T.C.
GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

YÜKSEK
LİSANS
TEZİ

KABLOSUZ ALGILAYICI AĞLARIN SİBER GÜVENLİK AÇISINDAN İNCELENMESİ VE ÖZGÜN BİR SALDIRI TESPİT SİSTEMİNİN ÖNERİLMESİ

MERT MELİH ÖZÇELİK

BİLİŞİM SİSTEMLERİ ANABİLİM DALI

TEMMUZ 2017


GAZİ ÜNİVERSİTESİ
Gazi
1926

KABLOSUZ ALGILAYICI AĞLARIN SİBER GÜVENLİK AÇISINDAN İNCELENMESİ VE ÖZGÜN BİR SALDIRI TESPİT SİSTEMİNİN ÖNERİLMESİ

Mert Melih ÖZÇELİK

YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMLERİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

TEMMUZ 2017

Mert Melih ÖZÇELİK tarafından hazırlanan "KABLOSUZ ALGILAYICI AĞLARIN SİBER GÜVENLİK AÇISINDAN İNCELENMESİ VE ÖZGÜN BİR SALDIRI TESPİT SİSTEMİNİN ÖNERİLMESİ" tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Ana bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Erdal IRMAK

Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Başkan: Doç. Dr. Suat ÖZDEMİR

Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Üye: Yrd. Doç. Dr. Murat AYDOS

Bilişim Sistemleri Anabilim Dalı, Hacettepe Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Tez Savunma Tarihi: 12.07.2017

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Doç. Dr. Bünyamin CİYLAN

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mert Melih ÖZÇELİK

12.07.2017

KABLOSUZ ALGILAYICI AĞLARIN SİBER GÜVENLİK AÇISINDAN İNCELENMESİ VE ÖZGÜN BİR SALDIRI TESPİT SİSTEMİNİN ÖNERİLMESİ

(Yüksek Lisans Tezi)

Mert Melih ÖZÇELİK

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2017

ÖZET

Bu tez çalışmasında, kablosuz algılayıcı ağların (KAA'ların) siber güvenlik bakış açısıyla incelemesi yapılmış, KAA'ların karakteristik özellikleri, KAA'larda bulunan kısıtlar ve zafiyetler ile KAA'ların kullanım alanları incelenmiştir. Ayrıca KAA'lara yönelik tehdit ve saldırılar ile söz konusu saldırılardan korunma yöntemleri araştırılmış, görev kritik işlerde kullanılan KAA'lardaki güvenlik gereksiniminin önemi vurgulanmıştır. KAA'lar için en büyük sınırlamanın enerji olduğu ve düğümlerde kullanılan bataryaların ağ ömrüne doğrudan etki ettiği konusu üzerinde özellikle durulmuştur. KAA'ların doğasında bulunan zafiyetler nedeniyle saldırıları tamamen önlemenin mümkün olmadığı belirtilmiş, bu nedenle ikinci savunma hattı olarak değerlendirilen saldırı tespit sistemlerinin (IDS) incelenmesi yapılmıştır. Saldırıları tespit etmeye yönelik IDS'lerin kapsamlı olarak incelenmesi neticesinde, geleneksel olarak kullanılan saldırı tespit yöntemlerinden farklı yaklaşımların geliştirilmesi gerektiği sonucuna varılmıştır. Bu kapsamda, saldırıları zamanında ve etkin bir şekilde tespit edebilecek, güven ve kötüye kullanım tabanlı yöntemleri kullanan özgün bir hibrit saldırı tespit sistemi önerilmiştir. Önerilen sistemin geçerliliği ve performans analizi OMNET++ tabanlı Castalia Framework isimli benzetim programı ile yapılmıştır. Bu tez çalışmasının, KAA'lardaki güvenlik ve saldırı tespit sistemleri konularının anlaşılmasına katkı sağlayacağı, önerilen IDS yöntemi ile alanda çalışan akademisyenlere faydalı olacağı değerlendirilmektedir.

Bilim Kodu : 92403
Anahtar Kelimeler : Kablosuz algılayıcı ağ, siber güvenlik, saldırı tespit sistemi, Castalia Framework.
Sayfa Adedi : 101
Danışman : Doç. Dr. Erdal IRMAK

INVESTIGATION OF WIRELESS SENSOR NETWORKS FROM CYBER SECURITY PERSPECTIVE AND PROPOSING A NOVEL INTRUSION DETECTION SYSTEM

(M. Sc. Thesis)

Mert Melih ÖZÇELİK

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

July 2017

ABSTRACT

In this study, wireless sensor networks (WSNs) are investigated from a cyber security perspective by analyzing characteristics, constraints, vulnerabilities and application fields of them. Security issues such as threats and attacks against WSNs as well as the protective measures for those attacks are searched. It is mentioned that security is of great importance for WSNs because of the mission-critical tasks achieved by them. It is specifically stressed that the biggest constraint in WSNs is the energy and lifetime of the network is completely dependent on the batteries. Since preventive measures will fail eventually due to the inherent vulnerabilities in WSNs, intrusion detection systems (IDSs) as a second line of defense are investigated. After studying the methods proposed to detect the attacks against WSNs in the literature comprehensively, it is concluded that traditional IDS methods cannot be used directly for WSNs because of their characteristics. It is also seen that novel methods are required to timely detect and notify the attacks. In this respect, a novel hybrid IDS based on trust and misuse detection is proposed. The validation and performance analysis of the proposed system is accomplished using Castalia Framework simulator based on OMNET++. It is hoped that this thesis will help the academicians understand the security issues and intrusion detection systems for WSNs.

Science Code : 92403
Key Words : Wireless sensor network, cyber security, intrusion detection system, Castalia Framework.
Page Number : 101
Supervisor : Assoc. Prof. Erdal IRMAK

TEŞEKKÜR

Çalışmalarım boyunca değerli katkılarını, yardımlarını esirgemeyen, tecrübesini ve ilmini cömertçe aktarmaya çalışan değerli tez danışmanım Doç. Dr. Erdal IRMAK hocama; tez sürecinde yoğun mesai programına rağmen her fırsatta beni dinleyen, yolumu aydınlatan ve büyük destek sağlayan Doç.Dr. Suat ÖZDEMİR hocama teşekkürü bir borç bilirim.

Ayrıca; başarılı olmam için desteğini hiçbir zaman esirgemeyen, yaşantıma renk katan, sırdaşım, yoldaşım, hayat arkadaşım ve değerli eşim Neslihan ÖZÇELİK ile hayatıma anlam veren, gözümün nuru, biricik kızım Nisa ÖZÇELİK'e şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

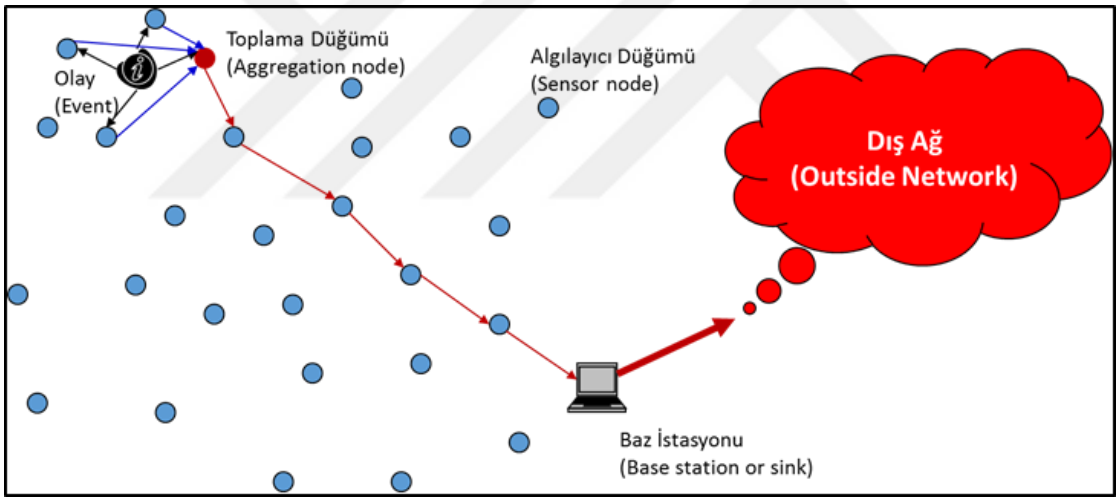
Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BAN	Vücut Alan Ağı (Body Area Network)
BS	Baz İstasyonu (Base Station)
CA	Sertifika Otoritesi (Certificate Authority)
CH	Küme Başı (Cluster Head)
CP	Kontrol Paketi (Control Packet)
CPU	Merkezi İşlem Birimi (Central Processing Unit)
CTV	Birleştirilmiş Güven Değeri (Consolidated Trust Values)
DoS	Servis Dışı Bırakma (Denial of Service)
DDoS	Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
ECC	Eliptik Eğri Kriptografisi (Eliptic Curve Cryptograhy)
FHSS	Frekans Atlamalı Geniş Spektrum (Frequency-Hopping Spread Spectrum)
FRT	Fonksiyonel itibar Tablosu (Functional Reputation Table)
GEAR	Coğrafi Enerji Haberdar Yönlendirme (Geographical Energy Aware Routing)
GTMS	Grup Tabanlı Güven Yönetim Sistemi (Grouped Based Trust Management System)
HIDS	Uç Nokta Tabanlı Saldırı Tespit Sistemi (Host-Based Intrusion Detection System)
KAA	Kablosuz Algılayıcı Ağ
IDS	Saldırı Tespit Sistemi (Intrusion Detection System)

Kısaltmalar	Açıklamalar
IoT	Nesnelerin İnterneti (Internet of things)
IP	İnternet Protokolü (Internet Protocol)
IPS	Saldırı Önleme Sistemi (Intrusion Prevention System)
MAC	Ortam Erişim Kontrolü (Medium Access Control)
MAC	Mesaj Kimlik Doğrulama Kodu (Message Authentication Code)
MITM	Araya Girme Saldırısı (Man-in-the-Middle Attack)
NIDS	Ağ Tabanlı Saldırı Tespit Sistemi (Network-Based Intrusion Detection System)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
OMNET	Nesne Tabanlı Modüler Ayrık Olay Ağ Benzetim Çerçevesi (Object-oriented Modular Discrete Event Network Simulation Framework)
RAM	Rasgele Erişim Belleği (Random Access Memory)
RSA	Ron Rivest, Adi Shamir ve Leonard Adleman
TET	Güven Değerlendirme Tablosu (Trust Evaluation Table)
TCP	Aktarma Kontrol Protokolü (Transmission Control Protocol)
TDMA	Zaman Bölmeli Çoklama (Time Division Multiplexing)
UML	Birleştirilmiş Modelleme Dili (Unified Modelling Language)
WSN	Kablosuz Algılayıcı Ağ (Wireless Sensor Network)

1. GİRİŞ

Kablosuz algılayıcı ağlar (KAA'lar), fiziksel dünyadaki olayları algılayabilme, tespit edilen olaylar hakkında matematiksel bir takım işlemler yapabilme ve komşu diğer ağ elemanları ile haberleşebilme yeteneklerine sahip yüzlerce hatta bazen binlerce küçük cihazlardan oluşabilen özel bir ağ türüdür [1]. KAA'larda kullanılan cihazlar düğüm olarak tanımlanmaktadır. Mekânsal olarak dağıtık bulunan otonom düğümler sıcaklık, ses, basınç vb. fiziksel veya çevresel olayları algılamakta ve elde edilen veriler düğümlerin arasındaki iş birliği sayesinde merkezi bir noktaya aktarılmaktadır. Bu merkezi nokta düğümlere oranla daha karmaşık işlemler yapabilme yeteneğine sahip, daha büyük bant genişliği olan ve daha uzak mesafeler ile haberleşebilen baz istasyonudur (BS). Tipik bir KAA mimarisi Şekil 1.1'de görülmektedir.



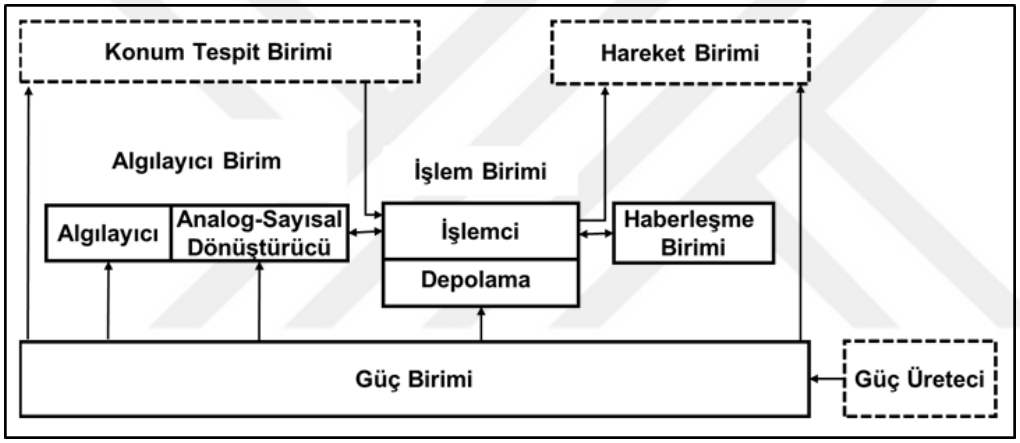
Şekil 1.1. Tipik bir kablosuz algılayıcı ağ mimarisi

Şekil 1.1'den de görüleceği üzere düğümler genellikle görev yapılacak bölgeye sayıca bol miktarda yerleştirilmekte ve aynı fiziksel olay birden fazla düğüm tarafından algılanabilmektedir. Ayrıca her düğümün elde ettiği veriler enerji verimliliği sağlamak, bant genişliğini daha etkin kullanmak, ağ içerisindeki trafiği azaltmak ve bu sayede ağ ömrünü uzatmak maksadıyla birleştirilmekte ve veri kümelemesi (data aggregation) işlemi uygulanabilmektedir. KAA'larda veri kümelemesi işleminin uygulanması gerekliliği yapılan birçok bilimsel çalışmada ortaya konmuştur [2–5].

KAA'larda kullanılan düğümler dört temel bileşenden meydana gelmektedir [1]. Bunlar;

- Algılama birimi,
- İşlem birimi,
- Haberleşme birimi,
- Güç birimidir.

Ayrıca bu birimlere ilave olarak icra edilecek görevin özelliğine göre konum tespit birimi ve hareket birimi gibi üniteler de ilave edilebilmektedir. KAA'larda kullanılan düğümlerin temel bileşenleri Şekil 1.2'de görülmektedir.



Şekil 1.2. KAA'larda kullanılan düğümün temel bileşenleri

Algılayıcı birim; genellikle algılayıcı cihazlardan ve analog-sayısal dönüştürücülerden meydana gelmektedir. Fiziksel olaylar neticesinde üretilen analog sinyaller sayısala dönüştürülerek işlem birimine iletilmektedir.

İşlem birimi; düğümün verilen vazifeyi yerine getirmesi için gerekli olan hesaplamalar ve diğer düğümlerle olan iş birliğinin yönetilmesinden sorumludur. Çoğunlukla küçük bir depolama birimi ile ilişkilendirilmektedir.

Haberleşme birimi; düğümün ağa bağlanmasını, diğer ağ elemanları ile irtibat kurmasını sağlayan birimdir. Genellikle alma-gönderme birimleri olan kablosuz haberleşme elemanlarından oluşmaktadır.

Güç birimi; düğümün çalışması için gerekli olan enerjiyi sağlayan birimdir. Birçok durumda iki adet AA pil kullanılmaktadır.

Konum tespit birimi; yüksek hassasiyet derecesinde konum verisinin gerekli olduğu yönlendirme protokolleri ve algılama görevlerinde kullanılmaktadır.

Hareket birimi; düğümlerin hareket edebilir olması gereken durumlarda kullanılmaktadır. Görevin niteliğine ve kritikliğine göre ilave bileşenlerin eklenmesi enerji ve hesaplama ihtiyacı ile düğüm maliyetinde artışa neden olmaktadır. Ayrıca kullanılan bileşenler düğümlerin boyutlarını etkilemektedir. Kullanılan düğümlerin boyutları küçük bir elbise düğmesinden ayakkabı kutusu büyüklüğüne varıncaya kadar değişen ebatlarda olabilmektedir [6].

Kablosuz algılayıcı ağların çok farklı alanlarda uygulamaları mevcuttur. Bu uygulamalardan bazıları şöyledir [6];

1) Dost kuvvetlerin teçhizat ve cephanesinin izlenmesi, savaş alanının gözlenmesi, arazi hakkında keşifte bulunma, hedefin konumu, sürati gibi hedef bilgilerinin tespiti, düşmana verdirilen hasar miktarının tespit edilmesi, nükleer, biyolojik ve kimyasal (NBC) saldırı ihbarının alınması ya da keşfi gibi *askeri uygulamalar*,

2) İnsanların fiziksel durumlarının uzaktan izlenmesi, hasta ve doktorların hastane içinde takip edilmesi, uyuşturucu ile mücadelede kullanım gibi *sağlık uygulamaları*,

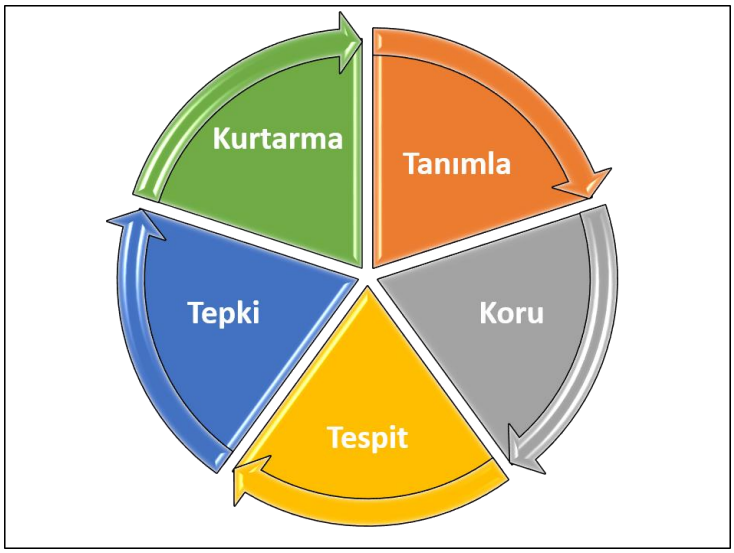
3) Orman yangını, sel, deprem gibi doğal afetlerin hızlı ve doğru bir şekilde ihbar edilmesi, hava kirliliği tespiti ve ayrıntılı rapor alınması, doğal yaşamın gözlenmesi gibi *çevresel uygulamalar,*

4) Ev ve ofis otomasyonu, akıllı ev uygulamaları gibi *ev ve ofis uygulamaları*,

5) İnteraktif müzeler, araç hızlarının fark edilmesi ve yakalanması, malzeme döküm tespiti uygulamaları, araç takip sistemi uygulamaları ve otomotiv sektörü uygulamaları gibi *diğer bazı uygulama* alanları bulunmaktadır.

Yukarıda ifade edildiği gibi son derece geniş uygulama alanına sahip kablosuz algılayıcı ağlar maliyetlerin de ucuzlaması ile oldukça yaygınlaşmıştır. Ayrıca KAA'lar birçok görev kritik işlemleri gerçekleştirmek maksadıyla kullanılmakta ve bu nedenle *kritik alt yapı* olarak değerlendirilmektedir.

Kritik alt yapıların siber güvenlik seviyesini artırmak maksadıyla herkes tarafından kabul edilecek ve ortak akıl neticesinde geliştirilmiş yöntemlerin kullanılmasına ihtiyaç vardır. Amerikan hükümetinin desteği ve çeşitli sivil toplum kuruluşlarının katkılarıyla kritik alt yapıların siber güvenliğini artırmak maksadıyla hazırlanan *NIST Kritik Alt Yapı Siber Güvenliğinin Geliştirilmesine Yönelik Çerçeve* (*The NIST Framework for Improving Critical Infrastructure Cybersecurity*) dokümanı [7] ortak bir aklın ürünüdür. Bu dokümana göre kritik bir alt yapının siber güvenliğini artırmak ancak iyi tanımlanmış bir süreç neticesinde gerçekleşebilir. Bunun için uygulanması gereken beş temel fonksiyon ise Şekil 1.3'te görülen *tanımla, koru, tespit, tepki* ve *kurtarma*dır. Burada tanımlanan fonksiyonlar, sürekli takip ve kontrol ile uygun şekilde gerçekleştirilirse kritik alt yapılara yönelik siber saldırıları azaltacaktır.



Şekil 1.3. Kritik alt yapı siber güvenlik fonksiyonları

Söz konusu çerçevede belirtilen;

- *Tanımla fonksiyonu* sistemlerin, varlıkların, verinin ve yeteneklerin belirlenmesini ve korunacak değerlerin ortaya konmasını ifade etmektedir.
- *Koru fonksiyonu* değerli hizmetlerin aksamadan yürütülmesi için gerekli olan tedbirlerin alınmasını ve bunun için gerekli olan koruyucu tedbirleri kapsamaktadır.
- *Tespit fonksiyonu* siber ortamdaki koruyucu tedbirlerin yetersiz kalması durumunda kritik alt yapılara yönelik saldırılardan haberdar olunmasını, saldırganlar tarafından yürütülmekte olan bir saldırının tespit edilmesini kapsamaktadır.
- *Tepki fonksiyonu* tespit edilen saldırı veya siber olaylara karşılık verilmesini belirtmektedir.
- *Kurtarma fonksiyonu* ise yaşanan saldırı veya siber olaylardan sonra sistemlerin normale döndürülmesini, tekrardan hedeflenen hizmetlerin verilmesi için yapılması gerekenleri ve olaylarla ilgili alınan derslerin ortaya konmasını ifade etmektedir.

Özetle, değerli varlıklar tanımlanmalı ve bunların korunması için gerekli tedbirler alınmalı, alınan tedbirler yetersiz kalıyorsa var olan saldırı veya siber olay tespit edilmeli ve derhâl bir tepki göstermek suretiyle saldırıların önlenmesi sağlanmalı, müteakiben sistemler normale döndürülmeli ve yaşanan her saldırı veya siber olaydan sonra alınan dersler belirlenmelidir.

Bu tez çalışmasında, KAA'lara yönelik siber güvenlik değerlendirmesi yapılırken söz konusu dokümandaki yaklaşım göz önünde bulundurulmuştur. Öncelikli olarak KAA'ların karakteristik özellikleri ile bu özel ağ türüne yönelik tehditler ve saldırılar tanımlanmıştır. Sistemlerin korunması için gerekli olan koruyucu tedbirlerin KAA'ların doğasında bulunan zafiyetler nedeniyle yetersiz kalacağının görülmesi üzerine, tez çalışması saldırı tespit sistemleri üzerine odaklanmış ve saldırıları tespit edecek özgün bir saldırı tespit sistemi önerilmiştir.

2. MATERYAL VE METOD

Bu tez çalışmasında, siber güvenlik alanında ortak aklın ürünü olan ve konusunda uzman kişilerin katkı sağladığı NIST kritik alt yapı siber güvenliğin geliştirilmesine yönelik çerçeve dokümanında [7] belirtilen yöntem rehber olarak alınmış ve özel bir kablosuz ağ türü olan KAA'ların siber güvenlik değerlendirmesi için;

- KAA'lardaki kısıtlar ve karakteristik özellikler tanımlanmış,
- KAA'lara yönelik tehditler ve bu tehditlerden korunma yöntemleri için önerilen yöntemler incelenmiş,
- KAA'ların doğasında bulunan zafiyetler ve açıklıklar nedeniyle koruyucu tedbirlerin yetersiz kalacağı değerlendirilmiş,
- Koruyucu tedbirleri tamamlayıcı ikinci bir savunma hattı olarak değerlendirilen saldırı tespit sistemleri üzerine odaklanılmış ve KAA'lar için önerilen mevcut saldırı tespit yöntemleri incelenmiş,
- KAA'lar için güven ve kötüye kullanım yaklaşımlarının beraber kullanıldığı özgün bir saldırı tespit sistemi önerilmiş,
- Önerilen sistemin geçerlilik ve performans analizi OMNET++ [8] tabanlı Castalia Framework [9] benzetim programı vasıtasıyla yapılmıştır.

Çalışmanın KAA'larda güvenlik ve saldırı tespit sistemleri konularında araştırmalar yapanlara katkı sağlayacağı kıymetlendirilmektedir.

3. KABLOSUZ ALGILAYICI AĞLARDA SİBER GÜVENLİK

KAA'lar teknolojik ürünlerdeki ucuzlamaya paralel olarak yaygınlaşmış, uygulama alanları genişlemiş ve söz konusu ağların görev kritik işlemlerde kullanılması artmıştır. Günümüzde birkaç dolar maliyetle üretilen düğümleri piyasadan temin etmek mümkün hale gelmiştir. KAA'larda işlenen, saklanan ve işlem gören verinin hassaslığı ile fiziksel olarak düğümlerin kolaylıkla ele geçirilebilir olması bu özel kablosuz ağ türüne yönelik saldırıları artırmaktadır. Bu nedenle KAA'lara yönelik saldırıları azaltmak maksadıyla güvenlik tedbirleri alınmakta ve her geçen gün yeni çıkan saldırı vektörlerine karşın söz konusu tedbirler geliştirilmektedir. Tez çalışmasının bu bölümünde KAA'ların güvenliği konusu detaylı olarak incelenmiştir.

3.1. Kısıtlar

KAA'ların yanardağ faaliyetlerinin izlenmesi gibi fiziksel olarak erişimin mümkün olmadığı durumlarda veya düşman hareketlerinin takip edilmesi gibi askeri uygulamalarda olduğu gibi *at-unut* mantığıyla çalışması gerekebilmektedir. Düğümlerin bir defa yerleştirildikten sonra tekrardan toplanamaması ve görev yapılacak bölgeye sayıca çok fazla miktarda yerleştirilmesi nedeniyle mümkün olduğunca ucuz olması hedeflenir. Düğümlerin ucuza üretilmesi gereksinimi depolama kapasitesi, hesaplama yeteneği, algılama becerisi, algılama menzili, haberleşme mesafesi ve bant genişliği açısından oldukça kısıtlı özellikleri olan cihazların üretilmesine neden olmaktadır [10]. Bununla birlikte genel olarak KAA'lardaki temel kısıtlar aşağıda açıklanmıştır.

Enerji: KAA'lardaki *en büyük sorun son derece enerji kısıtlı olmalarıdır* [11]. Çoğunlukla kullanılan enerji kaynağının iki adet AA pilden oluşması düğüm ömrünü belirleyen en önemli etkendir. Pillerin şarj edilmesi veya bittiğinde değiştirilmesi, düğümlerin zorlu arazilere veya düşman hatlarına yerleştirilmesi gibi durumlarda mümkün olamamaktadır. Her ne kadar güneş panelleri veya şarj ünitesi bulunan düğümler yapılan çeşitli çalışmalarda [9-11] önerilmiş olsa da hem maliyetlerin artması hem de görev yapılacak alanların her zaman güneş ışığı almaya müsait olmaması gibi nedenlerle bu önerilerin geliştirilmeye ihtiyacı olduğu değerlendirilmektedir.

Düğümler için üç temel enerji tüketim kaynağı bulunmaktadır. Bunlar;

- Analog sinyallerin dijitale dönüştürülmesinde enerji tüketimi,
- Düğümler arası haberleşmede enerji tüketimi,
- Hesaplamaların yapılabilmesi için işlemci tarafından harcanan enerji tüketimidir.

Bu kaynaklar arasındaki en büyük enerji tüketimi *düğümler arası haberleşmede* meydana gelmektedir. Enerji açısından son derece sınırlı bir yapıya sahip olan düğümlere güvenlik mekanizmalarının eklenmesi enerji tüketimini artırmaktadır. Bununla birlikte güvenlik mekanizmalarının olmaması kaynakların tüketilmesine yönelik saldırıların kolaylıkla gerçekleştirilebilmesine neden olmaktadır. Ayrıca kriptografik çözümlerin çoğunlukla fazla enerji tüketimi gerektirmeleri KAA'larda yüksek güvenlik çözümlerinin uygulanamamasına neden olmaktadır. Bu nedenle KAA'lar için önerilecek güvenlik çözümlerinin öncelikle enerji tüketimi açısından ilave yük getirmeyen çözümler olması gerekmektedir.

Hafıza: Algılayıcı düğümler kısıtlı bir hafıza ve depolama kapasitesine sahip çok küçük cihazlardır. Hafıza genellikle anlık bellek (flash memory) ve rastgele erişim belleğinden (RAM) oluşmaktadır. Anlık bellek yüklenen uygulama kodları için kullanılmakta, RAM ise uygulama programlarının, algılayıcı verisi ve ara hesaplama değerlerinin saklanmasında kullanılmaktadır. Çoğunlukla işletim sisteminin ve algılayıcı programların yüklenmesinden sonra karmaşık algoritmaların çalışabileceği yeterli hafıza düğümlerde kalmamaktadır. Bu nedenle mevcut güvenlik algoritmalarının KAA'lara doğrudan uygulanabilmesi mümkün değildir.

Güvensiz Haberleşme: Algılayıcı ağlardaki paket tabanlı yönlendirme doğal olarak bağlantısız protokollere (connectionless protocols) dayanmakta ve neticede güvenilir olmayan haberleşmenin ortaya çıkmasına neden olmaktadır. Kanaldaki hatalar ve paket kayıpları nedeniyle düğümlerde tıkanıklıklar meydana gelebilmektedir. Dahası, güvenilir olmayan kablosuz haberleşme kanalı da paketlerin bozulmasına veya zarar görmesine neden olabilmektedir. Yüksek hata oranları güçlü hata tespit mekanizmalarının kullanılmasını gerekli kılmakta, bu durum ise düğümlerdeki ilave yükü (overhead)

artırmaktadır. Bazı durumlarda kanal güvenilir olsa bile, haberleşme güvenilir olmayabilir. Bu durum kablosuz haberleşmenin doğasındaki radyo yayını (broadcast) yapma özelliğinden kaynaklanmaktadır. Ağ üzerinden paketler gönderilirken çarpışmalar olabilir ve tekrar gönderim gerekebilir [1].

Haberleşmedeki Yüksek Gecikme: Çok sıçramalı yönlendirme (multihop routing), ağ tıkanıklıkları (network congestion) ve ara düğümlerdeki işlemler paketlerin iletilmesinde yüksek gecikmelerin yaşanmasına neden olabilmektedir. Bu durum senkronizasyonun sağlanmasını oldukça güçleştirmektedir. Senkronizasyon özellikle kritik olayların raporlanması ve şifreleme anahtarlarının dağıtılması gibi bazı güvenlik mekanizmaları için hayati öneme sahiptir.

Ağların Gözetimsiz Çalışması: Birçok durumda KAA'lardaki düğümler fiziksel olarak erişimin kolay olmadığı bölgelere yerleştirilmekte ve ağ elemanlarının gözetimsiz (unattended operation of networks) olarak çalışması beklenmektedir. Bu nedenle düğümlerin fiziksel saldırılara maruz kalma olasılığı oldukça yüksektir. KAA elemanlarının fiziksel olarak bir saldırıya maruz kalıp kalmadığının anlaşılması örneğin saldırganlar tarafından ele geçirilip geçirilmediğinin tespitini uzaktan yapabilmek neredeyse imkânsızdır. Bu durum KAA'larda güvenliğin sağlanmasını zorlaştıran bir diğer kısıttır.

3.2. Güvenlik Gereksinimleri

KAA'ların geleneksel bilgisayar ağları ile birçok benzerlikleri olduğu gibi birtakım farklılıkları, kendine has özellikleri de bulunmaktadır. KAA'lardaki en temel güvenlik gereksinimi; ağ üzerinden iletilen verinin ve ağ kaynaklarının saldırılara karşı korunması ile normal dışı davranışlar sergileyen düğümlerin tespit edilebilmesidir. Bu temel gereksinimi sağlamak maksadıyla KAA'larda gerçekleştirilmesi gereken en önemli güvenlik gereksinimleri aşağıda listelenmiştir [14]:

Veri gizliliği (Data confidentiality): KAA'lardaki güvenlik mekanizmaları ağdaki mesajların yetkisiz kullanıcı ve düğümler tarafından anlaşılmasını engellemelidir. Veri gizliliğinin sağlaması gereken üç temel gereksinim şunlardır:

- Bir düğüm yetki verilmemiş komşu diğer düğümlerin kendi algılama verisine erişmesini engellemelidir.
- Anahtar dağıtım mekanizmaları hatalara ve saldırılara karşı son derece sağlam olmalıdır.
- Trafik analizi saldırılarını engellemek maksadıyla algılayıcı kimlik bilgisi ve açık anahtar gibi tüm ağ elemanları tarafından bilinen açık veriler özel durumlarda şifrelenebilmelidir.

Veri bütünlüğü (Data integrity): Göndericiden alıcıya giden mesajların yetkisiz bir şekilde değiştirilmesinin engellenmesini ifade eden gereksinimdir.

Erişilebilirlik (Availability): Ağın içinden veya dışından gelebilecek her türlü saldırı durumlarında bile hizmetin aksamadan yürütülebilmesini ve ağın verilen görevi yapmaya devam edebilmesini ifade eden gereksinimdir. Bu gereksinimin sağlanabilmesi maksadıyla literatürde iki temel yaklaşım önerilmektedir. Birinci yaklaşım düğümler arasında ilave haberleşme metotlarının uygulanmasıdır. İkinci yaklaşım ise gönderenin alıcı tarafından yollanan mesajı başarılı bir şekilde aldığını anlaması için merkezi erişim kontrol sisteminin uygulanmasıdır.

Veri tazeliği (Data freshness): Herhangi bir düğüm tarafından gönderilen algılama verisinin güncel olmasını ve araya girecek saldırganların bu mesajları yeniden göndermesi durumunda bunun fark edilebilmesini ifade eden gereksinimdir. Bu gereksinim KAA'lar için son derece önemlidir. Örneğin sıcaklık verisinin kritik olduğu bir tesisi gözetleyen düğümlerdeki veriler güncel değilse veya araya giren saldırgan önceden kaydettiği verileri yeniden yollayabiliyor ve bu durum tespit edilemiyorsa görev kritik işlerin başarılması mümkün olmayacaktır. Ayrıca ağ genelinde aynı şifreleme anahtarının kullanılması durumunda bu gereksinim daha da önemli hale gelmektedir. Tekrarlama saldırılarına karşı

rastgele bir değer (nonce) veya zaman bilgisi içeren bir sayaç kullanılarak koruma sağlanabilir.

Kendi kendine organize olma ve sorunları giderme (self-organization and self healing): KAA'lardaki her düğüm kendi kendine organize olabilme ve sorunları giderebilme özelliklerine sahip olmalıdır. Bu özellik güvenlik açısından oldukça büyük sorunların ortaya çıkmasına neden olmaktadır. KAA'ların doğasındaki dinamiklik bazen düğümlere ve baz istasyonuna önceden şifrelerin yüklenmesini imkansız hale getirir. Simetrik şifrelemenin kullanılması durumunda anahtarların önceden yüklenmesi tercih edilen bir yöntemdir. Ancak açık anahtar şifrelemesi için anahtar dağıtımı bir zorunluluktur. Düğümlerin kendi aralarında sadece çok sıçramalı yönlendirme için organize olması değil aynı zamanda anahtar yönetimi ve güven ilişkilerinin geliştirilmesini sağlaması da istenmektedir.

Güvenli yer tayini (Secure localization): Birçok durumda düğümlerin yerinin kesin olarak tayin edilmesi son derece önemli bir gereksinimdir. Örneğin, orman yangınlarını takip etmek için yerleştirilen bir KAA'da algılama işlemini yapan düğümün, dolayısıyla yangının yerinin belirlenmesi son derece önemlidir. Kötü niyetli saldırgan yanlış sinyal gücü yollamak ve önceden kaydedilen mesajları tekrar göndermek gibi yöntemler ile hatalı konum bilgisinin baz istasyonuna gönderilmesine sebep olabilir. Güvenli yer tayini işlemi genel olarak mesafe tabanlı (range-based) veya mesafeden bağımsız (range-free) olarak yapılmaktadır. Mesafe tabanlı yer tayini metodunda düğümlerin birbirine olan uzaklıkları ve düğümlerin konumu önceden bilinen çapa düğümlere (anchor nodes) olan uzaklıkları kullanılarak yer tayini yapılmaktadır. Mesafeden bağımsız yer tayin metodunda ise yeterli miktarda işaretçi düğümün (beacon node) ağ içerisine yerleştirilmesi ve bu çapa düğümlerinin periyodik olarak yayın yapması sayesinde düğümlerin konumu hakkında tahmin yapabilmek hedeflenmektedir.

Zaman eşlemesi (Time synchronization): Algılayıcı ağlardaki uygulamaların çoğu, zaman eşlemesini gerektirmektedir. Ayrıca KAA'lar için geliştirilecek güvenlik mekanizmaları da zaman eşlemesini mutlaka sağlamalıdır. Zaman eşlemesine yönelik çalışmalarda güvenli zaman eşlemesi sağlayan protokoller geliştirilmiştir [15].

Kimlik doğrulama (Authentication): KAA'larda haberleşen düğümlerin kimlik bilgilerinin doğrulanmasını ifade eden gereksinimdir. Bir alıcı düğüm kendisine gelen paketlere gönderenin kimliğini doğruladıktan sonra işlem yapmalıdır. Çünkü saldırganlar paketleri değiştirebilir ve yanlış paketleri ağa gönderebilir. İki düğüm arasındaki haberleşme esnasında, verinin aslına uygunluğunun doğrulanması düğümler arasında önceden paylaşılan gizli anahtarlar kullanılarak oluşturulan *mesaj kimlik kodu (MAC)* ile yapılmaktadır. KAA'lar için önerilen kimlik doğrulama mekanizmalarının çoğu güvenli yönlendirme işlemini gerçekleştirmek maksadıyla önerilmiştir.

3.3. Protokol Yığını

KAA'larda kullanılan protokol yığını geleneksel bilgisayar ağlarında kullanılan TCP/IP yığınına benzemektedir ve şu katmanlardan oluşmaktadır [1]: Uygulama katmanı, taşıma katmanı, ağ katmanı, veri bağlantı katmanı ve fiziksel katman. Bu katmanların görevleri özetle şöyledir:

Fiziksel katman frekans seçimi, taşıyıcı frekans üretimi, sinyal tespiti, modülasyon ve veri şifrelemesinden sorumlu olan katmandır.

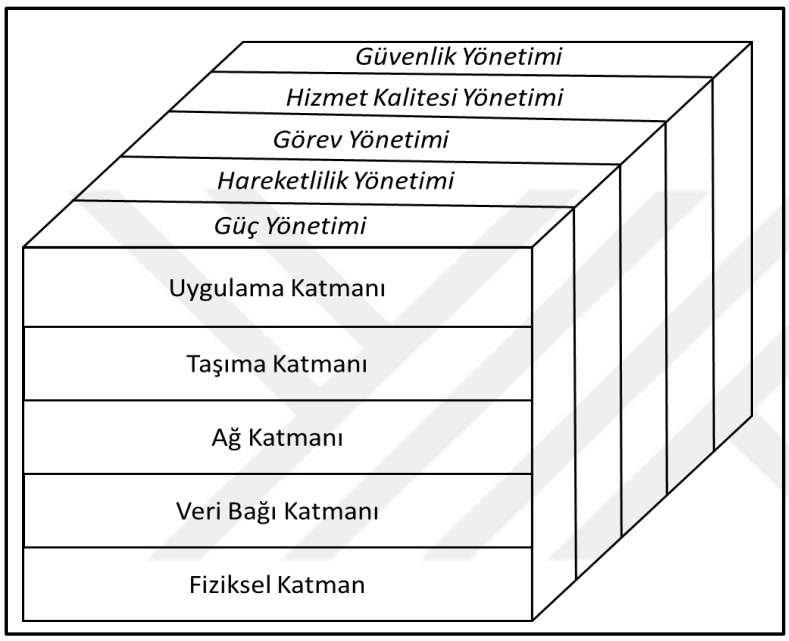
Veri bağlantı katmanı veri akışlarının çoklanması, veri çerçevesi tespiti, ortam erişimi ve hata kontrolünden sorumlu olan katmandır. Ayrıca haberleşme ağı içerisindeki noktadan noktaya ve tek noktadan çok noktaya güvenilir bağlantı yapılmasını sağlar.

Ağ katmanı taşıma katmanından gelen verinin yönlendirilmesinden sorumlu olan katmandır. Ağ katmanı tasarlanırken güç verimliliği, veri merkezli haberleşme, veri kümelemesi gibi KAA'lara özgü gereksinimler göz önünde bulundurulmalıdır.

Taşıma katmanı veri akış kontrolünün sağlanmasına yardım eden katmandır. Ağ katmanı KAA'ların internete veya başka bir dış ağa bağlanması durumunda daha da önem kazanmaktadır.

Uygulama katmanı algılama görevlerine göre farklılık gösteren uygulamaları barındıran katmandır.

Akyildiz ve arkadaşları [1] tarafından ortaya konan KAA'lardaki haberleşme protokol yığını Wang ve arkadaşları [16] tarafından Şekil 3.1'de görüldüğü gibi geliştirilmiş ve var olan katmanlara yeni düzlemlerin eklenmesi gerektiği ortaya konmuştur.



Şekil 3.1. Haberleşme protokol yığını [16]

KAA'lardaki özel gereksinimler nedeniyle eklenen yeni düzlemlerden:

Güç yönetim düzlemi, düğümlerdeki enerji tüketiminin asgari seviyeye indirilmesinden ve enerji tasarrufu sağlamak için düğümlerin uyuma ve kapanma durumuna geçmesinden sorumludur.

Hareketlilik yönetimi düzlemi, düğümlerin hareketli olması durumunda verilerin baz istasyonuna her zaman uygun bir şekilde iletilmesinden sorumlu olan düzlemdir.

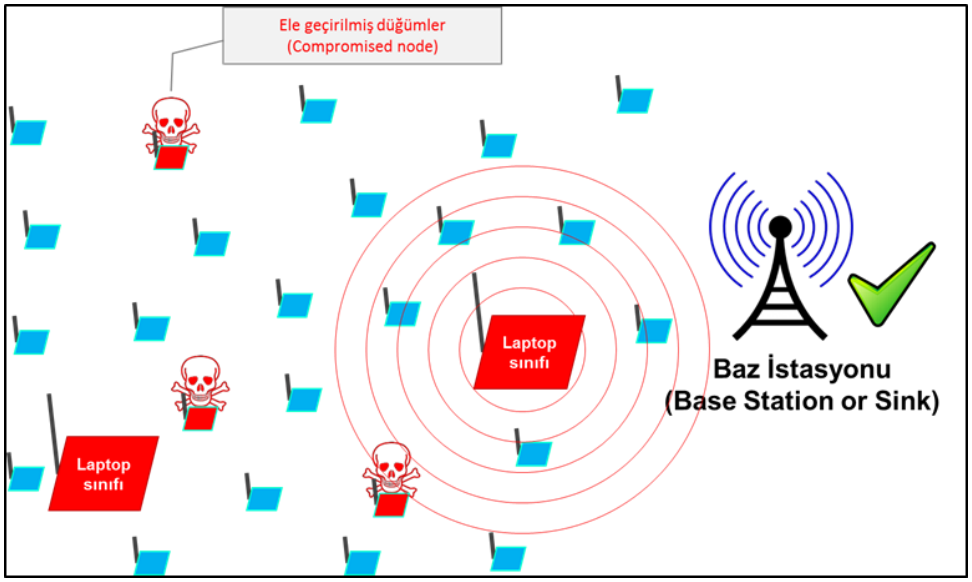
Görev yönetimi düzlemi, algılama işlerini dengeli bir şekilde dağıtarak ve zamanlama yaparak sadece ilgili düğümlerin işlem yapmasını, diğer düğümlerin ise yönlendirme ve veri kümeleme gibi başka faaliyetlere odaklanmasını sağlamaktadır.

Hizmet kalitesi düzlemi, özellikle gerçek zamanlı algılama gereksinimi mevcut ise önem kazanmaktadır. Ayrıca bu düzlem hizmet kalitesi ölçüleri olan hata toleransı, hata kontrolü ve performansın en iyi duruma getirilmesi gibi konularla ilgilenmektedir.

Güvenlik yönetimi düzleminde ise ağdaki güvenlikle alakalı hareketlerin yönetilmesi, izlenmesi ve kontrolü işlemleri gerçekleştirilmektedir. Güvenlik yönetiminin en temel görevi kritik veya hassas verilere olan erişim noktalarının kontrol edilmesidir. Ayrıca bu düzlem şifreleme, kimlik doğrulama ve saldırı tespiti gibi farklı güvenlik bileşenlerinin aksaksız bir şekilde uyumundan da sorumludur.

3.4. Saldırılar

Kablosuz ağların özel bir türü olan KAA'lar, kablosuz ağların maruz kaldığı tüm saldırılara karşı hassastır. Ayrıca KAA'lara özgü bir takım özellikler nedeniyle, [17]'deki çalışmada bu sistemlere özgü saldırılar *Algılayıcı düğüm sınıfı (node class)* ve *Laptop sınıfı (Laptop class)* saldırılar olarak ikiye ayrılmıştır. Şekil 3.2'te KAA'lara özgü bu iki saldırı gösterilmektedir.



Şekil 3.2. Algılayıcı düğüm ve laptop sınıfı saldırılar

Algılayıcı düğüm sınıfı saldırılarda, saldırganlar birkaç düğümü ele geçirmekte ve normal düğümlerin yetenekleri oranında saldırılar gerçekleştirmektedir. Saldırılarda kullanılan

düğümlerin kapasiteleri ve yetenekleri normal düğümlerden daha üstün değildir. Bu nedenle saldırganlar ele geçirdikleri düğümlerin depolama, hesaplama ve bant genişliği gibi kısıtlı olan kaynaklarını tüketmeden saldırılarını gerçekleştirmek durumundadır. Ayrıca saldırganların kapsama alanları, ele geçirdikleri düğümlerin kapsama alanları ile sınırlıdır.

Laptop sınıfı saldırılarda ise saldırganlar kaynak açısından sorun yaşamamakta, yüksek iletim gücü, daha uzun batarya ömrü, hızlı işlemciler ve tüm yönlerden algılama yapabilen anten kullanımı yeteneğine sahip olabilmektedir. Böylelikle daha geniş kapsama alanına sahip ve daha karmaşık saldırılar gerçekleştirilebilmektedir.

KAA'lara yönelik siber saldırıları genel olarak pasif ve aktif saldırılar olarak ikiye ayırmak mümkündür.

Pasif Saldırılar

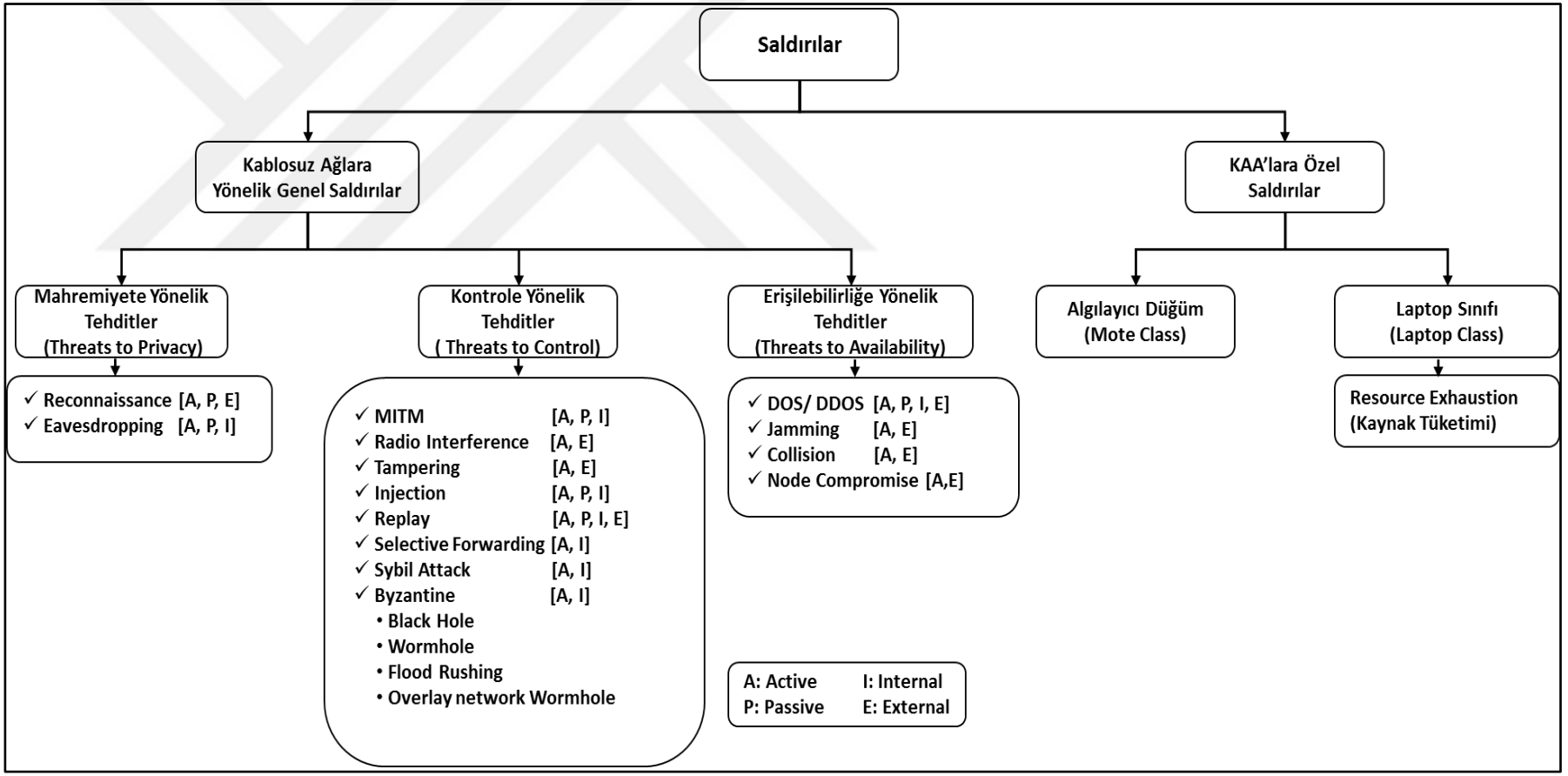
Bu tür saldırılarda, saldırganın düğümler arasındaki haberleşmeyi izleme ve gönderilen verilere ulaşabilme imkânı vardır. Ancak düğümler tarafından kötü niyetli davranışlarının fark edilmemesi amacıyla paketlerde herhangi bir değişlik veya oynama yapmaz. Örneğin, saldırgan trafik analizi yaparak şifreli olarak gönderilen paketleri çözebilir, paketlerin başlık, büyüklük ve gönderim sıklığı gibi verileri analiz ederek kendisi açısından faydalı olacak bilgilere ulaşabilir. Ayrıca keşif saldırılarını (reconnaissance) başta veri kümeleme noktalarındaki haberleşme olmak üzere, düğümler arasındaki gönderilen ve alınan mesajların öğrenilmesi amacıyla gerçekleştirir. Bunun yanında yine trafik analizi ile yönlendirme bilgileri açığa çıkarılabilir.

Aktif Saldırılar

Bu tür saldırılarda, saldırgan aktif bir şekilde haberleşmedeki tüm işlemlere müdahale edebilmektedir. Saldırgan mesajları değiştirebilir, silebilir, sırasını değiştirebilir veya önceden kaydedilen mesajları yeniden gönderebilir. Ayrıca ağdaki düğümlere kendisinin ürettiği sahte mesajları gönderebilir. Bazı aktif saldırılarda ise düğümlerin çalınması/ele

geçirilmesi, yönlendirme bilgisinin değiştirilmesi ve kaynakların tüketilmesi gibi hedefler yer almaktadır. Ayrıca KAA'lara özgü olarak, saldırgan algılama işleminin yapıldığı ortamı değiştirmek suretiyle algılayıcıların yanlış fiziksel olayları rapor etmesini sağlayabilir.

Literatürde KAA'lara yönelik saldırıların birçok sınıflandırılması mevcut olsa da [18]'de yapılan ve Şekil 3.3'te görülen sınıflandırmanın kapsayıcılık açısından uygun olduğu değerlendirilmiştir. Ayrıca saldırıların kullanılan haberleşme protokol yığınındaki katmanlara göre sınıflandırılması da yine literatürde kullanılan bir yöntemdir ve Çizelge 3.1'de görülmektedir [14, 17].



Şekil 3.3. KAA'lara ağlara yönelik saldırıların sınıflandırılması [18]

Çizelge 3.1. Katmanlı yaklaşım kullanılarak saldırıların sınıflandırılması

Katmanlar	Saldırılar
Fiziksel Katman	Karıştırma (Jamming) Kurcalama (Tampering)
Veri Bağlantı Katmanı	Çarpışma (Collision) Kaynak Tüketme (Exhaustion) Adaletsizlik (Unfairness)
Ağ Katmanı	Yönlendirme Bilgisinin Kandırılması ve Seçilen Paketlerin Gönderilmesi (Selective Forwarding) Gider Deliği (Sinkhole) Saldırıları Sybil Saldırıları Solucan Deliği (Wormhole) Saldırıları HELLO Seli Saldırıları Onaylama (Acknowledgement) Seli Saldırıları
Taşıma Katmanı	Paket Seli (flooding) Saldırıları Uyumu Bozma (Desynchronization) Saldırıları

Kablosuz ağlara yönelik saldırıların detayları aşağıda açıklanmıştır.

3.4.1. Genel saldırılar

Tüm kablosuz ağların maruz kalabileceği saldırı türüdür. Burada anlatılan saldırı türlerinin özellikle kablosuz haberleşmenin gizlilik, bütünlük ve erişilebilirliğine yönelik olduğu akılda tutulmuştur. Ayrıca saldırılar anlatılırken kablosuz algılayıcı ağlarda gerçekleşme şekilleri de belirtilmiştir.

<u>Mahremiyete yönelik tehditler</u>

Mahremiyete yönelik tehditleri iki temel başlık altında toplamak mümkündür.

Keşif (Reconnaisance)

Saldırgan büyük çaplı bir saldırı başlatmadan önce ağ içerisindeki düğümler ve haberleşme hakkında bilgi toplamak ve ağ içerisinde bulunan zafiyetleri tespit etmek maksadıyla keşif

yapmaktadır. Bu bilgi toplama, ağ topolojisini açığa çıkarma ve saldırı esnasında kullanacağı zafiyetleri belirleme işlemini doğrudan veya dolaylı olarak gerçekleştirebilir. Pasif ve aktif saldırı kavramlarında açıklandığı üzere hedef düğümlerle etkileşime girmeden veya girerek bu işlemleri gerçekleştirebilir.

Gizli dinleme (Eavesdropping)

Haberleşen düğümler arasındaki özel iletişimin saldırgan tarafından gizlice dinlenmesi işlemidir. KAA'larda daha çok, tüm ağdan toplanan ve veri kümeleme (data aggregation) işlemi neticesinde birleştirilen verinin öğrenilmesi maksadıyla icra edilmektedir. Çünkü herhangi iki düğüm arasındaki haberleşmenin dinlenmesi saldırgana ağ hakkında yeterli bilgi sunmayacaktır. Gizli dinleme de aktif ve pasif olarak ikiye ayrılabilmektedir. Aktif gizli dinlemede saldırgan diğer düğümlere sorgular göndermek suretiyle düğümlerin ağ içerisindeki görevlerini ve işlevlerini anlamaya çalışmaktadır. Ayrıca araya girme saldırıları bölümünde detayları açıklandığı üzere, diğer düğümleri kendisinin baz istasyonuna erişmek için kullanılacak yol üzerinde bulunduğuna ikna etmeye çalışmaktadır. Pasif gizli dinlemede ise saldırgan kendisini haberleşme güzergâhına yerleştirir ve üzerinden geçen tüm trafiği dinler. Bu şekilde ağa yerleşen kötücül düğümlerin tespiti oldukça zordur. Çünkü saldırgan bir taraftan trafiğin akışını sağlarken verileri de bu esnada dinlemektedir.

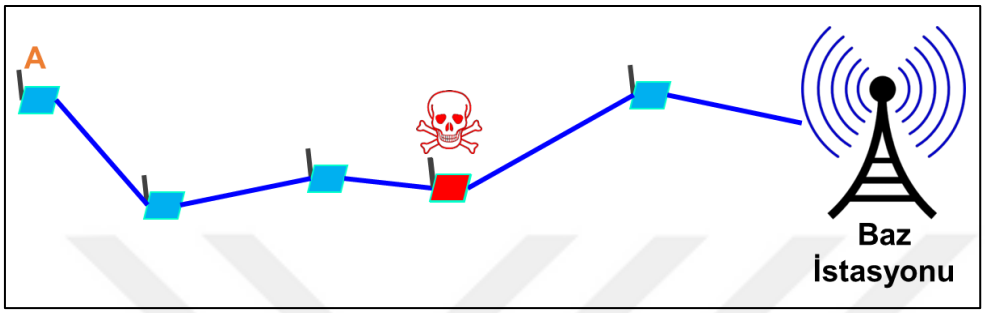
<u>Kontrole yönelik tehditler</u>

KAA'larda işlenen, saklanan ve iletilen verilerin bütünlüğünü bozmayı hedef alan tehditlerdir. Bu tür saldırı türlerinin detayları aşağıda açıklanmıştır.

Araya girme saldırıları (Man-in-the-Middle, MITM)

Bu saldırı türü KAA'lara yönelik yapılan en klasik saldırı yöntemidir. Saldırgan ağ içerisine sızmakta ve düğümler ile baz istasyonu arasındaki haberleşme kanalı arasına girmeye çalışmaktadır. Bu esnada ağdaki diğer düğümler ağa dâhil olan kötücül düğümün varlığından habersizlerdir. Şekil 3.4'den görüldüğü üzere kaynak ile hedef arasındaki tüm

haberleşme trafiği kötücül düğüm üzerinden geçmektedir. Saldırganın motivasyon ve becerisine bağlı olarak bu saldırılar da yine aktif veya pasif olarak gerçekleştirilebilir. Aktif saldırganlar gönderilen paketler üzerinde değişiklik yapmakta, pasif saldırganlar ise paketleri sadece izlemekte ve takip etmektedir. Bu saldırı türü fiziksel katman, veri bağı katmanı, ağ katmanı ve uygulama katmanında gerçekleşebilmektedir [19].



Şekil 3.4. Araya girme saldırısı

Radyo girişimi (Radio interference)

Kablosuz ağ teknolojilerinin yaygınlaşması ve aynı frekans bandını (2.4 GHz, 5 GHz, 900 MHz vb.) kullanan cihazların artması KAA'larda kullanılan düğümlerin radyo girişimlerine maruz kalmasına neden olmaktadır. Örneğin, kablosuz cihazların yoğun olarak bulunduğu bir bölgede düğümlerin transfer edeceği bilgi radyo girişimini artırmakta ve kayıplar çoğalmaktadır. Bu durum alıcı tarafından alınmayan veya eksik alınan veri miktarını artırmakta ve haberleşmenin güvenilirliğini olumsuz yönde etkilemektedir [20]. Radyo girişimi nedeniyle detayları aşağıda açıklanacağı üzere *servis dışı bırakma (DoS)* saldırılarının gerçekleşmesi mümkün olmaktadır. Radyo girişiminin neden olabileceği en kötü durum ise karıştırmadır (jamming).

Sahte veri gönderme saldırısı (Injection attack)

Gizli bir şekilde kablosuz algılayıcı ağa sızan saldırgan, algılayıcı düğümleri ve hatta baz istasyonunu kandırabilmekte ve ağa kötücül verileri enjekte etmektedir. Bu kötücül veriler düğümün komşuları hakkındaki sahte ilanlar, kendisini baz istasyonu olarak tanıtma veya veri kümelemesi yapan nokta olarak kendisini lanse etme şeklinde olabilmektedir.

Yeniden gönderme saldırısı (Replay attack)

KAA'lara karşı yapılan çok yaygın bir saldırı şeklidir. Saldırgan düğümler arasındaki haberleşme trafiğini kaydetmekte daha sonra ele geçirdiği bu veriyi ağa yeniden göndermektedir. Örneğin, kritik bir bölgenin sıcaklık verisini takip eden bir ağda, beklenen zaman dilimi dışında verinin gelmesi kullanılan ağın amacı dışına çıkmasına neden olacaktır. Bu saldırı türü özellikle zaman damgası içermeyen zayıf kimlik doğrulama mekanizmalarının kullanılması durumunda oldukça etkili olmaktadır. Ayrıca ağdaki tüm cihazlarda ortak anahtar kullanımının olması durumunda yine oldukça etkili olabilmektedir.

Seçilen paketlerin iletilmesi (Selective forwarding)

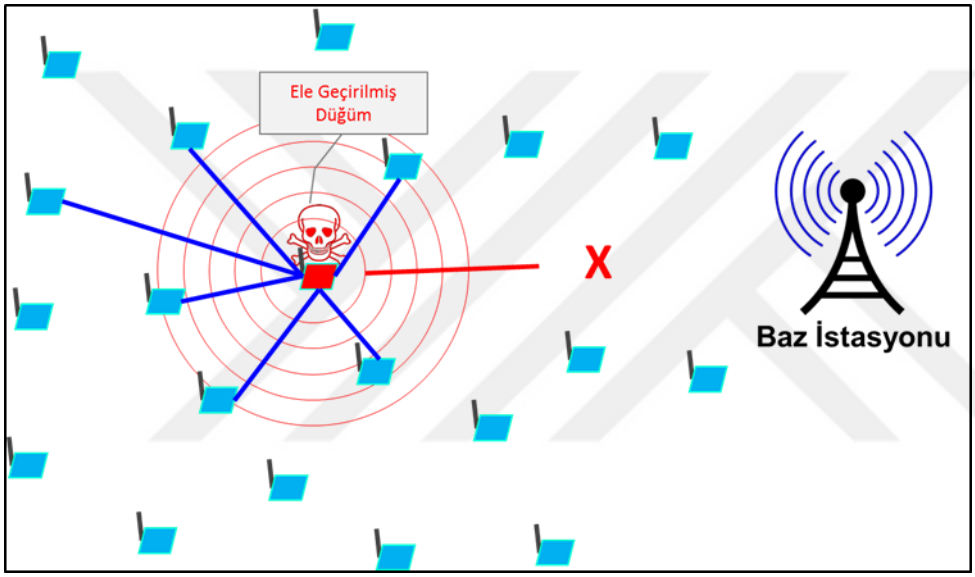
Bu saldırı şekli *araya girme saldırılarının (MITM)* özel bir türüdür ve ağdaki performansı yavaşlatmak, gönderilen verilerin güvenilirliğini azaltmak vb. amaçlarla gerçekleştirilmektedir. Saldırgan iletilen paketlerden bazılarının bir sonraki düğüme gönderimini sağlamakta bazılarını ise göndermemekte veya geciktirmektedir. Böylelikle veriler bozulmakta ve alıcı tarafta gelecek olan veri için bir kaynak tahsisi yapılmakta ancak paketler tam gelmediği için ağ saldırıya maruz kalmaktadır.

Bizans saldırıları (Byzantine Attacks)

Saldırganın uygun şekilde ağa dâhil olmuş (kimlik doğrulaması yapılmış ve verilen algılama görevlerini gerçekleştiren) düğümlerden bir veya bir kaçını ele geçirmesi ve müteakiben ele geçirdiği düğümleri kullanarak içerden saldırılar gerçekleştirdiği saldırı türleridir. Bu saldırı türüne; kara delik saldırıları (black hole attacks), solucan deliği saldırıları (wormhole attacks), paket seli boğma saldırıları (flood rushing attacks) ve ağ solucan deliklerini üst üste bindirme saldırıları (overlay network wormholes) örnek olarak verilebilir. Aşağıda bu saldırı örneklerinin detayları incelenmektedir.

Kara delik saldırısı (Black Hole Attack)

Bu saldırı türünde saldırgan ağ içinde iletilmek istenen veri ve kontrol paketlerinden bazılarının veya tamamının iletilmesini engelleyebilmektedir. Bu nedenle araya giren bu kötücül düğüm üzerinden aktarılacak her paket kısmen veya tamamen kaybolacaktır. Şekil 3.5'den de görüldüğü üzere bir kötücül düğüm kendini komşularına baz istasyonuna en yakın düğüm olarak lanse etmekte ve verileri toplamaktadır. Bu saldırının esas amacı toplanan verilerin baz istasyonuna ulaştırılmasının engellenmesidir.

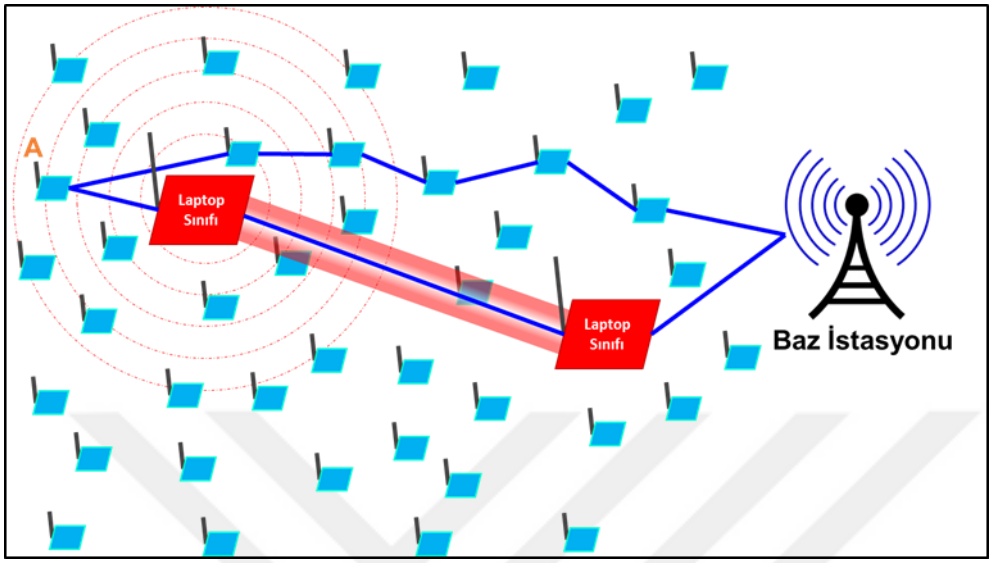


Şekil 3.5. Kara delik saldırısı (Black hole attack)

Solucan deliği saldırısı (Wormhole attack)

Bu tür saldırılarda iki kötücül düğüm birbirleri arasında yüksek iletişim kalitesine sahip bir kanal oluştururlar. Daha sonra yönlendirme için bu kanalın reklamını yaparak çevredeki algılayıcılardan baz istasyonuna gönderilmek üzere veri toplarlar. Ancak kötücül düğüm toplanan veriyi baz istasyonuna iletmeyebilir ya da verileri değiştirerek baz istasyonuna gönderebilir. Şekil 3.6'da gösterilen bu saldırı türü oldukça etkili olabilmektedir. Ayrıca detayları aşağıda açıklanan, yönlendirme gider deliği saldırıları (Sinkhole attacks) ile yakından ilişkilidir. Çünkü düğümlere oranla daha yüksek yeteneklere sahip kötücül

düğümler yaptıkları reklam ile kendilerinin baz istasyonuna en yakın düğüm olduğuna diğerlerini ikna etmektedir.



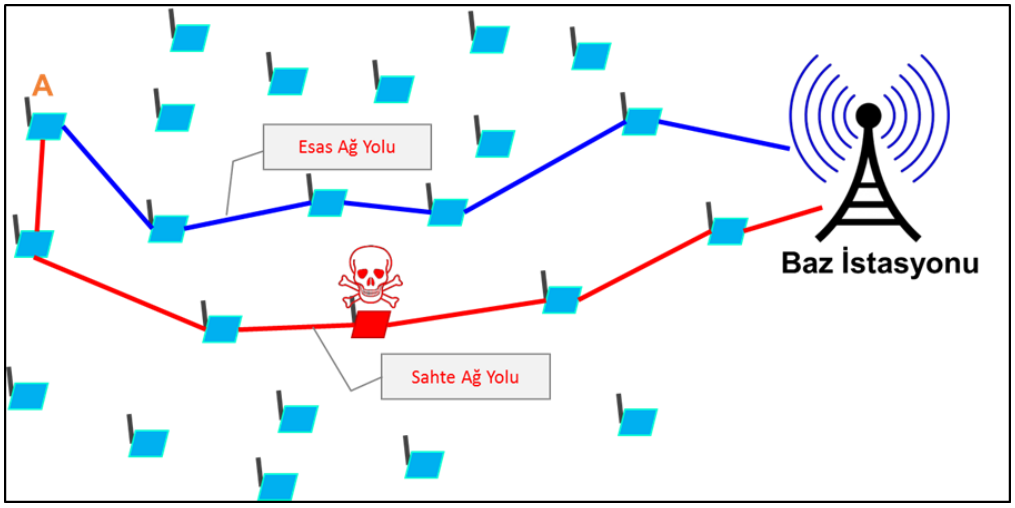
Şekil 3.6. Solucan deliği saldırısı (Wormhole attack)

Ağ solucan deliklerini üst üste bindirme saldırısı (Overlay network wormholes attack)

Solucan deliği saldırılarının özel bir türüdür. Solucan deliği olarak kullanılacak düğümlerin çok daha fazla olması ve ele geçirilen bu düğümler üzerinden yapılan saldırıların etki alanlarının çakıştırılması ile gerçekleşmektedir. İki adetten fazla solucan deliği oluşması durumunda gerçek düğümlerin kandırılması daha kolay olmaktadır ve verilerin daha kolay bu sahte kanal üzerinden baz istasyonuna iletilmesi sağlanmaktadır.

Paket seli boğma saldırısı (Flood rushing attack)

KAA'larda oldukça yaygın bir saldırı türüdür ve esas ağ trafiğinin akması gereken yolun meşgul edilerek trafiğin kötücül düğüm üzerinden akması mantığı ile çalışır. Saldırgan gönderdiği sahte paketlerle asıl ağ yolunu meşgul etmekte ve düğümlerin kendisini daha az yoğun olan ancak üzerinde kötücül düğümün bulunduğu ağ yoluna adapte etmesini sağlamaktadır. Klasik kimlik doğrulama yöntemleri saldırganın gerçek düğümleri kullanması nedeniyle yetersiz kalmaktadır. Şekil 3.7'de saldırının yapılış şekli görülmektedir.

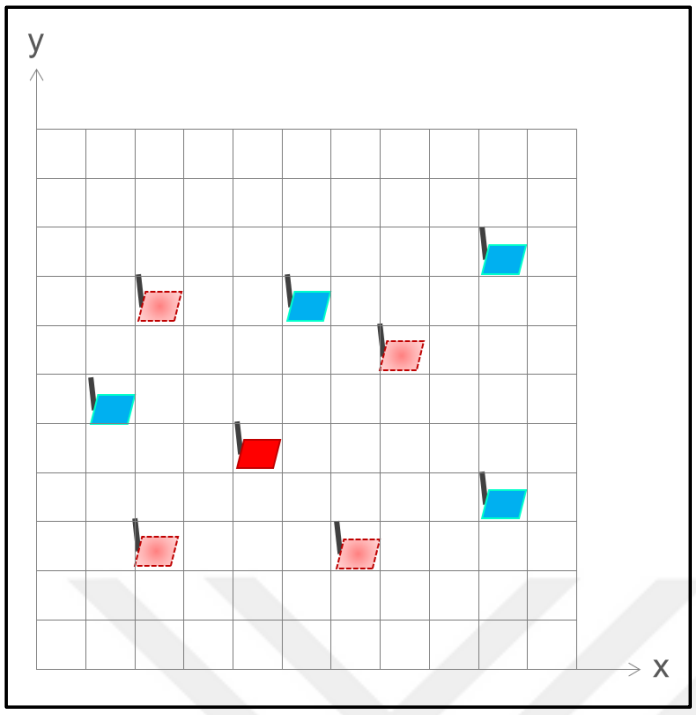


Şekil 3.7. Paket seli boğma saldırısı (Flood rushing attack)

Sybil saldırısı (Sybil attack)

Bu tür saldırılarda Şekil 3.8'de görüldüğü üzere bir kötücül düğüm ağdaki diğer düğümlere kendisini birden fazla kimlikle tanıtır. Bu durumda, kurban olarak seçilen düğüm bu kötücül düğümden gelen mesajları farklı düğümlerden geliyormuş gibi algılar. Kötücül düğüm bu şekilde kurban olarak seçtiği düğümlerin mesaj alıp vermesini engelleyebilir. Dahası, Sybil saldırıları ile bir kötücül düğüm sürekli yanlış bilgi göndererek ağda toplanan bilgiyi fazlasıyla değiştirebilir. Böylece baz istasyonunda yanlış bilgi toplanmasına neden olarak karar verme mekanizmasını yanıltabilir.

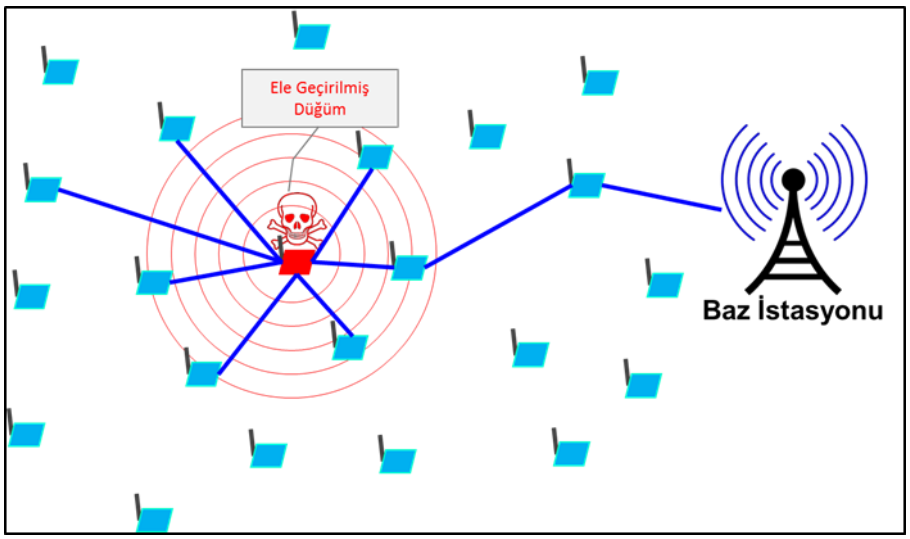
Bu saldırı şekli ilk defa [21]'deki çalışmada Douceur tarafından uçtan uca ağların (peer-to-peer networks) incelenmesi esnasında ortaya konmuştur. Daha sonra Karlof ve Wagner tarafından bu saldırı şeklinin kablosuz algılayıcı ağlar için tehdit oluşturabileceği ilk defa tespit edilmiştir [17]. Düğümlerin çoğunlukla rastgele ve dağıtık bir şekilde yerleştirilmesi ile kablosuz haberleşmenin kullanılması bu saldırı türünün KAA'larda kolaylıkla gerçekleşmesine neden olmaktadır. Veri kümeleme, oy kullanma mekanizmaları, güven değerlendirmesi ve coğrafik yönlendirme gibi durumlarda bu saldırı şekli oldukça kötü sonuçlara neden olmaktadır.



Şekil 3.8. Sybil saldırısı (Sybil attack)

Yönlendirme gider deliği saldırıları (Sinkhole attacks)

Saldırgan ele geçirdiği kötücül düğüm vasıtasıyla en kısa rota bilgisinin kendisinde olduğu bilgisini komşularına yayarak, trafiğin kendi üzerinden geçmesini sağlamaktadır. Böylece; seçilen paketleri gönderme veya göndermeme ile veri paketlerinin manipüle edilmesi gerçekleşebilmektedir. Saldırının yapılışı Şekil 3.9'da görülmektedir.



Şekil 3.9. Yönlendirme gider deliği saldırısı (Sinkhole attack)

Erişilebilirliğe Yönelik Tehditler

Erişilebilirlik; verilmesi amaçlanan hizmetin istenen zamanda istenen şekliyle talep edenlere verilmesi, hizmetlerin sunulmasında devamlılığın sağlanarak kesintilerin yaşanmamasını ifade etmektedir.

Servis dışı bırakma (DoS) veya dağıtık servis dışı bırakma (DDoS) saldırısı

Saldırgan, düğümlerin programlandığı şekilde çalışmasını engellemek maksadıyla çok miktarda sahte paketi hedef düğüme göndermekte ve böylelikle düğümün aşırı derecede paket alması nedeniyle işlevini yapamaz hale gelmesine sebep olmaktadır. Örneğin, laptop sınıfı saldırgan kaynak açısından (bant genişliği, hafıza, işlem gücü, kapsama alanı vb.) daha yüksek kapasiteye sahip olduğu için rahatlıkla kısıtlı kaynakları olan düğümlere çok fazla sayıda paket göndermek (flooding) suretiyle servis dışı bırakma saldırısını uygulayabilmektedir. Saldırgan açısından bu durum özellikle gerçek zamanlı veri aktarımı yapan KAA'lar için kolaylık sağlamaktadır. Bunun yanında haberleşme bandının karıştırılması (Jamming) ile yine servis dışı bırakma saldırıları gerçekleştirilebilmektedir. Servis dışı bırakma saldırılarının daha gelişmiş bir türü olan dağıtık servis dışı bırakma saldırılarında ise saldırgan ağdaki birden fazla düğümü ele geçirmekte, aynı anda birden fazla düğüm ile bu saldırıları gerçekleştirmektedir.

HELLO paketleri gönderme saldırısı

KAA'lardaki en temel komşu düğümleri tespit etme metodu HELLO paketlerinin gönderilmesidir. Eğer bir düğüm HELLO paketini alırsa bu durum kendi haberleşme kapsamı içinde başka bir düğüm olduğu anlamına gelmektedir. Ancak özellikle laptop sınıfı saldırganlar düğümleri yanıltabilecek kadar yeterli güç kullanarak söz konusu mekanizmayı istismar edebilmektedir. Hatta bu yöntem ile saldırgan düğümleri kendisinin bir baz istasyonu veya küme başı (cluster head) olduğuna ikna edebilmekte ve düğümleri kandırabilmektedir.

Haberleşme bandının karıştırılması (Jamming)

Sadece KAA'lar için değil kablosuz ağ ile haberleşen tüm sistemler için en tehlikeli saldırı türüdür. Yeteri kadar güce sahip bir karıştırıcı (Jammer) ile haberleşme bandı bastırılmaya, dolayısıyla düğümler arasındaki haberleşme engellenmeye çalışılmaktadır. Karıştırıcının gücüne bağlı olarak ağın bir kısmı hedef alınabileceği gibi tüm ağ da hedef olarak seçilebilir. Karıştırma işlemi kesintisiz olarak yapılabileceği gibi ara ara karıştırma işlemini durdurarak da gerçekleşebilir. Karıştırma işleminin ara ara durdurulması bir bitlik veri çerçevesindeki değişikliğe dahi tahammülü olmayan, alıcı tarafta bu tarz bir değişikliğin kabul edilmediği uygulamalarda oldukça etkilidir. Genellikle bu tür uygulamalarda gelen paketler alıcı tarafından düşürülmekte, karıştırma işlemi servis dışı bırakma saldırısına dönüşmektedir. Saldırıya maruz kalan düğüm açısından, karıştırmanın gerçek bir saldırı nedeniyle mi yoksa fiziksel olarak iletim kanalında meydana gelen değişmeler (elektromanyetik girişim vb.) sebebiyle mi gerçekleştiğinin tespiti oldukça güçtür. Böyle bir durumda düğümler öncelikli olarak alma ve gönderme güç seviyelerini artırmak suretiyle sorunun giderilmesine çalışmaktadır. Bu durum ise kısıtlı olan düğüm enerjisinin kısa sürede tükenmesine neden olmaktadır. Karıştırma saldırıları özellikle fiziksel ve veri bağlantı katmanını (MAC katmanını) hedef almaktadır. [22]'de yapılan çalışmada dört tür karıştırma saldırısı olduğu ortaya konmuştur. Bunların; rastgele (random), tepkisel (reactive), aldatıcı (deceptive) ve sürekli (constant) olduğu belirtilmiş ve bu saldırıların kolaylıkla servis dışı bırakma saldırılarına yol açtığı vurgulanmıştır. Ayrıca bu tür saldırıların tespit edilmesinde üç çözüm yönteminin olduğu bunların ise; ön alıcı (proactive) tedbirler, tepkisel (reactive) tedbirler ve mobil ajan tabanlı (mobile agent-based) tedbirler olduğu vurgulanmıştır.

Çarpışma (Collision)

Özellikle MAC katmanını hedef alan ve üssel bir şekilde geri çekme (back-off) işleminin ortaya çıkmasını hedef alan bir saldırı türüdür. Herhangi bir şekilde çarpışmanın meydana gelmesi durumunda düğümler etkilenen paketleri yeniden göndermek suretiyle sorunu aşmaya çalışır, bu durum paketlerin çok sayıda yeniden gönderilmesine yol açar. Saldırganın bu tür saldırıyı gerçekleştirmek için harcadığı enerji, düğümlerin paketleri tekrar

göndermek için harcadığı enerjiye kıyasla oldukça düşüktür. Yani, küçük bir enerji kullanımı ile düğümlerin enerjilerini tüketmek hedeflenir. Çarpışma saldırıları bu nedenle kaynak tüketme saldırıları arasında gösterilmektedir.

Düğümlerin ele geçirilmesi (Node compromise)

KAA'lardaki en yaygın ve en tehlikeli sonuçlar doğurabilecek saldırı türüdür. Düğümlerin sıklıkla savaş alanı, deniz dibi, yanardağ ağzı, sınır hatları vb. örneklerde olduğu gibi fiziksel erişimin ve gözetimin devamlı yapılamadığı durumlarda kullanılabilmesi nedeniyle, fiziksel olarak ele geçirilme ve çalınma saldırıları ortaya çıkmaktadır. Örneğin, hasım kuvvetler muharebe sahasında kullanılan düğümleri ele geçirmek suretiyle kıymetli verilere ulaşmayı hedefleyebilmektedir. Dahası, fiziksel olarak ele geçirilen bir düğüm yeniden programlanarak muharebe sahasında hasım kuvvetlerin istediği şekilde görev yapmaya devam etmesi mümkün olabilmektedir.

3.4.2. Özel saldırılar

Buraya kadar anlatılan saldırı türleri tüm kablosuz ağlara yönelik saldırıları içermekteydi ve özellikle KAA'larda kullanımı göz önüne alarak anlatılmaya çalışıldı. Bu bölümde ise KAA'lara özel bir takım saldırılar incelenmiştir.

<u>TinyOS yayma protokolüne (TinyOS Beaconing Protocol) yönelik saldırılar</u>

TinyOS yayma protokolü [23] KAA'lardaki yönlendirme güncellemelerinin (routing updates) yayımlanması için *önce genişliğine arama algoritmasını* (*Breadth-first spanning tree algorithm*) kullanmaktadır. Burada baz istasyonu yönlendirme bilgisini periyodik olarak en yakınındaki komşularına göndermekte, bu bilgiyi alan komşu düğümler ise yine benzer şekilde yönlendirme bilgisini kendi komşularına yeniden yayımlamaktadır. Bu işlem öz yinelemeli olarak devam etmekte ve her düğüm kendisinin bağlı olduğu en üst düğümü (parent node) belirlemektedir. En üst düğüm ağaç yapısında altındaki düğümler ile haberleşebilen ve yönlendirme bilgisini gönderebilen düğümü ifade etmektedir. Ancak, bu

protokol birçok saldırıya karşı hassastır. Örneğin, taklit etme (impersonation) veya araya girme (MITM) saldırıları ile tüm ağın ele geçirilmesi mümkün olabilmektedir.

Bu tür saldırıları önlemek için kimlik doğrulama mekanizmaları kullanılmaktadır. Ancak laptop sınıfı saldırganlar tarafından gerçekleştirilen seçilen paketlerin iletilmesi, gizli dinleme ve kara delik saldırılarına karşı bu koruma da yetersiz kalmaktadır. Saldırganlar en az iki adet laptop sınıfı cihaz kullanmak suretiyle bir solucan deliği yaratmaktadır (Bkz. Şekil 3.6). Bu cihazlardan birisi özellikle baz istasyonuna yakın diğeri ise hedef alınan bölgeye yakın yerleştirilmektedir. Baz istasyonuna yakın olan cihaz komşularını kandırarak gerçek mesajların kendisine gönderilmesini sağlamakta ve pasif bir görev yapmaktadır. Bu pasif durum nedeniyle de fark edilmesi daha da güçleşmektedir. Kendisine gelen gerçek mesajları uzaktaki cihaza göndermesi ile görevi sona ermektedir. Hedef ağın asıl yakınında bulunan cihaz ise aldığı gerçek paketler üzerinden kara delik veya seçilen paketlerin iletilmesi saldırılarını gerçekleştirebilmektedir.

Yukarıda anlatılan saldırı türü, kimlik doğrulama işleminin dijital imza ile sağlanması durumunda yine etkili olabilmektedir. Örneğin baz istasyonu kendisine ait özel anahtarın ele geçirildiğini fark etmiş ve yeni bir anahtar çifti yaratarak yeni açık anahtarını düğümlere iletmek istemiş olsun. Bu durumda yine baz istasyonuna yakın olan laptop sınıfı cihaz yeni açık anahtarı temin edecek ve saldırılarına devam edebilecektir.

Coğrafi ve enerji tabanlı yönlendirme protokollerine yönelik saldırılar

Bu kategorideki tüm protokoller, düğümlerin koordinat ve konum bilgilerinin düğümler arasında paylaşılması esasına dayanır. Bunlardan en önemlisi GEAR (Geographical Energy Aware Routing) protokolüdür [24]. GEAR protokolü konum bilgilerine ilave olarak düğümlerde bulunan enerji seviyelerini de dikkate almaktadır. Saldırganlar ele geçirdikleri düğümlerdeki enerji seviyesi bilgisini değiştirmek suretiyle, düğümleri düşük enerjili göstermekte ve diğer düğümler üzerinden geçen trafiğin artmasını böylelikle sürekli alma gönderme yapan düğümlerdeki enerjinin hızlı bir şekilde tükenmesini sağlamaktadırlar. Bu

tür saldırılar ile sybil, solucan deliği, seçilen paketlerin iletimi ve yönlendirme döngüleri oluşturma türünden saldırıların gerçekleştirilmesi mümkün olabilmektedir.

Yönlendirilmiş yayılma (directed diffusion) protokolüne yönelik saldırılar

Detayları [4]'deki çalışmada açıklanan protokol, *veri merkezli* yönlendirmenin sağlanmasını hedeflenmektedir. Baz istasyonu bir adet sorgu (interest) yayımlar (flooding). Sorguya cevap verecek düğümler, sorgu sonucunu geri yayımlar. Baz istasyonu gelen cevaplar içerisinden en uygun yolu belirler, güçlendirir (reinforcement) ve daha sık aralıklarla göndermesini istediği bilgiyi yayınlar. Böylelikle hedef kaynak istenen bilgileri daha sık aralıklarla baz istasyonuna gönderir. Bu protokolün bir takım güvenlik sorunları bulunmaktadır. Örneğin ağdaki bilgi talep sorgusu (flooding) ve sorguya cevap döndürülmesi süreçlerinde herhangi bir güvenlik mekanizması bulunmamaktadır. Bu nedenle servis dışı bırakma, solucan deliği, sybil ve seçilen paketlerin iletilmesi saldırılarına karşı savunmasızdır ve veri paketlerinin manipüle edilmesine olanak tanır.

3.4.3. Güven yönetim sistemlerine yönelik saldırılar

KAA'lardaki güvenlik seviyesinin artırılmasına yönelik olarak önerilen güven yönetim sistemleri (trust management systems) hakkında detaylı bilgi tez çalışmasının 5'inci bölümünde sunulmuştur. Özetle, güven yönetim sistemleri KAA'lardaki düğümlerin davranışlarını göz önünde bulundurarak her düğüm için bir güven değerinin hesaplanması ve bu güven değerinin kullanılarak düğümlerin *güvenilir, şüpheli* veya *güvenilmez* gibi sınıflara ayrılmasını hedefleyen bir yaklaşımdır. Tez çalışmasının 6'ncı bölümünde güven ve kötüye kullanım tabanlı saldırı tespit sistemi önerilmiştir. Bu nedenle güven yönetim sistemlerine yönelik mevcut saldırıların bu bölümde incelenmesinin faydalı olacağı değerlendirilmektedir. [25, 26]'da yapılan çalışmalarda güven yönetim sistemlerine yönelik saldırılar dört grup olarak belirlenmiştir. Bunlar;

- *Kötüleme saldırısı (bad mouthing attack):* Güven yönetim sistemlerinde komşu düğümlerden hedef hakkındaki görüşleri alınmakta ve bu görüşler dikkate alınarak

güven değeri hesaplanmaktadır. Düğümlerden kötü niyetli olanlar bilerek hedef düğüm hakkında yanlış bilgi vermekte ve hedef düğümün güven değerinin gerçekten farklı çıkmasına neden olmaktadır.

- *Doğru-yanlış davranma saldırısı (on-off attack):* Kötücül düğümün bir iyi bir kötü davrandığı saldırı türüdür. Kötü davranışın iyi bir davranış ile telafi edilmesi suretiyle kötücül düğümün fark edilmesi zorlaşmaktadır.
- *Seçilen davranış saldırısı (selective behaviour attack):* Güven sisteminin kullanılması durumunda düğümler belirli komşularından veya tüm komşularından görüşleri alabilme imkânına sahiptir. Bu saldırı türünde kötücül düğüm birçok düğüm için iyi davranışlar sergilerken kendisine hedef olarak belirlediği bazı düğümler için kötücül davranışlarda bulunmaktadır. Böylelikle güven değerini yüksek tutarken kötü niyetli faaliyetlerine devam edebilmektedir.
- *Sybil ve yeni gelen saldırısı (Sybil attack and newcomer attack):* Bir düğüm kendisi için birden fazla kimlik bilgisi yayınlamakta kullandığı her sahte kimlik ile kendisinin güven değerini yüksek olarak duyurmaktadır. Birden fazla kimlik bilgisi kullanımı ile kötü itibara sahip olan düğüm, bu kimlik bilgisini kullanmak yerine güven değeri yüksek sahte kimliği ile ağ içerisinde gizlenebilmektedir.

3.5. Güvenlik Mekanizmaları

KAA'lara yönelik saldırıların engellenmesi veya etkisinin azaltılmasına yönelik alınabilecek güvenlik tedbirleri;

- Şifreleme (cryptography)
- Anahtar yönetimi (key management)
- Servisi dışı bırakma (DoS) saldırılarına yönelik tedbirler başlıkları altında incelenmiştir.

Geleneksel ağlardaki kimlik doğrulama, yeniden oynatma (replay) saldırılarına karşı tedbirler, yetkilendirme vb. tedbirlerin KAA'lar için de gerekli olduğu aşikârdır. Ancak

özellikle yukarıda belirtilen güvenlik mekanizmaları KAA'lar için önem arz ettiğinden detaylı olarak ele alınmıştır.

3.5.1. Şifreleme

KAA'larda kullanılacak en uygun şifreleme yönteminin belirlenmesi kimlik doğrulama, gizlilik ve bütünlük başta olmak üzere tüm güvenlik hizmetlerinin şifreleme yöntemleri ile sağlanması nedeniyle hayati öneme haizdir [27, 28]. Uygun şifreleme yöntemi belirlenirken algılayıcılardaki kısıtlar göz önünde bulundurulmalı ve kodun büyüklüğü, verinin büyüklüğü, işlem zamanı ve güç tüketimi gibi son derece hassas gereksinimlere uygun yöntem belirlenmelidir. KAA'lardaki güvenlik protokollerinde uygun şifreleme ilkelerinin kullanılması, ağın etkinliği ve ömrünün belirlenmesinde son derece önemlidir. Bu nedenle burada KAA'larda kullanılacak şifreleme yönteminin seçimi üzerinde durulmuş, önce açık anahtar şifrelemesi daha sonra da simetrik şifreleme ele alınmıştır.

Kablosuz algılayıcı ağlarda açık anahtar şifrelemesi

KAA'larda açık anahtar şifrelemesinin kullanılmasına yönelik çalışmalarda kodun büyüklüğü, verinin büyüklüğü, işlem zamanı ve güç tüketimi açısından bakıldığında "Diffie-Helman Anahtar Anlaşması Protokolü" [28] ve "RSA imzası" [29] gibi açık anahtar şifreleme algoritmalarının KAA'larda kullanılmasının istenen durum olmadığı ortaya konmuştur. Bunun nedeni olarak da açık anahtar algoritmalarının, yoğun hesaplamalar yapması ve basit bir şifreleme işlemi için bile binlerce hatta milyonlarca çarpma işlemi gerçekleştirmesi nedeniyle enerji tüketimini artırması gösterilmektedir.

[30]'da yapılan çalışmaya göre, bir mikroişlemcinin açık anahtar algoritması kullanıldığındaki performansı, tek bir çarpma işlemi gerçekleştirmek için gerekli olan saat çevrimi (clock cycle) ile ölçülmektedir. Ayrıca, RSA gibi açık anahtar şifreleme yöntemlerinin, şifreleme ve şifre çözme işlemleri için dakikalar mertebesinde sürecek zaman gerektirebildiği, kısıtlı kaynaklara sahip KAA'larda bu sürenin oldukça fazla olduğu

ve bu durumun servis dışı bırakma saldırılarına karşı cihazları hassaslaştırdığı ortaya konmuştur.

Yapılan bir diğer çalışmada ise Carman ve arkadaşları [31] basit bir çarpma fonksiyonu kullanarak 128 bitlik bir sonuç üretmek için mikroişlemcinin binlerce nanojule'lük enerji tükettiğini tespit etmişlerdir. Yine aynı çalışmada, simetrik şifreleme algoritmalarının ve Hash fonksiyonlarının açık anahtar şifrelemesine oranla çok daha az enerji harcadığı ortaya konmuştur.

Açık anahtar şifrelemesinin algılayıcı ağlarda kullanılabilmesi için doğru algoritma seçiminin yapılması ve uygun parametre, optimizasyon ve düşük güç kullanım yönteminin belirlenmesi gerektiğini ortaya koyan ve bu şartlar altında açık anahtar algoritmasının algılayıcı ağlarda kullanılabileceğini ifade eden çalışmalar da bulunmaktadır [32-34]. Bu çalışmaların çoğunlukla RSA ve ECC (eliptik curve cryptograhy) üzerinde yoğunlaştığı görülmektedir. Özellikle ECC'nin tercih edilmesindeki temel amacın, RSA'ya oranla daha küçük anahtar kullanarak aynı seviyede güvenliğin sağlanabilmesi, böylelikle işlem ve haberleşme için daha az ilave yük getirmesi gösterilmektedir. Örneğin RSA'da 1024 bitlik bir anahtar ile sağlanan güvenlik seviyesinin, ECC kullanılması durumunda 160 bitlik anahtar ile sağlanabildiği [35]'de yapılan çalışmada ortaya konmuştur. 2010 yılından sonra verilerin korunması için 2048 bitlik RSA anahtarının kullanılması gerekmektedir. Bunun için gerekli olan ECC anahtar uzunluğu ise 224 bittir.

KAA'larda yaygın olarak kullanılan MICA2 algılayıcılarda bulunan Atmel ATmega 128 mikro işlemcisinin RSA ve ECC algoritmalarına tepkime süresi üzerine yapılan bir araştırmada [36], Çizelge 3.2 ve Çizelge 3.3'de görülen değerler elde edilmiştir. Çizelge 3.2'de görülen secp160r1 ve secp224r1 değerleri *tavsiye edilen eliptik eğri etki alanı parametreleri* dokümanında [37] belirtilen değerlerdir. Çizelge 3.2'ye göre RSA, sayıların çarpılmasında ECC'ye göre çok az bir miktar hızlıdır. Ancak, Çizelge 3.3'den de görüleceği üzere ECC, özel anahtar ile yapılan işlemlerde (*imzalama, imza doğrulama ve anahtar değişimi vb.*) RSA'dan çok daha verimlidir ve daha az enerji tüketmektedir. KAA'lardaki en temel kısıtlamanın enerji olduğu ve RSA'nın özel anahtar işlemlerinde çok daha yavaş olduğu göz önüne

alındığında, algılayıcı ağlarda ECC algoritmasının tercih edilmesi gerektiği değerlendirilmektedir.

Çizelge 3.2. ECC ve RSA ortalama işlem süreleri [36]

Algoritma	İşlem Süresi (sn)
ECC secp160r1	0,81
ECC secp224r1	2,19
RSA-1024 açık anahtar, e=2^{16}+ 1	0,43
RSA-1024 özel anahtar (Çin Kalan Teoremi ile)	10,99
RSA-2048 açık anahtar, e=2^{16}+ 1	1,94
RSA-2048 özel anahtar (Çin Kalan Teoremi ile)	83,26

Çizelge 3.3. Dijital imza ve anahtar değişimi ortalama enerji tüketimleri (MiliJoule) [36]

Algoritma	**İmzalama**		**Anahtar Değişimi**	
	İmzala	Doğrula	İstemci	Sunucu
RSA 1024	304	11,9	15,4	304
ECDSA-160	22,82	45,09	22,3	22,3
RSA-2048	2302,7	53,7	57,2	2302,7
ECDSA-224	61,54	121,98	60,4	60,4

[38]'de yapılan çalışmada MICA2DOT, MICA2, MICAz ve TelosB düğümleri kullanılarak açık anahtar şifrelemesinin, düğümlerin pil ömrü üzerindeki etkileri araştırılmıştır. Yazarlar, çalışmalarında; KAA'larda açık anahtar şifrelemesi kullanılarak güçlü şifreleme uygulamalarının mümkün olduğunu, en sınırlı kapasiteye sahip düğümlerde bile açık anahtar şifrelemesinin kullanılabileceğini, örneğin ECC-160 imzası kullanılması durumunda her 10 dakikalık görev süresi döngüsünde sadece % 0,5'lik bir ilave yükün geldiğini

ölçmüşler, ancak yine de açık anahtar şifrelemesinin KAA'larda başarıyla kullanılabilmesi için son derece hassas planlama yapılmasını, aksi takdirde ağ ömrünün olumsuz etkileneceğini belirtmişlerdir.

Açık anahtar şifrelemesinin KAA'larda kullanılabileceğini öneren [32-34, 38]'deki gibi çalışmalarda, özel anahtar ile yapılan işlemlerin sadece baz istasyonu veya üçüncü bir birim tarafından yapılacağını varsaymışlardır. Böyle bir varsayımda bulunmak, açık anahtar mimarisi ile geleneksel ağlarda elde edilen birçok faydanın KAA'lar için geçersiz olmasına neden olmaktadır. Örneğin, uçtan uca şifreleme ve güvenli veri kümelemesi gibi KAA'lar için son derece gerekli olan güvenlik kazanımları elde edilememektedir. Neticede açık anahtar şifrelemesinin KAA'larda kullanımı karmaşıklık, enerji tüketimi, ilave hafıza alanı ve özel anahtarla yapılan işlemlerin sadece baz istasyonu tarafından gerçekleştirildiğinin varsayılması gibi nedenlerden ötürü çok fazla tercih edilmemektedir. Bu konu halen araştırılan ve üzerinde çalışmaların yapılması gereken bir konudur.

Kablosuz algılayıcı ağlarda simetrik anahtar şifrelemesi

Açık Anahtar Şifrelemesinin çoğunlukla hesaplama açısından yoğun işlemler gerektirmesi ve fazla enerji tüketimi nedeniyle, KAA'larda genellikle simetrik anahtar şifrelemesi tercih edilmektedir. Simetrik anahtar şifrelemesinde, haberleşen düğümler arasında ortak bir anahtar kullanılmakta ve bu ortak anahtar ile hem şifreleme hem de şifre çözme işlemleri gerçekleştirilmektedir. Bu şifreleme yöntemindeki en temel sorun kullanılacak anahtarın güvenli bir şekilde düğümlere dağıtılmasıdır. Anahtarların başlangıçta düğümlere yüklenmesi ve görev yapılacak bölgeye daha sonra düğümlerin yerleştirilmesi her zaman verimli bir çözüm olmamaktadır.

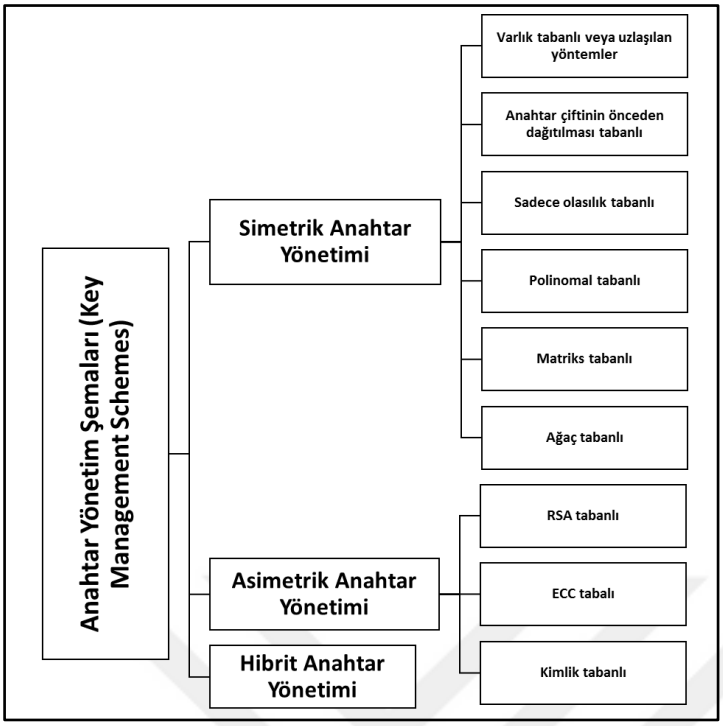
Yapılan çalışmalarda [39-41] özellikle vurgulanan konu, istenen güvenlik seviyesinin sağlanması için uygun şifreleme yöntem ve algoritmasının seçilmesinin hayati öneme sahip olduğudur. Yapılacak olan seçimi ise etkileyen en temel faktör, kullanılacak düğümlerin kapasiteleridir. Açık anahtar şifrelemesini algılayıcı ağlarda kullanmanın mümkün olduğu yapılan çalışmalarda gösterilmiştir [32-34, 38]. Ancak özel anahtar kullanılarak yapılan

işlemler, hesaplama ve enerji maliyeti bakımından halen oldukça pahalıdır. Bu nedenle algılayıcı ağlardaki özel anahtar şifreleme uygulamaları daha detaylı olarak incelenmeli ve geliştirilmelidir.

Simetrik şifreleme, hız ve düşük enerji maliyeti açısından açık anahtar şifrelemesinden üstündür. Ancak, anahtar dağıtım işlemi özellikle kullanılacak düğüm sayısı artıkça oldukça büyük bir sorun olarak ortaya çıkmaktadır. Bu nedenle esnek ve verimli anahtar dağıtım yöntemlerinin tasarlanmasına ihtiyaç vardır. Ayrıca, güvenliğin sağlanması hafıza, depolama ve işlem gücü bakımından daha güçlü düğümlerin üretilmesini, bunu yaparken de üretim maliyetlerinin asgari seviyede tutulmasını gerektirmektedir.

3.5.2. Kablosuz algılayıcı ağlarda anahtar yönetimi

KAA'larda güvenliğin sağlanmasına yönelik alınacak tedbirlerden bir tanesi de uygun anahtar yönetim metodunun belirlenmesi suretiyle düğümler arasında kullanılacak anahtarların uygun şekilde dağıtılmasıdır. Yapılan çalışmalarda birçok anahtar yönetim sınıflandırması ve önerisi bulunmaktadır [42, 43]. Bu konu araştırmacılar tarafından yoğun olarak çalışılan bir alandır. Tez çalışmasının bütünlüğü kapsamında konu özet olarak ele alınmış ve önerilen anahtar yönetim mekanizmaları hakkında özet bilgi sunulmuş, konunun derinlemesine analizi yapılmamıştır. Şekil 3.10'da görüldüğü üzere genel olarak anahtar yönetim sistemleri üzerine yapılan çalışmalar üç ana başlık altında toplanmaktadır.



Şekil 3.10. Anahtar yönetim şemaları [43]

Simetrik anahtar yönetimi

Birçok KAA'da daha az enerji tüketimi nedeniyle simetrik anahtar yönetim şemaları kullanılmaktadır. Anahtar dağıtımı, keşfi ve üretilmesi açısından değerlendirildiğinde bu yöntemleri altı başlığa ayırmak mümkündür.

Varlık tabanlı veya uzlaşılan yöntemler tabanlı şemalar: Anahtar dağıtım ve üretim işlemlerinin güvenli başka bir varlık tarafından yapıldığı şemalardır. Bu yöntemlerden ilki temel bir anahtarın (master key) önceden dağıtılması ve her düğümde bu anahtarın saklanması yaklaşımıdır. Düğümler arasında kullanılacak anahtar çifti, bu temel anahtar ve düğümler arasında anlaşılacak rastgele numaralar kullanılmak suretiyle yaratılmaktadır. Bu yaklaşım oldukça basit ve az enerji tüketen bir yaklaşımdır. Düğümlerin tek yapması gereken haberleşmek istediği hedef düğüm ile rastgele sayılar üzerinde anlaşıp daha sonra anahtar çiftini üretmektir. Ancak eğer temel anahtar saldırganlar tarafından ele geçirilirse tüm anahtar çiftleri ifşa olmuş sayılır. Tüm düğümlerin aynı temel anahtarı kullanması nedeniyle düğümler arasında herhangi bir kimlik doğrulama da söz konusu değildir. Bu anahtar yönetim şeması ile ilgili bir diğer yaklaşım; baz istasyonunun (BS) anahtar yönetim

faaliyetlerine katılması ve her düğümün BS ile aralarında bir anahtar çifti oluşturması esasına dayanmaktadır. Ancak düğüm sayısının artması durumunda bu yöntem ölçeklenebilir olmaktan çıkmaktadır. Bir diğer alternatif yöntem ise aradaki düğümlerden bir tanesinin güvenilir düğüm olarak kabul edilmesi, A ile B arasındaki haberleşmede C gibi başka bir güvenilen düğüm tarafından üretilecek anahtarın kullanılması durumudur. Bu durumda da aradaki güvenilen düğümün, saldırgan düğüm olmamasının tespiti önem arz etmektedir.

Anahtar çiftinin önceden dağıtılması tabanlı şemalar: Haberleşilecek tüm düğümler için anahtar çiftlerinin üretilmesi ve önceden üretilen tüm anahtarların düğümlere kaydedilmesi mantığına dayanmaktadır. Haberleşilecek her düğüm ile farklı anahtar kullanılmasını önermesi açısından iyi görünse de ölçeklenebilirlik açısından uygun değildir.

Sadece olasılık tabanlı anahtar çiftinin önceden dağıtılması esasına dayanan şemalar: Düğümlerin hepsine anahtar çiftlerinin tamamının yüklenmesi durumunun ölçeklenebilir olmaması nedeniyle belirli bir anahtar havuzunun düğümlere yüklenmesi ve değişik olasılık hesaplarıyla anahtarların seçilmesi esasına dayanmaktadır.

Polinomal tabanlı anahtar çiftinin önceden dağıtılması esasına dayanan şemalar: Asal sayılar kullanmak suretiyle anahtarların polinomal şekilde üretilmesi ve bu üretilen anahtarların bir anahtar havuzunda (key pool) toplanarak kullanılması esasına dayanır. Düğümler güvenli haberleşmede kullanacakları anahtar çiftlerini belirlenmiş olan polinomal fonksiyonları kullanarak kendileri üretmektedirler.

Matris tabanlı anahtar çiftinin önceden dağıtılması esasına dayanan şemalar: Bir adet simetrik anahtar kullanarak oluşturulan ve gizli anahtarları saklayan matris, bir adette açık anahtarları saklayan matris önceden düğümlere yüklenmektedir. Haberleşecek düğümler açık anahtarla oluşturulan matristeki kullanacağı anahtar çiftini şifrelemeden hedef düğüme gönderebilmektedir. Hedef düğüm aldığı açık anahtar ile hesaplamasını yapmakta, şifreli haberleşmede kullanacağı anahtar için gerekli olan matris değerini bulmaktadır.

Teorik olarak oldukça güçlü olsa da dikkatli planlama ve düğümler arası yüksek iş birliği gerektirmektedir.

Ağaç tabanlı anahtar çiftinin önceden dağıtılması esasına dayanan şemalar: Özellikle kullanılan ağın küçük olması durumunda düğümlerde saklanılacak anahtar sayısını azaltmak maksadıyla ağaç mimarisinin kullanılması önerilmiş, bu durumda düğümlerin ağacın kollarındaki gibi yerleştirileceği varsayılmıştır. Böylelikle düğümler ağaç mimarisinde sadece altındaki ve üstündeki düğümler için haberleşmede kullanacağı anahtarları saklayacak ve bu anahtarlarda kolaylıkla önceden dağıtılabilecektir. Ancak KAA'lar çoğunlukla görev yapılacak bölgeye sayıca yoğun miktarda bırakılmaktadır. Bu nedenle uygulanabilirliğinin düşük olduğu değerlendirilmektedir.

Asimetrik Anahtar Yönetimi

KAA'larda asimetrik anahtar yönetiminin yapılması için RSA, ECC ve kimlik tabanlı yaklaşımlar önerilmektedir. Geleneksel olarak bilgisayar ağlarında kullanılan söz konusu yöntemlerin KAA'lar için uyarlanması durumunda karşılaşılan iki temel problem bulunmaktadır. Birincisi asimetrik anahtarlamanın güç tüketimi açısından düğümler için sorunlar çıkarması ve düğümlerdeki enerjinin çok çabuk tükenmesine neden olmasıdır. İkinci problem ise sertifika otoritesi (CA) belirlenmesi sorunudur. Sertifika otoritesi olarak baz istasyonunun seçilmesi durumunda tüm düğümlerin anahtar güncelleme, sil listelerinin alınması, yasaklı düğümlerin tespit edilmesi gibi konularda baz istasyonu ile haberleşmesi gerekecektir. Bu durum veri kümeleme gibi enerji tasarrufu maksadıyla uygulanan mekanizmaların da devre dışı kalmasına neden olacaktır. Daha önce ifade edildiği üzere KAA'lar için asimetrik şifreleme ve anahtar yönetim sistemlerinin enerji verimli olmadığı değerlendirilmektedir.

3.5.3. Servis dışı bırakma saldırılarına karşı koruma

KAA'lara yönelik saldırıların en tehlikesi, en başarılısı, en kolay icra edilebileni ve önlenmesi en zor olanı servis dışı bırakma (DoS) veya dağıtık servis dışı bırakma (DDoS) olarak bilinen

saldırılardır. Bu saldırılar haberleşme protokol yığınının her katmanına yönelik yapılabilmektedir [44]. Bu nedenle tez çalışmasının bu bölümünde, DoS saldırısının önlenmesine yönelik olarak protokol yığınının her katmanı için önerilen güvenlik tedbirleri detaylı olarak açıklanmıştır.

Fiziksel katmandaki koruma mekanizmaları

Fiziksel katmandaki DoS saldırıları frekans atlamalı geniş spektrum (FHSS) ve kodu parçalara bölme teknikleri kullanılarak azaltılabilmektedir [18]. FHSS yönteminde iletim bant genişliği, çok sayıda örtüşmeyen frekans dilimlerine ayrılmaktadır. Düğümler bir frekans bandından belirli bir süre iletim yaptıktan sonra başka bir frekans bandına çok hızlı bir şekilde atlamakta ve iletimi bu yeni frekansta sürdürmektedir. İletim yapılan frekansın değişmesi neticesinde saldırganlar haberleşme yapılan frekansın tamamını karıştıracak kadar güce sahip olamayacağı için saldırılar başarısız olmaktadır. Kodu parçalara bölme tekniği ise karıştırma saldırılarına karşı geleneksel ağlarda kullanılmaktadır. Ancak bu yöntem KAA'lar için tasarım karmaşıklığı ve enerji tüketimi açısından uygun değildir. Fiziksel olarak düğümlerin çalınması veya düğümlerin imha edilmesi saldırılarına karşı ise düğümlerin dışardan kolayca görünmeyecek şekilde saklanması veya görev kritik bazı işler için kurcalamaya karşı dayanıklı (tamper-proof) düğümlerin kullanımı saldırıların etkisini azaltabilmektedir. Kurcalamaya karşı dayanıklı düğümleri herhangi bir şekilde yetkisiz kişiler tarafından açılması veya içindeki bilgilerin elde edilmeye çalışılması durumunda, içindeki tüm verileri silebilen özelliktedir. Bu tür düğüm kullanımı, maliyetleri oldukça artıracak olması nedeniyle çok özel durumlarda tercih edilmektedir.

Veri bağı katmanındaki koruma mekanizmaları

Bu katmandaki saldırılar, düğümlere gönderilecek sorgular nedeniyle düğümün sürekli uyanık kalmasını, çarpışma saldırıları ile mesajların tekrar gönderilmek zorunda kalınmasını ve böylelikle düğüm enerjisinin tüketilmesini hedeflemektedir. Kimlik doğrulama, hata kodları ve yeniden oynatma saldırılarına karşı bu katmanda alınacak tedbirler saldırıların etkisini azaltacaktır. Saldırılara karşı kullanılabilecek yöntemlerden bir tanesi mesaj

doğrulama kodlarının (MAC) kullanılmasıdır. Bir diğer yöntem ise *zaman bölmeli çoklama* (TDMA) ile her düğüme belirli zaman tahsis etmek ve o zaman aralığı dışında gelecek mesajlara işlem yapmamaktır. Ayrıca düğümlerin uyku durumuna geçmesini engellemek ve bu şekilde kaynakların tükenmesini hedefleyen DoS saldırıları için yine kimlik doğrulama ve saldırıların tespit edilerek uyku durumuna geçilmesi yöntemleri uygulanmalıdır.

Ağ katmanındaki koruma mekanizmaları

Ağ katmanı paketlerin yönlendirme işlemlerinin gerçekleştiği katmandır ve [17]'deki çalışmada bu katmana yönelik saldırılar detaylı olarak ele alınmıştır. Sahte paketlerin gönderilmesi, yeniden oynatma veya yönlendirme bilgisinin değiştirilerek trafiğin kontrol edilmesi saldırılarına yönelik kimlik doğrulama ve rasgele sayı (nonce) kullanımı gibi tedbirler alınmalı, saldırıların tespit edilmesi durumunda düğümlerin tekrardan uyumaya geçmesi sağlanmalıdır. HELLO seli saldırıları için düğümler arasında anahtar çiftlerinin kullanılması gerekmektedir. Ayrıca coğrafi yönlendirme protokollerinin kullanılması da bu saldırıların etkisini azaltmaktadır.

Taşıma katmanındaki koruma mekanizmaları

Uçtan uca haberleşmenin yönetildiği taşıma katmanında, taşırma (flooding) saldırıları kullanılan protokolün normal dışı çalışmasını hedeflemektedir. Örneğin, TCP SYN (*syn*chronize) seli saldırılarında kötücül düğümler aşırı miktarda bağlantı isteği göndermekte, hedef düğümün her bağlantı için belirli bir miktar kaynak ayırmasını ve neticede kaynakların tükenmesini hedeflemektedir. Bağlantısız (connectionless) protokollerin kullanıldığı haberleşmede bu saldırılar gerçekleştirilememektedir. SYN seli saldırılarının önlenmesi için SYN çerezleri (cookies) kullanılmaktadır [45]. Senkronizasyonu bozma saldırısında ise saldırgan düğümler arasındaki haberleşmeyi bozmak için sahte sıra numarasına sahip paketler gönderilmekte ve aynı paketin tekrar tekrar gönderilmesine neden olmaktadır. Başlık kısmının veya paketin tamamının kimlik doğrulamasından geçirilmesi bu saldırıların etkisini azaltmaktadır.

Uygulama katmanındaki koruma mekanizmaları

Düğümlerin baz istasyonuna büyük veri paketlerini göndermesini sağlayarak kaynakların tüketilmesini hedef alan saldırılardır. Bu saldırılar kaynak tüketiminin yanı sıra bant genişliğinin tüketilmesini de hedeflemektedir. Örneğin fiziksel hareketleri algılamak amacıyla yerleştirilen bir düğümün karşısına sürekli hareket eden basit bir düzenek konması ve sayede düğümün sürekli gönderim yapması en basit saldırı yöntemidir. Bu durumda düğümlerin dikkatlice ayarlanması ve sadece ilgili olayların gerçekten meydana gelmesi durumunda algılama yapılması sağlanmalıdır. Ayrıca iletim yolu üzerindeki tüm düğümlerin enerjilerini tüketmek maksadıyla aynı paketin tekrar tekrar gönderilmesi ile baz istasyonuna giden yoldaki düğümlerin sürekli uyanık kalması ve bu düğümlerdeki enerjinin tükenmesi söz konusu olabilmektedir. Yeniden oynatma saldırılarına karşı alınacak tedbirler, kimlik doğrulama ve şifreleme gibi yöntemler bu saldırıların etkisini azaltmak için kullanılabilmektedir.

4. KABLOSUZ ALGILAYICI AĞLARDA SALDIRI TESPİT SİSTEMLERİ

İster kablolu isterse kablosuz olsun tüm ağlara yönelik saldırılara karşı izlenecek güvenlik tedbirleri temelde üç temel başlıkta sıralanabilir [46] . Bunlar

- Koruma (Prevention)
- Tespit Etme (Detection)
- Etki Azaltma (Mitigation)'dır.

Daha önce kritik alt yapıların siber güvenliği konusunda ele alındığı üzere [7]; koruma herhangi bir saldırı gerçekleşmeden önce alınan tedbirleri ve yapılan işlemleri, tespit etme maruz kalınan mevcut saldırılardan haberdar olabilmek maksadıyla yapılması gerekenleri ve etki azaltma ise saldırıların vereceği zararları asgari seviyeye indirmek amacıyla yapılacak faaliyetleri tanımlamaktadır.

Bir ağa yapılan saldırı veya girişim (intrusion), aktif ve/veya pasif saldırı yöntemlerini kullanarak yetkisiz şekilde sistemlere erişmeyi, bilgileri elde etmeyi, hassas verileri okumayı veya değiştirmeyi, sistemlerin programlanan amaç için kullanılmasının engellenmesini veya farklı amaçlar için kullanılmasını ifade etmektedir. Sistemlerin güvenliğini sağlamak maksadıyla kullanılan saldırı koruma sistemlerinin yetersiz kalması durumunda, *derinliğine savunma prensibi* kapsamında ikinci bir koruma tedbiri olarak değerlendirilen ve yapılan saldırıları veya şüpheli hareketleri tespit etmek, böylelikle durumsal farkındalığı artırmak maksadıyla kullanılan sistemler *saldırı tespit sistemleri (intrusion detection systems, IDSs)* olarak tanımlanmaktadır.

KAA'larda kullanılan IDS'ler saldırganın veya şüpheli hareketlerin tanımlanması, olayın yeri (tek düğüm mü birden fazla düğüm mü), zamanı, faaliyetin ne olduğu (aktif/pasif), saldırı türü (solucan deliği, kara delik, seçilen paketlerin iletilmesi vb.) ve saldırının gerçekleştiği katmanın (fiziksel katman, veri bağ katmanı, ağ katmanı) tespit edilmesinde yardımcı olmayı hedefleyen sistemlerdir [47]. Kısaca IDS, saldırıları tanımlamak, değerlendirmek ve raporlamak maksadıyla araçların, yöntemlerin ve metotların toplamıdır denebilir. Burada

vurgulanması gereken bir diğer konu da, IDS'ler herhangi bir sistemin güvenliğini tek başına sağlamaya yeterli değildir [48]. Herhangi bir sistemde üretilen, işlenen veya iletilen verinin gizlilik, bütünlük ve erişilebilirliğini bozmayı hedefleyen saldırıların tek başına saldırı tespit sistemleri ile fark edilmesi ve önlenmesi güvenlik bakış açısına uygun değildir. Bunun yerine *derinliğine savunma prensibi* uygulanmalı ve katmanlı güvenlik tedbirleri alınarak korunması hedeflenen varlıklara yönelecek saldırılar azaltılmalıdır. Ancak, IDS'lerden elde edilecek bilgiler vasıtasıyla saldırılardan haberdar olmak dolayısıyla durumsal farkındalığın artırılması, şüpheli hareketlere karşı uyanık olunması ve gerekli tedbirleri alarak saldırıların neden olacağı zararların azaltılması mümkün olabilmektedir. Bu nedenle KAA'larda IDS kullanımı, ağ güvenliği ve sistemin genel güvenliği açısından son derece önemlidir.

Sınırlı güç kapasitesi, düşük bant genişliği, küçük hafıza boyutu ve kısıtlı depolama birimi gibi sınırlılıklar nedeniyle, geleneksel kablolu/kablosuz ağlarda kullanılan güvenlik tedbirlerini ve saldırı önleme metotlarını doğrudan KAA'lar için uygulamak mümkün değildir. Ayrıca sistemlerin güvenliğini sağlamak maksadıyla yine geleneksel ağlarda kullanılan şifreleme (encryption) ve kimlik doğrulama (authentication) yöntemlerini de doğrudan bu özel ağ türüne uygulamak mümkün değildir [49]. Yukarıda ifade edilen kısıtların yanı sıra, KAA'lardaki gözetimsiz veya otonom çalışma gereksinimi de bu durumu zorlaştırmaktadır. Ayrıca düğümlerin fiziksel olarak güvensiz ortamlara bırakılması ve kurcalamaya karşı (tamper-proof) dayanıklı düğüm kullanılmasının maliyeti artırması da söz konusu yöntemlerin kullanılmamasına bir nedendir. Son olarak, KAA'larda anahtar dağıtımı ve sil listelerinin güncellenmesi (revocation) işlemi özellikle ağın büyüklüğü artıkça imkânsız hale gelmektedir. Hem KAA'lardaki kısıtlılıkları dikkate alacak hem de saldırıları yüksek doğruluk oranı ile tespit edebilecek saldırı tespit sistemlerinin tasarlanması oldukça zor bir problemdir.

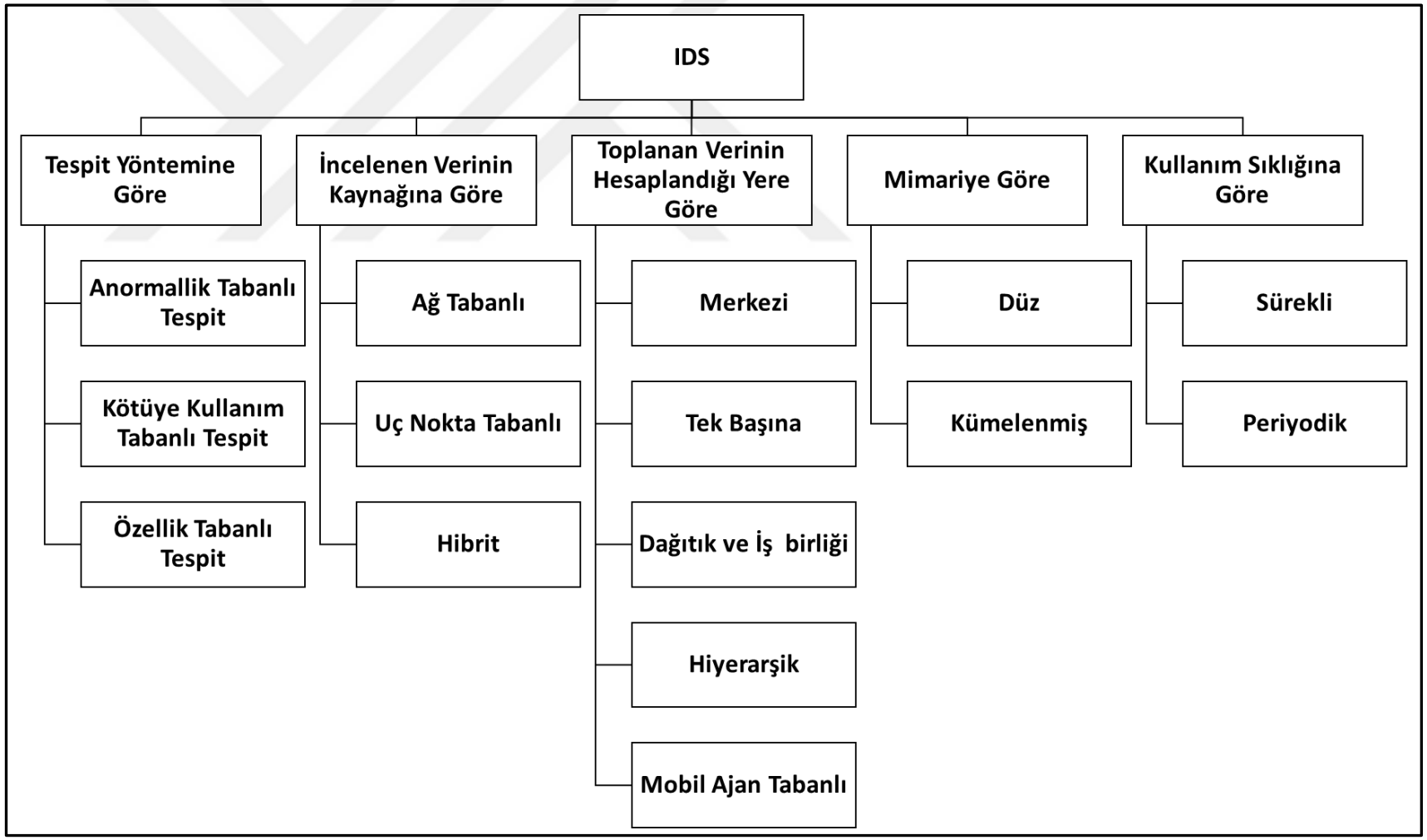
4.1. Gereksinimler

Saldırıları doğru bir şekilde tespit edecek aynı zamanda KAA'lardaki kısıtları göz önüne alacak bir IDS tasarlarken karşılanması gereken gereksinimler şunlardır [50];

- Sistemlere yeni zafiyetler yaratmamalı,
- Asgari kaynak tüketmeli ve sisteme getireceği yeni yükler ile sistem performansını olumsuz etkilememeli,
- Sistem ve kullanıcılardan habersiz olarak sürekli çalışmalı,
- İş birliğini desteklemek için açık olmalı ve standartları kullanmalı,
- Güvenilir olmalı, tespit aşamasında yanlış pozitif (false positives) ve yanlış negatif (false negatives) oranları düşük olmalıdır.

4.2. Sınıflandırma

KAA'larda kullanılan saldırı tespit sistemleri birçok çalışmanın konusu olmuş ve bu sistemlerin farklı farklı sınıflandırılmaları yapılmıştır.[47, 51-54]'de yapılan çalışmalar incelendiğinde genel olarak algılayıcı ağlarda özel olarak da KAA'larda kullanılan saldırı tespit sistemlerini Şekil 4.2'deki gibi sınıflandırmak mümkündür. Bu bölümde anılan sınıflandırma esaslarında her bir saldırı tespit sistemi açıklanmıştır.



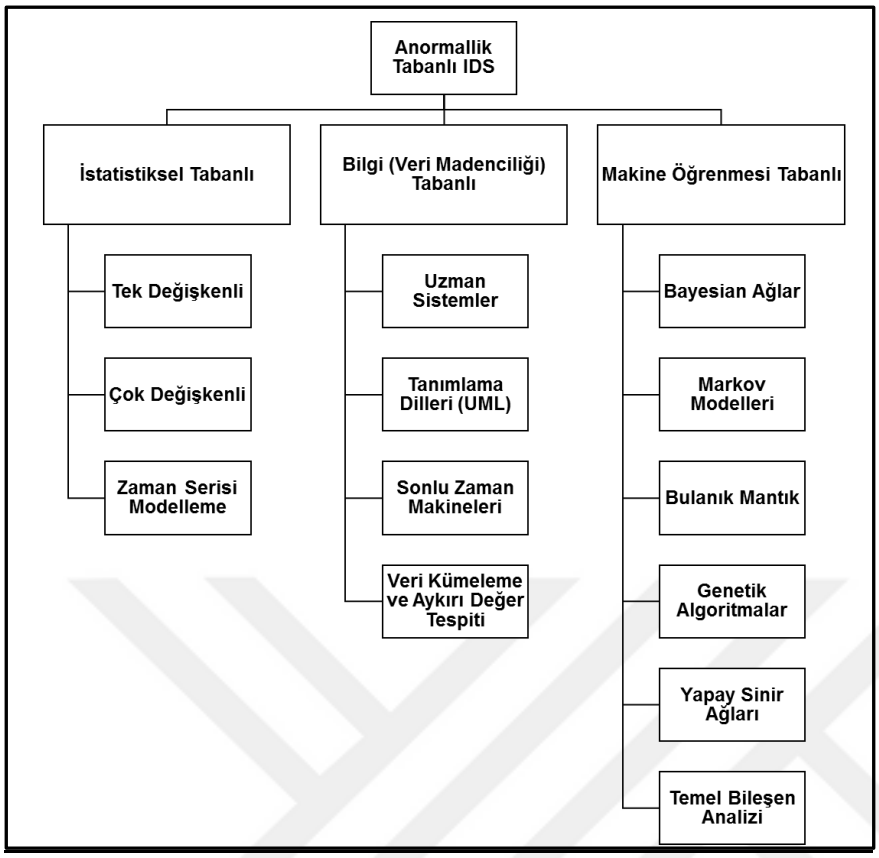
Şekil 3.3. Şekil 4.1. Saldırı tespit sistemlerinin sınıflandırılması [47]

4.2.1. Tespit yöntemine göre

Tespit yöntemleri göze önüne alındığında IDS'ler üç temel kategoriye ayrılmaktadır: anormallik tabanlı tespit, kötüye kullanım (imza) tabanlı tespit ve özellik tabanlı tespit.

Anormallik tabanlı tespit

Bu yöntemde ağ içerisindeki davranışlar istatistiksel olarak modellenmektedir. Ağ elemanlarının normal hareketleri tanımlanmakta ve bu tanımlanmış normal davranışlardan belli bir miktar sapma *anormallik* olarak değerlendirilmektedir. Bu yaklaşımın dezavantajı *normal davranışların* sürekli güncellenmesi gereksinimidir. Ağ içerisindeki elemanların davranışları devamlı değişebilir nitelikte olabileceği için her zaman *güncel normal davranışlar* listesini bulundurmak zordur ve bunu başarmak ise iş gücünü artırmaktadır. Söz konusu yöntem, ağ davranışlarının sabit veya çok az değişim gerektirmesi durumunda saldırıları çok yüksek oranda doğru bir şekilde tespit edebilmektedir (Düşük yanlış pozitif ve yanlış negatif oranlarına sahiptir). Teodoro ve arkadaşları yapmış oldukları çalışmada [52], anormallik tabanlı saldırı tespit yöntemini Şekil 4.2'de görüldüğü üzere üç temel gruba ayırmışlardır.



Şekil 4.2. Anormallik tabanlı IDS'lerin sınıflandırılması [52]

İstatiksel tabanlı

Bu yaklaşımda ağdaki trafik kaydedilmekte ve daha sonra ağın rastgele davranışını tanımlayan model ortaya konmaktadır. Herhangi bir saldırı olmadan ağın çalışması durumunda (normal şartlarda), bir referans model oluşturulmaktadır. Ağ periyodik veya sürekli olarak takip edilmekte, yaratılan referans değeri mevcut durumda ortaya konan anormallik değeri ile karşılaştırılmaktadır. Eğer mevcut durumdaki değer belli bir eşik değerini geçerse, saldırı tespit sistemi anormal bir davranışın olduğunu belirten alarm üretmektedir.

Bilgi (veri madenciliği) tabanlı

Bilgi (knowledge) tabanlı anormallik tespit eden saldırı tespit sistemleri, normal şartlarda çalışan ağın parametreleri ile saldırı anındaki parametrelerin önceden elde

bulundurulmasına dayanmaktadır. *Uzman sistemler*, denetim verisi kural sınıflandırılmasını esas almaktadır. *Tanımlama dilleri*, UML diyagramları gibi diyagramların veri özelliklerine göre oluşturulması mantığına göre çalışmaktadır. *Sonlu durum makineleri*, mevcut veri kümelerine göre durumların ve geçişlerin tanımlandığı yöntemdir. *Veri kümeleme ve aykırı değer tespiti*, gözlemlenen verinin benzer veya farklılık özellikleri dikkate alınarak kümelere (gruplara) ayrılması esasına dayanır. Herhangi bir kümeye dâhil olmayan noktalar aykırı değer olarak tanımlanmaktadır.

Makine öğrenmesi tabanlı

Makine öğrenmesi tabanlı saldırı tespit sistemlerinde analiz edilen örneklerin açık (explicit) ve kapalı (implicit) modelleri oluşturulmaktadır. Saldırı tespit sisteminin önceki sonuçlara dayalı olan tespit performansını artırmak için, bu modeller periyodik olarak güncellenmektedir. *Bayesian ağlar*, ilgili değişkenler arasındaki olasılıksal ilişkileri kullanarak hesaplamalar yapmaktadır. *Markov modelleri*, sistem topolojisi ve yeteneklerinin belirli geçiş olasılıkları ile birbirine bağlandığı durumlar olarak modellenen olasılıksal Markov teorisini esas almaktadır. *Bulanık mantık*, yaklaşıklık ve belirsizlik kavramları üzerine kuruludur. *Genetik algoritmalar*, biyolojideki evrim kuramından esinlenmektedir. *Yapay sinir ağları*, insan beyni temellerine dayanmaktadır. *Temel bileşen analizi*, boyutluluk azaltma tekniğini kullanmaktadır.

Kötüye kullanım (imza veya kural) tabanlı tespit

Bu tespit yönteminde önceden bilinen saldırıların imzaları oluşturulmakta ve gelecekteki saldırıları tespit etmek maksadıyla referans olarak kullanılmaktadır. Örneğin, bir dakika içerisinde yapılacak on başarısız oturum açma işlemi, parolanın kırılması için saldırganlar tarafından gerçekleştirilen bir kaba kuvvet (brute force) parola saldırısı olarak değerlendirilebilir. Bu metodun en büyük avantajı önceden bilinen saldırı şekillerinin yüksek doğruluk derecesiyle etkin bir şekilde tespit edilebilmesidir. Ayrıca düşük yanlış pozitif oranlarına sahiptir. Ancak, daha önceden karşılaşılmamış (profili ortaya konmamış) bir saldırının gerçekleşmesi durumunda, bu yöntemin saldırıları tespit etme şansı

bulunmamaktadır. Bu sistemleri günümüzde kullanılan anti virüs programları gibi değerlendirmek uygun olacaktır. Nasıl ki anti virüs programlarının imza veri tabanı düzenli olarak güncellenmeli ve böylelikle sistemlerin yeni saldırılara karşı korunması sağlamalı ise benzer şekilde bu yöntemi kullanan saldırı tespit sisteminin de kural veri tabanı sürekli güncellenmelidir. KAA'larda bu metodun kullanılmasına yönelik olarak [53]'de yapılan çalışmada yazarlar ağdaki anormallikleri tespit edecek aşağıdaki kuralları tanımlamışlardır:

- Fasıla (interval) kuralı: Art arda gelen iki mesaj arasındaki gecikme belirli bir limit dâhilinde olmalıdır.
- Yeniden gönderim (retransmission) kuralı: Aradaki düğümler kendilerine gelen mesajları kendilerinden sonraki düğüme iletmelidir.
- Bütünlük (integrity) kuralı: Gönderenden alıcıya ulaşan mesajın bütünlüğü korunmalı, aradaki düğümler tarafından değiştirilmemelidir.
- Gecikme (delay) kuralı: Bir mesajın yeniden gönderimi belirli bir bekleme zamanı sonrasında olmalıdır.
- Tekrarlama (repetition) kuralı: Aynı mesaj aynı düğümden sadece belirli sayıda yeniden gönderiliyor olmalıdır.
- Radyo iletim (radio transmission) menzili: Mesajlar yalnızca komşu düğümlerden geliyor olmalıdır.
- Karıştırma (Jamming) kuralı: Paket iletimlerindeki çarpışma sayısı belirli bir eşik değerinden daha düşük olmalıdır.

Özellik tabanlı tespit

Bu yöntemde programın veya protokolün doğru işlemleri gerçekleştirebilmesi için gerekli olan özellikler ve kısıtlar tanımlanmaktadır. Daha sonra tanımlanan özellikler ve kısıtlar esas alınarak ilgili programın çalışması takip edilmektedir. Söz konusu metot daha çok anormallik tabanlı ve kötüye kullanım tabanlı saldırı tespit yaklaşımlarının uygun bir şekilde harmanlanması ile oluşmaktadır. Saldırı tespit sistemlerinin sınıflandırılmasına yönelik Sobh tarafından yapılan çalışmada [54], anormallik tabanlı tespit ile kötüye kullanım tabanlı tespit arasındaki fark vurgulanmış, bu kapsamda anormallik tabanlı saldırı tespit

sistemlerinin *kötü davranışları* bulmaya odaklandığı, kötüye kullanım tabanlı saldırı tespit yönteminin ise *bilinen kötü davranışları* ortaya çıkarmaya çalıştığı belirtilmiştir.

Özellik tabanlı saldırı tespit sistemleri manuel olarak geliştirilen özellikleri ve kısıtları göz önüne alarak anormallik ve kötüye kullanım tabanlı saldırı tespit yöntemlerinin birlikte kullanılmasını, böylelikle saldırıların daha etkin bir biçimde tespit edilmesini sağlamaktadır. Bu nedenle özellik tabanlı saldırı tespiti *hibrit* bir yöntemdir. Yüksek yanlış alarm oranına sahip anormallik tabanlı yönteme nazaran daha düşük yanlış alarmlar üretmek ve her iki yöntemin iyi taraflarının bir araya getirilmesi ile oluşmaktadır.

4.2.2. İncelenen verinin kaynağına göre

Saldırı tespit sistemleri incelenen verinin kaynağı göz önüne alındığında üç farklı gruba ayrılmaktadır. Bunlar; ağ tabanlı, uç nokta tabanlı ve hibrit saldırı tespit sistemleridir.

Ağ tabanlı saldırı tespit sistemi (NIDS)

Ağ trafiğinin aktif veya pasif olarak dinlenmesi, iletilen paketlerin kaydedilmesi ve bu paketler üzerinde analizlerin yapılması suretiyle, saldırıları ortaya çıkaracak alarmları üreten sistemlerdir. NIDS ile ağ içerisinde iletilen paketlerin başlık bilgileri, paket içinde taşınan verinin kendisi, IP adresleri veya port numaraları kontrol edilebilmektedir. Sistemlere herhangi bir yük getirmemekte, ağ elemanları çoğu kez böyle bir güvenlik sisteminin varlığından haberdar olmamaktadır. Bu özelliği nedeniyle *saydam* bir yapıya sahiptir. Genellikle merkezi olarak hizmet veren örün sunucusu, veri tabanı sunucusu, uygulama sunucusu vb. kritik sistemlere gelen/giden trafiğin incelenmesi maksadıyla geleneksel ağlarda kullanılmaktadır. Ağ içerisinde istenilen korumayı sağlaması, saldırılar hakkında gerekli alarmları üretebilmesi için ilgili tüm trafiğin NIDS üzerinden geçmesi gerekir. Kablosuz algılayıcı ağlardaki kısıtlar nedeniyle ağdaki tüm trafiğin NIDS üzerinden geçirilmesi uygulanabilir değildir. Bu nedenle söz konusu yöntemin tam anlamıyla KAA'larda uygulanması mümkün olamamaktadır. Ancak baz istasyonuna gelen/giden

trafiğin incelenmesi ve muhtemel saldırıların tespit edilmesine yönelik çeşitli kullanımları kısıtlı da olsa bulunmaktadır.

Uç nokta tabanlı saldırı tespit sistemi (HIDS)

Sistemlerde kullanılan her bir ağ elemanı veya uç nokta birimi üzerinde çalışmak suretiyle ilgili uç nokta biriminde meydana gelebilecek muhtemel saldırıları tespit etmeyi hedefleyen sistemlerdir. HIDS, ilgili uç birime yani hizmet verdiği birime yönelebilecek saldırıları ortaya çıkarmayı hedeflemektedir. Üzerinde çalıştığı sistemin kritik dosyalarında yapılacak değişliklerin izlenmesi, parolanın çok fazla deneme neticesinde yanlış girilmesi, yetkisiz erişim girişimleri, olağan dışı hafıza erişim talepleri, anormal CPU ve girdi/çıktı birimi faaliyetleri gibi ancak bir saldırı durumunda olabilecek anormallikleri tespit etmeyi amaçlamaktadır. HIDS üzerinde çalıştığı sisteme işlem gücü, hafıza gereksinimi, enerji tüketimi açısından ilave bir takım yükler getirmektedir. Enerji kısıtının KAA'larda temel sorun olması bu sistemleri tasarlarken son derece dikkatli olmayı gerektirmektedir. HIDS ile sağlanacak güvenlik hizmetinin düğümlerin görevlerini yapması için gerekli olan bataryalarının kısa sürede tükenmesine yol açmayacak şekilde programlanması hayati öneme sahiptir. Aksi takdirde saldırganlar, düğümlerdeki enerjinin tüketilerek servis dışı bırakma saldırılarını gerçekleştirebilmektedir.

Hibrit saldırı tespit sistemi (HIDS, NIDS)

Bu tür sistemler ağ ve uç nokta tabanlı saldırı tespit sistemlerinin hareketli (mobil) ajanlar kullanılarak bir araya getirilmesi neticesinde ortaya çıkmaktadır. KAA'lardaki uygulaması genellikle mobil ajanların düğümleri dolaşması ve düğümlerdeki kritik dosyaların kontrolünün sağlanması, merkezi ajanın ise tüm ağ trafiği üzerindeki anormallikleri tespit etmeye odaklanması ile gerçekleşmektedir. Böylelikle hem ağın merkezi olarak izlenmesi hem de düğümlerde meydana gelebilecek olağan dışı aktivitelerin açığa çıkarılması amaçlanmaktadır. Her ne kadar teoride yapılabilir olduğu vurgulansa da mobil ajan kullanımı, ilave enerji ihtiyacı, toplanan verilerin analizindeki sorunlar ve yüksek koordinasyon gibi zorunlulukları ortaya çıkarmaktadır.

4.2.3. Toplanan verinin hesaplandığı yere göre

Saldırı tespit sistemlerini toplanan verinin işlem yapıldığı yere göre beş gruba ayırmak mümkündür.

Merkezi IDS

Tüm trafiğinin merkezde bulunan bir bilgisayar vasıtasıyla takip edildiği ve normal dışı davranışların merkezde yapılan işlemler neticesinde ortaya çıkarıldığı saldırı tespit sistemleridir.

Tek başına IDS

Her bir düğüm üzerinde ayrı bir saldırı tespit sisteminin çalışması ve kötücül faaliyetlerin ilgili düğüm üzerinde tespit edildiği sistemlerdir. Ağdaki diğer elemanlar tek başına çalışan IDS'nin varlığından habersizdir. Düğümlerdeki IDS'ler arası iş birliğinin bulunmaması nedeniyle gerçekleşen saldırılardan ve IDS tarafından üretilen alarmlardan diğer düğümlerin bilgisi yoktur.

Dağıtık ve iş birliği IDS

Düz (flat) ağ mimarisinin kullanılması durumu için önerilen saldırı tespit sistemidir. Her düğüm genel olarak ağda yapılan saldırı tespit ve reaksiyon faaliyetlerine katılmakta, bunun için gerekli olan IDS ajanlarını üzerlerinde barındırmaktadır. Bu tür sistemlerde düğümlerden bir tanesi zayıf olasılıkla bir saldırının varlığını tespit ederse, bu şüphesini güçlendirmek veya kötücül davranışı/düğümü ortaya çıkarmak için diğer düğümlerle bir iş birliği başlatabilir. Benzer şekilde herhangi bir düğüm, yüksek olasılıkla veya emin olduğu bir saldırıyı tespit etmesi durumunda konudan diğer düğümleri haberdar etmek suretiyle tüm ağın güvenliğinin artırılmasına katkı sağlayabilir ve dağıtık olarak çalışan diğer IDS ajanlarının durumdan haberdar olmasını gerçekleştirebilir.

Hiyerarşik IDS

Çok katmanlı ağ mimarilerinin kullanıldığı sistemlerin güvenliği için önerilmiş saldırı tespit sistemleridir. Küme başları (CH) kendi kümelerine mensup düğümlerin hareketlerini izlemekten ve aynı zamanda ağın genelinde yapılacak olan saldırı tespit işlemlerine katılmaktan sorumludur.

Mobil ajan tabanlı IDS

Her bir mobil ajan seçilen düğüm üzerinde belirlenmiş saldırı tespit faaliyetini yapmaktan sorumludur. Yani mobil ajanların her birine farklı görevler atanabilmektedir. Daha sonra mobil ajanlar arasındaki iş birliği ve koordinasyon ile saldırılar tespit edilmektedir. Bu yöntemde belirli bir süre geçtikten veya kendilerine verilen görev tamamlandıktan sonra mobil ajanlar farklı düğümlere yönelmekte, sürekli aynı düğümler üzerinde işlem yapmayarak ağ ömrünün uzatılmasına katkı sağlamaktadır. Mobil ajanların kullanılması durumunda ajanlarda bulunması gereken özellikler şunlardır;

- *Hareketlilik (Mobility):* Mobil ajanlar topladıkları verileri daha detaylı analizlerin yapılması maksadıyla merkezi bir noktaya taşıyacak hareketliliğe sahip olmalıdır.
- *Özerklik (Autonomy):* Mobil ajanlar kendilerine verilen görevleri dışarıdan başka bir yardım almadan icra edebilme yeteneğine sahip olmalıdır.
- *Uyarlanabilme (Adaptability):* Mobil ajanlar kendilerine verilen vazifeleri icra ederken (gerekli verileri toplarken) kendi davranışlarını yeni durumlara karşı uyarlayabilmelidir.

4.2.4. Mimariye göre

KAA'larda kullanılan saldırı tespit sistemleri, kullanılan mimari açısından iki farklı gruba ayrılmaktadır.

Düz (Flat) Mimari

Tüm düğümlerin sahip olunan yönlendirme yeteneği açısından özdeş veya benzer olduğu durumlardaki yapıdır. Bu mimariler sivil uygulamalarda olduğu gibi özdeş düğüm kullanmanın sorun teşkil etmeyeceği uygulamalarda tercih edilmektedir. Böyle bir ağ mimarisi kullanılması durumunda uygulanacak saldırı tespit sistemi düz mimarili IDS olarak tanımlanmaktadır.

Kümelenmiş (Clustered) Mimari

Tüm düğümlerin özdeş olmadığı mimaridir. Kapsama alanı içindeki düğümler bir küme oluşturur ve içlerinden bir tanesi küme başı (CH) olarak atanır. Daha sonra ağın diğer birimleriyle yapılacak haberleşme, CH vasıtasıyla yürütülür. Tüm düğümler yaptıkları algılama işlemini baz istasyonuna iletmek üzere CH'e gönderir. CH gelen algılayıcı veriler üzerinde işlem yapabilme yeteneğine sahiptir. Ayrıca CH olarak seçilen düğümlerin daha uzun batarya ömrüne (veya yedek güç ünitesine) ve haberleşme mesafesine sahip olması tercih edilir. Eğer böyle bir durum söz konusu değilse, CH olarak belirlenen düğüm diğer düğümler ile özdeş ise belirli dönem aralıklarıyla CH olarak seçilen düğüm değişir ve böylelikle CH'deki enerjinin kısa sürede bitmesi engellenir. Burada amaç tüm düğümlerin baz istasyonuna ulaşmak için enerji tüketmesini önlemek ve ağın yaşam süresini artırmaktadır. Özellikle askeri uygulamalar başta olmak üzere ağ ömrünün uzatılması ve haberleşme trafiğinin asgari seviyede tutulması gereken durumlarda bu tür ağ mimarisi kullanılmaktadır.

4.2.5. Kullanım sıklığına göre

Kablosuz algılayıcı ağlardaki saldırı tespit sistemleri kullanım sıklığı açısından iki gruba ayrılmaktadır.

Sürekli (on the fly)

Ağın sürekli izlendiği, saldırı tespit sisteminin kesintisiz olarak çalıştığı ve düğümlere yönelik meydana gelebilecek saldırıların derhâl tespit edilmesini sağlayan sistemlerdir. Ağ ömrünün kısaltılmasına neden olmakla beraber gerçek zamanlı koruma sağlamaktadır.

Periyodik

Saldırı tespit sisteminin belirli zamanlarda çalıştığı veya çalışmasının manuel olarak tetiklendiği sistemlerdir. Düğümlerdeki enerji tasarrufunu sağlamak maksadıyla görev yapılmayan zamanlarda uyuma/uyanma sağlayan mekanizmalara benzemektedir. Ağ ömrünün kısalmasına daha az etki etmektedir. Ancak gerçek zamanlı koruma ihtiyacının olmadığı durumlarda tercih edilmelidir.

4.3. Karar Verme

Saldırı tespit sistemlerinde koruması yapılacak sistem ile ilgili olarak karar verme işlemi iki türlü olarak yapılmaktadır.

4.3.1. İş birliği ile karar verme

Bu yöntemde ağ elemanlarının tamamı bir olay meydana gelmesi durumunda verilecek karara katılmaktadır. Örneğin, çoğunluk oyu (majority voting) yönteminin kullanılması durumunda nihai karar üyelerin vereceği oy neticesinde ortaya çıkmaktadır. KAA'lar için bu yöntemde düğümler *bu bir saldırıdır* veya *bu bir saldırı değildir* tarzında oylama da bulunmakta, çoğunluğun oyuna göre bir alarm üretilmekte ya da üretilmemektedir. Düğümler arasında iş birliği tespit oranını artırmakla birlikte koordinasyonu da beraberinde gerektirmektedir.

4.3.2. Bağımsız karar verme

Her düğümün etrafında cereyan eden olaylar hakkında kendi kararlarını vermesi durumudur. Önceden programlanan kurallar çerçevesinde her düğüm saldırının varlığı hakkında kendi kararını vermektedir.

Saldırı tespit sistemleri tarafından alınabilecek kararlar hakkında yapılan [55-56]'deki çalışmalara göre, meydana gelen olaylara yönelik bir IDS tarafından verilen kararların özellikleri aşağıda açıklanmış ve Çizelge 4.1'de özetlenmiştir.

- Yanlış negatif (False negative): Sisteme yönelik bir girişim oldu, ancak IDS bunu fark edemedi ve olayın anormallik olmadığına karar verdi.
- Yanlış pozitif (False positive): Sisteme yönelik herhangi bir saldırı olmadı, ancak IDS yanlışlıkla saldırı olduğuna karar verdi, normal bir olayı anormallik olarak tespit etti.
- Doğru negatif (True negative): Sisteme yönelik bir saldırı olmadı ve IDS anormal olmayan bir olay olduğuna karar verdi.
- Doğru pozitif (True positive): Sisteme yönelik bir saldırı gerçekleşti ve IDS doğru bir şekilde bunu tespit etti.

Çizelge 4.1. IDS karar türleri [55-56]

	Yanlış	Doğru
Negatif	• Saldırı var • IDS saldırıyı tespit edemedi	• Saldırı yok • IDS olayın anormal olmadığına karar verdi
Pozitif	• Saldırı yok • IDS yanlışlıkla normal davranışı saldırı olarak algıladı	• Saldırı var • IDS saldırıyı doğru bir şekilde tespit etti.

Kablosuz algılayıcı ağlarda kullanılan saldırı tespit sistemlerinin yanlış pozitif kararlar vermesinde kablosuz haberleşmenin doğasından kaynaklanan; paketlerin çarpışması ve düşürülmesi, sınırlı iletim kapasitesi ile azalan batarya gücü son derece etkili olmaktadır.

4.4. Saldırılara Tepki

Herhangi bir saldırının gerçekleşmesi durumunda, saldırı tespit sistemlerinin hiçbir şekilde engelleyici tedbirleri alması söz konusu değildir. Bu işlem, saldırı önleme sistemlerinin (IPS) görevidir. Saldırı tespit sistemlerinin herhangi bir tespitte bulunabilmesi için bir olayın vuku bulması, yani herhangi bir saldırı veya teşebbüsün gerçekleşmesi gerekmektedir. Bir saldırı alarmının oluşturulması durumunda saldırı tespit sisteminden aşağıdaki işlemleri yapması beklenir [57];

- Olay hakkında denetim kaydı oluşturulmalı,
- Tüm ağ elemanlarını, sistem yöneticisini ve baz istasyonunu durumdan haberdar edecek alarm üretilmeli,
- Eğer mümkünse söz konusu alarm saldırganın yeri ve kimliği hakkında bilgi içermeli,
- Yine eğer mümkünse saldırının etkisini azaltacak öneriler bu alarm içerisinde tavsiye niteliğinde bulunmalıdır.

5. KABLOSUZ ALGILAYICI AĞLAR İÇİN GÜVEN YÖNETİM SİSTEMLERİ

Kablosuz algılayıcı ağlar çok çeşitli saldırılara karşı son derece açıktır, hassastır ve savunmasızdır. Ayrıca doğasında bulunan karakteristik özellikleri nedeniyle farklı güvenlik yaklaşımlarının uygulanmasını zorunlu kılmaktadır. Bu nedenle KAA'ların güvenliğinin artırılması için geleneksel ağ güvenliği mekanizmalarından farklı yöntemlerin kullanılmasına ihtiyaç vardır. Bu yöntemlerden bir tanesi, [58]'deki çalışmada detaylı olarak incelenen güven yönetim sistemleridir (trust management systems). KAA'lar için söz konusu sistemler kötücül düğümlerin tespit edilmesi maksadıyla ve özellikle iç tehdit unsurlarına yönelik bir güvenlik tedbiri olarak önerilmektedir. KAA'lar için önerilen güven yönetim sistemleri çeşitli çalışmalarda [58–61] incelenmiş ve genellikle söz konusu sistemlerin, güvenin oluşturulması (trust establishment) ve itibar sistemleri (reputation systems) olarak iki bileşenden oluştuğu belirtilmiştir. Ayrıca güven yönetim sistemlerinin daha geniş bir kavram olduğu, güvenin oluşturulması, güven değerinin izlenmesi, değişen durumlar ışığında değerlendirilmesi ve kontrollerin yapılarak tekrardan güven tesisinin yapılmasını içeren kapsamlı bir süreç olduğu [60]'daki çalışmada vurgulanmıştır.

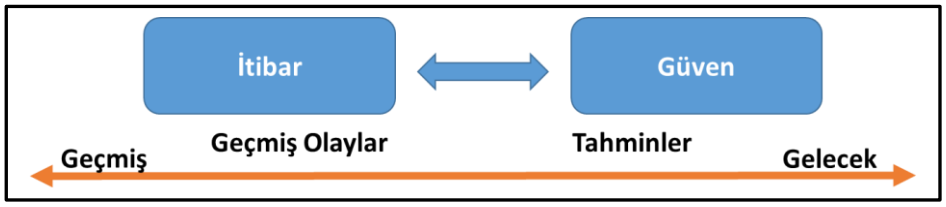
KAA'larda kullanılan güven yönetim sistemlerinin temel amacı kötücül ve bencil davranışların etkisini azaltmaktır. Bu nedenle KAA'lar için hayati öneme sahip olan güvenli yer tayini yapma, güvenli yönlendirme, erişim kontrolü, saldırı tespit sistemi ve güvenli veri kümeleme işlemleri gibi alanlarda uygulamaları mevcuttur. Bu tez kapsamında KAA'lardaki saldırılar ve saldırıları tespit edecek IDS'ler ele alındığı için burada özellikle güven yönetim sistemlerinin IDS olarak kullanılması üzerinde durulacaktır.

Güven yönetim sistemleri mevcut IDS yöntemleri ile uyum sağlayabilmekte, izleme, analiz ve meydana gelen olaylara gösterilecek reaksiyonlara karar verilmesi sürecini desteklemede kullanılabilmektedir. Ayrıca güven yönetim sistemlerinin tek başlarına saldırı tespit sistemi olarak kullanılabileceği [61]'deki çalışmada özellikle vurgulanmıştır. Günümüzde güven yönetim sistemleri KAA'lara ilave olarak; elektronik ticaret, ağ tabanlı hizmetler, noktadan noktaya ağlar gibi çok farklı alanlarda kullanılmaktadır.

Tez çalışmasının bu bölümünde KAA'lar için düğümlerin güven derecelerini göz önüne alarak kötücül düğümleri tespit etmeyi amaçlayan çeşitli güven yönetim sistemleri açıklanmıştır. Önerilen sistemleri ele almadan önce güven ve itibar kavramlarının incelenmesinin uygun olacağı değerlendirilmektedir.

5.1. Güven ve İtibar Kavramları

Günlük yaşantımızda güven (trust) ve itibar (reputation) sıklıkla kullandığımız ve aldığımız birçok kararda bilerek veya bilmeyerek sürekli başvurduğumuz kavramlardır. Bir kişinin herhangi başka bir kişiye ait gelecekteki davranışları doğru bir şekilde tahmin edebilmesi güven kavramıyla ilişkilidir. İtibar ise geçmişte yaşanan tecrübe ve olaylar neticesinde kazanılmış bir değerdir ve geleceğin tahmin edilmesi ile ilgisi yoktur. Konu hakkında yapılan [62]'deki çalışmada vurgulandığı gibi, "*itibar belli bir şahsiyete bağlı olan hafızadır*" ("*memory connected to specific identity*"). Yani geçmişte yaşanan olaylar karşımızdaki kişinin algıladığımız itibarını belirlemektedir. Oysa bir kişinin gelecekte neyi nasıl yapacağını tahmin etmek için ona duyulan güven kullanılmaktadır. Güven ve itibar kavramları aralarındaki ilişki Şekil 5.1'de görülmektedir.



Şekil 5.1. Güven ve itibar kavramları arasındaki ilişki

KAA'lardaki güven ise algılama verisinin doğru olması, çok sıçramalı iletişimdeki düğümlerin kendilerine gelen paketleri iletmesi, düğümlerdeki işlem yeteneklerinde hata bulunmaması, hizmetlerin sürekli işler olması gibi konular göz önüne alınarak başka bir düğüm veya fonksiyonun güvenilirliği hakkında yapılan öznel bir değerlendirmedir. Söz konusu iki kavram arasındaki ilişki günlük hayatta kullandığımız şekliyle şöyle ifade edilmektedir: "*Sana güveniyorum çünkü iyi bir itibarın var*", "*sana güvenmiyorum çünkü*

kötü bir itibarın var". İtibarın iyi veya kötü olması gelecekteki muhtemel hareketler hakkında ipuçları vermektedir.

5.2. Güvenin Karakteristik Özellikleri ve Güven Değerleri

Güven hakkında literatürde yapılan çeşitli çalışmalarda [63-66], güvenin bir takım karakteristik özelikleri olduğu vurgulanmaktadır. Bu özellikler özetle şöyledir:

- *Öznellik (Subjective):* Geçmişteki belirli olayları gözlemleyen veya önerilerde bulunan üçüncü şahıs görüşlerinin dikkate alınması ile gerçekleşmektedir.
- *Birleştirilebilirlik (composable):* Düğümler belirli bir düğüm için komşularından gelen güven bilgisini birleştirebilir.
- *Dinamiklik (Dynamic):* Güven, zaman ve mekânsal olarak değişebilmektedir.
- *Asimetrik olma (Asymmettric):* Güven kavramında karşılıklı olma durumu söz konusu değildir. Örneğin A düğümü B düğümüne güvenirken tam tersi geçerli olmayabilir.
- *Tam olmayan geçişlilik (Incomplete transitive):* Güven yolu oluşturulabilir, örneğin A düğümü B'ye, B düğümü de C'ye güvenebilir. Ancak A düğümü C'ye güvenebilir veya güvenmeyebilir.
- *Dönüşlü olma (reflexive):* Her bir varlık kendisine güvenir.
- *İçeriğe duyarlı (context sensitive):* Güvenin bir takım gereksinimleri ile etkin olması durumudur.

Yukarıda ifade edilen güven özelliklerine ilave olarak KAA'lar göz önüne alındığında güvenin üç özgü ilave özelliği bulunmaktadır:

- *Düşük delil (low evidence):* KAA'larda düğümler hakkında yapılan gözlemler veya diğer düğümlerin önerileri, ağın karakteristik özellikleri nedeniyle oldukça kısıtlıdır.
- *Belirsiz kararsızlık (ambiguous instability):* Güvenilirlik seviyesi kablosuz haberleşme ortamı nedeniyle çok fazla kararsızlık göstermekte ve sürekli değişmektedir.

- *Karmaşık güven sistem mimarileri (complicated trust system structure):* KAA'lardaki birçok farklı mimaride olduğu gibi karmaşıklık söz konusudur. Güven değerlendirmesi, güven değerinin hesaplandığı yere göre merkezi güven sistemi, dağıtık güven sistemi veya hibrit güven sistemi kullanılabilmektedir.

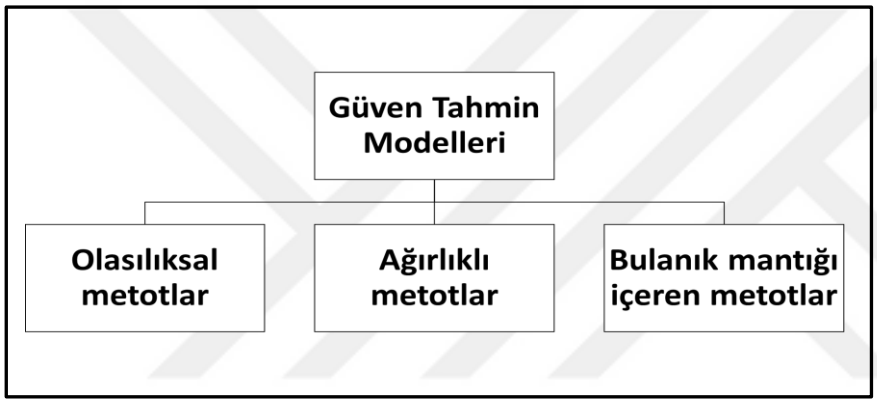
Yapılan çalışmalarda güven değerinin nasıl hesaplanacağı ve başlangıç güven değerinin nasıl belirleneceği hakkında farklı yaklaşımlar bulunmaktadır. Güven değeri konusunda genel kabul edilen yaklaşım değerin *devamlı* ya da *kesintili* olacağı yönündedir. Güven değerinin sürekli olması, örneğin bu değerin [-1, 1] aralığında sürekli bir fonksiyon şeklinde tanımlanmasıyla mümkün olabilmektedir. Kesintili güven değerlerinde ise her bir düğüme tam sayı değerleri atanmaktadır. Güven başlangıç değerinin belirlenmesinde de temel olarak üç farklı yaklaşım bulunmaktadır.

- *Yüksek başlangıç değeri*: Ağın kurulumu esnasında herhangi bir saldırının bulunmaması ve güvenliğin tam olarak sağlandığından emin olunması durumunda kullanılır. Yapılan gözlemler ve tecrübeler zamanla bu değerin azalmasına neden olabilir.
- *Düşük başlangıç değeri*: Eğer ağın kurulacağı ortam güvensiz ise bu durumda kullanılması gereken yöntemdir. Kurulum aşamasından itibaren saldırıların olabileceğini göz önüne almak mantıklı bir yaklaşım olacaktır.
- *Orta başlangıç değeri:* Tüm ağ elemanlarının aynı güvenilirlik seviyesine haiz olduğu başlangıç durumlarında dikkate alınacak yaklaşımdır.

Güven değerinin hesaplanmasında kullanılacak sayıların tam sayı, kesirli veya ondalık sayı olması, geleneksel ağlar için çok anlamlı değil iken kablosuz algılayıcı ağlarda hesaplama, depolama ve iletim kısıtları nedeniyle bu değerlerin gerçek sayılardan oluşması ilave yükler getirmektedir. Bu nedenle KAA'larda hesaplanacak güven değerinin tam sayı olması arzu edilmektedir.

5.3. Güven Yönetim Yaklaşımları

KAA'larda kullanılan güven yönetim sistemlerinin en önemli aşaması düğümlerin sahip olduğu güven değerinin tahmin edilmesi veya yapılan değerlendirmeler neticesinde hesaplanabilmesidir. Yapılan çalışmaların çoğunluğu [60, 61], güvenin tahmin edilmesi üzerine kuruludur. Güven tahmin modellerini Şekil 5.2'de görüldüğü gibi dört ana başlık altında toplamak mümkündür. Ayrıca güven tespitinin yapıldığı seviye açısından da düğüm seviyesi (node level) ve sistem seviyesi (system level) güven tespiti olmak üzere bir sınıflandırma yapmak mümkündür.



Şekil 5.2. Güven tahmin modelleri [60]

5.3.1. Olasılıksal güven tahmini tabanlı metotlar

Bu yöntemde güven, *Bayesian Teorisi* ile birlikte olasılık dağılımının kullanılmasını esas almaktadır. Güven değeri düğümün gelecekteki hareketlerinin beklenen olasılığı olarak ifade edilmektedir. *Bayesian Teorisi* matematiksel olarak sağlam temelleri olan ve güven değerlendirme metotları ile uyumlu olması nedeniyle birçok çalışmada [64-66] üzerinde durulan bir yöntemdir. Bir olayın geçmişte olma olasılığı kullanılmakta, meydana gelen olayların ışığında bu olasılık değeri güncellenmektedir. Hesaplamaların yapılmasında genellikle *Beta dağılımı* kullanılmaktadır. *Beta Dağılım;* [0, 1] aralığında iki tane pozitif şekil parametresi (tipik olarak α ve β) ile normalize edilmiş bir sürekli olasılık dağılımıdır. *Beta dağılımın* KAA'larda kullanılabileceği ve detayları ilk defa [67]'deki çalışmada

vurgulanmıştır. Bu dağılımının güven yönetim sistemlerinde kullanılması aşağıda açıklanmıştır.

Beta itibar sistemi (beta reputation system)

İkili olayların geçmişteki gerçekleşme olasılıkları α ve β gibi iki farklı parametre ile tanımlanabilir. Bu durumda Beta dağılımı $f(p|\alpha,\beta)$ gamma fonksiyonu Γ kullanılarak Eş. 5.1'deki gibi ifade edilebilir:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (5.1)$$

$$0 \leq p \leq 1,\ \alpha > 0, \beta > 0$$

Eş. 5.1'deki olasılık değişkeni $p \neq 0$, $\alpha < 1$ ve $p \neq 1$, $\beta < 1$ durumunda, Beta dağılımı beklenen değeri Eş. 5.2'deki gibi yazılabilir:

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad (5.2)$$

Beta dağılımının KAA'larda nasıl kullanıldığının daha net anlaşılabilmesi maksadıyla şöyle bir örnek verilebilir. Örneğin Düğüm A Düğüm B'nin paket iletim hareketlerini izlemekte olsun. Burada paket iletiminin başarılı olması veya başarısız olması gibi iki farklı durum söz konusudur. Başarılı paket iletim sayısının r ile başarısız paket iletim sayısının ise s ile gösterildiğini varsayalım. Bu durumda Beta fonksiyonu geçmişteki başarılı ve başarısız olay sayılarını (olay sayıları tam sayı olmak durumunda) almakta ve gelecekteki başarılı paket iletim olasılığını Eş. 5.3'de gösterildiği şekilde hesaplamaktadır:

$$\alpha = r+1,\ \beta = s+1,\ r,s \geq 0,\ E(p) = \frac{r+1}{r+s+2} \quad (5.3)$$

p değişkeni başarılı paket iletim sayısını, $f(p|\alpha,\beta)$ ise p'nin belirli bir değeri için gerçekleşme olasılığını ifade etmektedir. $E(p)$ ise Düğüm B'nin gelecekte paketleri başarılı bir şekilde iletme olasılığıdır. Bu örnekten de anlaşılacağı üzere Beta dağılımı ve Beta dağılım

fonksiyonu vasıtasıyla KAA'larda düğümlerin gelecekteki muhtemel davranışları tahmin edilebilmektedir.

5.3.2. Ağırlıklı güven tahmini tabanlı metotlar

Ağırlıklı metotlar kullanarak güven tahmini, bir düğümün zaman içerisindeki davranış ve performansındaki değişimler göz önüne alınarak yapılmaktadır. Basit bir yöntemdir, uygulaması kolaydır ancak matematiksel olarak temelleri sağlam olan bir alt yapıya sahip değildir. Shaikh ve arkadaşları tarafından [68]'de yapılan çalışmada, kümelenmiş mimariye sahip KAA'lar için *grup tabanlı güven yönetim sistemi* (GTMS) geliştirilmiştir. Geliştirilen GTMS sisteminin detayları tez çalışmasının 6'ncı bölümünde sunulan modelin anlaşılmasına katkı sağlamak maksadıyla aşağıda açıklanmıştır.

Grup tabanlı güven yönetim sistemi (Grouped Based Trust Management System, GTMS)

Sistemde güven hesabı; düğüm seviyesinde, küme başı (CH) seviyesinde ve baz istasyonu (BS) seviyesinde olmak üzere ayrı ayrı yapılmaktadır. Düğümler doğrudan (direct) veya dolaylı (indirect) gözlemleri ile güven değerini hesaplamaktadır. Hesaplanan güven değeri üzerindeki zaman etkisini azaltmak için bir zamanlama pencere mekanizması kullanılmaktadır. Birçok değişik birimden oluşan zamanlama penceresi (Δt) başarılı ve başarısız etkileşimleri saymaktadır. Bu zaman diliminde gerçekleşen etkileşimler sayılmakta ve zaman penceresinin ilerlemesi ile bir önceki dönemde gerçekleşen olaylar silinmektedir. Zaman penceresindeki bilgi kullanılarak, Düğüm A tarafından Düğüm B'nin etkileşim güven değeri $T_{A,B}$ Eş. 5.4'deki gibi hesaplanmaktadır:

$$T_{A,B} = \left[100\left(\frac{(S_{A,B})^2}{(S_{A,B}+U_{A,B})+S_{A,B}+1}\right)\right] \tag{5.4}$$

Eş. 5.4'deki ifade en yakın tam sayı fonksiyonudur. $S_{A,B}$ Düğüm A ve B arasındaki Δt sürede gerçekleşen toplam etkileşim değeridir. $U_{A,B}$ ise yine aynı zaman periyodunda iki düğüm arasında gerçekleşen toplam başarısız etkileşim sayısıdır. Önerilen yöntemde, güven değerinin hesaplanmasını müteakip düğümlerin durumları güvenilir (trusted), belirsiz

(uncertain) veya güvenilmez (untrusted) olarak işaretlenmektedir. Ayrıca her CH periyodik olarak kendi kümesi hakkındaki güven bilgisini yayımlamak suretiyle kendi elemanları hakkında daha iyi bir değerlendirme yapmaya çalışır. CH komşularından kümesindeki üyeler hakkında güven durumlarını almayı müteakip Eş. 5.5'de gösterildiği şekilde bu değerleri bir matriste saklamaktadır.

$$TM_{ch} = \begin{pmatrix} S_{ch,1} & \cdots & S_{n,1} \\ \vdots & \ddots & \vdots \\ S_{ch,n} & \cdots & S_{n,n-1} \end{pmatrix} \tag{5.5}$$

Eş. 5.5'deki TM_{ch} CH için güven durum matrisidir ve $S_{ch,1}$ise 1 numaralı düğüm için CH tarafından tutulan güven değeridir. Bir düğümün güven durumundaki göreceli farklar belirlendikten sonra küresel değer CH tarafından belirlenmektedir. Göreceli fark standart normal dağılım vasıtasıyla belirlenmektedir.

Düğüm seviyesindeki hesaplamalara ilave olarak baz istasyonu da CH'ler için geçmişteki davranışları göz önüne alarak bir güven değerini, Eş. 5.6'yı kullanarak hesaplamaktadır.

$$T_{BS,ch_i} = \left[100\left(\frac{(S_{BS,\ ch_i})^2}{(S_{BS,\ ch_i} + U_{BS,\ ch_i})\,(S_{BS,\ ch_i}+1)}\right)\right] \tag{5.6}$$

$S_{BS,\ ch_i}$ değeri BS ile CH_i arasındaki toplam başarılı etkileşim sayısını $U_{BS,\ ch_i}$ise toplam başarısız etkileşim sayısını ifade etmektedir.

Yukarıdaki yönteme benzer şekilde ağırlıklı güven tahmini tabanlı güven yönetim sistemleri çeşitli çalışmalarda [69-70] önerilmiştir. Burada temel amaç her bir düğümün güvenlik değerini belirli ağırlıklar kullanarak hesaplayabilmektir. Bu ağırlıklar düğümün kendisi tarafından yapılan gözlemler ile komşu düğümler tarafından dolaylı olarak elde edilen güven bilgisinin uygun yöntemlerle bir araya getirilmesini içermektedir. Dolayısıyla herhangi bir düğüm hakkında güven hesaplaması yaparken yalnızca doğrudan gözlemlere dayanmamak ve diğer düğümler ile iş birliği yapıyor olmak daha doğru sonuçların ortaya çıkmasına neden olacaktır. Tez çalışması kapsamında 6'ncı bölümde benzer durum kullanılmıştır.

5.3.3. Bulanık mantık tabanlı güven yönetimi

Birçok deneysel ve bilimsel çalışmada Aristo Mantığı esas alınmakta yani olaylar, doğru ya da yanlış, siyah ya da beyaz kavramlarında olduğu gibi iki seçenekli olarak değerlendirilmektedir. Ancak, günlük yaşantımızda bütün olayları böylesine net bir şekilde tanımlamak her zaman mümkün olmayabilir. İnsanlar günlük hayatlarına ilişkin olaylar hakkında kararlar alırken zihinlerinde bir takım karmaşık süreçleri işletmekte ve çeşitli belirsizlikleri de göz önünde bulundurarak kararlar vermektedir. Çeşitli nedenler ve bilgi eksikliğinden dolayı ortaya çıkan karmaşıklık ve belirsizlikler *bulanık mantıkla* modellenebilmektedir.

Bulanık mantık özellikle incelenecek olayın çok karmaşık olması ve konuyla ilgili bilginin de yetersiz olması durumlarında kullanılan bir yöntemdir. KAA'lardaki karakteristik özellikler nedeniyle belirsizliklerin fazla olması bu sistemlerde bulanık mantık uygulamasının geliştirilmesi konusunda araştırmacıları motive etmiştir. Düğümlerin güvenilirlik derecelerini bulanık mantıkla tespit etmek için izlenmesi gereken adımlar şöyledir [71]:

- *Bulanık eşleme (fuzzy matching):* Girdi seviyesinin tahmin edilmesi
- *Çıkarım (inference):* Eşleşme derecesine uygun olarak kural sonucunun hesaplanması
- *Birleştirme (combination):* Tüm bulanık mantık kuralları tarafından çıkarım yapılan sonuçların birleştirilmesi ve nihai kararın verilmesi.

Feng ve arkadaşları tarafından KAA'larda bulanık mantığın düğüm hareketlerini göz önüne alarak değerlendiren [72]'deki çalışmada, doğrudan ve dolaylı güven değerleri aşağıda belirtilen güven faktörleri ile hesaplanmış ve bu faktörler ile bulanık mantık uygulanması durumunda verimli sonuçlar alınacağı belirtilmiştir:

- Alınan paket oranı
- Başarılı bir şekilde gönderilen paket oranı
- Kendisine gelen paketleri iletme oranı

- Zaman açısından tutarlılık
- Düğümün erişilebilir olması
- Güvenlik seviyesi

Konu hakkında yapılan diğer bazı çalışmalarda [73-74], yine bulanık mantığı KAA'larda kullanmaya yönelik öneriler getirilse de söz konusu yöntemlerin uygulanabilir olmadığı değerlendirilmektedir.

Bu bölümde güven değerinin tahmin edilmesine yönelik yöntemler üzerinde durulmuştur. Her ne kadar literatürdeki çalışmaların çoğunluğu yukarıda bahsedilen sınıflandırmaya girse de yukarıda belirtilen sınıflandırmaya girmeyen yöntemlerde yazarlar tarafından önerilebilmektedir. Örneğin karınca kolonileri sistemi tabanlı güven değerlerinin hesaplanması [75]'de önerilmiştir. Söz konusu algoritma beş adımdan oluşmaktadır. Birinci adımda, algoritma çalıştırılmakta ve sanal olarak oluşturulan karıncalar grubu ağa yerleştirilerek bilgi toplanmaktadır. İkinci safhada, puanlama ve derecelendirme yapılmaktadır. Eğer karınca hedef düğümü bulursa kendisine bir puan atanmaktadır. Üçüncü adımda, ağ içinde alıcı ve hedef arasındaki en güvenilir yolun seçilmesi yapılmaktadır. Dördüncü aşamada, işlemin tamamlanmasını müteakip ağdan alınan hizmete ilişkin memnuniyet anketi yapılmakta ve son olarak beşinci adımda ise ödüllendirme veya cezalandırma işlemi gerçekleşmektedir.

6. KABLOSUZ ALGILAYICI AĞLAR İÇİN GÜVEN VE KÖTÜYE KULLANIM TABANLI HİBRİT SALDIRI TESPİT SİSTEMİ

Tez çalışmasının bu bölümünde, kümeleme mimarisindeki KAA'lar (clustered-based WSNs) için önerilen güven ve kötüye kullanım tabanlı hibrit saldırı tespit sistemi detaylı olarak açıklanmış, önerilen sistemin benzetim yoluyla değerlendirmesi yapılmış ve elde edilen sonuçlar tartışılmıştır.

Bu bölümde geliştirilen saldırı tespit sistemi ilk defa Özdemir tarafından [76]'daki çalışmada önerilen *fonksiyonel itibar (functional reputation)* ile 4'üncü bölümde detayları açıklanan *kötüye kullanım (misuse based) tabanlı veya imza tabanlı (signature based)* yaklaşımları uygun bir şekilde birlikte kullanmayı önermektedir. Bu sayede saldırılar etkin bir şekilde tespit edilirken sistemlere asgari ilave yük getirilmektedir.

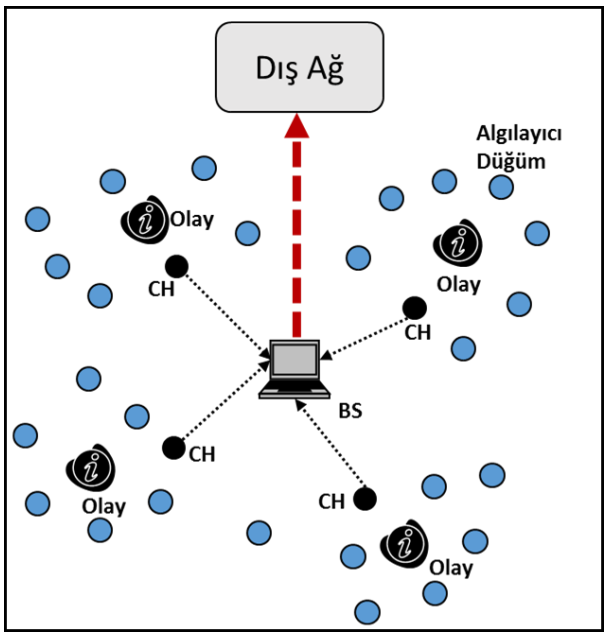
Önerilen yöntem ile saldırıların tespit edilmesi, tüm düğümler arasındaki iş birliği sayesinde merkezi olarak gerçekleştirilmektedir. Düğümler arasındaki bu iş birliği yoğun koordinasyonu ve eşlemeyi gerektiren bir çalışma değildir. Her düğümün kendisine verilen gözlem yapma, yapılan gözlem neticesinde güven değerini hesaplama (doğrudan güven), hesaplanan değerlerin komşu düğümler ile paylaşılması ve neticede komşu düğümlerden gelen bildirimlerinde (dolaylı güven) hesaplamalara katılarak düğümler hakkında gerçeğe daha yakın güven değerinin hesaplanması esasına dayanmaktadır. Her düğüm bu işlemleri gerçekleştirmekte ancak sistemlere yönelik bir saldırının varlığı hakkında alarmın üretilmesi işlemi tüm ağdaki verilerin merkezi olarak toplandığı BS tarafından güven sistemlerine ilave olarak imza tabanlı kurallarında işletilmesi ile yapılmaktadır.

İmza tabanlı saldırı tespit yaklaşımının yüksek tespit oranı ile güven yönetim sistemlerinin anormal davranış sergileyen düğümlerin ortaya çıkarılması özelliklerini birlikte kullanmak temel hedef olarak belirlenmiştir. Söz konusu hedefe ulaşmak maksadıyla, her düğüm sistem tarafından önerilen *beş fonksiyonel itibar* ölçütünden ilgili olanını kullanarak komşuları hakkında elde ettiği direkt (doğrudan) gözlemler ile her bir komşusu için güven değerini hesaplamaktadır. Bu güven değerleri düğümler arasında paylaşılmakta ve komşulardan gelen bildirimler göz önüne alınarak birleştirilmiş güven değeri (consolidated

trust value, CTV) hesaplanmaktadır. Komşularına ait kimlik bilgilerinin ve CTV değerlerinin paylaşılması kontrol paketleri (control packets, CPs) vasıtasıyla gerçekleşmektedir. BS merkezi olarak tüm ağı görselleştirmek maksadıyla kendisine gelen tüm verileri birleştirmekte, hem güven değerlerini hem de imza tabanlı saldırı tespit kurallarını çalıştırarak kötücül düğümleri tespit etmektedir.

6.1. Haberleşme ve Sistem Modeli

Önerilen sistemde çok sayıda algılayıcı düğümün bulunduğu büyük kümeleme tabanlı KAA'nın kullanıldığı düşünülmektedir. Söz konusu sistemde ağ; algılayıcı düğümler, küme başları (CHs) ve baz istasyonu (BS) olmak üzere üç katmandan oluşmaktadır. Genel olarak düğümler mesajlarını CH'e göndermektedir. Ancak bir düğüm, CH'in hareketlerinden şüphe duyarsa (CH için hesaplanan CTV değerinin eşik değerinin altına düşmesi durumu) çok sıçramalı yönlendirme vasıtasıyla mesajını doğrudan BS'ye gönderebilmektedir. Bu işlemin detayları müteakip bölümde açıklanmıştır. Önerilen sistemin mimarisi ve haberleşme modeli Şekil 6.1'de görülmektedir.



Şekil 6.1. Önerilen modelin haberleşme ve sistem mimarisi

Önerilen sistemde, BS normal düğümlere oranla kaynak açısından çok daha güçlü ve donanımlıdır. Bu nedenle tüm algılayıcı düğümlerin yönetilmesinden sorumludur. Kimlik bilgilerinin düğümlere atanması, önceden paylaşılan anahtarların üretilmesi, başlangıç güven değerlerinin atanması, sistemdeki tüm düğümlere ait güven değerlerinin saklanması, kendisine gelen sorgulara ilgili cevapların verilmesi ve neticede saldırı tespiti ile kötücül düğümlerin belirlenerek tüm ağa durumun bildirilmesi işlemleri BS tarafından gerçekleştirilmektedir.

Küme başları (CHs), düğümlerden alınan verinin birleştirilmesi, kontrol paketlerinin (CPs) BS'ye gönderilmesi ve BS sorgularına cevap verilmesi gibi görevleri gerçekleştirmektedir. Düğümler dinamik bir şekilde CH olarak görev yapabilmekte ve BS ile doğrudan haberleşebilme yeteneği olduğu sürece her bir düğümün CH olabileceği varsayılmaktadır. Düğümlerde kalan artık enerji miktarı her ne kadar enerji yoğun işlemler gerçekleştiren CH olmak için en büyük seçim kıstası olsa da düğümlerin ne şekilde CH olarak seçildiği bu çalışmanın kapsamı dışındadır.

Sistemin bir diğer elemanı olan algılayıcı düğümler ise fiziksel dünyadaki olayları algılama ve ilgili olayları CH'ye iletmekten, kendilerine tek sıçrama (single hop) uzakta bulunan komşularının güven değerlerini hesaplamaktan, bu değerleri güven tablosunda saklamaktan ve bu bilgiyi komşuları ile paylaşmaktan sorumludur. Ayrıca düğümler belirlenen eşik güven değeri altına düşen CH olması durumunda, CH'nin kimlik bilgilerini şifreleyerek konu hakkında BS'yi haberdar etmek maksadıyla yayın (broadcast) yapmaktan sorumludur.

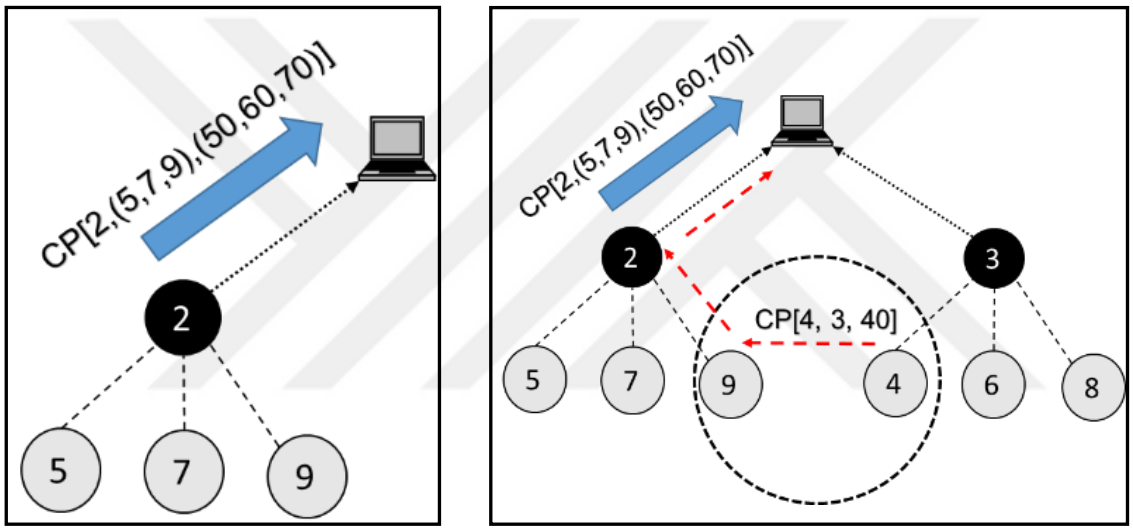
6.2. Tehdit Modeli

Önerilen sistemde saldırganlar düğümleri fiziksel olarak elde edebilir veya kablosuz haberleşmeye yönelik çeşitli saldırılar vasıtasıyla düğümleri ele geçirebilir. Bir düğüm ele geçirildiğinde üzerindeki tüm bilginin saldırganlar tarafından öğrenildiği düşünülmektedir. Buna ilave olarak ağ hem iç hem de dış tehditlere maruz kalabilir. Sistemin kurulumu

aşamasında herhangi bir saldırı olmayacağı, saldırganların sistemin kurulup çalışmaya başlamasını müteakip ortaya çıkacağı varsayılmaktadır.

6.3. Kontrol Paketleri

Önerilen sistemde, CH'ler BS'nin karar verme süreçlerine katkı sağlamak maksadıyla periyodik olarak Şekil 6.2 (a)'da görüldüğü gibi kontrol paketleri (CPs) göndermektedir. Ayrıca, CH'nin hareketlerinden şüphelenen algılayıcı düğümler alternatif yolları kullanmak suretiyle Şekil 6.2 (b)'de görüldüğü gibi BS'ye durum hakkında bilgi iletmektedir.



(a) (b)

Şekil 6.2. Kontrol paketleri (CPs)

Kullanılan CP'lerin içerdiği bilgiler Eş. 6.1'de görülmektedir:

$$CP = [ID, [NB\_ID], [CTV]] \quad (6.1)$$

Eş. 6.1'deki ID, kontrol paketini gönderen düğümün kendi kimlik bilgisini, NB_ID düğümün tüm komşularına ait kimlik bilgilerini, CTV ise tüm komşu düğümler için birleştirilmiş güven değerini ifade etmektedir. Söz konusu CTV değerleri yapılan doğrudan ve dolaylı gözlemler neticesinde hesaplanmakta olup detayları ilerleyen bölümlerde açıklanmıştır. Örneğin Şekil 6.2 (a)'da CH olan 2 numaralı düğümün 5, 7 ve 9 numaralı komşu düğümleri bulunmakta,

bu komşular için hesaplanan güven değerleri ise sırasıyla 50, 60 ve 70 olarak gönderilen CP'de görülmektedir.

Eğer kontrol paketini CH değil de bir algılayıcı düğüm gönderiyorsa, CH'nin hareketlerinden bir şüphe duyma durumu mevcut demektir. Bu durumda CP'deki ID algılayıcı düğümün kendi kimlik bilgisi, NB_ID ise şüpheli hareketleri olan CH'ye ait kimlik bilgisi ve CTV ise o CH için düğüm tarafından hesaplanan güven değeri olmaktadır. Örneğin Şekil 6.2 (b)'de 4 numaralı algılayıcı düğüm CH olan 3 numaralı düğüm hakkında doğrudan ve dolaylı gözlemler yoluyla güven değeri hesaplamış, hesaplanan değer 40 olarak bulunmuş, bu değer eşik değerden düşük olduğu için bir anormallik olduğu düşünülerek CH kimlik bilgisi ile CTV değeri şifrelenerek farklı yollar kullanmak suretiyle BS'ye iletilmeye çalışılmıştır.

6.4. Fonksiyonel İtibar Değerlerinin Hesaplanması

Güven ile itibar kavramları arasındaki ilişki ile Beta dağılımının KAA'larda kullanılabileceği tez çalışmasının 5.1'inci bölümünde detaylı olarak ele alınmıştır. Kısaca itibar geçmiş tecrübeler veya gözlemler neticesinde kazanılmaktayken, güven bir olayın gelecekte gerçekleşme olasılığını ifade etmektedir. KAA'larda olaylar ikili olay (binary event) olarak ifade edilebilir ve bu sayede Beta dağılımı kullanılarak düğümlerin gelecekteki muhtemel hareket tarzları tahmin edilebilir. Burada önemli olan KAA'larda kullanılacak uygun *güven ölçütlerini* belirlemek ve Eş. 5.3'de ifade edilen beklenen değerin hesaplanabilmesidir.

Önerilen sistemde algılayıcı düğümler dâhil tüm KAA elamanları komşularına ait fonksiyonel itibar değerlerini uygun güven ölçütlerini kullanarak hesaplamaktan, hesaplanan değerleri fonksiyonel itibar tablosunda (Functional Reputation Table, FRT) saklamaktan ve periyodik olarak bu tabloları komşuları ile paylaşmaktan sorumludur. KAA elemanları tarafından kullanılması uygun olacağı değerlendirilen güven ölçütleri (fonksiyonel davranışlar) şunlardır:

- Haberleşmede güvenilirlik (m_1)
- Algılanan veride güvenilirlik (m_2)

- Verinin zamanında raporlanmasında güvenilirlik (m_3)
- Olay raporlama oranında güvenilirlik (m_4)
- Verinin yönlendirilmesinde güvenilirlik (m_5)

Düğümler arasındaki etkileşim başarılı veya başarısız olabilir. Bu nedenle her bir fonksiyonel davranış için iki adet sayaç tutulmaktadır. Başarılı etkileşimler için $S_{count^{(m_i)}}$, başarısız etkileşimler için ise $F_{count^{(m_i)}}$ kullanılmaktadır. Bu iki sayacın başlangıçtaki varsayılan değeri 0 olarak atanmakta ve iki düğüm arasındaki her bir etkileşim durumuna göre değer artırılmaktadır. Yukarıda ifade edilen beş güven ölçütünün detayları aşağıda açıklanmıştır.

Haberleşmede güvenilirlik (m_1): Haberleşmedeki güvenilirlik, gönderilen ve alınan paketler göz önüne alınarak hesaplanmaktadır. Örneğin, CH düğümlerdeki algılama verilerini toplamak istediğini bir mesaj yolu ile düğümlere iletmekte, gönderilen mesaja cevap gelmesi başarılı etkileşim olarak değerlendirilmekte ve ilgili düğüm için $S_{count^{(m_1)}}$ sayaç değeri artırılmakta, cevap gelmemesi ise başarısız etkileşim olarak kabul edilmekte ve $F_{count^{(m_1)}}$ değeri artırılmaktadır.

Algılanan veride güvenilirlik (m_2): Her düğüm fiziksel olaylar ile ilgili algılama verisini CH'ye iletmektedir. Daha sonra CH, verileri birleştirmekte ve birleştirilmiş veriyi BS'ye göndermektedir. Bu nedenle düğümler tarafından gönderilen veriler son derece önemlidir ve bu verilerin taze olması önem arz etmektedir. Birçok senaryoda düğümler sıcaklık, nem, basınç vb. örneklerde olduğu gibi sayısal değerler olarak ölçülmektedir. Örneğin, CH'nin n tane düğümden d_1, d_2, …. d_n gibi algılama verisini aldığı varsayıldığında i düğümünün algıladığı veri değerinin $d_i \, \epsilon \, |d_{avg} \pm 3 * \sigma_d|$ arasında olması durumunda güvenilir olarak değerlendirilmektedir. Ancak bu durumda i düğümü için $S_{count^{(m_2)}}$ değeri artırılmakta, aksi durumda $F_{count^{(m_2)}}$ değeri artırılmaktadır. Eğer algılama verisi söz konusu aralıkta değilse veride veya ilgili algılayıcıda bir sorun olduğu aşikârdır. Burada d_{avg} algılama verisinin ortalama değerini, σ_d ise algılama verisinin standart sapma değerini ifade etmektedir.

Verinin zamanında raporlanmasında güvenilirlik (m_3): Kümeleme mimarisindeki KAA'larda her düğüm *zaman bölmeli çoklama* (TDMA) zamanlamasındaki kendilerine tahsis edilen

zaman diliminde algıladıkları verileri CH'ye bildirmek durumundadırlar. Özellikle güvenlik bakış açısından verinin tazeliği hayati öneme haizdir. Örneğin ΔS_t, ΔR_t, ve T_{th} değerleri sırası ile planlanan zaman, verinin alındığı zaman ve gecikme için eşik değeri olsun. Bu durumda CH herhangi bir düğüm ile olan etkileşimini $|\Delta R_t - \Delta S_t| \leq T_{th}$ durumunda başarılı olarak nitelendirecek, aksi takdirde verinin zamanında raporlanmadığını ve bu nedenle verinin taze olmadığını değerlendirecektir.

Olay raporlama oranında güvenilirlik (m_4): Aynı küme içerisinde bulunan tüm algılayıcı düğümler çoğunlukla aynı fiziksel olayları izlemek ile görevlidir. Bu nedenle olay raporlama oranının belirli bir eşik değeri arasında olması gerekmektedir. Örneğin aynı kümede bulunan i ve j düğümlerinin aynı fiziksel olayları takip etmek üzere görevlendirildiği, ayrıca ΔR_i, ΔR_j, ve ΔR_{th} değerlerinin de sırasıyla i ve j düğümünün belirli bir dönemde meydana gelen fiziksel olay hakkındaki rapor sayısı ve ΔR_{th}'nin ise belirlenen eşik değeri olduğu varsayılırsa, i düğümü tarafından $|\Delta R_j - \Delta R_i| < \Delta R_{th}$ olması durumunda $S_{count^{(m_4)}}$ değeri artırılacak ve bu durum başarılı bir etkileşim olarak değerlendirilecektir.

Verinin yönlendirilmesinde güvenilirlik (m_5): Herhangi bir CH'den BS'ye gönderilen CP'ler tüm küme elemanları tarafından duyulmakta ve bu paketler düğümler tarafından da alınmaktadır. Bu durumda, her düğüm paketi kontrol etmekte ve kendi kimlik bilgisinin CP'de olup olmadığına bakmaktadır. Eğer CH düğümün kimlik bilgisini gönderdiği CP içine eklemiyorsa o düğüm CH hakkındaki $F_{count^{(m_5)}}$ sayacını artırmaktadır.

Önerilen sistemde bütün fonksiyonel itibar ölçütlerinin tüm ağ bileşenleri tarafından kullanılması söz konusu değildir. Her ne kadar kullanılan ölçüt sayısının artırılması anormal düğüm davranışlarının tespit edilmesi olasılığını artıracak olsa da, sistemlere asgari ilave yük getirecek saldırı tespit sistemini tasarlamak amacıyla her bir ağ bileşeni tarafından kullanılacak ölçütler sınırlandırılmış ve Çizelge 6.1'de sunulmuştur.

Çizelge 6.1. Ağ bileşenleri fonksiyonel itibar ölçütleri

Fonksiyonel İtibar Ölçütleri	**Ağ Bileşenleri**		
	Düğümler	***CHs***	***BS***
Haberleşmede güvenilirlik (m_1)	Evet	Evet	Evet
Algılanan veride güvenilirlik (m_2)	Hayır	Evet	Evet
Verinin zamanında raporlanmasında güvenilirlik (m_3)	Hayır	Evet	Evet
Olay raporlama oranında güvenilirlik (m_4)	Evet	Hayır	Hayır
Verinin yönlendirilmesinde güvenilirlik (m_5)	Evet	Hayır	Hayır

Yukarıda verilen bilgiler ışığında fonksiyonel itibar değerinin nasıl hesaplandığının net bir şekilde anlaşılması maksadıyla aşağıda bir örnek verilmiştir. Buna göre, CH olan i düğümü, davranışlarını izlediği j düğümünün güven değerini Çizelge 6.1'de gösterilen ölçütleri kullanarak Eş. 6.2'de gösterildiği şekilde hesaplamaktadır.

$$T_{ij} = \sum_{k=1}^{3} W(m_k) * T_{ij}^{m_k} \tag{6.2}$$

Eş. 6.2'deki $W(m_k)$ fonksiyonel itibar ölçütü ağırlık değeridir ve Eş. 6.3'de gösterildiği şekilde hesaplanmaktadır.

$$W(m_k) = \frac{S_{count}(m_k)}{TS_{count}(j)} \tag{6.3}$$

$TS_{count}(j)$ değeri i düğümünün j düğümü hakkında hesapladığı tüm başarılı etkileşimleri sayısıdır. Bu örnekte m_1, m_2, ve m_3 ölçütleri için gerçekleşen tüm başarılı etkileşimler toplamıdır ve Eş. 6.4'de görüldüğü şekilde hesaplanmaktadır.

$$TS_{count}(j) = \sum_{k=1}^{3} S_{count}(m_k) \tag{6.4}$$

Son olarak tahmin edilen güven değeri Eş. 5.3 kullanılarak Eş. 6.5'deki gibi yeniden yazılabilir.

$$T_{ij}^{m_k} = E(Beta(\alpha,\ \beta)) = \frac{S_{count}(m_k)+1}{S_{count}(m_k)+F_{count}(m_k)+2} \tag{6.5}$$

$$\alpha = S_{count}(m_k) + 1, ve\ \beta = F_{count}(m_k) + 1$$

Eş. 6.2 ve Eş. 6.5'deki ifadelerin yeniden yazılması neticesinde önerilen sistemdeki CH'ler için güven değeri hesaplama denklemi Eş. 6.6'daki gibi olmaktadır.

$$T_{ij} = \sum_{k=1}^{n} \left(\frac{S_{count}(m_k)}{TS_{count}(j)}\right) * \left(\frac{S_{count}(m_k)+1}{S_{count}(m_k)+F_{count}(m_k)+2}\right) \quad (6.6)$$

$n\ \epsilon\ (1, 2, 3)$

Eş. 6.6 kullanılarak hesaplanan güven değerleri her düğümün kendi fonksiyonel itibar tablosunda (FRT) saklanmaktadır. Bu değerler düğümün yaptığı doğrudan gözlemler neticesinde elde ettiği değerlerdir. Verilen örnekte i düğümü j düğümü hakkında kendi tecrübelerine dayanak bir güven değeri hesaplamaktadır. Söz konusu değerler (FRT tablosu) düğümler arasında paylaşılmaktadır. KAA'lardaki en büyük kısıtın enerji olması nedeniyle hesaplanan fonksiyonel güven değerlerinin saklanması veya iletilmesinde de yine enerji etkin olunmalıdır. Bu nedenle Eş. 6.6 kullanılarak [0, 1] aralığında hesaplanan değerler Eş. 6.7'de gösterildiği şekilde tam sayıya dönüştürülmekte, bu haliyle FRT'de saklanmakta ve düğümler arasında paylaşılmaktadır.

$$T_{ij} = ceil(T_{ij} * 100) \quad (6.7)$$

6.5. Birleştirilmiş Güven Değerlerinin (CTV) Hesaplanması

Sadece doğrudan gözlemleri (birincil el bilgiyi) dikkate alan güven yönetim sistemlerinin güven değerinin hesaplanmasında yetersiz kalması veya yanlış sonuçlar hesaplaması oldukça yüksek olasılıktır [65, 77]. Bu nedenle önerilen çalışmada güven değeri hesaplanırken hem doğrudan düğümlerin kendi elde ettiği bilgiler hem de hedef düğüm hakkında komşulardan alınmış olan bilgiler göz önüne alınmaktadır. Her düğüm doğrudan gözlemleri neticesinde oluşturduğu FRT tablosu ile komşuları tarafından gönderilen bilgilerden istifade ederek güven değerlendirme tablosu (trust evaluation table, TET)

oluşturmaktadır. TET tablosu oluşturmak için her iki bilginin uygun bir şekilde bir araya getirilmesi gerekmektedir.

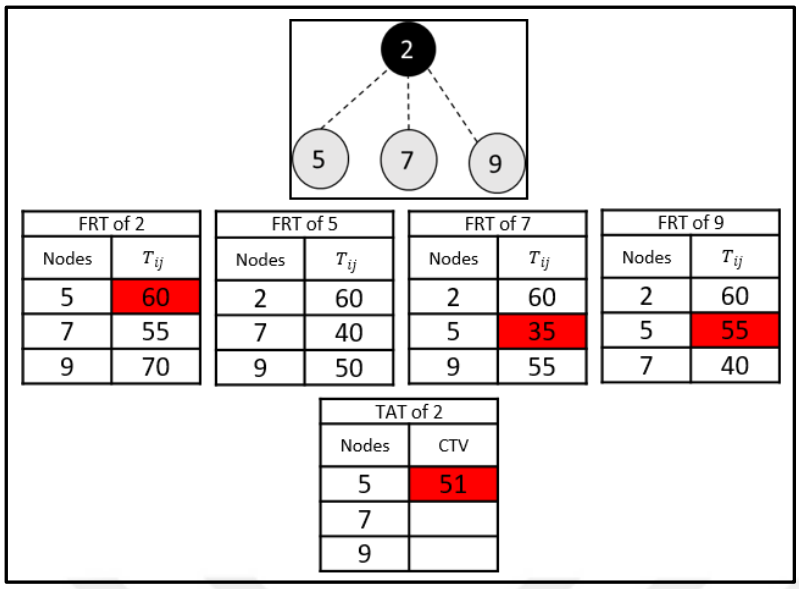
CTV değeri hesabının anlaşılması maksadıyla i düğümünün hedef j düğümü hakkında n tane düğümden değerlendirmeleri aldığı (ikinci el bilgi veya dolaylı değerlendirme bilgisini) varsayılmış ve bir örnek ile konu detaylı olarak açıklanmıştır. Sadelik olması açısından $n \in (1,2,\dots,t)$ olduğu kabul edilmiştir. Bu durumda i düğümü j düğümü hakkındaki birleştirilmiş güven değerini Eş. 6.8'de görüldüğü gibi hesaplamaktadır.

$$CTV_{ij} = ceil(\sum_{n=1}^{t} W(T_{nj}) * T_{nj}^{n}) \quad (6.8)$$

Eş. 6.8'deki T_{nj}^{n} değeri j düğümü hakkında komşu düğümler tarafından rapor edilen güven değerleridir. Komşu düğümlerin FRT tablosundan alınmıştır. $W(T_{nj})$ değeri ise i düğümünün kendi FRT tablosu göz önüne alınarak her bir komşu düğüm hakkında oluşturulan ağırlık değeridir ve Eş. 6.9'da görüldüğü şekilde hesaplanmaktadır.

$$W(T_{nj}) = \frac{T_{nj}}{\sum_{k=1}^{n} W(T_{nk})} \quad (6.9)$$

CTV değeri hesabı için matematiksel olarak örneklendirme yapmanın konunun anlaşılmasına katkı sağlayacağı düşünülmektedir. Bu kapsamda, Şekil 6.3'deki basit ağ yapısı ile düğümlerin FRT tabloları ve 2 numaralı düğümün TET tablosu bu maksatla sunulmuştur. 2 numaralı düğüm kendi gözlemlerine dayanarak komşuları olan 5, 7 ve 9 numaralı düğümler hakkında FRT tablosu tutmaktadır.



Şekil 6.3. CTV değeri hesabı için basit ağ örneği

Şekil 6.3 göz önüne alınarak 2 numaralı düğüm, 5 numaralı düğüm hakkındaki CTV_{25} değerini iki aşamada hesaplamaktadır.

1) Öncelikle Eş. 6.9'da belirtildiği şekilde kendi FRT tablosundan yararlanarak her bir düğüm için ağırlıkları hesaplamaktadır:

$$(\mathrm{W}_{25}) = \frac{60}{60+55+70} = 0{,}324, \mathrm{W}(\mathrm{T}_{27}) = 0{,}298, \text{ve } \mathrm{W}(\mathrm{T}_{29} = 0{,}378).$$

2) Daha sonra Eş. 6.8 kullanılarak CTV değerleri bulmaktadır:

$$CTV_{25} = W(T_{25}) * T_{25} + W(T_{27}) * T_{75} + W(T_{29}) * T_{95}$$

$$CTV_{25} = 0{,}324 * 60 + 0{,}298 * 35 + 0{,}378 * 55 = 51$$

Burada dikkat çekici ve üzerinde durulması gereken iki husus bulunmaktadır;

- Her ne kadar 2 numaralı düğüm komşularından almış olduğu güven değerlerini kullanarak CTV_{25} değerini hesaplıyor olsa da ağırlıkların oranı 2 numaralı düğümün diğer düğümlere olan güveni ile yakından ilgilidir. Böylesine bir yaklaşım sosyal bir konu olan güven ilişkisinin günlük hayattaki uygulamasından esinlenerek

yapılmıştır. Örneğin bir işveren bir çalışanı hakkında doğrudan gözlemler yapmakta ve onun performansını veya güvenilirliğini doğrudan yaptığı hareketler ile değerlendirmektedir. Ancak üçüncü şahıslar tarafından ilgili çalışan hakkında yapılacak yorumlar işverenin güven değerini olumlu veya olumsuz yönde değiştirebilir, etkileyebilir. Burada işverenin yorum yapan üçüncü şahıslara olan güven derecesi, onlar tarafından yapılacak yorumların kabul edilebilirlik olasılığını etkilemektedir. Eğer işveren yorum yapan şahsa çok güveniyorsa onun yorumlarına daha fazla itibar edecektir. Önerilen yöntemde CTV hesaplanmasında bu durum düşünülmüştür.

- 2 numaralı düğüm kendi gözlemleri ile 5 numaralı düğüm hakkında güven değerini hesapladığında 60 bulmuşken, düğümler arası iş birliği neticesinde bu değer son hesaplama neticesinde 51 olarak bulunmuştur. Düğümler arasındaki iş birliği 2 numaralı düğümün tek başına yapmış olduğu gözlemlerin değişmesine neden olmuştur.

6.6. Saldırı Tespiti

Önerilen saldırı tespit sisteminde normal dışı aktiviteler hem imza tabanlı (kötüye kullanım) hem de sistem seviyesindeki güven modeli yaklaşımları beraber kullanılarak tespit edilmektedir. Baz istasyonu söz konusu her iki yaklaşımın güçlü yanlarını kullanmak suretiyle saldırıları merkezi olarak tespit etmektedir.

Önerilen merkezi saldırı tespit sistemi [53] ve [78]'deki çalışmalara benzer şekilde imza tabanlı tespit yapmaktadır. Bu amaçla kullanılan kurallar şöyledir:

- *Algılama ve gecikme kuralı:* Tüm CH'ler kontrol paketlerini veri paketlerinden önce göndermeli ayrıca gönderim işlemini kendilerine tahsis edilen zaman içerisinde iletmelidir. Eğer bir CP zamanında gönderilmiyorsa veya gelen mesajlar müsaade edilen limitler içinde değilse normal olmayan bir davranışın (saldırının) varlığı düşünülmektedir. Burada aşırı miktarda CP alınması bir hizmet dışı bırakma (DoS) saldırısı olarak değerlendirilirken, eksik paket alımı da seçilen paketlerin gönderimi

saldırısını (selective forwarding) veya kara delik (black hole) saldırılarını akıllara getirmektedir. Ayrıca bu kural ile CP'lerini iletmeyen veya geciktiren kötücül bir CH tespit edilebilmektedir.

- *Küme elemanları kuralı*: CH'ler kendilerinin sorumluluk sahasında bulunan düğümleri bildirirken tüm düğümleri eksiksiz bir şekilde BS'ye bildirmelidir. Önerilen modelde başlangıç (kurulum) safhasında herhangi bir saldırı olmadığı varsayıldığından, BS her kümedeki düğümleri bilmektedir. Bu nedenle eksik düğüm bilgisinin gönderilmesi anormallik olarak değerlendirilmektedir.
- *Kontrol paketlerinin gönderim sıklığı:* Bir düğüm belirli bir CP'yi sadece izin verilen sayıda tekrar gönderebilir ve bu sayı sınırlıdır. Ele geçirilen paketlerin aynısını yollamak suretiyle yeniden gönderme saldırısı (replay attack) gerçekleştirmek isteyen saldırganlar bu kural sayesinde tespit edilebilmektedir.

BS imza tabanlı saldırı tespit kurallarına ilave olarak düğümler hakkında CTV değerlerini hesaplamakta ve merkezi olarak bu değerleri saklamaktadır. Bu maksatla BS kendi TET tablosunu oluşturmakta ve bu tabloda tüm CH'leri ve herhangi bir CH'ye bağlı olmayan algılayıcı düğümleri kaydetmektedir. BS kaynak açısından çok daha güçlü olması, birçok düğümden CP almak suretiyle merkezi olarak tüm ağı izlemesi ve hesaplama yeteneğinin güçlü olması nedeniyle, gerekli olan eşik değerlerinin belirlenmesinden sorumludur.

Bilinen saldırıların tespit edilmesi açısından imza tabanlı saldırı tespit kuralları son derece etkilidir. Ancak, yeni tür saldırıların tespit edilmesinde bu yaklaşım yetersiz kalmaktadır. Bu nedenle önerilen saldırı tespit sisteminde imza tabanlı kuralların yanı sıra güven değerlerinin kullanılması yeni tip saldırıların tespit edilmesini hedeflemektedir. Kullanılan güven değerlerinin düğümler arasındaki iş birliği ile hesaplanması komşu düğümlerden gelen bilgilerin hesaplamalara eklenerek birleştirilmiş güven değerinin bulunması saldırı tespit oranını artırmaktadır.

BS tarafından belirlenecek eşik güven değeri (CTV_{th}) tüm düğümlere yayınlanmakta, belirlenen eşik güven değeri saldırıların tespiti ve iş birliğinde düğümler tarafından kullanılmaktadır. Eğer herhangi bir algılayıcı düğüm mensubu olduğu CH için CTV_{th}

değerinden daha düşük bir değer hesaplarsa (algılayıcı düğümün kötücül CH olduğunun tespiti), kurulum aşamasında paylaşılan parolalar kullanılarak veri şifrelenmekte ve BS'na iletilmek üzere gönderilmektedir. Bu mesaj bir CH'nin saldırganlar tarafından ele geçirilmiş olabileceğinin BS'ye haber verilmesi işlemidir. BS kendisine farklı farklı kaynaklardan gelen tüm verileri birleştirmekte ve neticede son kararı kendisi vermektedir.

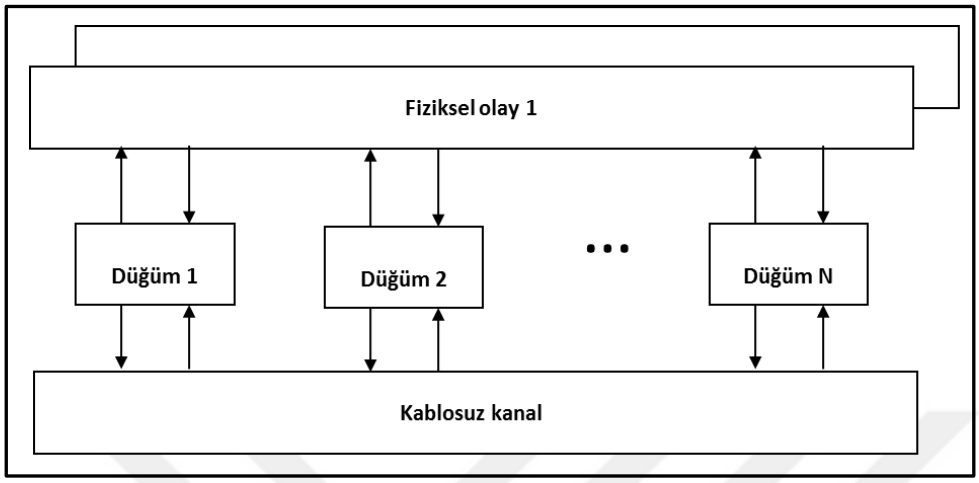
6.7. Benzetim

Önerilen saldırı tespit sisteminin değerlendirilmesi maksadıyla, kablosuz algılayıcı ağ ve vücut alan ağları (Body Area Networks, BAN) için benzetim yapılmasına olanak sağlayan *OMNET++* tabanlı *Castalia Framework* benzetim programı kullanılmıştır.

OMNET++ ağ benzetimleri yapmak için ortaya konmuş, geliştirilebilir, modüler, bileşen tabanlı C++ benzetim kütüphanesi ve çerçevesidir [8]. OMNET++ tek başına bir benzetim programı değildir, benzetim programlarının üzerinde yazılabildiği bir alt yapıdır. OMNET++'daki mimariye göre; modül denilen bileşenler kendi aralarında herhangi bir veri yapısındaki mesajlar ile haberleşirler. Modüller basit ve bileşik modül olmak üzere ikiye ayrılır. Modüller mesajları önceden belirlenen yollar (path) üzerinden kapılar (gates) veya bağlantılar (connections) ile gönderir veya alırlar. Modüllerin çeşitli parametreler alması sayesinde yetenekleri değişebilmektedir. Basit modüller daha az bileşene ayrılamayan modüllerdir ve model davranışının temelini oluştururlar. Basit modüller C++ ile programlanmakta ve benzetim kütüphanelerini kullanmaktadır. Yapboz parçacıklarının bir araya gelerek şekiller oluşturulması gibi modüller de bir araya gelerek daha karmaşık bileşik modülleri oluşmaktadır. İyi programlanmış modülleri tekrardan kullanmak mümkündür.

Castalia Framework [9] ise başta kablosuz algılayıcı ağlar ve vücut alan ağları olmak üzere genel olarak düşük güçlü gömülü cihazların kullanıldığı ağların test edilmesi maksadıyla kullanılan bir benzetim programıdır. Castalia, OMNET++ tabanlıdır ve dağıtık algoritmaların veya protokollerin gerçekçi kablosuz kanal veya radyo modeli ile değerlendirilmesinde kullanılmaktadır. Son derece parametrik olması nedeniyle birçok farklı platform için tasarlanan farklı uygulamaların benzetiminde kullanılabilmektedir. Genel olarak Castalia

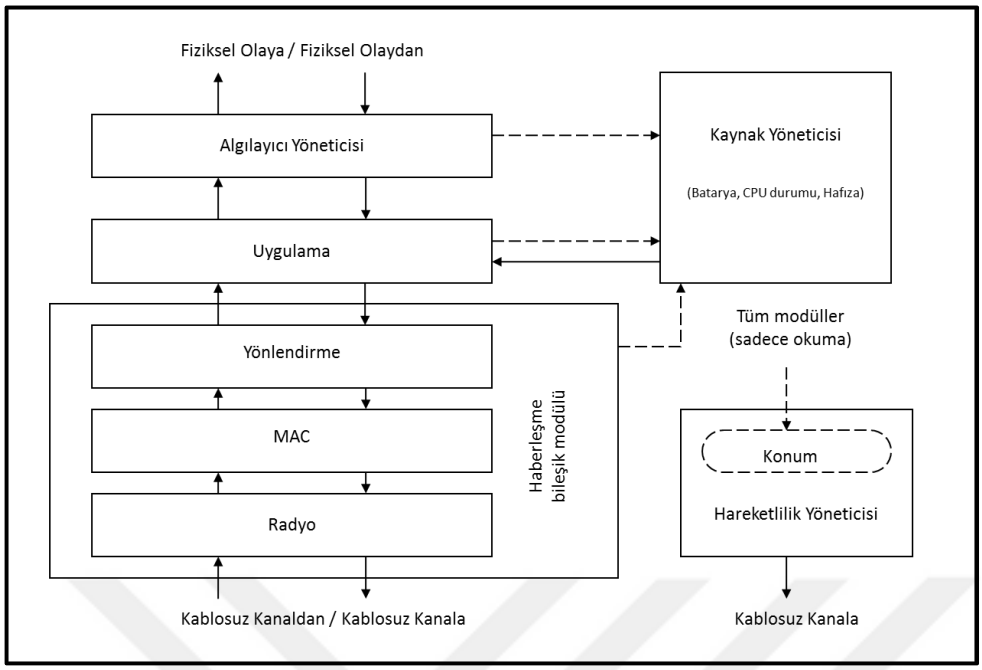
benzetim programındaki bileşenler ve bileşenler arasındaki bağlantılar Şekil 6.4'de görülmektedir.



Şekil 6.4. Castalia bileşenleri ve bağlantıları

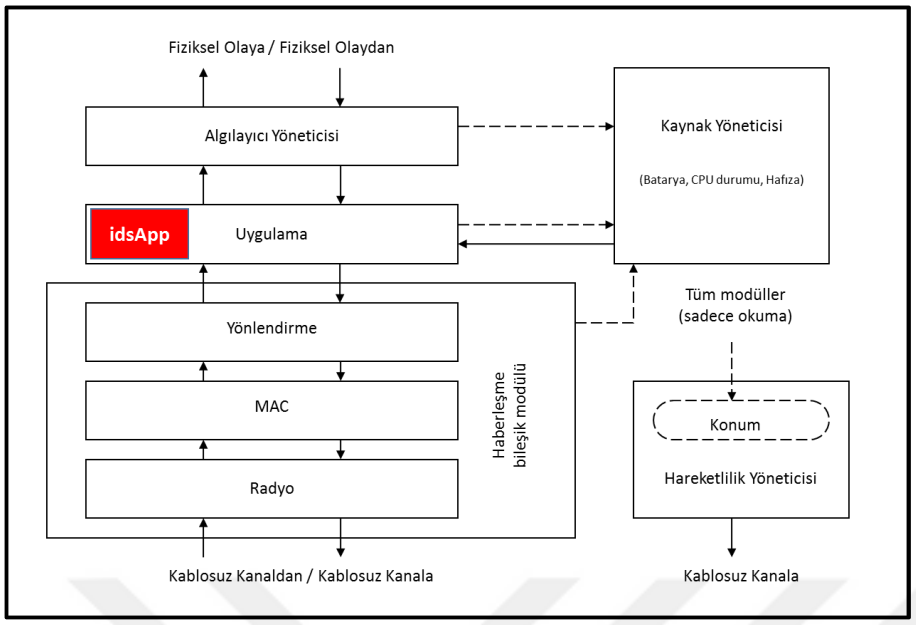
Şekil 6.4'den görüldüğü üzere Castalia benzetim programında her algılayıcı düğüm algılayıcı yöneticisi (sensor manager) birimi vasıtasıyla *fiziksel olayları* takip etmekte ve komşu düğümler ile olan bağlantısı *kablosuz kanal* bileşeni vasıtasıyla gerçekleşmektedir. Benzetim programının bu şekilde modüler olması her bir bileşenin değişik zamanlarda diğer bileşenlerden farklı olarak geliştirilebilmesine imkân sağlamaktadır.

Şekil 6.4'de bulunan düğüm bileşik modülünün bileşenleri ise Şekil 6.5'de görülmektedir. Kullanılan her düğüm fiziksel olayları izlemekten sorumlu algılayıcı yöneticisi, verilen görevin yerine getirilmesini sağlayacak uygulama, yönlendirme, MAC ve radyo gibi işlemleri yerine getiren haberleşme bileşik modülü ile kaynak yöneticisi modüllerinden oluşmaktadır. İcra edilecek görevin özelliğine bağlı olarak düğümlerden konum bilgisinin alınması gerekli ise veya düğümlerin hareketli olması söz konusu ise düğümlere hareketlilik yöneticisi modülü ilave edilmektedir.



Şekil 6.5. Castalia düğüm bileşik modül bileşenleri

Kablosuz algılayıcı ağlardaki saldırıları tespit etmek maksadıyla geliştirilen saldırı tespit sisteminin Castalia ile benzetilebilmesi için Şekil 6.6'da görüldüğü üzere *idsApp* isimli uygulama geliştirilmiş ve tüm düğümlerde bu uygulamanın çalışması sağlanmıştır. Bu uygulama ile önerilen sistemdeki kontrol paketlerinin alınması ve gönderilmesi ile düğümlerin komşularına ait CTV değerlerinin fonksiyonel itibar ölçütlerini kullanarak hesaplaması sağlanmıştır. Bu uygulama sürekli çalışan, düğümlerin üzerinde taramalar yapan ve böylelikle düğümlerin enerjilerinin süratle tükenmesine neden olan bir uygulama değildir. Tıpkı birçok algılayıcı düğümde olduğu gibi kesikli çalışmakta, düğüm algılama ve gönderme-alma işlemlerini gerçekleştirirken işlem yapmaktadır.

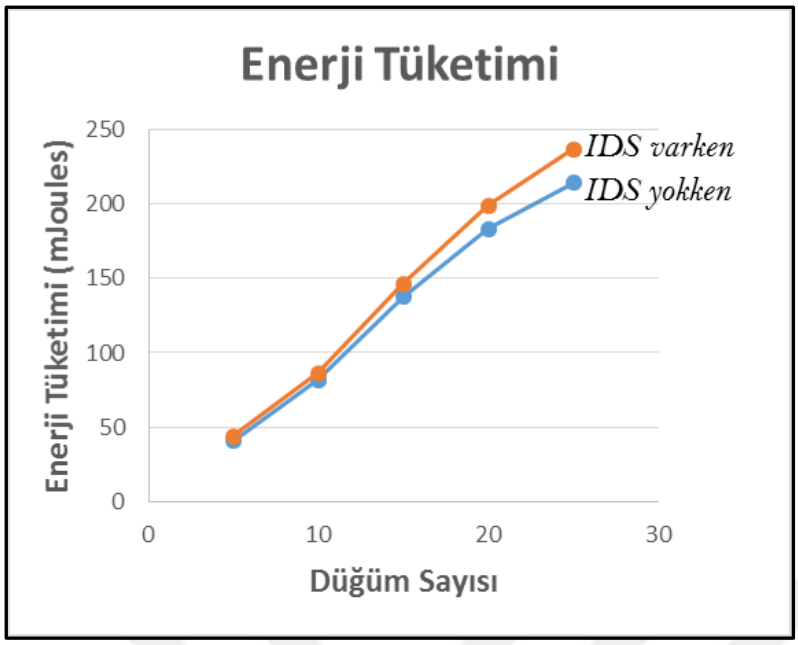


Şekil 6.6. Önerilen modelin benzetimi için uygulama

6.8. Deneysel Sonuçlar

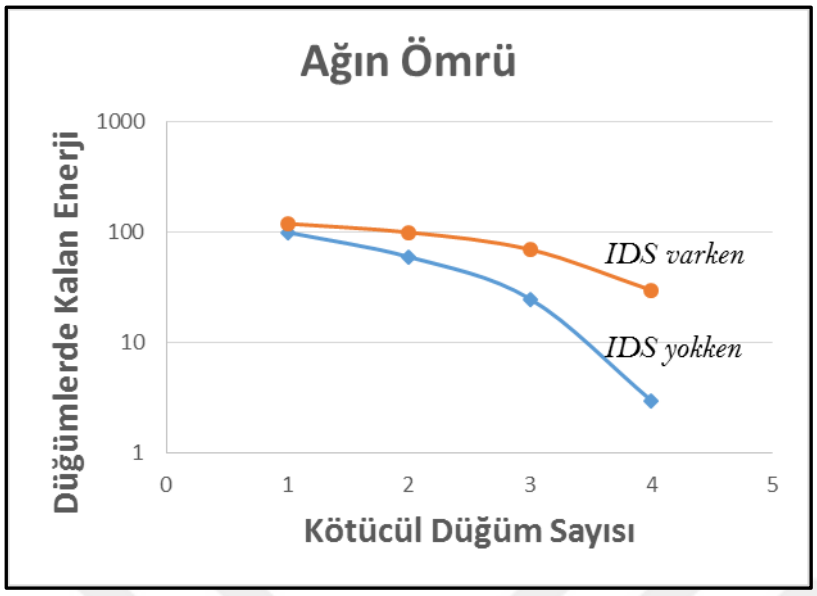
Önerilen modelin Castalia benzetim programı ile test edilmesi işlemi iki aşamalı olarak gerçekleştirilmiştir. Birinci aşamada önerilen modelin ilave enerji yükü açısından uygulanabilir olup olmadığı ve ağ ömrüne olan etkileri incelenmiş, ikinci aşamada ise söz konusu modelin saldırıları tespit etmedeki performansı değerlendirilmiştir.

Öncelikli olarak kümeleme tabanlı (cluster-based) kablosuz algılayıcı ağ mimarisi oluşturulup herhangi bir saldırı olmaması durumunda düğümlerde arta kalan enerji (residual energy) seviyeleri incelenmek suretiyle değerler elde edilmiş, daha sonra da önerilen sistemin uygulanması durumundaki enerji tüketimi tespit edilmiştir. Şekil 6.7, sistemlere yönelik herhangi bir saldırı olmaması, sistemin *normal modda* çalıştığı durumlarda enerji tüketimini göstermektedir. Herhangi bir saldırının olmadığı durumlarda önerilen sistemin kullanılan kontrol paketleri nedeniyle sistemlere bir miktar yük getirdiği ancak bu ilave yükün kabul edilebilir sınırlar içinde olduğu değerlendirilmektedir. Bu nedenle önerilen sistemin kümeleme tabanlı mimariye sahip kablosuz algılayıcı ağlarda kullanılabileceği kıymetlendirilmiştir.



Şekil 6.7. Normal işlemler durumunda enerji tüketimi

Normal ağ işlemlerinin gerçekleştiği yani herhangi bir saldırının bulunmadığı durum incelendikten sonra sistemlere yönelik kötücül düğümlerin olduğu yani ağın saldırıya maruz kaldığı durumda önerilen sistemin performansı incelenmiştir. Bu senaryoda sıcaklık verisinin takibi maksadıyla kullanılan kablosuz algılayıcı ağa kötücül düğümlerin yanlış verileri göndermesi durumu incelenmiştir. Bütün düğümler aynı fiziksel olayı takip ettiği için farklı veriler gönderen kötücül düğümlerin tespit edilmesi ile ağın görevini doğru bir şekilde gerçekleştirmesi hedeflenmiştir. Çalışmada amaç saldırı tespit sistemi gerçekleştirmek ve doğru bir şekilde kötücül düğümleri tespit etmektir. Saldırı önleme sistemleri (IPS) çalışmanın kapsamı dışında olması nedeniyle doğru bir şekilde alarm üretilmesi durumunda ilgili kötücül düğüm devre dışı bırakılmıştır. Şekil 6.8'de ağın saldırıya maruz kalması durumunda ağ ömrünün önerilen IDS kullanılması ve kullanılmaması durumunda değişimi görülmektedir. Neticede önerilen IDS ile kötücül düğümler tarafından saldırıya maruz kalan ağın ömrünü uzatabilmek mümkün görünmektedir.



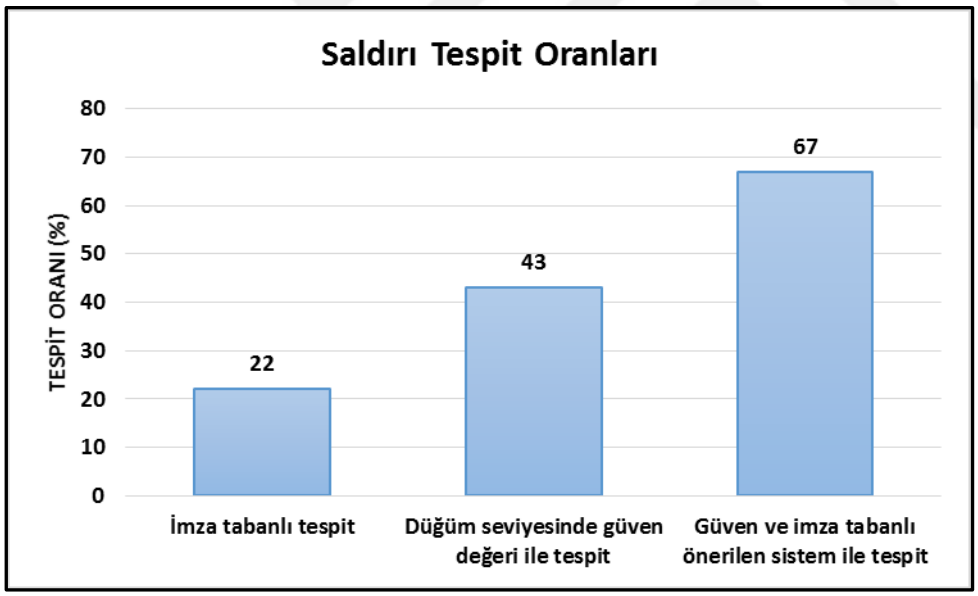
Şekil 6.8. Saldırı durumunda ağ ömrü

Önerilen IDS'nin normal çalışma şartlarında sistemlere getirdiği yükün ihmal edilebilir seviyede olduğunun ve saldırıların mevcut olması durumunda ise kötücül düğümleri tespit etmek suretiyle ağ ömrünü uzatabileceğinin tespit edilmesinden sonra sistemin saldırıları tespit etmedeki performansı incelenmiştir. Bu noktada önerilen sistem, sadece kötüye kullanım (imza tabanlı tespit) yöntemini kullanan [78]'deki çalışma ve sadece güven değerlerini göz önüne alan ve düğüm seviyesinde tespit yapan [79]'deki çalışma ile, saldırıların tespiti açısından karşılaştırılmıştır.

Yapılan benzetim çalışmalarında, ağa yönelik gerçekleştirilen çeşitli saldırıların tespitine dair incelemelerde bulunulmuş ve saldırı karşısında alarm üretilmesi durumunda ilgili tespit yönteminin başarılı olduğu kabul edilmiştir. Şekil 6.9'da yapılan deneyler neticesinde elde edilen tespit oranları bulunmaktadır. Bu kapsamda; sadece imza tabanlı yöntemlerle saldırıların ancak % 22'si tespit edilebilmiştir. Tespit edilen saldırıların özellikle kara delik saldırılarında olduğu gibi çok net bir şekilde tanımlanabilen saldırılar olması gerektiği dikkat çekmektedir. Saldırıların çok küçük bir şekilde değiştirilmesi durumunda bile yeni saldırının imza veri tabanında bulunmaması nedeniyle saldırılar tespit edilememiştir. Ayrıca saldırı veri tabanının oluşturulması ve saldırılar için karakteristiklerin çıkarılması oldukça dikkat gerektiren bir işlemdir.

Düğüm seviyesinde güven değerinin hesaplanarak saldırıların tespit edilmesinde ise başarı oranı % 43'dür. Burada dikkat çekici nokta düğüm seviyesinde tespit yapılması durumunda her düğümün alarm ürettiği ve üretilen alarmların bölgesel olarak kaldığıdır. Yani bir CH sadece kendi kümesindeki kötücül düğümlerle ilgilenmekte ve saldırıları tespit etmekte, ürettiği alarmı BS'na göndermek için alarmı yayımlamaktadır. Bu durumda kötücül düğüm de bu bilgiyi elde etmekte ve hareketlerini değiştirmek suretiyle kendisi tekrardan normal düğüm olarak tanımlanana kadar beklemektedir.

Bu tez çalışmasında önerilen güven ve imza tabanlı saldırı tespit yöntemlerinin beraber kullanılması durumunda ise saldırıların tespit oranı % 67 olarak gerçekleşmiştir. Alınan kontrol paketlerinin öncelikle imza tabanlı kurallardan geçirilmesi ve CTV değerlerinin göz önüne alınarak şüpheli düğümler hakkında verilen karar, diğer yöntemlere oranla daha yüksek oranda doğru tespitlerde bulunmuştur.



Şekil 6.9. Saldırı tespit oranlarının karşılaştırılması

7. SONUÇ VE ÖNERİLER

KAA'ların siber güvenlik bakış açısıyla incelendiği ve saldırıların etkin bir şekilde tespit edilebilmesi için özgün bir saldırı tespit sisteminin önerildiği bu tez çalışması neticesinde ulaşılan sonuçlar şöyledir:

- Hassas verilerin işlendiği, görev kritik işlerde kullanılan ve uygulama alanı her geçen gün artan KAA'ların güvenliğinin çeşitli zafiyetler nedeniyle yeterince sağlanamadığı ve bu ağların siber saldırılara karşın son derece korumasız olduğu görülmüştür. Ayrıca söz konusu ağları tasarlarken güvenliğin tasarım aşamasından itibaren göz önünde bulundurulmadığı, ancak sonradan geliştirilen yöntemlerle güvenliğin sağlanmaya çalışıldığı tespit edilmiştir. Güvenlik önlemlerinin, sistemlerin tasarım aşamasından itibaren göz önüne alınmasının ve tıpkı sistemi oluşturan bir bileşen gibi değerlendirilmesinin uygun olacağı kıymetlendirilmektedir.
- KAA'ların kablosuz ağlardaki tüm saldırı vektörlerine karşı hassas olduğu, ancak bu ağın en büyük kısıtının enerji olduğu üzerinde özellikle durulmuştur. Buna ilave olarak detayları anlatılan karakteristik bazı özellikler sebebiyle KAA'lara yönelik güvenlik tedbirleri geliştirilirken çok daha dikkatli ve titiz olunması gerektiği tespit edilmiştir. Bu kapsamda, *KAA'lar için geliştirilecek güvenlik mekanizmaları her şeyden önce enerji etkin olmalıdır*. Güvenlik seviyesi artırılacak diye düğümlerin işlemlerini yapması için barındırdığı pillerin çok hızlı tükenmesine neden olacak yöntemlerin kullanılmasından kaçınılmalıdır.
- KAA'ların birer kritik alt yapı olarak değerlendirilmesi gerektiği ve kritik alt yapı güvenliğinin sağlanmasında ortak aklın ürünü olan yaklaşımların kullanılmasının gayret sarfiyatını azaltacağı ön görülmektedir.
- KAA'lara yönelik birçok konunun araştırmacılar tarafından detaylı olarak çalışıldığı görülmüştür. Bu alanda bilime katkı sağlamak isteyenlerin özgün konular bulmak noktasında daha yaratıcı olması gerektiği düşünülmektedir.

- KAA'ların özellikle nesnelerin interneti (IoT) teknolojisinin temellerini oluşturduğu ve giderek yaygınlaşan IoT ürünlerindeki güvenlik ihtiyacının karşılanmasında KAA'larda elde edilen bilgi ve tecrübelerin kullanılabileceği değerlendirilmektedir.
- KAA'lara yönelik saldırıların çeşitliliği ve bu ağ türünün doğasında bulunan zayıflıklar nedeniyle sadece koruyucu veya caydırıcı tedbirler alarak saldırıların önlenemeyeceği çok net bir şekilde ifade edilmiştir. Bu nedenle tez çalışmasında ikinci bir savunma hattı olarak nitelendirilen saldırı tespit sistemleri üzerinde durulmuştur. IDS konusu KAA'lar için geliştirilmeye muhtaç bir alan olarak karşımıza çıkmaktadır. Geleneksel ağlarda kullanılan saldırı tespit sistemleri başta olmak üzere güvenlik tedbirlerinin birçoğu doğrudan KAA'lara uygulanamamaktadır. Bu yüzden *farklı, yeni, enerji etkin* ve *iyi sonuçlar* üretecek özgün yaklaşım ve yöntemlere ihtiyaç vardır.
- Güven yönetim sistemleri geleneksel güvenlik yaklaşımlarından ayrılmakta ve KAA'lardaki birçok problem sahasında kullanılabilmektedir. Hatta güven yönetim sistemlerinin tek başına saldırı tespit sistemi olarak kullanılması da söz konusudur.
- Sistemlerin güvenliğinin sağlanması ile maliyetler arasında her zaman bir denge olmak zorundadır. Sistemlerin güvenliğini almak her zaman pahalı bir işlemdir.
- Güven değerinin hesaplanması ve kötüye kullanım (imza tabanlı) yaklaşımının hibrit bir şekilde kullanılması ile önerilen saldırı tespit sistemi, hem getirdiği ilave yük hem de saldırıları tespit oranı açısından uygulanabilir bir öneridir. Önerinin geçerliliği ve performans analizi benzetim yoluyla yapılmıştır. KAA'larda IDS konusu üzerinde yapılacak araştırmaların, farklı yöntemlerin güçlü yanlarını bir araya getirmek suretiyle enerji etkin sistemler geliştirilmesi üzerinde odaklanmasının yararlı olacağı düşünülmektedir.
- Sadece güven tabanlı saldırı tespitinin kullanılması durumunda saldırganların *akıllı saldırı yöntemleri* kullanarak bu sistemleri atlatabileceği akıldan çıkarılmamalıdır.
- Yalnızca imza tabanlı tespit yöntemlerini kullanmak, yeni çıkacak saldırıları tespit etmede yetersiz kalacaktır. Saldırı imzalarının güncellenmesine kadar geçecek sürede saldırganların hedefine ulaşabileceği unutulmamalıdır.

- Hibrit yöntemler geliştirirken düğümler arasındaki iş birliği ve koordinasyon ihtiyacının asgari seviyede olmasını sağlayacak yöntemler geliştirilmesinin enerji verimliliğine katkı sağlayacaktır.
- Sonuç olarak, KAA'larda güvenlik ve saldırı tespit sistemleri konularında araştırma yapacaklar için bu tez çalışmasının referans bir doküman olarak kullanılabileceği değerlendirilmektedir.

KAYNAKLAR

1. I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam ve E. Cayirci (Aug. 2002), *A survey on sensor networks*, IEEE Communications Magazine, 40 (8), 102–114.
2. W. R. Heinzelman, J. Kulik ve H. Balakrishnan (1999), *Adaptive protocols for information dissemination in wireless sensor networks*, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, 174–185.
3. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler ve K. Pister (2000), *System architecture directions for networked sensors*, ACM SIGOPS Operating Systems Review, 34 (5), 93–104.
4. C. Intanagonwiwat, R. Govindan ve D. Estrin (2000), *Directed Diffusion: A Scalable and Robust Communication*, Proceedings of the 6th annual international conference on Mobile computing and networking, 56-67.
5. J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin ve D. Ganesan (2001), *Building efficient wireless sensor networks with low-level naming*, ACM SIGOPS Operating Systems Review, 35 (5), 146.
6. K. Sohraby, D. Minoli ve T. Znati (2006), *Wireless Sensor Networks: Technology, Protocols, and Applications*, Wiley Online Library, 1-75.
7. İnternet: NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, URL: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf. Son Erişim Tarihi: 01.07.2017.
8. İnternet: OMNET (2017), *OMNeT++ Simulation Manual*, URL: https://omnetpp.org/doc/omnetpp/manual/#sec:introduction:what-is-omnetpp. Son Erişim Tarihi: 30.06.2017.
9. İnternet: A. Boulis (May 2013), *Castalia - A simulator for Wireless Sensor Networks and Body Area Networks, User's Manual*, URL: https://github.com/boulis/Castalia adresinden 06 Ocak 2016 tarihinde alınmıştır.
10. Narendra Kumar Kamila (2016), *Handbook of Research on Wireless Sensor Network Trends, Technologies, and Applications*, IGI Global, 145-162.
11. M. A. M. Vieira, C. N. Coelho, D. C. da Silva ve J. M. da Mata (2003), *Survey on wireless sensor network devices*, 2003 IEEE Conference on Emerging Technologies and Factory Automation Proceedings,1, 537–544.
12. C. Alippi ve C. Galperti (July 2008), *An Adaptive System for Optimal Solar Energy Harvesting in Wireless Sensor Network Nodes*, IEEE Transactions on Circuits and Systems, 55 (6), 1742–1750.
13. D. Kruger, C. Buschmann ve S. Fischer (2009), *Solar powered sensor network design and experimentation*, 2009 6th International Symposium on Wireless Communication Systems Proceeding, 11–15.

14. S. Khan, A. Pathan ve N. Alrajeh (2012), *Wireless Sensor Networks: Current Status and Future Trends*, London:CRC Press, 379-381.

15. A. Boukerche (October 2007), *Secure time synchronization protocols for wireless sensor networks*, IEEE Wireless Communication, 64-69.

16. Q. Wang ve I. Balasingham (2010), *Wireless Sensor Networks-An Introduction*, Wireless Sensor Networks Appications*:* Centric Design, Intech Publications, 1-16.

17. C. Karlof ve D. Wagner (2003), *Secure routing in wireless sensor networks: attacks and countermeasures*, IEEE Sensor Network Protocol Application, 113–127.

18. H. K. Patil ve S. A. Szygenda (2012), *Security for Wireless Sensor Networks using Identity-Based Cryptography*, London:Auerbach Publications, 19-57.

19. V. Kumar, S. Chakraborty, F. A. Barbhuiya ve S. Nandi (2012), *Detection of stealth Man-in-the-Middle attack in wireless LAN*, in Proceedings of 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 290-295.

20. W. Xu, W. Trappe ve Y. Zhang (2008), *Defending wireless sensor networks from radio interference through channel adaptation,* ACM Trans. Sens. Networks, 4(4), 1–34.

21. J. R. Douceur (2002), *The Sybil Attack*, Proceeding of IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, 1–6.

22. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos ve G. Pantziou (2009), *A survey on jamming attacks and countermeasures in WSNs*, IEEE Communication Survey and Tutorials, 11(4), 42–56.

23. İnternet: *TinyOS Network Protocol Working Group - TinyOS Wiki*, URL: http://tinyos.stanford.edu/tinyos-wiki/index.php/TinyOS_Network_Protocol_Working_Group. Son Erişim Tarihi: 02.06.2017.

24. İnternet: Y. Yu, R. Govindan ve D. Estrin (2001), *Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks*, URL: https://pdfs.semanticscholar.org/0f2d/17c4827a9672d6899b3d450769c692a982b4. Son Erişim Tarihi:04.03.2017.

25. I. Maarouf, U. Baroudi ve A. R. Naseer (2009), *Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks*, IET Communications, 3(5), 846–858.

26. J. Lopez, R. Roman, I. Agudo ve C. Fernandez-Gago (2010), *Trust management systems for wireless sensor networks: Best practices*, Computer Communications, 33, 1086-1093.

27. K. Shim (2016), *A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks*, IEEE Communications Surveys and Tutorials, 18(1), 577-601.

28. D. J. Malan, M. Welsh ve M. D. Smith (2004), *A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography*, Sensor Ad Hoc Communication Networks Proceedings, 71–80.

29. İnternet: R. L. Rivest, A. Shamir ve L. M. Adleman (1978), *Method for Obtaining Digital Signatures and Public Key Cryptosystems*, URL: https://people.csail.mit.edu/rivest/Rsapaper.pdf. Son Erişim Tarihi: 10.05.2017.

30. M. Brown, D. Cheung, D. Hankerson, J. Lopez Hernandez, M. Kirkup ve A. Menezes (2000), *PGP in Constrained Wireless Devices*, Proceedings of the 9th USENIX Security Symposium, 2-7.

31. D. Carman, P. Kruus ve B. Matt (2000), *Constraints and approaches for distributed sensor network security (final)*, *DARPA Proj. Rep.*, 1-139.

32. F. Amin, a. H. Jahangir ve H. Rasifard (2008), *Analysis of public-key cryptography for wireless sensor networks security*, World Academy Science, Engineering and Technology, 40, 530-535.

33. A. S. Wander (2005), *Energy analysis of public-key cryptography for wireless sensor networks*, Third IEEE International Conference on Pervasive Computing and Communications Proceedings, 53(9), 324-328.

34. N. Gura, A. Patel, A. Wander, H. Eberle ve S. C. Shantz (2004), *Comparing elliptic curve cryptography and RSA on 8-bit CPUs,* CHES 2004: Cryptographic Hardware and Embedded Systems, 119–132.

35. İnternet: Certicom Research (2009), *SEC 1: Elliptic Curve Cryptography Standards for Efficient Cryptography,* URL: http://www.secg.org/SEC1-Ver-1.0.pdf. Son Erişim Tarihi: 05.02.2017.

36. Y. W. Y. Wang, G. Attebury ve B. Ramamurthy (2006), *A survey of security issues in wireless sensor networks*, IEEE Communications, Surveys and Tutorials, 8(2), 1–23.

37. İnternet: Certicom Research (2000), SEC 2: Recommended Elliptic Curve Domain Parameters, URL: http://www.secg.org/SEC2-Ver-1.0.pdf. Son Erişim Tarihi: 05.02.2017.

38. K. Piotrowski, P. Langendoerfer ve S. Peter (2006), *How Public Key Cryptography Influences Wireless Sensor Node Lifetime*, Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, 169-176.

39. J. Lee, K. Kapitanova ve S. H. Son (2010), *The price of security in wireless sensor networks*, Computer Networks, 54, 2967-2978.

40. M. Panda (2014), *Security in Wireless Sensor Networks using Cryptographic Techniques*, American Journal of Engineering, 1, pp. 50-56.

41. İnternet: G. S. Quirino, A. R.L.Ribeiro ve E. D. Moreno (2012), *Asymmetric Encryption in Wireless Sensor Networks*, URL: http://www.intechopen.com/books/wireless-sensor-networks-technology-and-protocols/asymmetric-encryption-in-wireless-sensor-networks. Son Erişim Tarihi: 02.06.2017.

42. Y. Xiao, V. K. Rayi, B. Sun, X. Du ve F. Hu (2007), *A survey of key management schemes in wireless sensor networks*, Computer Communications, 30, 2314-2341.

43. J. Zhang ve V. Varadharajan (2010), *Wireless sensor network key management survey and taxonomy*, Journal of Network and Computer Applications, 33, 63–75.

44. D. R. Raymond and S. F. Midkiff (2008), *Denial-of-service in wireless sensor networks: Attacks and defenses*, IEEE Pervasive Computing, 7(1), 74–81.

45. İnternet: *TCP SYN Cookies - DDoS defence - EtherealMind*, URL: http://etherealmind.com/tcp-syn-cookies-ddos-defence. Son Erişim Tarihi: 02.04.2017.

46. A. Fuchsberger (2005), *Intrusion Detection Systems and Intrusion Prevention Systems*, Journal of Information Security and Applications, 10 (3), 134–139.

47. I. Butun, S. D. Morgera ve R. Sankar (2013), *A Survey of Intrusion Detection Systems in Wireless Sensor Networks*, IEEE Communications, Surveys and Tutorials.

48. S. Mandala, M. A. Ngadi ve A. H. Abdullah (2008), *A Survey on MANET Intrusion Detection*, International Journal of Computer Scienece and Network Security, 2 (1), 1-11.

49. M. M. Ozcelik, E. Irmak ve S. Ozdemir (2017), *A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks*," Procedings of International Symposium on Networks, Computers and Communications (ISNCC-2017).

50. N. Sava, P. Budhwani, S. Talekar, S. Borle ve N. Jadhav (2014), *Survey on Intrusion Detection Systems*, International Journal of Advance Research in Computer Science and Management Studies, 2 (1), 2321-7782.

51. Y. Xiao ve X. Shen (2007), *Wireless Network Security*, Canada: Springer Publishings, 323-407.

52. P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández ve E. Vázquez (2009), *Anomaly-based network intrusion detection: Techniques, systems and challenges*," Computer Security, 28 (2), 18-28.

53. A. Paula (2005), *Decentralized Intrusion Detection in Wireless Sensor Networks*, *1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks Procedings*, 16-23.

54. T. S. Sobh (2006), *Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art*, Computer Standards and Interfaces, 28 (6), 670-694.

55. A. Patcha ve J. M. Park (2007), *An overview of anomaly detection techniques: Existing solutions and latest technological trends*, Computer Networks, 51 (12), 3448-3470.

56. C. Sample ve K. Schaffer (2013), *An overview of anomaly detection*, IT Professional, 15 (1), 8-11.

57. R. Mitchell ve I.R. Chen (Apr. 2014), *A survey of intrusion detection in wireless network applications*, Computer Networks, 42, 1-23.

58. Y. Yu, K. Li, W. Zhou ve P. Li (2012), *Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures*, Journal of Network and Computer Applications, 35, 867-880.

59. S. M. Sajjad, S. H. Bouk ve M. Yousaf (2015), *Neighbor node trust based intrusion detection system for WSN*," Procedia Computer Science, 63, 183-188.

60. F. Ishmanov, A. S. Malik, S. W. Kim ve B. Begalov (2015), *Trust management system in wireless sensor networks: design considerations and research challenges*, Transactions on Emerging Telecommunications Technologies, 26 (2), 107-130.

61. C. J. Fung, J. Zhang, I. Aib ve R. Boutaba (2011), *Dirichlet-based trust management for effective collaborative intrusion detection networks*, IEEE Transactions on Network and Service Management, 8 (2), 79-91.

62. A. Ljung and E. Wahlforss (2008), *People, profiles and trust : on interpersonal trust in web-mediated social spaces*, London: Lulu.com Publishings.

63. O. Garcia-Morchon, D. Kuptsov, A. Gurtov ve K. Wehrle (2013), *Cooperative security in distributed networks*, Computer Communications, 36 (12), 1284-1297.

64. R. Singh, J. Singh ve R. Singh (2016), *Trust Based Multi Attack Intrusion Detection System for Wireless Sensor Networks*, International Journal of Computer Science and Information Security (IJCSIS), 14 (11), 266-275.

65. S. Ganeriwal, L. K. Balzano ve M. B. Srivastava (2008), *Reputation-based Framework for High Integrity Sensor Networks,* ACM Transactions on Sensor Networks, 4,1-36.

66. W. T. Zhu, J. Zhou, R. H. Deng ve F. Bao (2012), *Detecting node replication attacks in wireless sensor networks: A survey*, Journal of Network and Computer Applications, 35 (3), 1022-1034.

67. A. Jøsang ve R. Ismail (2002), *The beta reputation system*, 15th Bled Electronic Commerce Conference Proceedings, 2502-2511.

68. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee ve Y. J. Song (2009), *Group-based trust management scheme for clustered wireless sensor networks*, IEEE Transactions on Parallel and Distributed Systems, 20 (11), 1698-1712.

69. Z. Yao, D. Kim ve Y. Doh (2008), *PLUS: Parameterized and Localized trUst management Scheme for sensor networks security*, International Journal of Sensor Networks, 3, 224-236.

70. G. Han, L. Shu, J. Ma, J. H. Park ve J. Ni (2010), *Power-Aware and Reliable Sensor Selection Based on Trust for Wireless Sensor Networks*, Journal of Communications, 5, 23-30.

71. T. K. Kim ve H. S. Seo (2008), *A Trust Model using Fuzzy Logic in wireless sensor network*, *World Academy of Science,* Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 42, 63-66.

72. R. Feng, X. Xu, X. Zhou ve J. Wan (2011), *A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory*, Sensors, 11 (2), 1345-1360.

73. G. M. Flix GM, Javier G ve Marn B (2010), *Linguistic fuzzy logic enhancement of trust mechanism for distributed networks*, International Conference on Computer and Information Technology Proceedings*,* 838-845.

74. R. Geetha, S. Raj Anand, ve E. Kannan (2015), *Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks*, 2014 International Conference on Information Communication and Embedded Systems, ICICES 2014.

75. F. G. Mármol ve G. M. Pérez (2011), *Providing trust in wireless sensor networks using a bio-inspired technique,*Telecommunication Systems 46 (2), 163-180.

76. S. Ozdemir (2008), *Functional reputation based reliable data aggregation and transmission for wireless sensor networks,* Computer Communications, 31 (17), 3941-3953.

77. S. Ganeriwal ve M. B. Srivastava (2004), *Reputation-based framework for high integrity sensor networks*, 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks Proceedings, 66-77.

78. F. Hidoussi, H. T. Cruz, D. E. Boubiche, K. Lakhtaria, A. Mihovska ve M. Voznak (2015), *Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensor Networks*, Wireless Personal Communications, 85 (1), 207-224.

79. W. Fang, C. Zhang, Z. Shi, Q. Zhao ve L. Shan (2015), *BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks*, Journal of Network and Computer Applications*,* 59, 88-94.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	:	ÖZÇELİK, Mert Melih
Uyruğu	:	T.C.
Doğum tarihi ve yeri	:	01 /02/1985 Kırşehir
Medeni hali	:	Evli
Telefon	:	0 (530) 322 42 23
e-posta	:	mertmelih2006@gmail.com

Eğitim Derecesi	**Okul/Program**	**Mezuniyet yılı**
Yüksek Lisans	Gazi Üniversitesi/Bilişim Enstitüsü Bilişim Sistemleri Anabilim Dalı	Devam Ediyor
Lisans	Kara Harp Okulu	2006
Lise	Maltepe Askeri Lisesi	2002

İş Deneyimi, Yıl	**Çalıştığı Yer**	**Görev**
2006-devam ediyor	Türk Silahlı Kuvvetleri	Subay

Yabancı Dili

İngilizce

Yayınlar

1. M. M. Ozcelik, E. Irmak ve S. Ozdemir, *A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks*, Procedings of International Symposium on Networks, Computers and Communications (ISNCC-2017).

Hobiler

Futbol, yüzme, doğa yürüyüşü,

GAZİLİ OLMAK AYRICALIKTIR…