerek, basitleştirilir. RIPPER algoritmasında da kurallar, değiştirilerek veya revize ederek kuralların doğruluğu artırılır. Her iki durumda da Cohen'in belirttiği gibi "hem RIPPER hem de C4.5 kuralları, bir ilk modelle başlar ve onu buluşsal teknikler kullanarak yinelemeli olarak geliştirir" [216]. Her ne kadar tümevarım sonrası optimizasyon ile kural kümelerinin hem boyutunun hem de performansının önemli ölçüde iyileştirildiği göstermişmişse de sürecin kendisi, oldukça karmaşık ve sezgiseldir.

PART algoritması söz konusu problemi ortadan kaldırmak için global optimizasyondan kaçınır. PART algoritmasında ana fikir, bütün bir ağaç oluşturmak yerine, kısmi karar ağaçları oluşturmaktır. Zira tek bir kural elde etmek için tam bir karar ağacı oluşturmak, maliyetlidir. PART algoritmasında karar ağacı oluştururken, ayır ve yönet stratejisi kullanılır. Şekil 4.5. PART algoritmasının çalışma mantığını göstermektedir [208].

Algoritmanın 1. ve 3. adımlarında ağaç oluşturma işlemi özyinelemeli olarak devam eder. Her adımda genişleme için en düşük entropili düğüm seçilir. İlk iki adımda 3. düğüm seçilmiş, gri olan düğümler ise henüz genişlememiştir. Siyah olarak karakterize edilenler ise yaprak düğümlerdir. 2. ve 3. adımda siyah düğüm, kardeşi olan 5. düğümden daha düşük entropiye sahiptir ancak yaprak düğüm olduğundan daha fazla genişleyemez. Bu adımda geri dönülür ve genişleme için 5. düğüm seçilir. 3. adımda 5. düğümün tüm alt öğeleri yapraklara dönüştüğünden, budama başlar. 5. düğüm için alt ağaç değişimi öngörülür ve kabul edilir. 4. adımda ise 3. düğüm için alt ağaç değişimi öngörülür ve kabul edilir.



Şekil 4.5. PART algoritmasının çalışma mantığı

Daha fazla genişleme olmayacağı için geri dönülür ve entropi değeri daha düşük olan 4. düğüm seçilir. 4. düğüm iki yaprağa genişletilir ve alt ağaç değişimi öngörülür ancak düğüm değiştirilmediği varsayılmıştır. Son adımda 3 yapraklı kısmi ağaç oluşturularak, işlem tamamlanmış olur. Kısmi ağaç mantığında, bir düğüm ancak tüm ardılları yapraksa budanabilir böylece aşırı budama etkisi ortadan kaldırılmış ve performans kazancı sağlanmış olur [217].

4.4. Algılayıcı Ağ Modeli

Algılayıcı ağların güvenliğini etkili ve verimli bir şekilde sağlamayı zorlaştıran birçok etken vardır. Düğümlerin fiziki olarak küçük, geniş ölçeğe kurulabilecek kadar fazla ve maliyeti de minimum düzeyde olması gerektiğinden hesaplama karmaşıklığı gerektiren işlemlerin yapılması zor, bazı durumlarda imkânsızdır. Donanımsal kısıtlarının yanı sıra, arızaya karşı hassastırlar. Bununla birlikte algılayıcı ağın mimari farklılıkları da saldırı tespitini zorlaştıran unsurlardandır. Söz konusu zorluklara rağmen etkili ve verimli bir STS modelinin, ağa uygulanabilmesi için şu faktörler göz önünde bulundurulmalıdır [218]:

- **Ağ mimarisi:** Algılayıcı ağın sürdürülebilirliği için en önemli parametre, kaynakların verimli kullanılmasıdır. Özellikle zorlu ve savunmasız mekanlara konuşlandırılan algılayıcı ağların güç kaynaklarını değiştirmek zor olduğundan, enerji verimli bir mimariye sahip olması gerekir. Kümelenmiş ağ mimarisinin; ölçeklenebilirlik, veri toplama/birleştirme, yük ve enerji tasarrufu, sağlamlık, çakışma ve gecikme azaltma ve

hata toleransı gibi önemli avantajları vardır. Bu tez çalışmasında modellenen STS'nin optimal düzeyde uygulanabilmesi için, ağın kümelenmiş mimariye sahip olduğu varsayılmıştır.

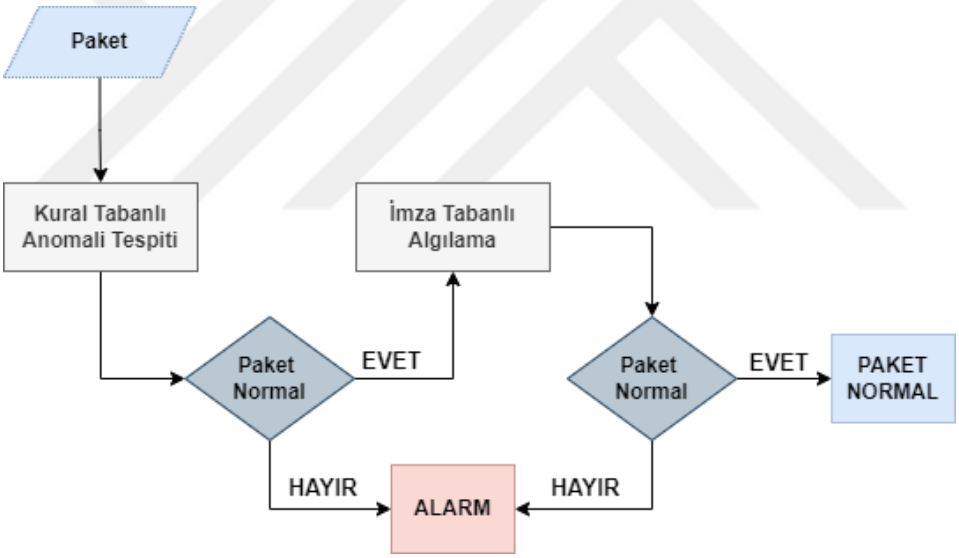
- **Ağ topolojisi:** Algılayıcı düğümlerin uygun konumlara yerleştirilmesi, ağın işlevselliği açısından önemlidir. Zira düğümlerin konumu, uygun bağlantı ve yeterli artıklık için belirleyicidir. Ağ topolojisi artıklık ölçümlerini destekliyorsa, diğer algılayıcı düğümler tarafından rapor edilen ölçümleri doğrulamak için her bir düğüme fırsat sağlaması beklenir. Örgü (mesh) topolojisinin, düğüm hatalarına karşı daha dayanıklı olduğu bulunmuştur. Ağda sık bağlantı kesilmelerine yol açan ağaç (tree) topolojisi tipi ağlarda, düğüm hataları daha yaygındır. Bu nedenle düğüm hatalarına karşı dayanıklı ve sağlam topolojiler kullanılması, STS'nin kapsamlı faaliyeti için zaruridir.
- **Konuşlandırma:** Algılayıcı ağların, zorlu ve savunmasız mekanlara konuşlandırılmaları, onları fiziki saldırılara açık hale getirir. Saldırı tespit sistemleri, bir düğümün fiziksel müdahale neticesinde kriptografik anahtarlarını kaybetmesine, devresinin veya program kodlarının değiştirilmesine engel olamaz. Ayrıca ele geçirilen düğümün, kötü niyetli bir düğüm ile değiştirilmesi, STS'nin işini zorlaştırabilir. Dolayısıyla kurcalamaya karşı gerekli önlemler alınmalıdır (Bkz. Bölüm 3).
- **Erişilebilirlik:** Algılayıcı ağa yönelik saldırıların bir kısmı, kötü niyetli düğümlerin hedef ağa yeterince yakın olmasından kaynaklıdır. Fiziki yakınlık ve erişilebilirlik, saldırganın ağı sıkıştırmasına, paketleri çakıştırmasına ve kaynaklarını tüketmesine neden olabilir. Bu nedenle ilgili riskleri belirlemek ve karşı önlemleri almak, ağın sürdürülebilir olması için elzemdir.
- **Yönlendirme algoritmaları:** Yönlendirme algoritmaları, kötü amaçlı etkinliği tespit etmek için ağ trafiği analizini kullanır. Bununla birlikte yaygın olarak kullanılan yönlendirme algoritmalarında bile birtakım güvenlik açıkları söz konusudur. Özellikle veri bağı katmanına yönelik tehdit oluşturan söz konusu saldırı tipleri (örneğin geri çekilme saldırısı), yönlendirme protokollerindeki bazı özellikleri manipüle eder. Bu nedenle yönlendirme algoritmalarının seçimi ve ilgili zafiyetlerin giderilmesi için gerekli önlemler alınmalıdır (Bkz. Bölüm 3).

Kablosuz algılayıcı ağların farklı altyapı ve mimarileri, donanımsal kısıtları, iletim ortamı, konuşlandırıldıkları zorlu ve savunmasız ortamlar gibi unsurlar göz önünde bulundurularak ağa ek veri ve enerji yükü getirecek uygulamalar hususunda optimal tercihler yapılmalıdır. Zira gerekli olmayan ağ trafiği ve işlemlerin, STS'nin ağa yüklediği hesaplama maliyeti ile birlikte ağın performansını ve sürdürülebilirliğini olumsuz etkilemesi kaçınılmazdır.

4.5. Saldırı Tespit Sistemi Modeli

Saldırı tespit sistemleri, algılayıcı ağın katmanlarına yönelik güvenlik ihlallerini tespit etmek ve gerekli önlemleri almak için kritik öneme sahiptir. Bununla birlikte saldırı tespiti için önerilen anomali, imza ve kural tabanlı algılama yöntemleri, günümüz şartlarında, tek başlarına yeterli güvenliği sağlamaktan uzaktırlar. Bu nedenle, bu tez çalışmasında, algılama metotlarının birlikte kullanıldığı hibrit bir saldırı tespit sistemi modellenmiştir.

Modellenen sistemin ilk savunması, kural tabanlı anomali tespit metodunu kullanır. Bu modelde ağ trafiği izlenerek, paketler normal veya kötü niyetli olarak sınıflandırılır. Ağın normali önceden tanımlanan kurallar ile belirlenir ve ağın normal davranışından sapan herhangi bir trafik, kötü niyetli olarak etiketlenir. Sistemin bir sonraki savunma hattını ise imza tabanlı algılama metodu oluşturur. Bu metotta, önceden bilinen güvenlik ihlallerinin imzaları, gelecekteki ihlallerin tespiti için referans olarak kullanılır. Bu adımda IDS2018 veri kümesindeki saldırı imzaları, referans olarak kullanılmıştır. Şekil 4.6, modellenen STS'nin çalışma mantığını açıklamaktadır.



Şekil 4.6. STS mekanizması

Modellenen saldırı tespit sistemi için dağıtık mimari kullanılmıştır. Bu mimaride algılayıcı ve küme başı düğümler ile baz istasyonu bulunmaktadır. Küme başı düğümlerin, diğer düğümlerden daha fazla yeteneğe sahip olduğu varsayılır.

Kullanılan mekanizmada yerel ve global STS ajanları ile saldırı tespiti yapılır. Algılayıcı düğümlere kurulan yerel STS ajanları, düğümlerin trafiğini izlemekten ve kural tabanlı anomali tespit metodu ile güvenlik ihlallerini tespit etmekten sorumludur. Küme başı düğümlere kurulan global STS ajanları ise hem yerel olaylara karar vermekten hem de radyo aralığında bulunan komşu düğümleri izlemekten sorumludur. Global STS ajanları, saldırı tespiti için, kural tabanlı anomali tespitine ilaveten, imza tabanlı algılama metodunu da kullanmaktadır.

4.5.1. Kural Tabanlı Anomali Tespiti

Kural tabanlı anomali tespiti, algılayıcı ağa yönelik savunma hattının ilk basamağını oluşturur. Bu metot ile ağın normal davranışı önceden tanımlı kurallar ile belirlenmiş olup, ağın normalinden sapan trafik, kötü niyetli olarak tespit edilir. Ağın normal trafiğini belirlemek için tanımlanan kurallar, Tablo 4.3'te gösterilmiştir [219].

Tablo 4.3. Anomali tespiti için tanımlanan kurallar

Kural Adı	Açıklama
Aralık	İki ardışık mesaj arasında alt ve üst süre limitini tanımlar. İki mesaj arasında geçen süre, izin verilen alt veya üst sınırları geçmemelidir. Bu kural ile hizmet reddi saldırıları, hello taşkını ve kaynakların tükenmesine yönelik saldırılar tespit edilebilir.
Bütünlük	Bir mesajın, kaynaktan hedef düğüme ulaşıncaya kadar orijinalliğini koruduğunu yani müdahale edilmediğini gösterir. Bu kural ile içerik değiştirme saldırıları tespit edilebilir.
Yeniden İletim	Düğüm, komşusuna gönderilen mesajı dinleyerek, söz konusu mesajın iletilip iletilmediği denetler. Bu kural ile yeniden iletilmesi gereken mesajların bazılarını veya tamamını iletmeyi reddeden seçici yönlendirme, düden ve kara delik saldırılarının tespiti yapılır.
Tekrarlama	Bir mesaj, aynı komşu düğüm tarafından yalnızca sınırlı sayıda yeniden iletilebilir. Komşu düğümün aynı mesajı yeniden iletim sayısının, belirlenen sınırı aşmaması gerekir. Bu kural ile hizmet reddi saldırıları tespit edilebilir.
Gecikme	Bir mesajın, komşu düğüm tarafından yeniden iletimi, tanımlanmış bir zaman aşımından önce gerçekleşmesi gerekir. Belirlenen zaman aşımından önce komşu düğümün mesajı yeniden iletip iletmediğini denetler. Bu kural ile hizmet reddi saldırıları tespit edilebilir.
Radyo İletim Aralığı	Bir düğüme gelen tüm mesajlar, komşularından birinden gelmelidir. Bu kural ile mesajların geldiği kaynağın bir önceki atlama düğümü olup olmadığı tespit edilir. Saldırganın daha güçlü radyo yayını yaparak uzaktaki bir düğüme mesaj gönderdiği solucan deliği, hello taşkını ve sybil saldırıları tespit edilebilir.
Sıkışma	İletim kanalındaki mesajların çakışma sayısı, belirlenen eşik değerden düşük olmalıdır. Bu kural ile sıkışma saldırıları tespit edilebilir.

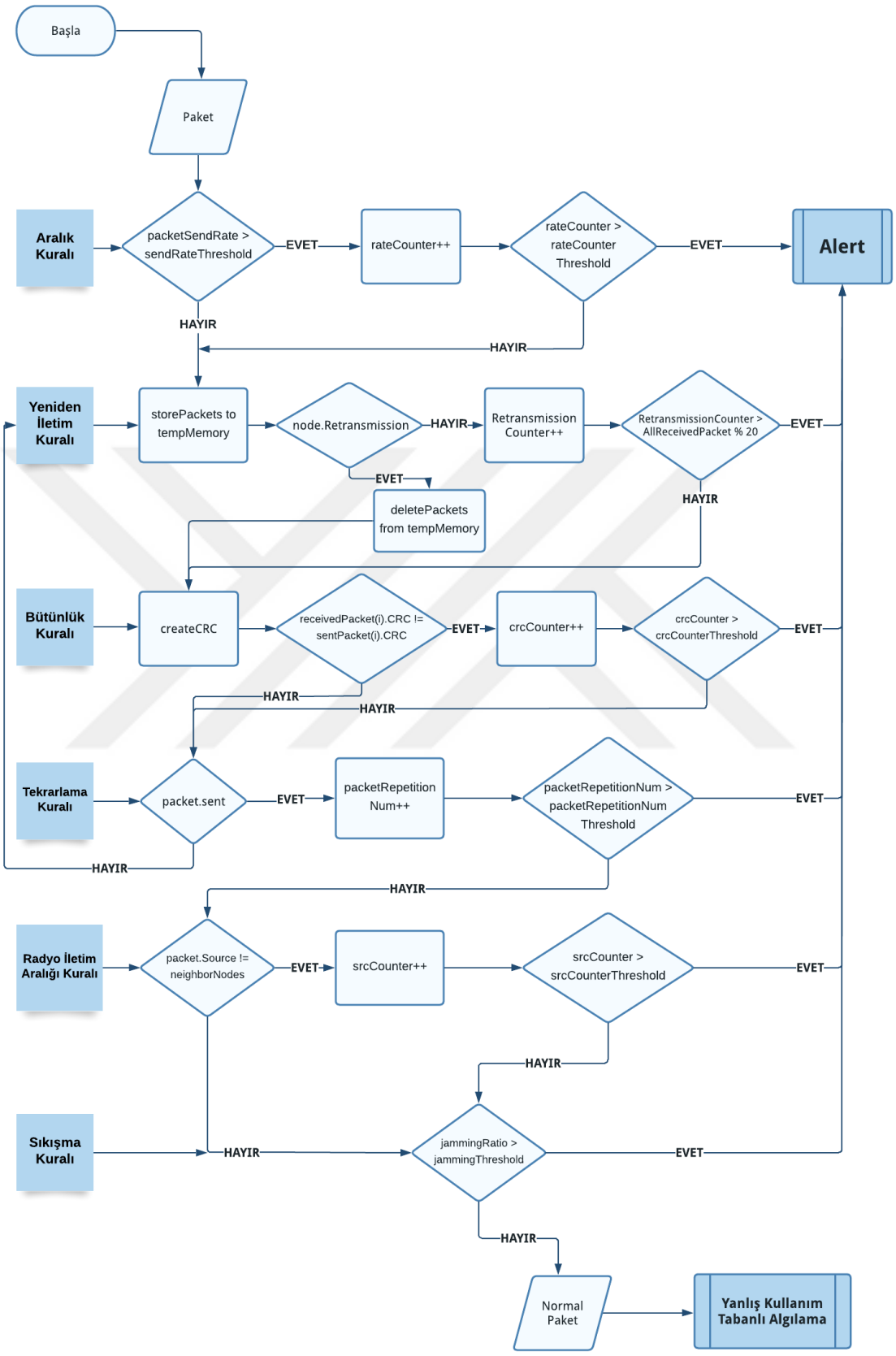
Anomali tespiti için tanımlanan kurallar ile ağ trafiğindeki normal paketler dolaşıma devam ederken, kural ihlali yapan paketler filtrelenir. Kural ihlalinin tespiti, paketin tanımlanan kurallardan herhangi birinden sapmasıyla yapılır. Herhangi bir kural ihlali, kural ile ilgili hata sayacının artmasına neden olur. Hata sayacı belirli bir eşiğin üzerine çıkarsa, alarm oluşturulur. Kural tabanlı anomali tespit modelinin sözde kodu Tablo 4.4'te verilmiştir.

Tablo 4.4. Kural tabanlı anomali tespit modelinin sözde kodu

```
1: for all neighbors do
2:     if packetSendRate > sendRateThreshold then
3:         rateCounter = rateCounter + 1
4:         if rateCounter > rateCounterThreshold then
5:             Alert
6:     do storePackets to tempMemory
7:     if node.Retransmission = false then
8:         RetransmissionCounter = RetransmissionCounter + 1
9:             if RetransmissionCounter > AllReceivedPackets % 20 then
10:                 Alert
11:    else
12:        deletePackets from tempMemory
13:    createCRC foreach packet
14:        if receivedPacket(i).CRC != sentPacket(i).CRC then
15:            crcCounter = crcCounter + 1
16:            if crcCounter > crcCounterThreshold then
17:                Alert
18:    if packet.sent = true then
19:        packetRepetitionNum = packetRepetitionNum + 1
20:        if packetRepetitionNum > packetRepetitionNumThreshold then
21:            Alert
22:    if packet.Source != neighborNodes then
23:        srcCounter = srcCounter + 1
24:        if srcCounter > srcCounterThreshold then
25:            Alert
26:    if jammingRatio > jammingThreshold then
27:        Alert
```

Kural tabanlı anomali tespiti; ağın özellikle sürdürülebilirliğine yönelik hizmet reddi saldırıları, ağ trafiğinin bir kısmını veya tamamını düşüren düden, karadelik veya seçici yönlendirme saldırıları ve paketlerin bütünlüğüne yönelik saldırılara karşı iyi bir güvenlik sağlar. Ayrıca yeni ve bilinmeyen saldırılara karşı da etkili bir güvenlik sağlanır. Kural tabanlı anomali tespitine ait akış şeması Şekil 4.7'de gösterilmiştir.

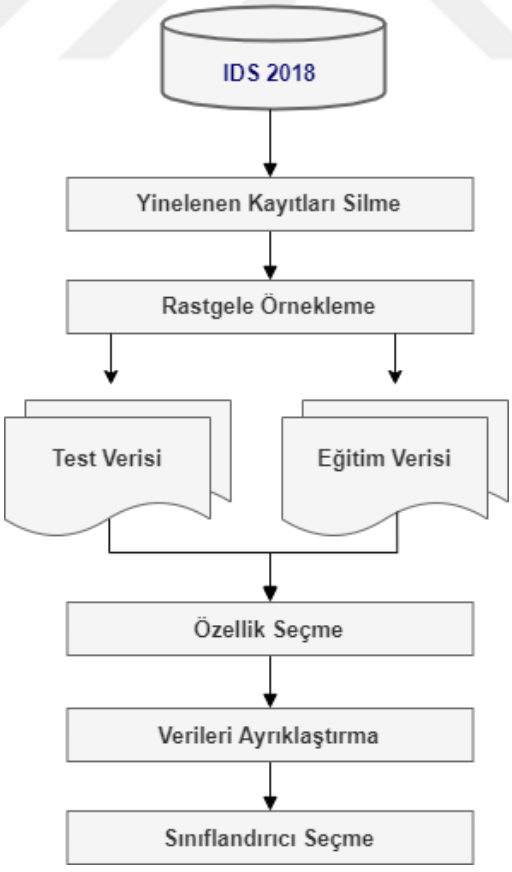
Kural tabanlı anomali tespiti; kötü niyetli trafiğin, normal trafiğe yakın olduğu durumlarda, yanlış sonuç üretme ihtimali söz konusudur. Bu nedenle sistemin ikinci savunma hattında imza tabanlı algılama metodu kullanılmıştır.



Şekil 4.7. Kural tabanlı anomali tespitinin akış şeması

4.5.2. İmza Tabanlı Algılama Metodu

Sistemin ikinci savunma hattında bulunan imza tabanlı algılama metodu, önceden bilinen saldırıların imzalarını/kalıplarını kullanarak, muhtemel saldırıların tespit edilmesi esasına dayanır. Model eşleştirme baz alındığı için bilinen saldırıların tespitinde etkili ve verimli sonuçlar elde edilebilmektedir. Saldırı tespiti için gerçek ağ trafiğinden elde edilmiş en güncel veri kümesi olan IDS2018'de bulunan kayıtlar referans alınmıştır. IDS2018 veri kümesinde DoS, DDoS ve Botnet gibi hizmet reddi saldırılarının yanı sıra ağa içeriden sızma saldırılarının da dahil olduğu 7 farklı saldırı senaryosuna ait yaklaşık 16 milyon kayıt bulunmaktadır. Bu miktarda kaydın, algılayıcı ağın eğitimi için kullanılması neredeyse imkânsızdır. Zira algılayıcı ağların donanımsal kısıtları ve limitli enerji kaynakları, hesaplama karmaşıklığı getiren kompleks işlemleri yapmaya engeldir. Bununla birlikte modellenen saldırı tespit sisteminde hem kural tabanlı anomali tespiti hem de imza tabanlı algılama metodu hibrit olarak kullanıldığından, veri kümesinin optimize edilmesi gerekir. Bunun için de veri kümesi ön işleme tabi tutulmuştur. Ön işleme adımları; veri kümesinde bulunan yinelenen verilerin kaldırılması, kayıtların rastgele örneklenmesi, saldırı profiline etkisi olmayan niteliklerin silinmesi, verilerin ayrıklaştırılması ve uygun sınıflandırma algoritmalarının seçilmesini kapsamaktadır. Ön işleme adımları Şekil 4.8'de gösterilmiştir.



Şekil 4.8. Veri ön işleme adımları

- **Yinelenen kayıtların silinmesi:** IDS2018 veri kümesinde bulunan 16 milyon kaydın bir kısmı tekrarlı verilerden oluşmaktadır. Söz konusu yinelenen veriler, ön işleme adımları kapsamında silinmiştir.
- **Rastgele örnekleme:** Yinelenen kayıtların silinmesi durumunda bile veri kümesinde yüksek miktarda veri kaydı bulunmaktadır. KAA'ların kaynak kısıtları ise bu ölçekteki verileri işlemeye elverişli olmadığından, tüm kayıtlar arasından rastgele 20 bin kayıt seçilmiştir. Seçilen kayıtların yarısı normal ağ trafiğini, yarısı ise saldırı profilini tanımlamak için kullanılmıştır.

  Veri kümesinde bulunan kayıtların yaklaşık %83'ü normal trafik davranışı gösterirken, %17'si saldırı özelliği taşımaktadır. Ayrıca bazı saldırılara ait kayıt sayıları çok yüksek iken, bazılarının çok düşüktür. Bu nedenle rastgele örnekleme işleminde, normal ağ trafiği ile saldırı trafiği dengelenmekle beraber yüksek kayıt içeren saldırı tipleri indirgenmiş, düşük kayıt sayısına sahip saldırıların ise tüm kayıtları alınmıştır.
- **Özellik seçme:** Veri kümesi, her kayıt için, CICFlowMeter-V3 uygulaması ile yakalanan trafikten çıkarılan 80 özelliği barındırmaktadır. Ancak söz konusu özelliklerin bir kısmı gereksiz olup saldırı profiline etkisi çok az veya yoktur. Bu nedenle saldırı profili tanımlamak için en değerli özellikleri belirlemek üzere Gain Ratio algoritması uygulanmıştır.
- **Verileri ayrıklaştırma:** Veri ayrıklaştırma, sürekli verilerin nitelik değerlerini, sonlu bir aralık kümesine dönüştürme yöntemidir. Ayrıklaştırma, verideki gürültüyü azaltarak tahmin modelinin doğruluğunu artırabilir. Verilerin ayrıklaştırılması süreci, veri boyutunun azaltılması ve performansın artırılması için de faydalı bir yöntemdir. IDS2018 veri kümesinde, özellik seçiminin ardından gözetimli ayrıklaştırma metodu ile veriler ayrıklaştırılmıştır.
- **Sınıflandırıcı seçme:** Modellenen STS'de çeşitli parametrelere göre en iyi performansın elde edilebilmesi için beş farklı makine öğrenme algoritması kullanılmıştır. BayesNet, Random Forest, J48, JRip ve PART algoritmaları ön işlemden geçirilen veri kümesine uygulanmış ve en iyi performans değeri gösteren algoritma seçilmiştir.

Verileri ön işleme adımından geçirdikten sonra kullanılan sınıflandırıcıların performans değerlerini artırmak için optimizasyon işlemleri yapılmıştır. Söz konusu optimizasyon işlemi için meta öğrenme algoritmalarından CVParameterSelection kullanılmıştır. CVParameterSelection, sınıflandırıcılar için çapraz doğrulama ile parametre seçimi yaparak, performans değerlerini artırır [220].

5. BULGULAR VE TARTIŞMA

Modellenen saldırı tespit sistemi, kural tabanlı anomali tespitine ve imza tabanlı algılama metoduna dayanmaktadır. İmza tabanlı algılama metodunda referans alınan veri kümesinin %66'sı ağı eğitmek, geri kalanı ise test etmek amacıyla kullanılmıştır. Modelin performans analizi için karmaşıklık matrisi kullanılmıştır. Karmaşıklık matrisinde kullanılan parametreler Şekil 5.1'de gösterilmiştir:

		Tahmin edilen	
		Saldırı	Normal
Gerçek	Saldırı	DP (doğru-pozitif)	YN (yanlış-negatif)
	Normal	YP (yanlış-pozitif)	DN (doğru-negatif)

Şekil 5.1. Karmaşıklık matrisi

- **Doğru Pozitif (DP):** Gerçekte saldırı sınıfında olan ve saldırı olarak tahmin edilen kayıt sayısı.
- **Yanlış Pozitif (YP):** Gerçekte normal olan ancak saldırı sınıfında tahmin edilen kayıt sayısı.
- **Doğru Negatif (DN):** Gerçekte normal olan ve normal sınıfında tahmin edilen kayıt sayısı.
- **Yanlış Negatif (YN):** Gerçekte saldırı olan ancak normal sınıfında tahmin edilen kayıt sayısı.

Karmaşıklık matrisi parametreleri ile kullanılan algoritmaların doğruluğu, kesinliği, duyarlılığı, F-ölçütü, MCC, ROC ve PRC değerleri ile işlem süresi gibi performans kriterleri hesaplanmıştır.

- **Doğruluk:** Doğru sınıflandırılan kayıtların, toplam kayıtlara oranı olup, Denklem 5.1'de gösterilmiştir.

$$Doğruluk = \frac{DP + DN}{DP + YN + YP + DN} \tag{5.1}$$

- **Kesinlik:** Doğru sınıflandırılan kayıtların, pozitif olarak tahminde bulunulan kayıtlara oranı olup, Denklem 5.2'de gösterilmiştir.

$$Kesinlik = \frac{DP}{DP + YP} \tag{5.2}$$

- **Duyarlılık:** Doğru sınıflandırılan (pozitif) kayıtların, toplam kayıtlara oranı olup, Denklem 5.3'te gösterilmiştir.

$$Duyarlılık = \frac{DP}{DP + YN} \tag{5.3}$$

- **F-Ölçütü:** Duyarlılık ve kesinlik parametrelerinin harmonik ortalamasıyla elde edilir ve sınıflandırıcı için performans ölçütü olarak kabul edilir. Denklem 5.4'te gösterilmiştir.

$$F - \text{Ölçütü} = 2 * \left(\frac{kesinlik * duyarlılık}{kesinlik + duyarlılık}\right) \tag{5.4}$$

- **MCC (Matthews Correlation Coefficients):** Dengesiz dağılımlı veri kümelerinde en gerçekçi sonucun belirlenmesini sağlar. Elde edilen değerin 1'e yakın olması doğru sınıflandırmanın ölçüsü olarak kabul edilir. Denklem 5.5 ile formülize edilmiştir.

$$MCC = \frac{(DP * DN) - (YP * YN)}{\sqrt{(DP + YP) * (DP + YN) * (DN + YP) * (DN + YN)}} \tag{5.5}$$

- **ROC:** Sınıflandırıcının performansını göstermek için kullanılan bir eğridir. ROC eğrisi, duyarlılık ve özgüllük değerlerinin kesişimleriyle elde edilir. Özgüllük değeri, Denklem 5.6 ile hesaplanır. Elde edilen en iyi değer 1 ile, başarısız değer ise 0.5 ile gösterilir.

$$\text{Özgüllük} = \frac{DN}{DN + YP} \tag{5.6}$$

- **PRC (Precision-Recall Curve):** Kesinlik ile duyarlılık arasındaki ilişkinin incelendiği parametredir. PRC eğrisini elde edebilmek için X ekseninde duyarlılık değeri, Y ekseninde ise kesinlik değeri kullanılır. Duyarlılık ve kesinlik değerlerinin kesişiminden elde edilen noktalar ile PRC eğrisi elde edilir. Elde edilen değer 1'e yakınlığı nispetinde doğru tahmin yapıldığını gösterir [221].

Benzetim sonuçlarında karmaşıklık matrisinde kullanılan parametreler ve bu parametrelerden elde edilen performans kriterleri kullanılmıştır. Ağ trafiğindeki normal ve saldırı trafiğini sınıflandırmak için imza tabanlı algılama metodunda BayesNet, Random Forest, J48, JRip ve PART algoritmaları yürütülmüştür [222]. İlgili algoritmalar, veri kümesine ön işleme adımlarının çeşitli safhalarında uygulanmış ve her aşamanın performans analizi yapılmıştır.

Veri kümesine yönelik ön işleme adımlarının ilki, yinelenen kayıtların silinmesidir. Bu adımda, 433.261 yinelenen kayıt tespit edilmiştir. Yinelenen kayıtların veri kümesinden kaldırılmasından sonra geriye 15.799.751 kayıt kalmıştır. Ön işleme adımları uygulanmadan önce normal ağ trafiği %83.07, saldırı trafiği ise %16,93 değerindedir [223].

Yinelenen kayıtların veri kümesinden kaldırılmasından sonraki trafik istatistiği ise Tablo 5.1'de gösterildiği gibidir.

Tablo 5.1. Yinelenen kayıtlar kaldırıldıktan sonra ağ trafiğinin istatistiği

Kategori	**Sayı**	**Yüzde**
Normal	13445500	85,099%
FTP-BruteForce	39352	0,249%
SSH-Bruteforce	117322	0,743%
DoS attacks-Slowloris	10285	0,065%
DoS attacks-GoldenEye	41455	0,262%
DoS attacks-SlowHTTPTest	19462	0,123%
DoS attacks-Hulk	434873	2,752%
DDoS attacks-LOIC-http	576175	3,647%
DDOS attack-HOIC	668461	4,231%
DDOS attack-LOIC-UDP	1730	0,011%
Brute Force -Web	611	0,004%
Brute Force -XSS	230	0,001%
SQL Injection	87	0,001%
Infilteration	161897	1,025%
Bot	282310	1,787%

Veri kümesinde bulunan kayıt sayısının hala çok yüksek olması, normal ve saldırı trafiğinin dengesiz dağılımı nedeniyle veri kümesinde rastgele örnekleme yapılmıştır. Çok yüksek miktarda kayıt sayısına sahip saldırı tiplerine ait kayıtlar indirgenmiş, düşük sayıdaki kayıtların ise tamamı alınmıştır. Bu kapsamda; normal ağ trafiğine ait 10 bin kayıt, saldırı tiplerinin her birine ait 825 kayıt bırakılmıştır. Kayıt sayısı 825'in altında olan saldırı tiplerine ait tüm örnekler ise olduğu gibi alınmıştır. Sonuçta 10 bini saldırı, 10 bini normal olmak üzere toplam 20 bin kayıt alınmıştır. Yinelenen kayıtların silinmesi ve rastgele örnekleme yapılarak kayıt sayısının indirgenmesi sonrasında algoritmaların performans değerleri Tablo 5.2'de gösterildiği gibidir.

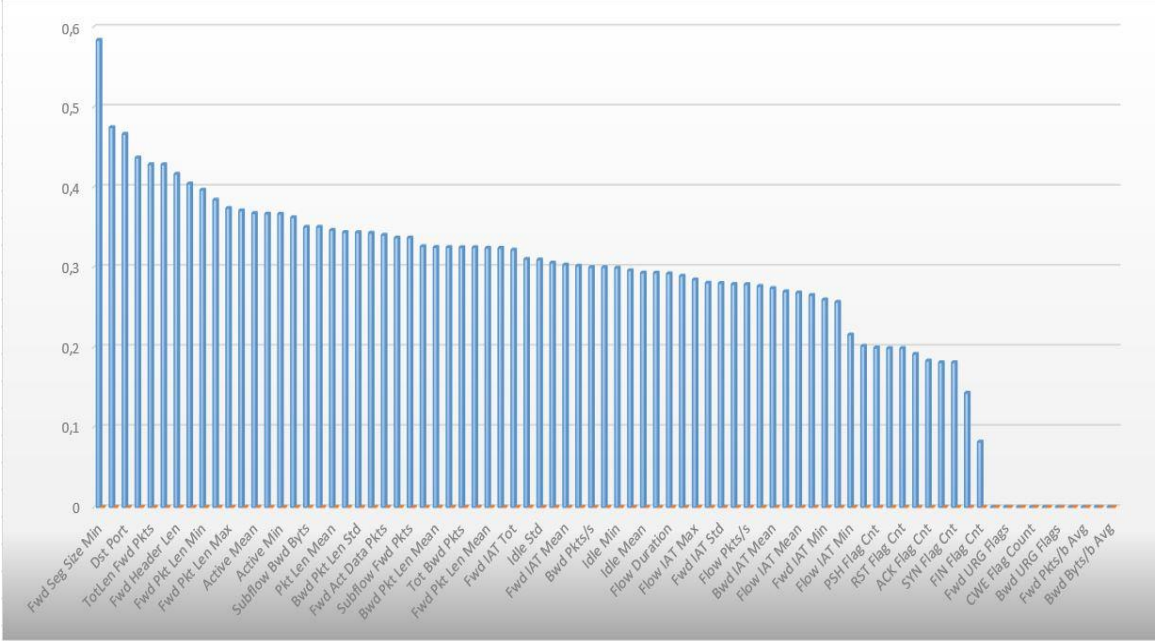
Tablo 5.2. Algoritmalara ait performans değerleri

Algoritma	**Doğruluk (%)**	**Kesinlik**	**Duyarlılık**	**F-Ölçütü**	**MCC**	**ROC**	**PRC**	**Eğitim Süresi**	**Test Süresi**
BayesNet	76.60	0,871	0,766	0,796	0,737	0,981	0,928	1.53	0.41
RandomForest	93.69	0,938	0,937	0,926	0,907	0,988	0,960	112.76	16.25
J48	91.57	?	0,916	?	?	0,973	0,892	3.17	0.1
JRip	93.95	0,934	0,940	0,931	0,913	0,971	0,907	397.82	0.52
PART	92.04	0,918	0,920	0,902	0,886	0,974	0,898	6.29	0.11

J48 algoritmasında, hizmet reddi saldırılarına ait DP ve YP değerleri sıfır olduğu için; kesinlik, F-Ölçütü ve MCC değerleri hesaplanamamıştır.

Model oluşturmak için geçen eğitim süresi performansının en iyi değeri BayesNet algoritmasında elde edilmiştir. Bununla birlikte BayesNet algoritmasının doğruluk oranı, diğer algoritmalara göre önemli ölçüde düşüktür. En yüksek doğruluk değerleri Random Forest ve JRip algoritmalarında olmasına rağmen, eğitim ve test süreleri KAA'ların kısıtları göz önünde bulundurulduğunda, kabul edilebilir düzeyde değildir. J48 ve PART algoritmalarının performans kriterleri birbirine yakın olmakla birlikte, eğitim ve test süresi bakımından J48 algoritması daha iyi sonuçlar üretmektedir.

Veri kümesinde bulunan her kayda ait 80 özelliğin bir kısmının, saldırı profili üzerindeki etkisi çok az veya sıfır olduğundan, Gain Ratio algoritması ile en önemli özellikler belirlenmiştir. Algoritmanın veri kümesinde uygulanması neticesinde, her bir özelliğin etki oranı Şekil 5.2'de gösterildiği gibidir.



Şekil 5.2. Veri kümesindeki özelliklerin etki oranı

Gain Ratio algoritması ile özelliklerin ortalama etki oranı 0,271299 olarak bulunmuştur. 80 özelliğin, 26'sı ortalama etki oranının altında olup, Şekil 5.2'de de görüleceği gibi bir kısım özelliğin etki oranı ise sıfırdır. Saldırı profili oluşturmak için etkisiz/gereksiz özellikler silindikten sonra geriye 39 özellik bırakılmıştır. Özellik seçimi sonrası performans analizi Tablo 5.3'te, özellik seçimi öncesi ve sonrası performans kıyası Tablo 5.4'te gösterildiği gibidir.

Tablo 5.3. Özellik seçimi sonrası algoritmaların performans analizi

Algoritma	Doğruluk (%)	Kesinlik	Duyarlılık	F-Ölçütü	MCC	ROC	PRC	Eğitim Süresi	Test Süresi
BayesNet	76.39	0,849	0,764	0,786	0,724	0,977	0,914	0.89	0.17
RandomForest	93.61	0,932	0,936	0,931	0,909	0,981	0,943	8.93	0.9
J48	93.70	0,933	0,937	0,929	0,912	0,977	0,921	1.26	0.06
JRip	93.83	0,932	0,938	0,930	0,912	0,973	0,913	13.35	0.06
PART	93.63	0,932	0,936	0,928	0,911	0,979	0,925	5.79	0.09

Tablo 5.4. Özellik seçimi işleminin performansa etkileri

Algoritma	Doğruluk Oranı (%)		Eğitim Süresi		Test Süresi	
	Önce	Sonra	Önce	Sonra	Önce	Sonra
BayesNet	76.60	76.39	1.53	0.89	0.41	0.17
RandomForest	93.69	93.61	112.76	8.93	16.25	0.9
J48	91.57	93.70	3.17	1.26	0.1	0.06
JRip	93.95	93.83	397.82	13.35	0.52	0.06
PART	92.04	93.63	6.29	5.79	0.11	0.09

BayesNet, RandomForest ve JRip algoritmalarının doğruluk yüzdelerinde ihmal edilebilir oranda düşüşler olmuşsa da eğitim ve test sürelerinde dramatik bir iyileşme söz konusudur. Bununla birlikte J48 ve PART algoritmalarının hem doğruluk yüzdelerinde hem de eğitim ve test sürelerinde ciddi iyileşmeler olduğu görülmektedir.

Veri kümesinde bulunan sürekli nitelikler, bazı sınıflandırıcılar tarafından işlenemez. Bazı veri madenciliği işlemlerinde sürekli nitelikler işlenebilse bile sürekli bir niteliğin ayrık değerlerle değiştirilmesiyle, performansı önemli ölçüde geliştirilebilir [224]. Bu nedenle ön işleme adımları, verileri ayrıklaştırma işlemi ile devam etmiştir. Bu kapsamda, sürekli nitelik değerleri, sonlu aralıklara dönüştürülmüş ve her bir aralıkla belirli bir veri değeri ilişkilendirilmiştir. Ayrıklaştırma işleminden sonra algoritmaların hem doğruluk oranlarında hem de işlem sürelerinde azımsanmayacak iyileşmeler görülmüştür.

Algoritmaların, veri ayrıklaştırma işleminden sonraki performans parametreleri Tablo 5.5'te gösterildiği gibidir. Veri ayrıklaştırma işleminden önceki ve sonraki performans değerleri ise Tablo 5.6'da gösterilmiştir.

Tablo 5.5. Veri ayrıklaştırma sonrası algoritmaların performans analizi

Algoritma	Doğruluk (%)	Kesinlik	Duyarlılık	F-Ölçütü	MCC	ROC	PRC	Eğitim Süresi	Test Süresi
BayesNet	77.5	0,856	0,775	0,796	0,737	0,979	0,918	0.17	0.16
RandomForest	93.88	0,932	0,939	0,932	0,913	0,983	0,941	5.36	0.73
J48	93.97	0,935	0,940	0,931	0,914	0,980	0,933	0.22	0.08
JRip	93.92	0,934	0,939	0,930	0,913	0,974	0,912	15.12	0.06
PART	93.73	0,931	0,937	0,930	0,911	0,983	0,939	1.18	0.11

Tablo 5.6. Veri ayrıklaştırma işleminin performansa etkileri

Algoritma	Doğruluk Oranı (%)		Eğitim Süresi		Test Süresi	
	Önce	Sonra	Önce	Sonra	Önce	Sonra
BayesNet	76.39	77.5	0.89	0.17	0.17	0.16
RandomForest	93.61	93.88	8.93	5.36	0.9	0.73
J48	93.70	93.97	1.26	0.22	0.06	0.08
JRip	93.83	93.92	13.35	15.12	0.06	0.06
PART	93.63	93.73	5.79	1.18	0.09	0.11

Veri ayrıklaştırma işlemi ile algoritmaların tamamında hem doğruluk hem de eğitim ve test süreleri bakımından önemli iyileşmeler tespit edilmiştir.

Sonuç olarak; BayesNet algoritması, model oluşturmak için en iyi eğitim süresine sahip algoritma olmasına rağmen, doğruluk ve diğer parametreleri kabul edilebilir seviyenin altındadır. Random Forest ve JRip algoritmalarının doğruluk oranı tatmin edici seviyede olsa da ağın eğitim süresi fazladır. J48 ve PART algoritmalarının performans kriterleri birbirine yakın olmakla birlikte J48 algoritması özellikle süre performansı bakımından daha iyi sonuçlar üretmektedir.

J48 algoritması optimal performansı sağlamakla birlikte daha iyi performans değerleri elde etmek için algoritma optimize edilmiştir. Bu kapsamda CVParameterSelection yöntemi kullanılmış ve J48 algoritması için bazı önemli parametreler manuel olarak ayarlanmıştır.

- **Güven faktörü:** Karar ağacı algoritmalarında budama sürecini etkileyen kritik bir parametredir. Güven faktörü, karar ağacı budanırken, verilerde izin verilen doğal hata eşiğini belirler. Eşik değeri düşürülerek, daha fazla budama sağlanabilir, sonuçta daha genel modeller üretilir. Veri kümesinde yapılan testlerde güven faktörü için optimal değerin 0.5 olduğu tespit edilmiştir.
- **Minimum örnek sayısı:** Yaprakların daha fazla sayıda örnek içerdiği daha basit modeller elde etmek için, tek bir yaprakta minimum sayıda nesne ayarlamak mümkündür. Bu

parametre, daha basit ve daha küçük karar ağaçları elde etmek için de kullanılabilir [225]. Minimum örnek sayısı 2 olarak belirlenmiştir.

Optimizasyon işleminden önce J48 algoritmasın doğruluk oranı %93,70 iken, optimizasyon sonrası %94,02 olmuştur. J48 algoritmasının optimizasyon öncesi ve sonrası değerleri Tablo 5.7 ve Tablo 5.8'de gösterilmiştir.

Tablo 5.7. Optimizasyon öncesi J48 algoritmasının performans değerleri

Algoritma	Doğruluk (%)	Kesinlik	Duyarlılık	F-Ölçütü	MCC	ROC	PRC	Eğitim Süresi	Test Süresi
J48	93.97	0,935	0,940	0,931	0,914	0,980	0,933	0.22	0.08

Tablo 5.8. Optimizasyon sonrası J48 algoritmasının performans değerleri

Algoritma	Doğruluk (%)	Kesinlik	Duyarlılık	F-Ölçütü	MCC	ROC	PRC	Eğitim Süresi	Test Süresi
J48	94.02	0,936	0,940	0,932	0,915	0,980	0,934	0.25	0.02

İmza tabanlı algılama metodunda, ön işleme tabi tutulan veri kümesi üzerinde gerek doğruluk oranı gerekse de eğitim ve test süreleri bakımından en başarılı sınıflandırma işlemi yapan algoritma J48 sınıflandırıcısıdır. Bununla birlikte J48 algoritmasının optimize edilmesiyle birlikte performans parametrelerinin daha iyi çıktılar ürettiği ve hibrit STS modelinde, ikinci savunma hattında kullanılabileceği görülmüştür.

6. SONUÇLAR

Kablosuz algılayıcı ağlar (KAA), giderek kullanımı yaygınlaşan ve veri gizliliğinin kritik önem taşıdığı alanlarda önemli görevler icra eden sistemlerdir. KAA'ların yaygın ve gizlilik gerektiren alanlardaki kullanımı nedeniyle etkili ve verimli güvenlik mekanizmalarının geliştirilmesi zaruridir. KAA'lara yönelik güvenlik hizmetlerinin nihai hedefi gerek ağ kaynaklarını gerekse de algılanan verileri güvenlik ihlallerine karşı korumaktır. Bununla birlikte etkili, enerji verimli ve güncel saldırı tespit sistemlerinin varlığı azdır. Literatürde var olan çalışmaların bir kısmında kullanılan algılama metotları, tek başına güvenliği sağlamada yetersizdir; bir kısmında ise güncelliğini yitirmiş veri kümeleri referans alınmıştır. Ancak gerçek ağ trafiğinden elde edilmemiş veya güncelliğini yitirmiş veri kümelerinin, modern saldırılar karşısında reel sonuçlar üretmeyeceği aşikârdır. Bu tez çalışmasında, KAA'ların güvenliğini sağlamak amacıyla saldırı tespit sistemi (STS) modellenmiştir. Modellenen STS'de algılama metotları birleştirilerek hibrit bir sistem ortaya konmuş, algılama metotlarından birinin tespit edemediği veya yanlış sonuçlar ürettiği durumlarda diğer metodun devreye girmesiyle daha etkili bir saldırı tespiti sağlanmıştır. Hibrit yapı, güvenliği sağlamada başarılı sonuçlar üretmektedir. Ancak KAA'ların donanımsal kısıtları da göz önünde bulundurulmuş, hesaplama karmaşıklığını ve kaynak kullanımını minimize etmek amacıyla referans alınan veri kümesi ön işleme tabi tutulmuştur. Literatürdeki mevcut çalışmaların büyük bir kısmının aksine, saldırı profilleri oluşturmak ve makine öğrenmesi için ağı eğitmek amacıyla güncel ve kapsamlı bir veri kümesi referans alınmıştır. Ağ trafiğini normal ve saldırı niteliği bakımından sınıflandırmak için farklı makine öğrenme algoritmaları kullanılmış ve çeşitli parametrelere göre algoritmaların performans değerleri karşılaştırılmıştır. Neticede J48 algoritmasının en iyi performansı verdiği tespit edilmiştir. J48 algoritmasının performans değerlerini iyileştirmek için algoritma optimize edilmiş ve bazı parametreleri manuel olarak ayarlanmıştır. Neticede daha yüksek bir doğruluk oranına ve test sürelerine ulaştığı gözlemlenmiştir. Benzetim sonuçları; modellenen hibrit STS'nin yüksek bir doğruluk oranına, düşük yanlış alarm oranına ve düşük çalışma süresine sahip olduğunu göstermektedir. Dolayısıyla geliştirilen STS modelinin, KAA'lar için enerji verimli ve etkili güvenliği sağlama kabiliyetinde olduğu düşünülmektedir.

Bu tez çalışmasında geliştirilen STS modelinin, konu ile ilgili araştırmacılara bakış açısı kazandırması ve modern çalışmalar yapılması konusunda yol gösterici olması beklenmektedir. Ayrıca ortaya konan model ile KAA güvenliğinin sağlanması, kritik öneme sahip verilerin gizliliğini ve bütünlüğünü garanti altına alacağından, güvenliğin yanı sıra enerji ve maliyet bakımından da önemli ekonomik avantajları beraberinde getirecektir. Bununla birlikte, bu çalışmanın; bilgisayar bilimi, mühendisliği ve veri güvenliği alanında akademik açıdan katkı sunduğuna inanılmaktadır.

ÖNERİLER

Tez çalışmasında modellenen hibrit saldırı tespit sistemi için kullanılan imza tabanlı algılama metodunda, saldırı profili oluşturmak için gerçek ağ trafiğinden elde edilmiş, güncel ve kapsamlı bir veri kümesi olan IDS2018 kullanılmıştır. IDS2018, saldırı tespit sistemi geliştirmek isteyen araştırmacılar tarafından genel amaçlı olarak kullanılmakta ve güvenilir sonuçlar üretmektedir. Bununla birlikte KAA'lara özgü tüm güvenlik ihlallerini barındıran bir veri kümesi oluşturmak daha isabetli sonuçlar üretebilir. Bu kapsamda, KAA'lar için kullanılan benzetim araçları (Network Simulator (NS-2), OMNET++ gibi) vasıtasıyla örnek bir ağ topolojisi oluşturulabilir. Söz konusu ortamdan, meşru düğümler ile güvenliği ihlal edilmiş ve çeşitli saldırılar gerçekleştiren düğümlere ait gerçek bir algılayıcı ağ trafiği elde edilebilir. İmza tabanlı algılama metodunda da benzetim ortamından elde edilen ağ trafiği kullanılabilir. Bu uygulama, çalışmanın daha özgün olmasına ve daha gerçekçi benzetim sonuçları üretmesine vesile olabilir.

KAYNAKLAR

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) A survey on sensor networks, *in IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, DOI: 10.1109/MCOM.2002.1024422.

[2] Silva, A.P.R., Martins, M.H.T., Rocha, B.P.S., Loureiro, A.A.F., Ruiz, L.B., Wong, H.C. (2005). Decentralized intrusion detection in wireless sensor networks, *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, pp.16-23. DOI:10.1145/1089761.1089765

[3] Roman, R., Zhou, J. and Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks, *3rd IEEE Consumer Communications and Networking Conference,* pp.640–644. DOI: 10.1109/CCNC.2006.1593102.

[4] Loo, C.E., Ng, M.Y., Leckie, C., Palaniswami, M. (2006). Intrusion detection for routing attacks in sensor networks, *International Journal of Distributed Sensor Networks*, Vol. II, No. 4, pp.313–332. DOI:10.1080/15501320600692044

[5] Drozda, M., Szczerbicka, H. (2006). Artificial immune systems: survey and applications in ad hoc wireless networks, *International Symposium on Performance Evaluation of Computer and Telecommunication Systems*

[6] Gupta, S., Zheng, R. and Cheng, A.M.K. (2007). ANDES: an anomaly detection system for wireless sensor networks, *International Conference on Mobile Ad hoc and Sensor Systems*, pp. 1-9. DOI: 10.1109/MOBHOC.2007.4428636.

[7] Krontiris, I., Dimitriou, T., Freiling, F. (2007). Towards intrusion detection in wireless sensor networks, *13th European Wireless Conference*

[8] Bojkovic, Z.S., Bakmaz, B.M. Bakmaz, M.R. (2008). Security issues in wireless sensor networks, *International Journal of Communications*, Vol. II, No. 1, pp.106–115.

[9] Rajasegarar, S., Leckie, C. and Palansiwami, M. (2008). Anomaly detection in wireless sensor networks, *IEEE Wireless Communications*, Vol. 15, No. 4, pp.34–40. DOI: 10.1109/MWC.2008.4599219.

[10] Shaikh, R.A., Jameel, H., Auriol, B.J., Lee, S. and Song, Y.J. (2008). Trusting anomaly and intrusion claims for cooperative distributed intrusion detection schemes of wireless sensor networks, *The 9th International Conference for Young Computer Scientists*, pp.2038–2043. DOI: 10.1109/ICYCS.2008.489.

[11] Ahmed, K.R., Ahmed, K., Munir, S. and Asad, A. (2008). Abnormal node detection in wireless sensor network by pair based approach using IDS secure routing methodology, *International Journal of Computer Science and Network Security,* Vol. VIII, No. 12, pp.339–342.

[12] Li, G., He, J. and Fu, Y. (2008). A group based intrusion detection scheme in wireless sensor networks, *The 3rd International Conference on Grid and Pervasive Computing - Workshops*, pp. 286-291. DOI: 10.1109/GPC.WORKSHOPS.2008.31.

[13] Zhang, Q., Yu, T. and Ning, P. (2008). A framework for identifying compromised nodes in wireless sensor networks, *ACM Transaction on Information System Security*, Vol. XI, No. 3, pp.1–37. DOI:10.1145/1341731.1341733

[14] Tiwari, M., Arya, K.V., Choudhari, R., Choudhary, K.S. (2009). Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information, *2009*

Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 824-828. DOI: 10.1109/ICCIT.2009.290.

[15] Farid D. M., Nouria, H., Rahman M. Z. (2010). Combining naive bayes and decision tree for adaptive intrusion detection, *International Journal of Network Security & Its Applications (IJNSA)*, p. 12-25. DOI:10.5121/ijnsa.2010.2202

[16] Mamun, M. S. I., Sultanul Kabir, A.F.M., Hossen, S., Khan, R. H. (2010). Policy based intrusion detection and response system in hierarchical WSN architecture

[17] Chitrakar R., Huang, C. (2012). Anomaly based Intrusion Detection using Hybrid Learning Approach of combining k-Medo IDS Clustering and Naïve Bayes Classification, *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-5. DOI: 10.1109/WiCOM.2012.6478433.

[18] Coppolino, L., D'Antonio, S., Garofalo, A., & Romano, L. (2013). Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks, *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,* pp. 247-254, DOI: 10.1109/3PGCIC.2013.43.

[19] Sajjad, S. M., Bouk, S. H., Yousaf, M. (2015). Neighbor Node Trust Based Intrusion Detection System for WSN, *6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, EUSPN-2015, p. 183-188. DOI:10.1016/j.procs.2015.08.331

[20] Balakrishnan, A., Rino, P. C. (2015). A Novel Anomaly Detection Algorithm for WSN, *2015 Fifth International Conference on Advances in Computing and Communications (ICACC),* pp. 118-121. DOI: 10.1109/ICACC.2015.29.

[21] Almomani, I., Kasasbeh, B., Al-Akhra, M. T. (2016). WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks, *Hindawi Publishing Corporation Journal of Sensors*, Volume 2016, Article ID 4731953, DOI:10.1155/2016/4731953

[22] Ozcelik, M., Irmak, E., Ozdemir, S. (2017) A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks, *International Symposium on Networks, Computers and Communications,* pp. 1-6. DOI: 10.1109/ISNCC.2017.8071998

[23] Amouri, A., Morgera, S. D., Bencherif, M. A., Manthena, R. (2018). A Cross-Layer, Anomaly-Based IDS for WSN and MANET, *Sensors 2018, 18, 651*; DOI:10.3390/s18020651

[24] Acharya, N., Singh, S. (2018) An IWD-based feature selection method for intrusion detection system, *Soft Computing* 22, 4407–4416. DOI: 10.1007/s00500-017-2635-2

[25] Ghugar, U., Pradhan, J., Bhoi, S. K., Sahoo, R. R. (2019). LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System, *Journal of Computer Networks and Communications*, Volume 2019, Article ID 2054298, DOI:10.1155/2019/2054298

[26] Darabi, M. (2019). Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining, *ArXiv*, abs/1912.12225

[27] Yang, H., Zhang, X., Cheng, F. (2020) A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks, *Mobile Networks and Applications*, vol. 26, 1564–1573. DOI: 10.1007/s11036-019-01492-4

[28] Paul, A., Sinha, S., Shaw, R. N., Ghosh, A. (2021). A Neuro-Fuzzy based IDS for Internet-Integrated WSN, *Computationally Intelligent Systems and their Applications*, pp.71-86. DOI:10.1007/978-981-16-0407-2_6

[29] Gandhimathi, L., Murugaboopathi, G. (2021). Mobile Malicious Node Detection Using Mobile Agent in Cluster-Based Wireless Sensor Networks. *Wireless Personal Communications,* 117, 1209–1222. DOI: 10.1007/s11277-020-07918-7

[30] Narayanan, K. L., Krishnan, R.S., Julie, E.G., Robinson, Y.H., Shanmuganathan, V. (2021). Machine Learning Based Detection and a Novel EC-BRTT Algorithm Based Prevention of DoS Attacks in Wireless Sensor Networks. *Wireless Personal Communications.* DOI: 10.1007/s11277-021-08277-7

[31] Wang, Q., Xu, K., and Hassanein, H.S. (2004). A Practical Perspective on Wireless Sensor Networks, Chapter 9, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems* (Ilyas/Mahgoub, Eds), CRC Press

[32] Kablosuz Sensör Ağları, https://e-bergi.com/y/kablosuz-sensor-aglari/, ODTÜ Bilgisayar Topluluğu, Erişim: 8 Kasım 2021

[33] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K. (2000). System Architecture Directions for Networked Sensors. *ACM SIGPLAN Notices*. 35. 10.1145/378995.379006. DOI:10.1145/378995.379006

[34] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S. and Srivastava, M. B. (2002). On communication security in wireless ad-hoc sensor networks, *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 139-144, DOI: 10.1109/ENABL.2002.1030000.

[35] Wang, Y., Attebury G. and Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks, *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, DOI: 10.1109/COMST.2006.315852.

[36] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002). A survey on sensor networks, *IEEE Communications Magazine,* Vol. 40, No. 8, pp. 102-114. DOI: 10.1109/MCOM.2002.1024422.

[37] Stankovic, J. A., Abdelzaher, T. E., Lu, C., Sha, L. and Hou, J. C. (2003). Real-time communication and coordination in embedded sensor networks, *IEEE*, vol. 91, no. 7, pp. 1002-1022, DOI: 10.1109/JPROC.2003.814620.

[38] List of wireless sensor nodes, https://en.wikipedia.org/wiki/List_of_wireless_sensor_nodes, Erişim: 15 Kasım 2021

[39] Altun, B. (2016). *Kablosuz sensör ağları ve uygulama alanları*, Bitirme Tezi, Karabük Üniversitesi, Mühendislik Fakültesi

[40] Bulusu, N., Estrin, D., Girod, L., Heideman, J. (2001). Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems, *Proceedings of the 6th IEEE International Symposium on Communication Theory and Application*

[41] Kakamanshadi, G., Gupta, S. and Singh, S. (2015). A survey on fault tolerance techniques in Wireless Sensor Networks, *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 168-173, DOI: 10.1109/ICGCIoT.2015.7380451.

[42] Younis, M., Senturk, I. F., Akkaya, K., Lee, S. and Senel, F. (2014). Topology management techniques for tolerating node failures in wireless sensor networks: A survey, *Computer Networks*, vol. 58, no. 1, pp. 254-283, DOI: 10.1016/j.comnet.2013.08.021

[43] Moreira, L., Vogt, H. and Beigl, M. (2007). A survey on fault tolerance in wireless sensor networks

[44] Gupta, G. and Younis, M. (2003). Fault-tolerant clustering of wireless sensor networks, *2003 IEEE Wireless Communications and Networking, WCNC 2003,* pp. 1579-1584 vol.3, DOI: 10.1109/WCNC.2003.1200622.

[45] Hoblos, G., Staroswiecki, M. and Aitouche, A. (2000). Optimal design of fault tolerant sensor networks, *Proceedings of the 2000. IEEE International Conference on Control Applications. Conference Proceedings (Cat. No.00CH37162)*, pp. 467-472, DOI: 10.1109/CCA.2000.897468.

[46] Curiac, D. I., Volosencu, C., Pescaru, D., Jurca, L. and Doboli, A. (2009). Redundancy and its applications in wireless sensor networks: a survey, *WSEAS Trans. on Computers*, vol. 8, no. 4, pp. 705-714.

[47] Lee, M. and Choi, Y. (2008). Fault detection of wireless sensor networks, *J. of Computer Communications*, vol. 31, no. 14, pp. 3469-3475. DOI: 10.1016/j.comcom.2008.06.014

[48] Korbi, I., Ghamri-Doudane, Y., Jazi, R. and Saidane, L. A. (2013). Coverage-connectivity based fault tolerance procedure in wireless sensor networks, *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 1540-1545, DOI: 10.1109/IWCMC.2013.6583785.

[49] Lai, Y. and Chen, H. (2007). Energy-Efficient Fault-Tolerant Mechanism for Clustered Wireless Sensor Networks, *2007 16th International Conference on Computer Communications and Networks*, pp. 272-277, DOI: 10.1109/ICCCN.2007.4317831.

[50] Chang, S. and Huang, T. (2012). A Fuzzy Knowledge Based Fault Tolerance Algorithm in Wireless Sensor Networks, *2012 26th International Conference on Advanced Information Networking and Applications Workshops*, pp. 891-896, DOI: 10.1109/WAINA.2012.48.

[51] Duh, D. R., Li, S. P., and Cheng, V. (2013). Distributed Fault-Tolerant Event Region Detection of Wireless Sensor Networks, *International Journal of Distributed Sensor Networks*, pp. 1-8, DOI:10.1155/2013/160523

[52] Bansal, N., Sharma, T. P., Misra, M. and Joshi, R. C. (2008). FTEP: A fault tolerant election protocol for multi-level clustering in homogeneous wireless sensor networks, *2008 16th IEEE International Conference on Networks*, pp. 1-6, doi: 10.1109/ICON.2008.4772563.

[53] Kaur, A. and Sharma, T. (2010). FTTCP: Fault Tolerant Two-level Clustering protocol for WSN, *Int. J. on Networking Security*, vol. 1, no. 3, pp. 28-33

[54] Bari, A., Jaekel, A., Jiang J. and Xu, Y. (2012). Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements, *Comput. Commun*., vol. 35, no. 3, pp. 320-333

[55] Kumar, R. and Kumar, U. (2012). A Hierarchal cluster framework for wireless sensor network, *Int. Conf. Adv. Comput. Commun IEEE*, pp. 46-50

[56] Shih, E., Cho, S. H., Ickes, N., Min, R., Sinha, A., Wang, A., & Chandrakasan, A. (2001). Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. *In Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 272-287. DOI: 10.1145/381677.381703

[57] Kablosuz algılayıcı ağlar, https://yazilimdnyasi.wordpress.com/2018/07/17/kablosuz-algilayici-aglar/, Erişim: 20 Kasım 2021

[58] SmartDust, https://en.wikipedia.org/wiki/Smartdust, Erişim: 21 Kasım 2021

[59] Robbins, A. (2002). More then meets the Eye, *PC Magazine,* Vol: 12 March 2002

[60] Kalaycı, T. E. (2009). Kablosuz Sensör Ağlar ve Uygulamaları, *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri*, pp: 37-46

[61] Karl, H., Willig, A. (2007). *Sensors and actuators*, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, Chichester, West Sussex, England

[62] Microcontroller vs Microprocessor - What are the Differences?, https://www.totalphase.com/blog/2019/12/microcontroller-vs-microprocessor-what-are-the-differences, Erişim: 22 Kasım 2021

[63] Karl, H., Willig, A. (2007). *Microcontrollers versus microprocessors, FPGAs, and ASICs*, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, Chichester, West Sussex, England

[64] Karl, H., Willig, A. (2007). *Memory*, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, Chichester, West Sussex, England

[65] Karl, H., Willig, A. (2007). *Communication device*, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, Chichester, West Sussex, England

[66] Myers, B. A., Willingham, J. B., Landy, P., Webster, M. A., Frogge, P. and Fischer, M. (2000). Design considerations for minimal-power wireless spread spectrum circuits and systems, *in Proceedings of the IEEE*, vol. 88, no. 10, pp. 1598-1612, DOI: 10.1109/5.888998.

[67] Wang, A., Cho, S., Sodini, C. G. and Chandrakasan A. P. (2001). Energy-Efficient Modulation and MAC for Asymmetric Microsensor Systems. *In Proceedings of ISLPED 2001*

[68] Raghunathan, V. Schurgers, C., Park, S. and Srivastava, M. B. (2002). Energy-aware wireless microsensor networks, *in IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40-50, DOI: 10.1109/79.985679.

[69] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. and Chandrakasan, A. (2001). Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks. *In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking 2001 (MobiCom)*, pages 272–286

[70] Schurgers, C., Raghunathan, V. and Srivastava, M. B. (2003). Power Management for Energy-Aware Communication Systems. *ACM Transactions on Embedded Computing Systems*, 2(3): 431–447.

[71] Bogliolo, A., Benini, L., Lattanzi, E. and Micheli, G. (2004). Specification and analysis of power-managed systems, *in Proceedings of the IEEE*, vol. 92, no. 8, pp. 1308-1346, DOI: 10.1109/JPROC.2004.831207.

[72] Sensor node, https://en.wikipedia.org/wiki/Sensor_node, Erişim: 26 Kasım 2021

[73] Pottie, G. J. and Kaiser, W. J. (2000). Embedding the Internet: Wireless Integrated Network Sensors. *Communications of the ACM*, 43(5): 51–58, DOI: 10.1145/332833.332838

[74] Karl, H., Willig, A. (2007). *Power supply of sensor nodes*, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, Chichester, West Sussex, England

[75] Sensor Network Architecture, https://www.geeksforgeeks.org/sensor-network-architecture/, Erişim: 16 Aralık 2021

[76] Reka Mca, N., Phil, M. (2015). Wireless Sensor Networks (WSN), *(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 6 (4), 3706-3708

[77] Rahman, M. A., Saddik, A. E., Gueaieb W. (2008). Wireless Sensor Network Transport Layer: State of the Art, *Sensors. Lecture Notes Electrical Engineering*, vol 21. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-540-69033-7_11

[78] Abbasi A. A., Younis M. (2007). A survey on clustering algorithms for wireless sensor networks, *Computer Communications*, Volume 30, Issues 14–15, Pages 2826-2841, DOI: 10.1016/j.comcom.2007.05.024

[79] Akkaya K., Younis M. (2005). A survey on routing protocols for wireless sensor networks, *Ad Hoc Networks*, Volume 3, Issue 3, Pages 325-349, DOI: 10.1016/j.adhoc.2003.09.010.

[80] Seah W., Tan Y. (2010). *Sustainable Wireless Sensor Networks*, InTech Open Access Publisher; Rijeka, Hırvatistan

[81] Randhawa, S., Jain, S. (2017). Data Aggregation in Wireless Sensor Networks: Previous Research, Current Status and Future Directions. *Wireless Personal Communications* 97, 3355–3425, DOI: 10.1007/s11277-017-4674-5

[82] Rajagopalan, R., Varshney, P. K. (2006). Data aggregation techniques in sensor networks: A survey, *Electrical Engineering and Computer Science. 22.*

[83] Liu X. (2012). *A survey on clustering routing protocols in wireless sensor networks*. Sensors, Basel, İsviçre, 12(8), 11113–11153. DOI: 10.3390/s120811113

[84] Lee S. H., Lee S., Song H., Lee H. S. (2011). Gradual Cluster Head Election for High Network Connectivity in Large-Scale Sensor Networks. *Proceedings of 13th International Conference on Advanced Communication Technology (ICACT2011)*, pp. 168-172.

[85] Sharmaa, R., Mishraa, N., Srivastavab, S. (2015). A proposed energy efficient distance based cluster head (DBCH) Algorithm: An Improvement over LEACH, *Procedia Computer Science*, Volume 57, Pages 807-814, DOI:10.1016/j.procs.2015.07.481.

[86] Yalçın, S. ve Erdem, E. (2019). Bacteria Interactive Cost and Balanced-Compromised Approach to Clustering and Transmission Boundary-Range Cognitive Routing in Mobile Heterogeneous Wireless Sensor Networks, *Sensors*, cilt 19, 867, ss.1-30.

[87] Azad, P., Sharma, V. (2013). Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment, *ISRN Sensor Networks*, Article ID 909086, DOI: 10.1155/2013/909086

[88] Rostami, A. S., Badkoobe, M., Mohanna, F., Keshavarz, H., Hosseinabadi, A. A. R. and Sangaiah, A. K. (2018) Survey on clustering in heterogeneous and homogeneous wireless sensor networks. *The Journal of Supercomputing*, 74, 277–323 (2018), DOI: 10.1007/s11227-017-2128-1

[89] Singh, J., Kumar, R. and Mishra, A. K. (2015). Clustering algorithms for wireless sensor networks: A review, *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 637-642.

[90] Yuste-Delgado, A-J., Cuevas-Martinez, J-C., Triviño-Cabrera A. (2020). A Distributed Clustering Algorithm Guided by the Base Station to Extend the Lifetime of Wireless Sensor Networks. *Sensors*; 20(8):2312. DOI: 10.3390/s20082312

[91] Boyinbode, O., Le, H., Mbogho, A., Takizawa, M., Poliah, R. (2010) A survey on clustering algorithms for wireless sensor networks, *13th International Conference on Network-Based Information Systems (NBiS)*, pp 358–364

[92] Heinzelman, W., Chandrakasan, A. and Balakrishnan, H. (2000). Energy efficient communication protocol for wireless micro sensor networks, *33rd Hawaii International Conference on System Sciences*, vol. 8.

[93] Younis, O. and Fahmy, S. (2004). HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks, *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 660-669

[94] Arjunan, S., Sujatha, P. (2019). A survey on unequal clustering protocols in Wireless Sensor Networks, *Journal of King Saud University - Computer and Information Sciences*, Volume 31, Issue 3, Pages 304-317, DOI: 10.1016/j.jksuci.2017.03.006.

[95] S. Soro and W. B. Heinzelman, (2005), Prolonging the lifetime of wireless sensor networks via unequal clustering," *19th IEEE International Parallel and Distributed Processing Symposium*, pp. 8 pp. DOI: 10.1109/IPDPS.2005.365.

[96] Chengfa, L., Mao, Y. and Guihai, C. (2005). An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks, *IEEE Mobile Adhoc and Sensor Systems Conference*, pp. 604

[97] Ever, E., Luchmun, R. and Shah, P. (2012). UHEED-An unequal clustering algorithm for wireless sensor network, *Sensornets 2012*, pp. 24-26

[98] Zhao, X. and Wang, N. (2010). An unequal layered clustering approach for large scale wireless sensor networks, *2010 2nd International Conference on Future Computer and Communication*, pp. V1-750-V1-756, DOI: 10.1109/ICFCC.2010.5497328.

[99] Ren, R., Qian, J., Li, L., Zhao, Z. and Li, X. (2010) Unequal Clustering Scheme Based LEACH for Wireless Sensor Networks, *2010 Fourth International Conference on Genetic and Evolutionary Computing*, pp. 90-93, doi: 10.1109/ICGEC.2010.30.

[100] Yu, J., Qi, Y. and Wang, (2011). An energy-driven unequal clustering protocol for heterogeneous wireless sensor networks, *Journal of Control Theory and Applications*, vol. 30, no. 12, pp. 133-139,

[101] Bagci, H., Yazici, A. (2010) An Energy Aware Fuzzy Unequal Clustering Algorithm for Wireless Sensor Networks, *2010 IEEE Internatıonal Conference On Fuzzy Systems (FUZZ-IEEE 2010).*

[102] Patra, A. and Chouhan, S. (2013). Energy Efficient Hybrid multihop clustering algorithm in wireless sensor networks, *2013 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, pp. 59-63, DOI: 10.1109/COMNETSAT.2013.6870861.

[103] Aslam, M. vd. (2014). HADCC: Hybrid Advanced Distributed and Centralized Clustering Path Planning Algorithm for WSNs, *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 657-664, doi: 10.1109/AINA.2014.81.

[104] Kumar, G., Mehra, H., Seth, A. R., Radhakrishnan, P., Hemavathi, N. and Sudha, S. (2014). An hybrid clustering algorithm for optimal clusters in Wireless sensor networks, *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 1-6, doi: 10.1109/SCEECS.2014.6804442.

[105] Tamil, K. and Sridharan, D. (2009). Security Vulnerabilities In Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security 5*, 031-044

[106] Sharifnejad, M., Sharifi, M., Ghiasabadi, M., & Beheshti, S. (2007). A Survey on Wireless Sensor Networks Security, *4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT 2007)*

[107] Kifayat, K., Merabti, M., Shi, Q., and Llewellyn-Jones, D. (2010). Security in Wireless Sensor Networks, *Handbook of Information and Communication Security*, (pp.513-552), DOI: DOI:10.1007/978-3-642-04117-4_26

[108] Padmavathi, G., Shanmugapriya, D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, *International Journal of Computer Science and Information Security, IJCSIS*, Vol. 4, No. 1 & 2

[109] Jain, M. K. (2011). Wireless Sensor Networks: Security Issues and Challenges, *International Journal of Computer and Information Technology (IJCIT)*, Volume 02, pages: 62-67

[110] Meghdadi, M., Özdemir, S. and Güler, İ. (2010). Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler, *Bilişim Teknolojileri Dergisi,* 1 (1)

[111] Shi, E., Perrig, A. (2004). Designing secure sensor networks, *in IEEE Wireless Communications*, vol. 11, no. 6, pp. 38-43, DOI: 10.1109/MWC.2004.1368895.

[112] Sen, J. (2009). A Survey on Wireless Sensor Network Security. *ArXiv*, abs/1011.1529.

[113] Capkun, S., Hubaux, J. P. (2006). Secure positioning in wireless networks, *in IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221-232, DOI: 10.1109/JSAC.2005.861380

[114] Lazos, L. Poovendran, R. (2005). SERLOC: Robust localization for wireless sensor networks, *ACM Transactions on Sensor Networks*, Vol. 1, No. 1, pp.73-100

[115] Chan, H. and Perrig, A. (2003). Security and privacy in sensor networks, *in Computer*, vol. 36, no. 10, pp. 103-105, DOI: 10.1109/MC.2003.1236475.

[116] Chelli, K. (2015). Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, *Proceedings of the World Congress on Engineering 2015*, Vol I WCE 2015

[117] Sharma, K. & Ghose, M. K. (2010). Wireless Sensor Networks: An Overview on its Security Threats. *International Journal of Computer Applications. MANETs.* DOI: 10.5120/1008-44.

[118] Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*, 7(1), 74-81, DOI:10.1109/MPRV.2008.6

[119] Korkmaz, I., Dagdeviren, O., Tekbacak, F., & Dalkiliç, M. E. (2013). A Survey on Security in Wireless Sensor Networks: Attacks and Defense Mechanisms.

[120] Xu, W., Trappe, W., Zhang, Y. & Wood, T. (2005). The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, DOI: 10.1145/1062689.1062697.

[121] Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks, in *Computer*, vol. 35, no. 10, pp. 54-62, DOI: 10.1109/MC.2002.1039518.

[122] Frekans atlamalı geniş spektrum, https://tr.wikipedia.org/wiki/Frekans_atlamal%C4%B1_geni%C5%9F_spektrum, Erişim: 3 Aralık 2021

[123] Wang, X., Chellappan, S., Gu, W., Yu, W. and Xuan, D. (2005). Search-based physical attacks in sensor networks, *14th International Conference on Computer Communications and Networks, ICCCN 2005*, pp. 489-496, DOI: 10.1109/ICCCN.2005.1523922.

[124] Hartung, C., Balasalle, J. and Han, R. (2004) Node compromise in sensor networks: The need for secure systems, *Technical Report CU-CS- 988-04*, Department of Computer Science, University of Colorado at Boulder

[125] Anderson, R. and Kuhn, M. (1997). Low cost attacks on tamper resistant devices, *in Proc. of the 5th International Workshop on Security Protocols*

[126] Law, Y. W., Hartel, P., den Hartog, J., & Havinga, P. (2005). Link-Layer Jamming Attacks on S-MAC. *In Proceedings of the Second IEEE European Workshop on Wireless Sensor Networks* (pp. 217-225), DOI: 10.1109/EWSN.2005.1462013.

[127] Saxena, M. (2007). Security In Wireless Sensor Networks - A Layer Based Classification, *CERIAS Tech Report 2007-04*, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086

[128] Khan, M. A., Khan, T. A., Beg, M. T. (2012). RTS/CTS Mechanism of MAC Layer IEEE 802.11 WLAN in Presence of Hidden Nodes, *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(5), 232-236, 2012.

[129] Poudyal, N., Lee, H. C., Lee, B. S., Byun, Y., Tao, E. Y.(2009). The impact of RTS/CTS frames on TCP performance in mobile ad hoc-based wireless LAN, *IEEE 11th International Conference on Advanced Communication Technology (ICACT),*1554 – 1559,

[130] Lee, H. C. (2010). The Effect of RTS/CTS Frames on the Performance of Ad Hoc-Based Mobile LAN, *IEEE Third International Conference on Advances in Mesh Networks,* 63-68,

[131] Ali, M. H., Odah, M. K. (2009). Simulation Study of 802.11b DCF Using OPNET Simulator, *Eng.& Tech. Journal*, 27(6), 1112 – 1117

[132] Jasani, H., Alaraje, N. (2007). Evaluating the Performance of IEEE 802.11 Network using RTS/CTS Mechanism, *IEEE International Conference on Electro/Information Technology,* 616-621

[133] Habib, G., Bassil, C. (2013). Influence of the RTS/CTS in VANET, *IEEE 13th Mediterranean Microwave Symposium (MMS),*1-4

[134] Manitpornsut, S., Landfeldt, B., Boukerche, A. (2011). Improving densely deployed wireless network performance in unlicensed spectrum through hidden-node aware channel assignment, *Performance Evaluation Journal (Elsevier ScienceDirect),* 68(9), 825–840

[135] Borsuk, B., Koçak, C. (2016). Kablosuz Ağlarda Gizli Düğüm Probleminde IEEE 802.11 MAC Katmanı RTS/CTS Mekanizmasının Çoklu Ortam Uygulamalarında Performansa Etkisi, *Bilişim Teknolojileri Dergisi,* Cilt: 9, Sayı: 2, DOI: 10.17671/btd.44133

[136] Sarma, H. K. D. and Kar, A. (2006). Security Threats in Wireless Sensor Networks, *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology,* pp. 243-251, DOI: 10.1109/CCST.2006.313457.

[137] Stajano, F. and Anderson, R. (1999). The Resurrecting Duckling: Security Issues for AdHoc Wireless Networks, *Proc. 7th Int'l Workshop Security Protocols, Springer*, pp. 172–194.

[138] Raymond, D.R., Marchany, R.C., Brownfield, M.I., & Midkiff, S.F. (2009). Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. *IEEE Transactions on Vehicular Technology,* 58, 367-380, DOI:10.1109/TVT.2008.921621

[139] Parras, J., & Zazo, S. (2018). Wireless Networks under a Backoff Attack: A Game Theoretical Perspective, *Sensors,* 18(2), 404. DOI: 10.3390/s18020404

[140] Radosavac, S., Cardenas, A., Baras, J. S., & Moustakides, G. V. (2007). Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies against Individual and Colluding Attackers. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks,* 15(1), 103-128, DOI:10.3233/JCS-2007-15105

[141] Cagalj M., Ganeriwal S., Aad I., Hubaux J.P (2005). On selfish behavior in CSMA/CA networks, *Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies,* pp. 2513–2524, DOI:10.1109/INFCOM.2005.1498536

[142] Demirkol I., Ersoy C., Alagoz F. (2006). MAC protocols for wireless sensor networks: A survey, *in IEEE Communications Magazine,* vol. 44, no. 4, pp. 115-121, April 2006, doi: 10.1109/MCOM.2006.1632658.

[143] Yadav R., Varma S., Malaviya N. (2009). A survey of MAC protocols for wireless sensor networks. *UbiCC Journal,* Volume 4, Number 3, 4:827–833.

[144] Raya, M., Hubaux, J-P. & Aad, I. (2004). DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. DOI: 10.1145/990064.990077.

[145] Kyasanur, P. & Vaidya, N.H. (2003). Detection and Handling of MAC Layer Misbehavior in Wireless Networks. *Proceedings of the International Conference on Dependable Systems and Networks.* 173-182. DOI:10.1109/DSN.2003.1209928

[146] Xiao, Y., Sethi, S., Chen, H-H. and Sun, B. (2005). Security services and enhancements in the IEEE 802.15.4 wireless sensor networks, *GLOBECOM '05. IEEE Global Telecommunications Conference*, DOI: 10.1109/GLOCOM.2005.1577958.

[147] Cryptographic nonce, https://en.wikipedia.org/wiki/Cryptographic_nonce, Erişim: 5 Aralık 2021

[148] Pawar, P. M., Nielsen, R. H., Prasad, N. R., Ohmori, S., & Prasad, R. (2012). Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach, *Journal of Cyber Security and Mobility*, 1(1), 65-82.

[149] Sokullu, R.I., Dagdeviren, O., & Korkmaz, I. (2008). On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack. *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*, 673-678, DOI: DOI:10.1109/SENSORCOMM.2008.75

[150] Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures, *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, DOI: 10.1109/SNPA.2003.1203362.

[151] Perrig, A., Szewczyk, R., Tygar, J.D, Wen, V. and Culler, D.E (2002). SPINS: Security Protocols for Sensor Networks, *In ACM Journal of Wireless Networks*, 8:5, pp. 521-534, DOI:10.1023/A:1016598314198

[152] Zia, T. & Zomaya, A. (2006). Security Issues in Wireless Sensor Networks, *Proceedings of the International Conference on Systems and Networks Communications (ICSNC 2006)*, DOI:10.1109/ICSNC.2006.66

[153] Ngai, E. C. H., Liu, J. and Lyu, M. R. (2006). On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, *2006 IEEE International Conference on Communications*, pp. 3383-3389, DOI: 10.1109/ICC.2006.255595.

[154] Newsome, J., Shi, E., Song, D. and Perrig, A. (2004). The Sybil attack in sensor networks: analysis & defenses, *Third International Symposium on Information Processing in Sensor Networks*, IPSN 2004, pp. 259-268, DOI: 10.1109/IPSN.2004.239019.

[155] Needham–Schroeder protokolü, https://tr.wikipedia.org/wiki/Needham%E2%80%93Schroeder_protokol%C3%BC, Erişim: 4 Aralık 2021

[156] Hu, Y., Perrig, A., & Johnson, D.B. (2002). Wormhole Detection in Wireless Ad Hoc Networks.

[157] Kalita, H.K. & Avijit, K. (2009). Wireless Sensor Network Security. *International Journal of Next-Generation Networks. 1.*

[158] Saghar, K.,Kendall, D. and Bouridane, A. (2015). RAEED: A solution for hello flood attack, *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 248-253, DOI: 10.1109/IBCAST.2015.7058512.

[159] Yu, Y., Govindan, R., Estrin, D. (2001). Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks. *UCLA Computer Science Department Technical Report. 463.*

[160] Deng J., Han R., Mishra S. (2006). INSENS: Intrusion-tolerant routing for wireless sensor networks, Elsevier Journal on Computer Communications, *Special Issue on Dependable Wireless Sensor Networks*, v.29, p.216–230, DOI: 10.1016/j.comcom.2005.05.018

[161] Zhu S., Setia S., Sajodia S. (2003). LEAP: Efficient Security Mechanisms for LargeScale Distributed Sensor Networks, *ACM*, DOI: 10.1145/958491.958534

[162] Srinivasan, A., Teitelbaum, J., Wu, J., Cardei, M., Liang, H. (2008). *Reputation-and-Trust-Based Systems for Ad Hoc Networks,* Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks (pp.375 - 403), DOI: 10.1002/9780470396384.ch13.

[163] Sun, Y., Han, Z., & Liu, K. J. R. (2008). Defense of Trust Management Vulnerabilities in Distributed Networks. *IEEE Communications Magazine,* 46(2), 112-119, DOI:10.1109/MCOM.2008.4473092

[164] Dellarocas, C. (2000). Mechanisms for Coping with Unfair Ratings and Discriminatory Behavior in Online Reputation Reporting Systems, *ICIS '00: Proceedings of the twenty first international conference on Information systems,* Pages 520–525

[165] Pathan, A. S. K. (Ed.). (2010). Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. *CRC Press*

[166] Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. *Journal of Network and Computer Applications,* 35(3), 867-880, DOI :10.1016/J.JNCA.2011.03.005

[167] Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A Survey of Attack and Defense Techniques for Reputation Systems. *ACM Computing Surveys,* 42(1), DOI: 10.1145/1592451.1592452

[168] Misaghi, M., da Silva, E., & Albini, L. C. P. (2012). Distributed Self-Organized Trust Management for Mobile Ad Hoc Networks. *Communications in Computer and Information Science,* 293, 506-518.

[169] Handshaking, https://en.wikipedia.org/wiki/Handshaking, Erişim: 5 Aralık 2021

[170] Aura, T., Nikander, P., & Leiwo, J. (2000). DOS-Resistant Authentication with Client Puzzles. *Security Protocols Workshop,* pp. 170-177, DOI:10.1007/3-540-44810-1_22

[171] Hui, J.W. and Culler, D. (2004). The Dynamic Behavior of a Data Dissemination Protocol for Network Programming at Scale, *Proc. 2nd ACM Conf. Embedded Networked Sensor Systems, ACM Press,* pp. 81–94

[172] Dutta, P., Hui, J.W., Chu, D., Culler, D.E. (2006). Securing the deluge Network programming system. *Proceedings of the Fifth International Conference on Information Processing in Sensor Networks, IPSN '06*. 326-333. DOI: 10.1109/IPSN.2006.243821.

[173] Deng, J., Han, R., Mishra, S. (2005). Defending against path-based DoS attacks in wireless sensor networks. *Proc. 3rd ACM Workshop Security of Ad Hoc and Sensor Networks, ACM Press*, pp. 89–96, DOI:10.1145/1102219.1102235

[174] Shrivastava, N., Buragohain, C., Agrawal, D., Suri, S. (2004). Medians and Beyond: New Aggregation Techniques for Sensor Networks. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems.* DOI:10.1145/1031495.1031524

[175] Marti, S.A., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *MobiCom '00.*

[176] Intrusion Detection System, https://en.wikipedia.org/wiki/Intrusion_detection_system, Erişim: 6 Aralık 2021

[177] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks*. DOI: 10.1155/2013/167575

[178] Chen, T. M., Kuo, G-S., Li, Z-P., Zhu, G-M. (2007). Intrusion Detection in Wireless Mesh Networks, *CRC Press*

[179] Ceylan, K.G. (2004). *Bilgisayar ağlarına yetkisiz erişimleri tespit eden yazılımlar*, Yüksek Lisans Tezi, İstanbul Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı

[180] Intrusion Detection System (IDS), https://www.geeksforgeeks.org/intrusion-detection-system-ids/, Erişim: 20 Aralık 2021

[181] Farooqi, A.H., Khan, F.A. (2009). Intrusion Detection Systems for Wireless Sensor Networks: A Survey. *International Journal of Ad Hoc and Ubiquitous Computing.* 9. 234-241. DOI:10.1504/IJAHUC.2012.045549

[182] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks.* DOI: 10.1155/2013/167575

[183] Darabi, M. (2019). Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining.

[184] Farooqi, A. & Khan, F. (2009). Intrusion Detection Systems for Wireless Sensor Networks: A Survey. *International Journal of Ad Hoc and Ubiquitous Computing.* 9. 234-241. DOI:10.1504/IJAHUC.2012.045549

[185] Brutch, P. and Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks, *2003 Symposium on Applications and the Internet Workshops,* pp. 368-373, DOI: 10.1109/SAINTW.2003.1210188.

[186] CICFlowMeter (formerly ISCXFlowMeter), https://www.unb.ca/cic/research/applications.html#CICFlowMeter, Erişim: 11 Aralık 2021

[187] CSE-CIC-IDS2018 on AWS, https://www.unb.ca/cic/datasets/ids-2018.html, Erişim: 11 Aralık 2021

[188] Weka 3: Machine Learning Software in Java, https://www.cs.waikato.ac.nz/ml/weka/index.html, Erişim: 11 Aralık 2021

[189] Larrañaga, P., Moral, S. (2011). Probabilistic graphical models in artificial intelligence, *Applied Soft Computing 11 (2),* pp. 1511-1528, DOI: 10.1016/j.asoc.2008.01.003

[190] Çinicioglu, E.N., Atalay, M. & Yorulmaz, H. (2013). Trafik Kazaları Analizi İçin Bayes Ağları Modeli. *Internatıonal Journal Of Informatıcs Technologıes*. 6. 41-54.

[191] Yang, X-S. (2019). *Bayesian network and Markov models,* Introduction to Algorithms for Data Mining and Machine Learning, Academic Press, DOI: 10.1016/C2018-0-02034-4

[192] Stochastic process, https://en.wikipedia.org/wiki/Stochastic_process, Erişim: 11 Aralık 2021

[193] Bayes teoremi, https://tr.wikipedia.org/wiki/Bayes_teoremi, Erişim: 11 Aralık 2021

[194] Uusitalo, L. (2007). Advantages and challenges of Bayesian networks in environmental modelling, *Ecological Modelling,* Volume 203, Issues 3–4, Pages 312-318, DOI: 10.1016/j.ecolmodel.2006.11.033

[195] Bayraktarli, Y., Ulfkjær, J., Yazgan, U. & Faber, M. (2005). On the Application of Bayesian Probabilistic Networks for Earthquake Risk Management. *Proc. to 9'th International Conference on Structural Safety and Reliability.*

[196] Nikovski, D. (2000). Constructing Bayesian Networks for Medical Diagnosis from Incomplete and Partially Correct Statistics, *in IEEE Transactions on Knowledge and Data Engineering,* vol. 12, no. 4, pp. 509-516, DOI: 10.1109/69.868904.

[197] Garbolino, P., Taroni, F. (2002). Evaluation of scientific evidence using Bayesian networks, *Forensic Science International,* Vol. 125, pp. 149-155, DOI: 10.1016/S0379-0738(01)00642-9

[198] Bromley, J., Jackson, N.A., Clymer, O.J., Giacomello, A.M., Jensen, F.V. (2005). The use of Hugin® to develop Bayesian networks as an aid to integrated water resource planning,

Environmental Modelling & Software, Volume 20, Issue 2, Pages 231-242, DOI: 10.1016/j.envsoft.2003.12.021

[199] Ohri, A. (2021). Bayesian Belief Networks: An Introduction In 6 Easy Points, https://www.jigsawacademy.com/blogs/data-science/bayesian-belief-network#What-are-the-Bayesian-Networks-used-for, Erişim: 11 Aralık 2021

[200] Breiman, L. (2001). Random Forests. *Machine Learning* 45, 5–32. DOI: 10.1023/A:1010933404324

[201] Erdem, F., Derinpınar, M.A, Nasirzadehdizaji, R., Oy, S., Şeker, D.Z, Bayram, B. (2018). Rastgele Orman Yöntemi Kullanılarak Kıyı Çizgisi Çıkarımı İstanbul Örneği, *Journal of Geomatics 2018*; 3(2);100-107, DOI: 10.29128/geomatik.362179

[202] Çebi, C.B. (2020). Rastgele Orman Algoritması, https://medium.com/@cemthecebi/rastgele-orman-algoritmas%C4%B1-1600ca4f4784, Erişim: 11 Aralık 2021

[203] Archer, K.J, Kimes, R.V. (2008). Empirical characterization of random forest variable importance measures, *Computational Statistics & Data Analysis*, Volume 52, Issue 4, Pages 2249-2260, DOI: 10.1016/j.csda.2007.08.015

[204] Hassan, N. Y., Gomaa, W., Khoriba, G. and Haggag, M. H. (2018). Supervised Learning Approach for Twitter Credibility Detection, *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, pp. 196-201, DOI: 10.1109/ICCES.2018.8639315.

[205] Breiman, L., Cutler, A. (2005). Random Forests. https://www.stat.berkeley.edu/~breiman/RandomForests/cc_home.htm, Erişim: 11 Aralık 2021

[206] Random Forest, https://www.ibm.com/cloud/learn/random-forest, Erişim: 11 Aralık 2021

[207] C4.5 algorithm, https://en.wikipedia.org/wiki/C4.5_algorithm, Erişim: 11 Aralık 2021

[208] Saravanan, N., Gayathri, V. (2018). Performance and Classification Evaluation of J48 Algorithm and Kendall's Based J48 Algorithm (KNJ48), *International Journal of Computational Intelligence and Informatics*, Vol. 7: No. 4, DOI:10.14445/22312803/IJCTT-V59P112

[209] Bilgi teorisi, https://tr.wikipedia.org/wiki/Bilgi_teorisi, Erişim: 11 Aralık 2021

[210] Yöntemler-4.1: C4.5 Algoritması, https://medium.com/@Emreyz/y%C3%B6ntemler-4-1-c4-5-algoritmas%C4%B1-7382de92584e, Erişim: 11 Aralık 2021

[211] Franczak, J.M. (2000). Fast Effective Rule Induction Overview, https://static.aminer.org/pdf/PDF/000/334/623/fast_effective_rule_induction.pdf, Erişim: 12 Aralık 2021

[212] Witten, I., Frank, E. (2005). *Using global optimization*, Data Mining: Practical Machine Learning Tools and Techniques, Second Edition, Elsevier

[213] R/Classification/JRip'te Veri Madenciliği Algoritmaları, https://en.wikibooks.org/wiki/Data_Mining_Algorithms_In_R/Classification/JRip, Erişim: 12 Aralık 2021

[214] Sonvane, S. (2020). The RIPPER Algorithm, https://medium.com/swlh/the-ripper-algorithm-a5eebbe3661d, Erişim: 12 Aralık 2021

[215] Ripper Algorithm, https://www.geeksforgeeks.org/ripper-algorithm/, Erişim: 12 Aralık 2021

[216] Cohen, W.W. (1995). Fast effective rule induction, ICML'95: *Proceedings of the Twelfth International Conference on International Conference on Machine Learning*, pp: 115-123

[217] Frank, E., & Witten, I.H. (1998). Generating Accurate Rule Sets Without Global Optimization. *ICML*.

[218] Ghosal, A,. Halder, S. (2013). *Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches.* Wireless Networks and Security (pp.329-367), DOI:10.1007/978-3-642-36169-2_10

[219] Silva, A. P., Martins, M., Rocha, B., Loureiro, A., Wong, H.(2005). Decentralized intrusion detection in wireless sensor networks, *Q2SWinet'05 - Proceedings of the First ACM Workshop on Q2S and Security for Wireless and Mobile Networks*, 16-23., DOI:10.1145/1089761.1089765

[220] Kohavi, R. (1995). *Wrappers for Performance Enhancement and Oblivious Decision Graphs.* PhD thesis, Stanford University

[221] Cavusoglu, U., Kacar, S. (2019). Anormal Trafik Tespiti için Veri Madenciliği Algoritmalarının Performans Analizi. *Academic Platform Journal of Engineering and Science* 7-2, 205-216

[222] Elbahadır, H., Erdem, E. (2021). Kablosuz Algılayıcı Ağlarda Hibrit Saldırı Tespit Sistemi Geliştirme, *Computer Science, 5th International Artificial Intelligence and Data Processing symposium*, 162-174 . DOI: 10.53070/bbd.990934

[223] Leevy, J.L., Khoshgoftaar, T.M. (2020). A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018, *Journal of Big Data volume 7*, Article number: 104, DOI/10.1186/s40537-020-00382-x

[224] Jin, R., Breitbart, Y. and Muoh, C. (2007). Data Discretization Unification, *Seventh IEEE International Conference on Data Mining (ICDM 2007),* pp. 183-192, DOI: 10.1109/ICDM.2007.35.

[225] Stiglic, G., Kocbek, S., Pernek, I., & Kokol, P. (2012). Comprehensive decision tree models in bioinformatics. *PloS one*, 7(3), e33812. DOI: 10.1371/journal.pone.0033812

ÖZGEÇMİŞ

Hamza ELBAHADIR

[redacted]

AKADEMİK FAALİYETLER

Bildiriler:

1. Elbahadır, H., & Erdem, E. (2021). Kablosuz Algılayıcı Ağlarda Hibrit Saldırı Tespit Sistemi Geliştirme. *Computer Science, 5th International Artificial Intelligence and Data Processing symposium,* 162-174. DOI: 10.53070/bbd.990934
2. Elbahadır, H., & Erdem, E. (2021). Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks, *2021 6th International Conference on Computer Science and Engineering (UBMK),* pp. 401-406, DOI: 10.1109/UBMK52708.2021.9558928.