



**T.C.**  
**HATAY MUSTAFA KEMAL ÜNİVERSİTESİ**  
**FEN BİLİMLERİ ENSTİTÜSÜ**

**GERÇEK ZAMANLI KABLOSUZ ALGILAYICI AĞLARDA SALDIRI  
TESPİT ve SALDIRI YANIT SİSTEMLERİNİN TASARLANMASI**

**ÇAĞLAR OFLAZOĞLU**

**ENFORMATİK ANABİLİM DALI**

**DOKTORA TEZİ**

**HATAY**  
**MAYIS - 2023**

T.C.  
HATAY MUSTAFA KEMAL ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ

**GERÇEK ZAMANLI KABLOSUZ ALGILAYICI AĞLARDA SALDIRI  
TESPİT ve SALDIRI YANIT SİSTEMLERİNİN TASARLANMASI**

**ÇAĞLAR OFLAZOGLU**  
**ENFORMATİK ANABİLİM DALI**  
**DOKTORA TEZİ**

**Prof.Dr. Bünyamin YILDIZ** danışmanlığında ve **Doç.Dr. İpek Abasıkeleş-Turgut** ikinci danışmanlığında hazırlanan bu tez **17/05/2023** tarihinde aşağıdaki jüri üyeleri tarafından **OYBİRLİĞİ** ile kabul edilmiştir.

Prof. Dr. Bünyamin YILDIZ  
Başkan

Prof.Dr. Resul DAŞ  
Üye

Doç.Dr. Gökhan ALTAN  
Üye

Dr.Öğr.Üyesi Ahmet GÖKÇEN  
Üye

Dr.Öğr.Üyesi Ersin ÖZDEMİR  
Üye

**Kod No:**

**Doç. Dr. Cengiz KARACA**  
**Enstitü Müdürü**

**Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.**

## ÖZET

### GERÇEK ZAMANLI KABLOSUZ ALGILAYICI AĞLARDA SALDIRI TESPİT ve SALDIRI YANIT SİSTEMLERİNİN TASARLANMASI

Nesnelerin İnterneti (IoT) ekosisteminin önemli bir bileşeni olan Kablosuz Algılayıcı Ağ (KAA)'lar; dış ortamdan topladıkları veriyi bağımsız olarak işleyebilen ve kablosuz ortam aracılığı ile istenilen hedefe ulaştırabilen aygıtların oluşturduğu ağlardır. KAA'yı oluşturan aygıtların uygulama gereği yoğunlukla korunmasız şartlara sahip olan arazilere yerleştirilmesi, bu aygıtların çeşitli saldırılara karşı dayanıksız kalma riskini de artırmaktadır. Bununla birlikte, kısıtlı donanım özelliklerine ve düşük işlem kapasitesine sahip olan aygıtlar nedeniyle bu ağlarda karmaşık güvenlik algoritmaları kullanılamamaktadır.

Bu tez çalışmasında, KAA'larda paket iletimini engellemeyi amaçlayan yönlendirme saldırılarına karşı kaynak kullanımını gözeten, komşu izleme tabanlı bir saldırı tespit ve yanıt sistemi geliştirilmiştir. Komşu izleme süreci için yönlendirme istatistikleri kullanmak yerine paketin içinde yer alan veri analiz edilmiştir. Ayrıca, MAC katmanında IEEE 802.15.4 protokolünde yapılan güncellemeler ile ek kontrol paketlerine ihtiyaç duymaksızın izleyici düğümlerin kapsama alanı dışında kalan paket trafiğini ve saldırıları tespit edebilmesi ve güvenli rotanın yeniden kurulması sağlanmıştır. Saldırgan olarak belirlenen düğümlerin engellenerek kara listeye alınması yerine yüksek ceza puanı uygulaması ile güvenli rota üzerinde tercih edilmemesi sağlanarak hem verinin hedefe sağlıklı bir rota üzerinden ulaşması garantilenmiş hem de gerçek zamanlı ortamın doğasından kaynaklanan olası hatalı tespite karşı düğüme yeniden aktif olma şansı tanınmıştır.

Yönlendirme mimarisi olarak Toplama Ağacı Protokolü (CTP) kullanıldığı ve bileşen tabanlı olarak tasarlanan algoritmalar, gerçek zamanlı test ortamında denenmiştir. Farklı sayıda saldırı düğümünün yer aldığı ağlar için yapılan ölçümlerde farklı saldırı türleri, çeşitli saldırı ve düğüm sayıları istatistikleri incelendiğinde %99'a varan paket iletim oranı elde edilmiştir.

2023, 126 sayfa

**Anahtar Kelimeler:** Kablosuz algılayıcı ağlar, toplama ağacı protokolü, saldırı tespit sistemi, saldırı yanıt sistemi, komşu izleme

## TEŞEKKÜR

Doktora çalışması sırasında her konuda yardımlarını esirgemeyen danışmanım Prof.Dr. Bünyamin YILDIZ hocama ve tez konumun belirlenmesinde ve araştırılmasında bilgi birikimi ve tecrübesiyle çalışmalarına ışık tutan ve yardımlarını esirgemeyen ikinci danışmanım Doç.Dr. İpek ABASIKELEŞ-TURGUT hocama sonsuz saygı ve teşekkürlerimi sunarım.

Tez çalışmalarının takibinde profesyonel yaklaşımları ve öngörülleri ile doktora çalışmalarımı zenginleştiren ve yardımlarını esirgemeyen Tez İzleme Komitesi üyeleri Dr.Öğr. Üyesi Ahmet GÖKÇEN ve Dr. Öğr. Üyesi Ersin ÖZDEMİR'e, evrak süreçlerinin yürütülmesinde yardımlarından dolayı Hatay Mustafa Kemal Üniversitesi (HMKÜ) Enformatik Anabilim Dalı Başkanlığı'na ve sekreteryası Zehra ÖZER'e, HMKÜ FBE Enstitüsü Müdürlüğü çalışanlarına ve ayrıca öğrenci işleri personeli Kenan BAŞÇEKEN'e teşekkürlerimi sunarım.

Eğitim hayatım boyunca beni maddi ve manevi olarak destekleyen, güvenen ve daima yanımda olan başta eşim Demet OFLAZOĞLU ve oğlum Toprak OFLAZOĞLU'na, anneme, babama ve kardeşime sonsuz minnet ve şükranlarımı sunarım.

*06 Şubat 2023 deprem felaketinde sonsuzluğa uğurladığımız; Cavit & Dilek ve Ege OFLAZOĞLU, Kemal & Sabahat, Çağla ve Ceren OFLAZOĞLU ve kardeşim Erdem UĞUN anısına...*

|                                                                                                |     |
|------------------------------------------------------------------------------------------------|-----|
| 4.3. Çok Seviyeli Topolojilerde Saldırı Tespit ve Yanıt Sistemi Performans Analizleri .....    | 100 |
| 4.3.1. Korumasız Bir Ağ İçin Saldırı Analizi .....                                             | 103 |
| 4.3.2. PLOST ve PACKB Bileşenleri ile Koruma Altına Alınan Ağ İçin Performans Analizleri ..... | 105 |
| 4.3.3. PCHANGE ve PACKB Bileşenleri ile Korunan Bir Ağ İçin Performans Analizleri .....        | 110 |
| 4.3.4. PLOST, PACKB ve PQUEUE Bileşenleri ile Korunan Bir Ağ İçin Performans Analizleri .....  | 112 |
| 4.4. Genel Değerlendirme ve Literatürdeki Benzer Çalışmalar .....                              | 113 |
| 5. SONUÇ ve ÖNERİLER .....                                                                     | 117 |
| KAYNAKLAR .....                                                                                | 120 |
| ÖZGEÇMİŞ .....                                                                                 | 126 |



## ŞEKİLLER DİZİNİ

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| Şekil 1.1. KAA'ların genel gösterimi .....                                                  | 1  |
| Şekil 1.2. Kablosuz algılayıcı blok diyagramı .....                                         | 2  |
| Şekil 3.1. IEEE 802.15.4/ZigBee protokol yığını mimarisi .....                              | 19 |
| Şekil 3.2. IEEE 802.15.4 PHY katman çerçeve yapısı .....                                    | 20 |
| Şekil 3.3. MAC Alt Katmanı ve Fiziksel Katman .....                                         | 21 |
| Şekil 3.4. Süper çerçeve yapısı .....                                                       | 22 |
| Şekil 3.5. Aygıttan koordinatöre veri iletim modelleri .....                                | 23 |
| Şekil 3.6. Koordinatörden aygıtı veri iletim modelleri.....                                 | 24 |
| Şekil 3.7. İşaret Çerçevesi.....                                                            | 25 |
| Şekil 3.8. Veri Çerçevesi.....                                                              | 26 |
| Şekil 3.9. Alındı Çerçevesi .....                                                           | 26 |
| Şekil 3.10. MAC Komut Çerçevesi.....                                                        | 27 |
| Şekil 3.11. CTP örnek topolojisi .....                                                      | 28 |
| Şekil 3.12. CTP kontrol ve veri düzlemleri.....                                             | 29 |
| Şekil 3.13. 4-bitlik kablosuz bağlantı tahmini .....                                        | 30 |
| Şekil 3.14. CTP yönlendirme çerçevesi .....                                                 | 32 |
| Şekil 3.15. CTP veri çerçevesi şablonu.....                                                 | 33 |
| Şekil 3.16. Yönlendirme paketlerinin gönderim sıklığı .....                                 | 34 |
| Şekil 3.17. IRIS Ana Birimi.....                                                            | 37 |
| Şekil 3.18. IRIS blok diyagramı.....                                                        | 38 |
| Şekil 3.19. IRIS Algılayıcı Birimi.....                                                     | 40 |
| Şekil 3.20. Termistörün bağlantı şeması .....                                               | 40 |
| Şekil 3.21. Termistörün sıcaklık-direnç değişimi grafiği .....                              | 41 |
| Şekil 3.22. Işık algılayıcısının bağlantı şeması .....                                      | 42 |
| Şekil 3.23. IRIS Ağ Geçidi Birimi .....                                                     | 42 |
| Şekil 3.24. TinyOS mimarisi.....                                                            | 44 |
| Şekil 3.25. Çıkış deliği saldırısı .....                                                    | 47 |
| Şekil 3.26. Karadelik saldırısı .....                                                       | 48 |
| Şekil 3.27. Seçici yönlendirme saldırısı .....                                              | 49 |
| Şekil 3.28. Komşu düğümün izlenmesi .....                                                   | 52 |
| Şekil 3.29. Geliştirilen ve önerilen saldırı tespit ve yanıt sisteminin blok diyagramı .... | 54 |
| Şekil 3.30. Komşu izleme tabanlı paket takibi.....                                          | 57 |
| Şekil 3.31. Paket izleme süreçleri kaba kodu.....                                           | 58 |
| Şekil 3.32. Paket izleme, veri değişikliği tespit ve onarım süreci akış diyagramı .....     | 59 |
| Şekil 3.33. Veri değişikliği tespit sistemine ilişkin kaba kod .....                        | 61 |
| Şekil 3.34. ACK çerçevesinin izlenmesi.....                                                 | 62 |
| Şekil 3.35. Alındı çerçevesi için yapılan düzenleme .....                                   | 63 |
| Şekil 3.36. Alındı mesajı takip sistemine ilişkin kaba kod .....                            | 64 |
| Şekil 3.37. Kapsama alanı kesişimlerindeki ortak saldırganların tespiti .....               | 65 |
| Şekil 3.38. İşbirliği/kalıtım paketlerinin iletimi .....                                    | 66 |
| Şekil 3.39. İşbirliği çerçeve şablonu .....                                                 | 67 |
| Şekil 3.40. İşbirlikçinin komşu düğüm listesi.....                                          | 68 |
| Şekil 3.41. Paket gönderim sürecinde paylaşılmış istatistiklerin kullanımı.....             | 69 |
| Şekil 3.42. İşbirliği paketi alım sürecine ilişkin akış diyagramı .....                     | 70 |
| Şekil 3.43. Onarım sisteminde paketlerin geçici listeden gönderim süreci .....              | 71 |
| Şekil 3.44. Komşu düğüme ilişkin yürütülen karar mekanizması kaba kodu.....                 | 74 |

## SİMGELER ve KISALTMALAR DİZİNİ

### SİMGELER

|                     |                                                                     |
|---------------------|---------------------------------------------------------------------|
| $\mu A$             | : mikroamper                                                        |
| $^{\circ}C$         | : santigrat derece                                                  |
| $\Omega$            | : Ohm                                                               |
| $CX_i$              | : i. seviyedeki saldırgan düğüm sayısı                              |
| dBm                 | : desibel-miliwatt                                                  |
| df                  | : Veri paketinin alıcıya başarıyla ulaşma olasılığı                 |
| dr                  | : Bilgilendirme paketlerinin göndericiye başarıyla ulaşma olasılığı |
| $ETX_i$             | : i. düğümün rota maliyeti                                          |
| $ETX_{link}$        | : Düğümler arası rota maliyeti                                      |
| $ETX_{penalty}$     | : Ceza maliyeti değeri                                              |
| GHz                 | : gigaHertz                                                         |
| hLevel <sub>i</sub> | : i. düğümün seviye bilgisi                                         |
| k $\Omega$          | : kiloOhm                                                           |
| kbps                | : saniye başına kilobit (kilobits per second)                       |
| lnX <sub>i</sub>    | : i-1 ile i+1. seviye bölgesindeki ortak saldırgan düğüm sayısı     |
| L_ETX <sub>ij</sub> | : i . düğümün j. komşu düğümüne ilişkin yerel rota maliyet değeri   |
| mA                  | : miliamper                                                         |
| MHz                 | : megaHertz                                                         |
| ms                  | : milisaniye                                                        |
| nKND                | : Kötü niyetli düğüm sayısı                                         |
| PCX <sub>ij</sub>   | : i . düğümün j. komşu düğümüne ilişkin ölçeklenmiş yerel maliyeti  |
| R <sub>thr</sub>    | : Termistörün direnç değeri                                         |
| SLX <sub>i</sub>    | : i. seviyedeki saldırgan düğümler                                  |
| V                   | : Volt                                                              |

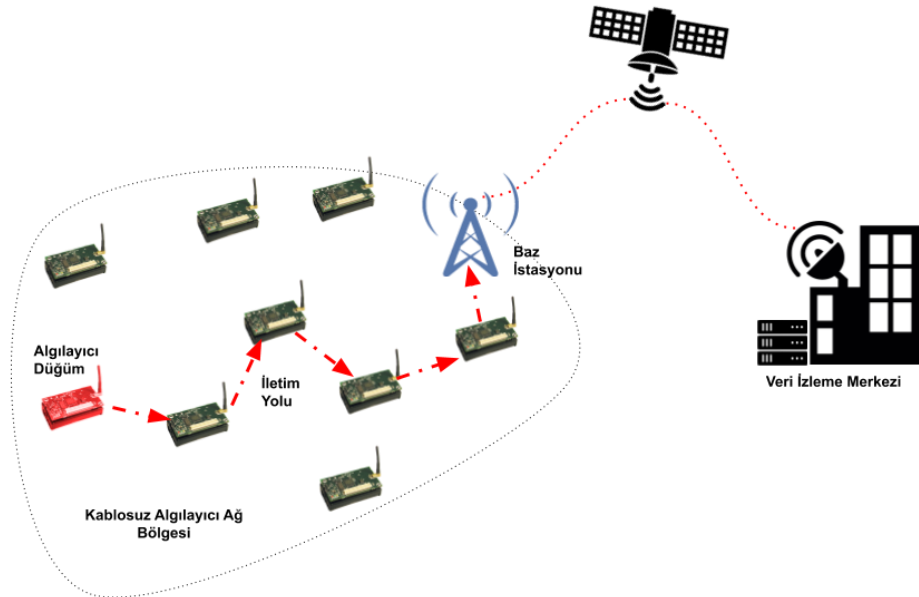
### KISALTMALAR

|          |                                                                                                                  |
|----------|------------------------------------------------------------------------------------------------------------------|
| ACK      | : Acknowledgement Frame (Alındı Çerçevesi)                                                                       |
| ADC, A/D | : Analog/Digital Converter (Analog-Dijital Dönüştürü)                                                            |
| APS      | : Alınan Paket Sayısı                                                                                            |
| CCA      | : Clear Channel Assessment (Açık Kanal Ataması)                                                                  |
| CS       | : Carrier Sense (Taşıyıcı Sezme)                                                                                 |
| CSMA/CA  | : Carrier Sense Multiple Access with Collision Avoidance<br>(Çarpışma Önleme ile Taşıyıcı Algılama Çoklu Erişim) |
| CRC      | : Cyclic Redundancy Check (Döngüsel Artıklık Kontrolü)                                                           |

## 1. GİRİŞ

Kablosuz Algılayıcı Ağlar (KAA); sınırlı işlem kapasitesi, düşük maliyet ve enerji tüketimine sahip kablosuz algılayıcılar ile elde etmiş oldukları çeşitli verileri kısa mesafeli olarak birbirleri üzerinden merkeze ulaştırmayı amaçlar. Bu ağlar; 1978 yılında “Proceedings of the Distributed Sensor Nets Workshop” etkinliği ile “Dağıtık Algılayıcı Ağlar” ismi ile anılmaya başlamış, 1993 ve sonraki yıllarda ise kablosuz iletişim ve mikro elektronik teknolojilerdeki imkânların artması ile birlikte araştırmacıların ilgisini çeken bir konu haline gelmiştir. KAA’nın düşük maliyet ve uygulama kolaylığı, bu aygıtların birçok alanda kullanılmasına olanak sağlar. Bu alanlar; askeri uygulamalar (gözetleme), ev/kişisel uygulamalar, çevresel olayların izlenmesi (su kalitesi, hava durumu, hava kirliliği, deprem, vb.), sağlık uygulamaları ve diğer ticari uygulama alanları olarak sınıflandırılabilir (Akyildiz ve ark., 2002; Butun ve ark., 2013).

Kablosuz algılayıcılar; kısıtlı işlem kapasitesine sahip bir mikrodenetleyici, isteğe bağlı özelleştirilebilir ortam algılayıcıları, radyo frekansı üzerinden haberleşme birimi ve dâhili bir güç kaynağına sahip olabilen elektronik bir devredir. Bu aygıtlar, Şekil 1.1’de de görüleceği üzere ortamdan almış oldukları verileri kablosuz haberleşme yolu ile birbirleri üzerinden merkeze aktarmak üzerine görevlendirilmiş bileşenlerdir. Aygıtların bir araya gelerek oluşturmuş oldukları iletişim ağı Kablosuz Algılayıcı Ağ (KAA, Wireless Sensor Network, WSN) olarak isimlendirilmektedir.



Şekil 1.1. KAA’ların genel gösterimi

Kablosuz algılayıcıların kısıtlı kaynaklara sahip olması üretim maliyetlerinin de daha az olmasını sağlar. Bu da özellikle büyük ölçekli kullanımlarda önemli bir tercih sebebidir. Aygıtların üzerinde bulunan dâhili güç kaynağı ve kablosuz iletişim birimi, bu aygıtların herhangi bir ortamda kendi başlarına çalışabilmelerine ve kablosuz olarak iletişim kurabilmelerine olanak sağlayarak işletme maliyetleri azaltır.

KAA aygıtlarında en önemli donanımsal kısıt, güç kapasitesidir. İşlem ve iletişim bileşenlerindeki üst seviye kullanımlar, aygıt gücünün hızla tükenmesine neden olmaktadır. Ayrıca bu aygıtlar, işlevsiz bulundukları zaman dönemlerinde uyku durumuna geçerek enerji kullanımlarını en az seviyeye düşürecek şekilde imal edilmektedirler. Aygıtların uyku durumuna geçebilmesi için aktif bir görev yürütmüyor olmaları gerekmektedir. Bu nedenle süreçlerin hızlıca tamamlanması aygıtların uyku döneminde geçirdikleri sürenin de artmasına ve enerji tasarrufuna imkân sağlar. Aygıtlar ile istenilen görevlerin daha uzun süre gerçekleştirilebilmesi için minimum enerji harcayacak enerji verimli iletişim ve çalışma modellerinin tasarlanması gerekir. Bu nedenle güç tüketimi, KAA aygıtları için önemli bir yaşam parametresi haline gelmektedir. Güç tüketimi üzerine yapılan çalışmalar; radyo optimizasyonu, veri azaltma, uyku/uyanma planları, enerji verimli yönlendirme ve pilin yenilenmesi/şarj edilmesi gibi konu başlıkları altında gösterilebilir (Rault ve ark., 2014). Özellikle enerji verimli yönlendirme protokolleri (Ogundile ve ark., 2017) ve pil enerjisinin yenilenmesi (enerji hasadı) (Panatik ve ark., 2016; Sah ve ark., 2020) üzerine yapılan çalışmalar araştırmacıların ilgisini çeken konuların başında gelmektedir.

KAA'da yer alan düğümlerin iletişim sırasında yaydıkları radyo sinyalleri, kapsama alanı içerisinde bulunan ve aynı kanalı dinleyen diğer aygıtlar tarafından da izlenebilmektedir. Kablosuz kanal yayınının aygıtlar tarafından dinlenebiliyor olması, bu ağı iç ve dış saldırılara karşı savunmasız hale getirmektedir. Bu durum, KAA'lar için önemli bir güvenlik problemidir (Zhou ve ark., 2008). Saldırıları, ağ trafiğinin erişilebilirliğini veya paket bütünlüğünü tehdit etmenin yanı sıra aygıtların kısıtlı işlem ve güç kapasitelerini tüketmeyi de hedefleyebilir. İletişimin güvenli olarak gerçekleştirilebilmesi için literatürde farklı kriptografik algoritma önerileri mevcuttur. Kriptografik çalışmalardaki en büyük zorluk anahtarların düğümlere güvenli olarak iletilmesinin gerekliliğidir. Özellikle dinamik ağlarda bu işlem için düğümler arasında ayrıca bir paket iletişimine ihtiyaç duyulmaktadır. Ayrıca kriptografik algoritmaların

algoritmaların gerçek zamanlı donanımlar üzerinde test edilmesi uygulama açısından oldukça önemlidir.

## 1.2. Tez Çalışmasının Amacı ve Kapsamı

Tez çalışmasında, KAA için kısıtlı donanıma sahip aygıtların paket iletişimi ve güç tüketimine yönelik saldırılara karşı saldırı tespit ve yanıt sistemi tasarımı hedeflenmiştir. KAA’larda yaygın olarak tercih edilen yönlendirme şemalarından birisi olan Toplama Ağacı Protokolünün (CTP, Collection Tree Protocol) enerji verimli rota oluşturmaya rağmen herhangi bir güvenlik çözümü sunmuyor olması, bu protokolü dış dünyadan gelen saldırılara karşı savunmasız duruma getirmektedir. Bu nedenle tasarlanan komşu izleme tabanlı saldırı tespit ve yanıt sistemi, CTP’nin sağlamış olduğu faydalardan yararlanarak yönlendirme katmanını güvenli duruma getirmeyi amaçlamaktadır. Çalışmaların gerçek zamanlı ortam kullanılarak gerçekleştirilecek olması ağ dinamiklerinden kaynaklanan koşulların da doğru olarak ortaya konmasına yardımcı olacaktır.

Çalışmada;

- Kötü niyetli düğüm olarak kullanılmak üzere tasarlanan saldırı modellerinin başarımlarının incelenmesi
- Komşu izleme tabanlı saldırı tespit sisteminin ilk bileşeni olan paket izleme bileşenin tasarımı
- Düğüm bazlı yerel rota metriklerine ceza değerleri ekleyerek saldırgan düğümlerin aktif rotadan çıkarılmasının sağlanması ve ağdaki yüksek seviyeli topolojik değişimlerin ceza değerine olan etkisinin azaltılması
- Alındı paketlerinin takibi ile saldırı tespit sisteminin geliştirilmesi
- İşbirliği/kalıtım bileşeni ile elde edilen deneyimlerin minimum paket iletişimi ile diğer düğümlere aktarılması
- Saldırı sebebi ile iletilemeyen/bozulan paketlerin yeni rotalar üzerinden baz istasyonuna iletiminin sağlanması

konuları ele alınmıştır.

kullanılabilmektedir. Naz ve ark. (2012) yapmış oldukları çalışma ile akustik ve sismik algılayıcılar kullanarak yaklaşan düşman askerlerinin sürünme, yürüme, silah taşıma vb. gibi kaynakların oluşturduğu verilerden yararlanarak konumlarının tespitine katkı sağlamayı amaçlamışlardır. Chang ve ark. (2006) önermiş oldukları KAA destekli saldırı erken tespit sistemi ile keskin nişancı silah seslerini algılayarak, kerteriz ve menzil bilgisi sağlamayı hedeflemişlerdir. Lim ve ark. (2010) gerçekleştirmiş oldukları KAA destekli gerçek zamanlı sağlık izleme sistemi ile giyilebilir fizyolojik ve biyomedikal algılayıcılar kullanarak askerlerin sahadaki sağlık verilerini izlemeyi hedeflemişlerdir. Askeri alanda yapılan çalışmalarla tehditlerin konumlarının önceden tespiti, askeri kayıpların azaltılması, askeri envanterin takibi, sınır güvenliği gibi kritik alanlarda daha etkin mücadele edilmesi gibi birçok amaç KAA'lar aracılığı ile gerçekleştirilebilmektedir.

KAA'lar; çevre, iklim, tarım ve afet yönetimi gibi alanlarda da yaygın olarak kullanılabilmektedir. Doğal afetlerin takibi ve uyarı sistemleri (fırtına, tsunami, deprem, sel vb. gibi), doğal kaynakların takibi (su kalitesi, hava kirliliği vb. gibi), çeşitli tarımsal uygulamaların (sera iklimlendirmesi, don, sulama vb. gibi) takibi bu kullanımlara örnek olarak verilebilir. Jha ve ark. (2015) yapmış oldukları çalışmada deprem ve tsunaminin sebep olduğu kayıpları azaltmak için KAA destekli erken uyarı sistemi için ağ tasarımı önerisi sunmuşlardır. Bouabdellah ve ark., (2013) orman yangınlarını erken algılamak için KAA tabanlı tespit sistemi geliştirmişlerdir ve geliştirdikleri bu sistemde yangının tespiti için kullandıkları farklı algoritmaların hız ve işlemci tüketimi açısından karşılaştırmalarını sunmuşlardır. Kassim ve ark., (2016) gerçekleştirdikleri KAA tabanlı tarım ortamı izleme sistemi ile algılayıcılar aracılığıyla (sıcaklık ve nem algılayıcıları ile kapalı devre kamera sistemi (CCTV)) toplamış oldukları verilerle sera ortamını uzaktan otomatik olarak kontrol etmeyi hedeflemişlerdir. Rosero-Montalvo ve ark. (2020) KAA aracılığı ile nehir üzerindeki farklı bölgelerden sıcaklık, su kalitesi, bulanıklık, pH seviyesi gibi ölçümler yaparak nehrin kirlilik seviyeleri üzerine bir çalışma yapmışlardır. Edwards Murphy ve ark. (2015) bal arıcılığı için kovan sağlığının takip edilebilmesini sağlamak amacıyla KAA destekli bir çalışma gerçekleştirmişlerdir. Bu çalışmada algılayıcılarla kovan içerisindeki sıcaklık, nem, oksijen ve karbondioksit düzeyi ve kirlilik seviyesi (nitrojen dioksit) ölçümlenerek arıcıya gerekli bilgilendirmelerin sağlanmasını hedeflemişlerdir. Araştırmacılar bu çalışmada aynı zamanda dış ortam koşullarının da ölçümlenmesini sağlamış ve kovan içerisindeki karbondioksit düzeyi ile

güvenlik mekanizmalarına sahip olmayışının ortaya çıkardığı sakıncalara vurgu yapmış ve akıllı şebeke uygulamalarındaki tehditlere yönelik çözümler ve araştırma konularını aktarmışlardır. Zaatouri ve ark. (2018); karayollarında kaza, ulaşım gecikmeleri, trafik sıkışıklığı gibi olumsuzlukları ortadan kaldırmak amacıyla akıllı ulaşım sistemlerini geliştirmek için kavşak ışıklarının kontrol edilebilmesinde kullanılmak üzere KAA destekli bir aygıt tasarımı ve kavşak yönetim algoritması önerisi sunmuşlardır.

KAA'nın farklı alanlarda kritik uygulamalar gerçekleştirilmesine imkân sağlaması, uygulamada karşılaşılan donanımsal kısıt ve güvenlik problemlerini önemli birer araştırma konusu haline getirmiştir. Ağ içerisinde konumlanmış olan aygıtların kapsama alanı sebebiyle doğrudan merkeze veriyi aktaramadığı durumlarda diğer aygıtlarla işbirliği yaparak bir rota oluşturması ve bu rota üzerinden veriyi merkeze iletmesi gerekir. Kısıtlı batarya enerjileri sebebiyle rota oluşturma ve yönetimi gibi konularda optimize edilmiş algoritmaların seçilmesi hem enerjinin verimli olarak kullanılmasına hem de aygıtlar arasındaki veri trafiğinin minimum düzeyde gerçekleşmesini sağlar. Tercih edilecek yönlendirme protokolleri, kullanım alanlarına göre farklılık gösterebilmektedir. Luo ve ark. (2020) yaptıkları çalışmada sualtında kullanılabilecek KAA'lar için tercih edilebilecek yönlendirme protokol önerileri sunarken, Khalil ve ark. (2018) yaptıkları diğer bir çalışmada ise akıllı şehir sistemlerinde farklı görevler (sıcaklık-kirlilik ölçümü, afet, sağlık vb. gibi) için kullanılabilecek protokolleri değerlendirmişlerdir. Aynı zamanda bu çalışmada ağın güvenlik riski için de vurgu yapılmıştır. Tuna ve Das (2020) yaptıkları çalışmada topolojideki önemli bir ağ dinamiği olan düğüm sayılarındaki değişimin güven ve itibar modeli performansına etkilerini incelemişlerdir. EigenTrust, LFTM, PeerTrust ve PowerTrust gibi popüler modeller için doğruluk ve yol uzunluğu performans ölçütü olarak belirlenmiştir. Değişen algılayıcı ağ ve düğüm sayısının doğrulukta azalma ve işlem süresinde artış olarak sonuçlanabildiği ve bu nedenle ağ parametrelerine göre uygun bir model seçilmesinin önemi vurgulanmıştır. Yönlendirme algoritmalarının enerji verimliliği ve güvenliği kapsamında Shafiq ve ark. (2020) yapmış oldukları çalışmada 2016-2018 yılları arasında yapılan akademik araştırmaları incelenmişlerdir. Araştırmada yönlendirme protokolleri; konum tabanlı, veri merkezli, hiyerarşik, hareketlilik tabanlı, çok yollu, heterojen tabanlı ve hizmet kalitesi (Quality of Service, QoS) tabanlı protokol olmak üzere yedi farklı kategoride sınıflandırılmıştır. Çalışma, farklı yönlendirme protokollerinin enerji verimliliği ve güvenli yönlendirme

edilmektedir. Fakat kullanılan aygıtların hesaplama, depolama ve batarya kısıtları göz önüne alındığında anahtarların uç aygıtlara iletilmesi için gerekli paket alışverişi, hesaplama maliyetleri ve gecikme; ağın ömrü ve paket trafiği gibi konularda olumsuzluklar oluşturmaktadır. Merad Boudia ve ark. (2015) KAA için önermiş oldukları kriptolojik çalışmada verilerin şifrelenerek iletilmesi üzerine yoğunlaşmıştır. Çalışmada, simetrik şifreleme özellikli durum tabanlı ortak anahtar şifreleme algoritması kullanmıştır. Her aygıt, kurulum aşamasında gizli bir anahtar yüklenerek aktif hale getirilmiştir. Anahtarlar baz istasyonu tarafından bilinmektedir. İletilen veriler uç aygıtlarda şifrelendikten sonra toplama aygıtına iletilir. Toplama aygıtı (küme başı) kendisine iletilen bilgileri kendi bilgisi ile de birleştirilerek baz istasyonuna iletir. Çalışma benzetim ortamında gerçekleştirilmiştir. Çalışma ile verilerin bütünlüğü ve gizliliği ilkeleri ön plana çıkarılmaktadır. Ağda veri kaybı yaratacak paket kayıplı saldırılar ile ağın enerjisini tüketerek yaşam ömrünü azaltacak paket tekrarlı saldırılar için bir çözüm sunulmaz. Pecho ve ark. (2006), TOSSIM benzetim ortamını kullanarak CTP protokolüne RFC ve MAC bölümleri ekleyerek akıllı kart şifrelemesi ile veri şifrelemeye dayalı bir yapı sunmuşlardır. Çalışma, veri transferinin şifreli olarak yapılabilmesi için akıllı kartların aktif olarak kullanılması durumunda protokolde yapılacak olan modifikasyonun veri trafiğinde ciddi etkileri olmayacağını savunmak amaçlı olarak gerçekleştirilmiştir. Ortak anahtarın güvenilir bir ortamda akıllı karta yüklenmesi ve aygıtın akıllı kart donanımıyla birlikte kullanılma gereksinimi vardır.

KAA uygulamalarında saldırganın; iletişim için kullanılan kriptografik anahtarları veya bir düğümü ele geçirerek ağa sızması durumunda ilgili önleyici güvenlik bileşenleri işlevsiz kalır. Bu nedenle de ağ üzerinde aktif olarak çalışabilen saldırı tespit ve yanıt sistemlerine ihtiyaç vardır. Saldırı vektörlerindeki çeşitlilik ve farklı yönlendirme algoritmalarının kullanılması araştırmacıları bu konularda ayrıntılı çalışmalara yönlendirmiştir. Ioannou ve Vassiliou (2016) yapmış oldukları çalışmada ağırlıklandırılmış en kısa yol (Weighted Shortest Path, WSP) protokolü üzerinde seçici yönlendirme (selective forwarding), karadelik (blackhole) ve çıkış deliği (sinkhole) saldırısını tespit etmek için izlenecek parametrelerle ilgili öneri sunmuşlardır. Saldırı etkilerini ve izlenen parametrelerin başarısını incelemek için TelosB düğümlerini COOJA benzetim ortamı kullanarak test etmişlerdir. Yönlendirme saldırılarının davranışları ve modelleri, yönlendirme mimarisine ve izlenen parametrelere bağlıdır. Benzetim

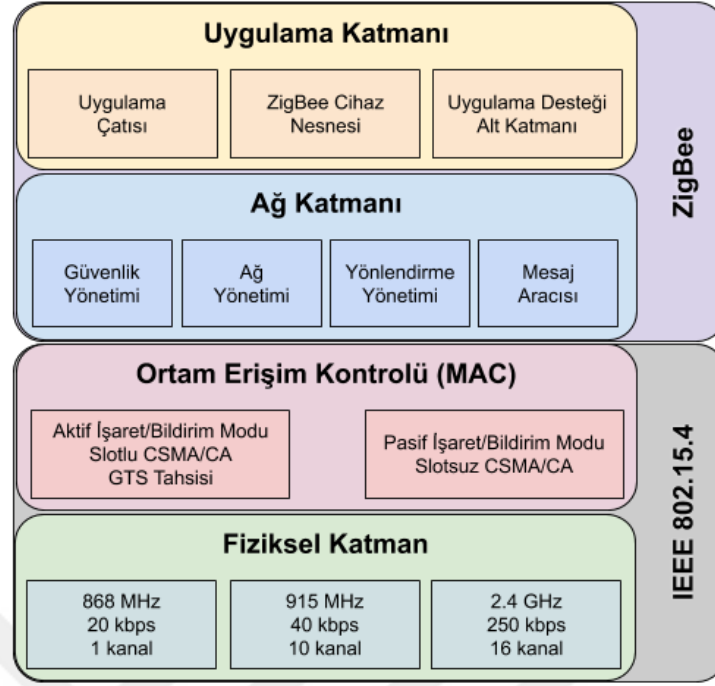
güvenlik algoritması önermişlerdir. Gönderilecek olarak veriler parçalara ayrılarak karıştırma işleminin ardından küme başı tarafından paketler halinde alıcı düğüme iletilir. Alıcı düğüm gelen paketlerin veri bütünlüğünü kontrol eder ve birleştirme işlemi ile verileri tekrar elde eder. Bu işlem için alıcı ve gönderici düğümlerin veri büyüklüğüne göre daha fazla bellek kullanımına, işlem gücüne ve zamana ihtiyaç duyulmaktadır. Cho ve Qu (2023), paket bırakma saldırılarının tespitini gerçekleştirebilmek için düğümlerin paket iletişimlerini izleyerek güven tabanlı hibrit bir model önermişlerdir. Araştırmacılar tasarladıkları modelde paket bırakma saldırısı için art arda paket kaybı ve iletimin gerçekleşmesi olasılığı üzerinden güven değerleri hesaplamışlardır. Benzetim ortamında gerçekleştirilen bu çalışmada ağ ve düğüm dinamikleri sonucu oluşan paket kaybı ve seçici yönlendirme saldırısı gibi belirli özellikteki paketlerin iletiminin engellenmesi gibi ardışık paket kaybı ile sonuçlanmayan saldırılar için yetersiz kalmaktadır.

Çizelge 2.1. Mevcut saldırı tespit sistemlerine genel bakış

| Yayın                       | Mimari | Yöntem   | Test Ortamı | Saldırı Türü        | Avantaj / Dezavantaj                                                                                                                                                                                                    |
|-----------------------------|--------|----------|-------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pecho ve ark. (2006)        | T      | K        | B           | VBG                 | +Akıllı kart ile veri şifrelemesi yapılmaktadır.<br>-Tüm akıllı kartlara ortak anahtarın yüklenme zorunluluğu vardır.                                                                                                   |
| Gupta ve ark. (2007)        | G      | A<br>İ   | GZ          | KD<br>ÇD<br>T<br>SY | +İstatistiklerin bir merkezde toplanarak değerlendirmesi ve sonucun uç düğümlere yayılımı sağlanmaktadır.<br>-Merkezi aygıtta ihtiyaç bulunmakta ve merkezi aygıttan uç cihazlara veri trafiğine ihtiyaç duyulmaktadır. |
| Stetsko ve ark. (2010)      | T<br>G | A<br>İ   | B           | T<br>SY             | -Komşu düğümler arasında işbirliği yoluyla periyodik olarak istatistik paylaşımına ihtiyaç vardır.                                                                                                                      |
| Zhan ve ark. (2012)         | T      | İ        | GZ<br>B     | ÇD<br>SD            | - Merkezi aygıtta ihtiyaç bulunmakta ve merkezi aygıttan uç cihazlara veri trafiğine ihtiyaç duyulmaktadır.                                                                                                             |
| Cui ve Yang (2014)          | T<br>G | İ<br>KDİ | B           | SY                  | +Ağın kararlı olması durumunda SY saldırılarının tespit oranı yüksektir.<br>-Çalışma parametrelerinin önceden belirlenmesine ihtiyaç duyar. Bu nedenle dinamik özellikli ağlarda verimi düşer.                          |
| Merad Boudia ve ark. (2015) | C      | K        | B           | VBG                 | +İletilen veriler uç aygıtlarda şifrelenir ve toplama aygıtına (küme başı) iletilir.<br>-Paket kayıplı saldırılara çözüm sunmamaktadır.                                                                                 |

Çalışmada kullanılan yönlendirme protokolü olan CTP (Fonseca ve ark., 2006) algoritması ağaç temelli bir hiyerarşik yapıda olup; ağ kurmak için gerekli olan aygıtlar arası mesajlaşma trafiğini azaltması, düğümler arası döngüleri ortadan kaldırması ve ölçeklenebilir olması sebebiyle tercih edilmiştir. Bu protokol, saldırılara karşı herhangi bir güvenlik mekanizmasına sahip değildir. Bu nedenle protokol için literatürde az sayıda da olsa önerilmiş saldırı tespit ve yanıt sistemleri yer almaktadır. Zhan ve ark. (2012) yapmış oldukları çalışmada çıkış ve solucan deliği saldırıları ile sahte baz istasyonlarından oluşan bir ortamda güven tabanlı bir yol kurma önerisinde bulunmuşlardır. Çalışma, gerçek zamanlı ve benzetim ortamları için test edilmiştir. Yönlendirme algoritması olarak CTP kullanılmıştır. Algoritma, enerji izleyici ve güven yöneticisi bileşenleri üzerinden çalışmaktadır. Enerji izleyici, düğümlerin ilettiği oldukları paketlere ilişkin güç bilgisini hesaplar. Güven yöneticisi ise baz istasyonu tarafından gönderilen bilgilendirme mesajları ile iletilen paketlerin başarı oranını test ederek güven katsayısı hesaplar. Baz istasyonu tarafından belirli aralıklarla ağa bilgilendirme mesajları yayınlanır. Yayınlanan bu mesajlar üzerinden enerji izleyici ve güven yöneticisi, ilgili düğümlere ilişkin parametreleri günceller ve düğümler yeniden değerlendirilir. Baz istasyonunun belirli aralıklarla hiyerarşik olarak ağa bildirim mesajlarını yayması sistemi merkeze bağımlı kılmakta ve bu yayılım, paket trafiğinin ve enerji tüketimin oluşmasına neden olmaktadır. Almon ve ark. (2017), CTP ve karmaşık (mesh) protokol üzerinde yaptıkları çalışmada KAA için karadelik ve farklı yayın bozma saldırıları için lojistik regresyon tabanlı işbirliği gerektirmeyen bir saldırı tespit sistemi tasarımı önermişlerdir. Regresyon modeli ile saldırı tespiti için farklı sayıda metriktan yararlanılmıştır. Metrik sayısının artırılarak tek bir model oluşturması, yapılan saldırılarda başarıyı azaltmaktadır. Farklı saldırılar için farklı regresyon modellerinin oluşturulması gerekmektedir. Bu işlem için de bellek ve işlemci üzerinde ekstra bir yüke ihtiyaç duyulmasına neden olmaktadır. Cui ve Yang (2014) seçici yönlendirme saldırılarını tespit edebilmek için yeni yönlendirme algoritmaları geliştirmişler ve bu başarımları savunmasız CTP ile kıyaslamışlardır. Önerilen algoritmalar, CTP tabanlı reaktif bir yönlendirme şeması olarak geliştirilmiştir. Geliştirilen yöntemler ile iletilmeyen paketlerin tespiti sonucunda saldırgan tespiti ve rota değişikliği yapılması amaçlanmaktadır. Kullanılan katsayılar, ağın benzetim ortamındaki davranışlarından elde edilen sonuçlara göre seçilmiştir. Çalışma, benzetim ortamında tek bir saldırı tespiti için

ortaya çıkarmaktadır. Çalışmada gerçek zamanlı test ortamı kullanılmıştır. Literatürdeki benzer çalışmalardan farklı olarak tasarlanan sistemde iletişim düzeyindeki istatistiksel verilerin yanı sıra paket içeriği ve düğüm düzeyinde elde edilen verilerden de yararlanılmıştır. Tespit ve yanıt sisteminin merkezi bir karar mekanizmasına ihtiyaç duymayacak şekilde tasarlanmış olması ek bir paket yükü de gerektirmez. Ayrıca çalışmada yönlendirme protokolü için tercih edilen CTP algoritmasının ağ içerisindeki rota değişikliklerinden en az düzeyde etkilenmesi de amaçlanmıştır. Tasarlanan sistem ile tespit edilen kötü niyetli düğümleri ağdan çıkarmak yerine daha yüksek rota maliyetleri ile cezalandırarak yeniden ebeveyn olarak seçilebilmelerinin yolu açılmıştır. Böylece kablosuz ortam ve düğümlerden kaynaklanabilecek hatalı kararlarda düğüm ağdan tamamen dışlanmaz ve ebeveyn düğüm için daha iyi bir alternatif yok ise bu düğüm yeniden seçilerek ağda veri iletimine katılabilir.



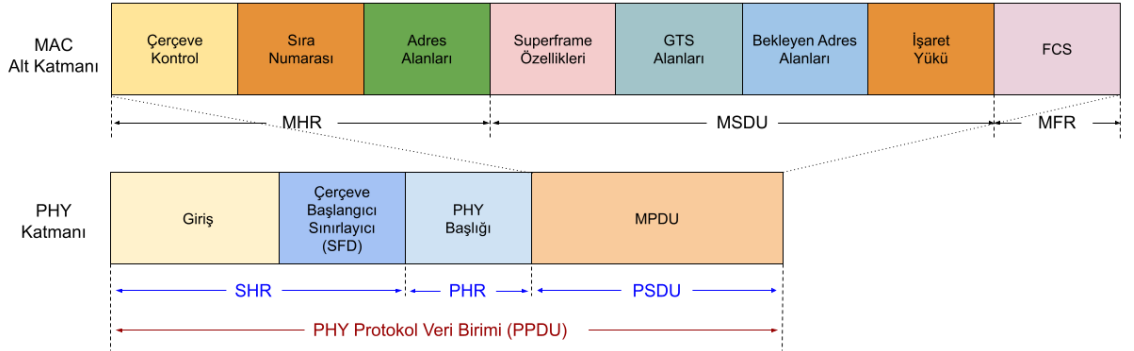
Şekil 3.1. IEEE 802.15.4/ZigBee protokol yığını mimarisi

Şekil 3.1 ile gösterilen mimaride IEEE 802.15.4 standardı fiziksel katman (PHY) ile ortam erişim kontrolü (MAC) katmanından, ZigBee olarak belirtilen yapı ise üst katmanlar olan ağ katmanı ve uygulama katmanından oluşmaktadır.

- **Fiziksel Katman**

Fiziksel katmanın asıl amacı veri paketlerin transferidir. Bu katman; veri ve yönetim servislerini sunar. Fiziksel katmandaki yönetim servislerine PHY alt katman yönetim varlığı (PHY Sublayer Management Entity, PLME) servis erişim noktası (Service Access Point, SAP) üzerinden erişebilmektedir. Yönetim servisleri (PLME-SAP) ile radyo alıcısı/vericisinin aktif/pasif duruma getirilmesi ve alıcının alma, gönderme ve uyku modları bu katmanda üst katmandan gelen taleplerle yürütmektedir. Kanal frekansının seçilmesi ve kanalın kullanımının denetimi, enerji algılama (Energy Detection, ED) ile açık kanal ataması (Clear Channel Assessment, CCA) süreçleri yine bu servisler üzerinden yürütülmektedir. Açık kanal ataması ile veri iletim kanalının kullanım durumu tespit edilmektedir. Tespit işlemi; sinyal enerjisinin eşik değeri olarak kabul edilen sınırdan daha yüksek olması, CS (Carrier Sense, Taşıyıcı Sezme) modu ile standarda uygun sinyalin varlığının tespiti veya iki yöntemin birlikte kullanılması

varlığı hizmet erişim noktası (MAC Sublayer Management Entity Service Access Point, MLME-SAP) olarak isimlendirilmiştir. Yönetim hizmeti ile işaret sinyalinin yönetimi, çerçeve doğrulama, kanal erişimi, garanti edilen zaman dilimleri (Guaranteed Time Slots, GTS) yönetimi, onay mesaj çerçevelerinin yönetimi gibi işlevler gerçekleştirilir. Şekil 3.3 ile verilen şekilde fiziksel katmanda yer alan PSDU, MAC alt katmanındaki MPDU ile aynı bölüme karşılık gelmektedir. MPDU içeriğinde MAC Başlığı (MAC Header, MHR), MAC Hizmet Veri Birimi (MAC Service Data Unit, MSDU) ve MAC Altbilgisi (MAC Footer, MFR) bölümleri yer alabilmektedir. MPDU içeriği, MAC alt katmanında işletilecek görevlere göre özelleştirilmiştir. MHR bölümünde çerçeve kontrol bitleri, sıra numarası ve adres bilgileri alanı yer alabilmektedir. MSDU bölümü, çerçevenin kullanım amacına göre özelleştirilebilir verilerin bulunduğu veri alanıdır. MFR bölümü ise Çerçeve Kontrol Dizisi (Frame Check Sequence, FCS) adı verilen ve çerçevenin bütünlüğünün kayıplı ortamda alıcı tarafından doğrulanabilmesine olanak sağlayan on altı bitlik kontrol dizisidir. Bu kontrol dizisi, Döngüsel Artıklık Kontrolü (Cyclic Redundancy Check, CRC) adı verilen yöntem ile hesaplanmaktadır (IEEE 802.15, 2003).



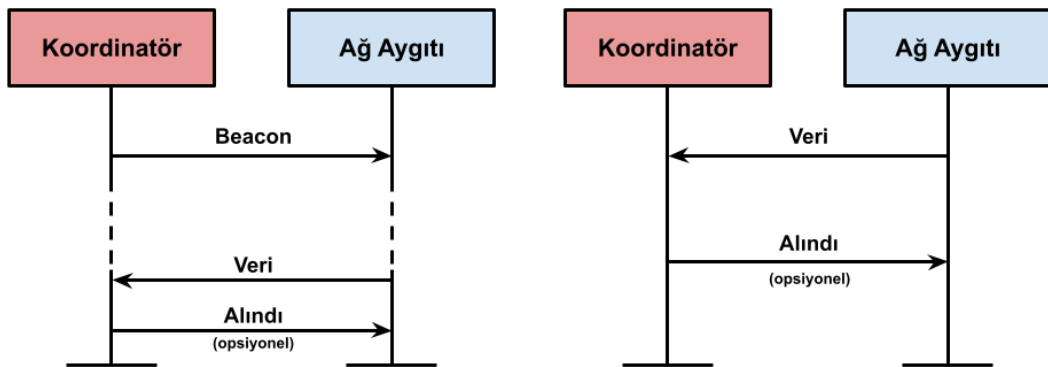
Şekil 3.3. MAC Alt Katmanı ve Fiziksel Katman

Ağ içerisinde birbirleri ile aynı kapsama alanı içerisinde bulunan cihazların sinyallerinin çarpışmasını engellemek ve sinyalin hedefe bozulmadan ulaşabilmesini sağlamak için, işaret sinyali temelli süper çerçeve yapısı ile bölümlendirilmiş CSMA/CA (Çarpışma önleme ile taşıyıcı algılama çoklu erişim, Carrier Sense Multiple Access with Collision Avoidance) kanal erişim mekanizması kullanılabileceği gibi senkronizasyona ihtiyaç duymayan bölümlendirilmemiş CSMA/CA kanal erişim mekanizması da tercih

kullanabilmektedirler. GTS bölgesi alım veya iletim yönlü olmak üzere koordinatör tarafından tahsis edilebilir.

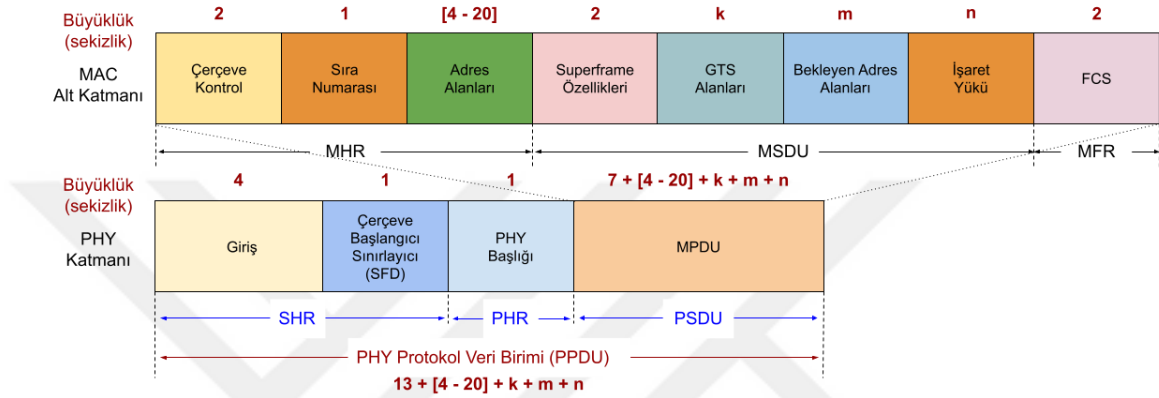
CSMA/CA kanal erişim mekanizması, aynı sinyal kanalının birden fazla cihaz tarafından kullanılması sonucu doğabilecek çarpışmaları engellemek için geliştirilmiştir. Bu mekanizmada paket göndermek isteyen aygıt, önceden belirlenmiş bir zaman dilimi için kanalı dinleyerek kanalın meşgul olup olmadığını tespit etmeye çalışır. Eğer devam eden bir iletişim var ise rastgele bir zaman dilimi süresince bekleyerek kanalın meşgul olup olmadığını yeniden test eder. Beklenen bu zaman dilimine geri çekilme faktörü adı verilmektedir. Bu süreç, kanal kullanılabilir hale gelene kadar tekrar eder. CAP olarak tanımlanmış olan zaman diliminde bölümlendirilmiş CSMA/CA kanal erişim yöntemi tercih edilmektedir. Bu yöntemde zaman dilimleri süper çerçeve ile senkronize edilir ve aygıt iletişimlerine paylaştırılır. Bu zaman dilimleri dışında iletişimin gerçekleşmemesi sağlanır. İşaret sinyalinin etkin olmadığı ağlarda ise süper çerçeve mekanizması yer almayacağından senkronizasyon kullanılamaz. Bu ağlar için bölümlendirilmemiş CSMA/CA kanal erişim yöntemi kullanılır. Bu erişim yönteminde aygıtlar kanalı boş olarak algılandığı herhangi bir anda veri iletimine geçerler.

Protokolde veri iletim modeli; Şekil 3.5 ile gösterildiği gibi aygıtlardan koordinatöre ve Şekil 3.6 ile gösterildiği gibi koordinatörden aygıtlara olmak üzere iki farklı şekilde gerçekleştirilebilmektedir. Tanımlamalarda kullanılan işaret sinyali (beacon) süper çerçeve ile birlikte ağ iletişimini senkronize etmek için kullanılmaktadır. Her iki tanımlamada da işaret sinyali ve süper çerçevenin kullanımı tercihe bırakılmıştır.



Şekil 3.5. Aygıttan koordinatöre veri iletim modelleri

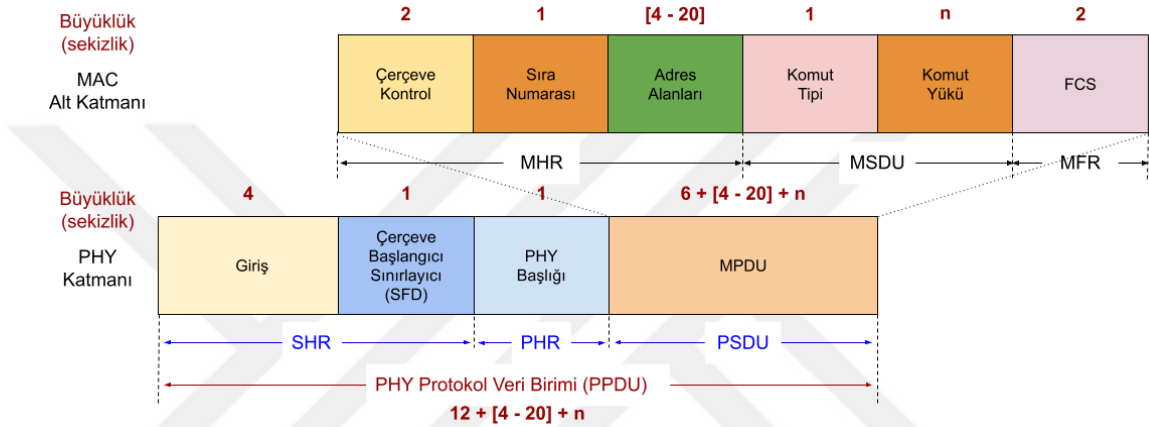
bölümlendirilmemiş CSMA/CA ile iletişim asenkron olarak gerçekleştirilir. Standart tarafından MAC katmanı için dört farklı çerçeve tanımı sunulmuştur; işaret çerçevesi, veri çerçevesi, bilgilendirme çerçevesi ve MAC komut çerçevesi. Şekil 3.7 ile verilen işaret çerçevesi, işaret sinyalinin aktif edildiği ağlarda koordinatörün süper çerçeve ile ilgili bilgileri aygıtlara ilettiği mesajdır. MAC Protokol Veri Birimi (MPDU); MHR, MSDU ve MFR bölümlerinden oluşmaktadır.



Şekil 3.7. İşaret Çerçevesi

MHR bölümünde; çerçeve kontrol bitleri ile çerçevenin bir İşaret Çerçevesi olduğu bilgisi, sıra numarası ile aygıt bazlı olarak tutulan artımsal çerçeve numarası ve adres alanı ile de hedef ve kaynak adres bilgileri alıcılara iletilir. MSDU bölümünde; süper çerçeveye ait çeşitli parametreler (CSMA/CA parametreleri vb. gibi), garantili zaman dilimleri alanı ile GTS kullanacak aygıtların iletişim yönü ve adres listesi, bekleyen adres listesi ile koordinatöre cevap vermesi istenen aygıtların listesi ve işaret yükü alanları ile üst katmana iletilmek istenen bilgiler alıcılara sunulur. MFR bölümü ise çerçeve bütünlüğünün alıcı tarafından doğrulanmasına olanak sağlamak için kullanılmaktadır.

içerisinde özelleştirilmiş bir MHR ve çerçevenin kontrol bitlerinin tutulduğu MFR bölümlerinden oluşmaktadır. MHR bölümü içerisinde çerçeve kontrol bitleri (2 byte) ve sıra numarası (1 byte) alanları yer almaktadır. Sıra numarası, veriyi ileten ve alındı mesajını bekleyen aygıtın çerçeve sıra numarasının geri dönüşü şeklinde gerçekleşir. Bu çerçeve yapısı herhangi bir adresleme bilgi alanına sahip değildir. İletilen paketin sıra numarası paketi ileten aygıta bilgilendirme mesajı olarak iletilirse paketin başarıyla iletildiği kabul edilir.

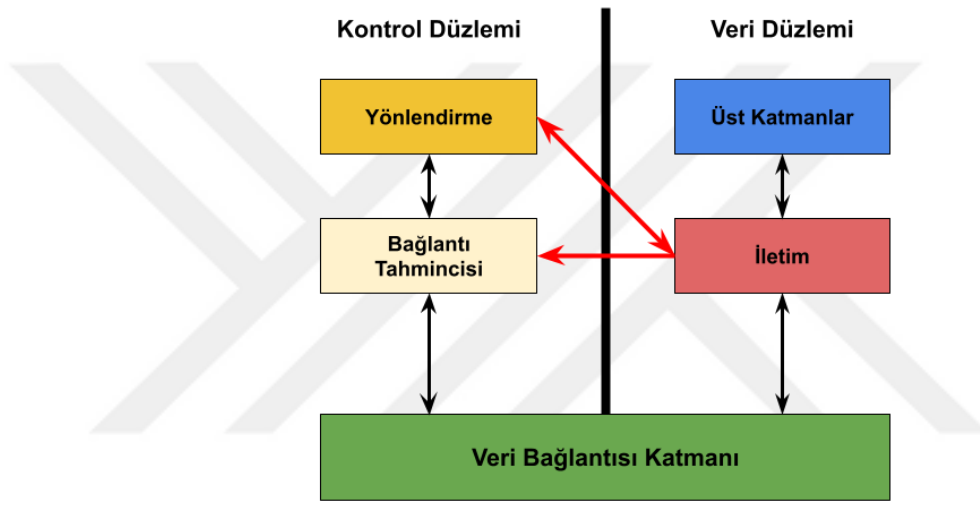


Şekil 3.10. MAC Komut Çerçevesi

Şekil 3.10 ile verilen MAC komut çerçevesi; bağlanma isteği/yanıtı, GTS isteği, veri talebi, alındı bilgisi talebi, ayrılma bildirimi gibi istek ve talepleri diğer ağ aygıtları ile paylaşmak için kullanılan mesaj türüdür. İşaret sinyalinin etkin olduğu ağlarda CAP bölgesinde, sinyalin etkin olmadığı ağlarda ise herhangi bir anda iletilebilmektedir. Çerçeve yapısı; MPDU içerisinde başlık alanları için MHR, komut bilgileri için MSDU ve çerçevenin kontrol bitlerinin tutulduğu MFR bölümlerinden oluşmaktadır. MHR ve MFR alanları işaret çerçevesi ile aynı özelliklere sahiptir. MSDU bölümü ise mesaj türü sebebi ile özelleşmiş bir yapıdadır. Komut türü alanı (1 byte) ile çerçevenin komut bilgisi hedef aygıtlara iletilebilir. Komut türüne bağlı olarak taşınacak veriler için komut yükü alanı çerçeveye eklenebilmektedir.

kök olarak kabul ederek veriyi bu düğüme iletir. Düğümlerin seçmiş oldukları dolaylı kökler gerçek kök düğüme doğru bir rota oluşmasını sağlar (Fonseca ve ark., 2006).

CTP, Şekil 3.12 ile verilen görselde olduğu gibi kontrol ve veri olmak üzere iki ayrı düzlem ile temsil edilmektedir. Veri düzleminde, gelen paketlerin iletim ve gönderim süreçleri yürütülürken kontrol düzleminde ise bağlantı kalitesinin tespiti ve uygun rota/ebeveyn seçim süreçleri gerçekleştirilmektedir. Veri ve alındı bilgisine ilişkin paketler iletim birimi tarafından, bilgilendirme çerçeveleri (beacon frame) ise bağlantı tahmincisi ve yönlendirme birimi tarafından işlenir (alma/gönderme).



Şekil 3.12. CTP kontrol ve veri düzlemleri

Düğümlerin en uygun komşuyu dolaylı kök olarak seçebilmesi için bağlantı tahmincisi tarafından hesaplanan düğümler arası bağlantı kalitesi değeri kullanılır. Hesaplama, kökten uç düğüme doğru kademeli olarak gerçekleşir. Bu hesaplamanın yapılabilmesi için ağda en az bir gerçek kök bulunmalıdır. Gerçek kök düğümünün başlangıç maliyeti sıfır olarak kabul edilir. Gerçek kök ile düğümler arasındaki bağlantı kalitesi hesaplanarak düğümün rota maliyet değerine ulaşılır. Kapsama alanı içerisindeki iki düğüm arasında beklenen iletim sayısı (Expected Transmission Count, ETX) adı verilen metrik, iletişimin kalitesini temsil etmektedir.

Beklenen iletim sayısı (ETX) (De Couto ve ark., 2003), yeniden iletimler dahil olmak üzere paket göndermek için gereken tahmini veri iletimi sayısı olarak tanımlanmıştır. ETX hesaplaması, veri paketinin alıcıya başarıyla ulaştığını ölçen olasılık

- Fiziksel katman tarafından alınan verilerdeki hata miktarı, kanal kalitesinin belirlenmesinde kullanılmaktadır. Fiziksel katmanda yapılacak ölçümler basit, ucuz ve hızlıdır. Bu nedenle de kanal kalitesinin yüksek olup olmadığını gösteren “beyaz bit” (white bit) tanımlanmıştır. Bilgi, alt katmandan alınarak kontrol düzleminde yer alan bağlantı tahmincisi tarafından doğrudan işlenir.
- Bağlantı katmanı, gönderilen bir paketin iletilip iletilmediğinin takibinin yapılabilmesini sağlar. Paketi gönderen düğüme alındı bilgisinin iletilmesi ile iletişimin başarılı bir şekilde gerçekleştirildiği bildirilebilir. Bu bilgi bir bitlik “alındı biti” (ack bit) ile temsil edilmektedir. Veri düzleminde yer alan iletim birimi tarafından gerçekleştirilecek bir çağrı ile bilgi, kontrol düzlemindeki bağlantı tahmincisine iletilir.
- Ağ katmanı, rotalar arasında en yüksek performansa sahip olanın tespit edilmesi sağlamak için tahminci tarafından kullanılabilir. Tahminci, aldığı kontrol çerçevelerindeki bilgileri kendi listesi ile kıyaslar. Alınan kontrol çerçevesi üzerindeki sıra numaraları önceki değerlerle uyuşmuyor ise alınamayan kontrol paketi olduğu anlamına gelir. Bu durum bağlantı kalitesinin kötü olduğuna işaretler. Eğer komşu düğüme ilişkin bilgiler mevcut değil ise bu bilgilerin listeye işlenmesi ile ilgili süreçler yürütülür. Listenin doluluk durumuna göre yeni düğüm bilgileri sırasıyla önce listedeki boş bir alana, eğer liste dolu ise metrik değeri eşik değerin üzerinde olan en verimsiz düğümün yerine listeye eklenir. Liste dolu olduğu halde eşik değerin üzerinde bir metrik değerine sahip düğüm bulunamıyorsa eklenmek istenen düğüme ilişkin metrik analizi gerçekleştirilir. Yapılan analizde bu düğümün kanal kalitesi bilgisini gösteren “beyaz bit” işaretli ise ve düğümün rota metrik değeri ebeveyn düğümden yüksek ise “karşılaştırma biti” aktif edilir. Karşılaştırma bitinin seçili olması ile birlikte listeden rastgele bir düğüm seçilir ve yeni düğümün bilgileri bu düğüme ilişkin kayda üzerine yazılır. Listedeki en iyi rota metriğine sahip düğümün işaretlenmesi “sabit biti” ile gerçekleştirilir. Bu işaretlemenin sağlanması ile hem düğümün listeden çıkarılmasının önüne geçilir hem de tahminci tarafından ebeveyn düğümün kimlik bilgisini elde etmek kolaylaşır (Fonseca ve ark., 2007). Bu süreçler protokolün kontrol düzleminde, yönlendirme birimi ve bağlantı tahmincisi tarafından yürütülür.

- “ETX” ismiyle temsil edilen 16 bitlik son bölümde ise veriyi gönderen düğümün rota maliyet bilgisini sunulmaktadır.

Şekil 3.15’te görüldüğü gibi veri çerçevesi, düğümlerin birbirilerine veri göndermede kullandıkları çerçeve türüdür. Şablon çerçeve; başlık ve veri bölümlerinden oluşmaktadır. Başlık bölümünde yönlendirme çerçevesinde olduğu gibi “P”, “C”, “Rezerve Alan” ve “ETX” alanları benzer amaçlar için bulunmaktadır. Çerçevenin son bölümünde ise iletilmek istenen veri yer alır. Yönlendirme çerçevesinden farklı olarak veri çerçevesi belirli bir düğüme yönelik olarak gönderilir ve sadece bu düğüm tarafından (unicast) dikkate alınır.

|         |   |              |   |   |   |   |   |             |   |   |   |   |   |   |   |
|---------|---|--------------|---|---|---|---|---|-------------|---|---|---|---|---|---|---|
| 0       | 1 | 2            | 3 | 4 | 5 | 6 | 7 | 8           | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| P       | C | Rezerve Alan |   |   |   |   |   | THL         |   |   |   |   |   |   |   |
| ETX     |   |              |   |   |   |   |   |             |   |   |   |   |   |   |   |
| Kaynak  |   |              |   |   |   |   |   |             |   |   |   |   |   |   |   |
| Sıra No |   |              |   |   |   |   |   | Protokol ID |   |   |   |   |   |   |   |
| [Veri]  |   |              |   |   |   |   |   |             |   |   |   |   |   |   |   |

Şekil 3.15. CTP veri çerçevesi şablonu

Çerçeve içerisinde yer alan alanlar;

- “P”, “C”, “Rezerve Alan” ve “ETX” bölümleri yönlendirme çerçevesindeki amaçlar için yerleştirilmiştir. Fakat yönlendirme çerçevesinden farklı olarak sadece çerçeveyi alacak olan düğüm tarafından dikkate alınır.
- “THL” (Time Has Lived), 8 bitlik bir alan olup bir çerçevenin ne kadar kez iletildiği bilgisini tutmak için kullanılmaktadır. Çerçeveyi ilk kez oluşturan düğüm (genellikle uç düğüm) bu değeri sıfır olarak belirler. Çerçeveyi alarak bir başka düğüme iletmek isteyen yönlendirici düğümler bu değeri bir arttırır.
- “Kaynak”, 16 bitlik bir adres alanını tanımlar. Bu adres veri paketini kimin oluşturduğu bilgisini tutmaktadır. Diğer yönlendirici düğümler tarafından bu veri alanı güncellenmez.
- “Sıra No”, 8 bitlik bir alan olup bu alan paketi oluşturan düğümün veri paketine atamış olduğu sıra numarasıdır. Bu bilgi, diğer yönlendirici düğümler tarafından güncellenmez. Kaynak adresi ile sıra numarası birlikte ele alındığında paketin

Uyarlanabilir zamanlayıcı tarafından kullanılan zaman bilgisi dört durumda sıfırlanır:

- Alınan çerçevelerdeki P bitinin aktif olduğu durumda. Bu durum bir yönlendirme veya veri çerçevesi ile gerçekleşebilir.
- Yönlendirme tablosunun boş olduğu durumda. Düğüm iletişim kurabileceği diğer aygıtlardan bilgi talebinde bulunmak için P biti aktif edilmiş yönlendirme paketleri de gönderir.
- ETX ve ebeveyn değişiminin gerçekleştiği durumda metrik bilgilerini diğer düğümlere duyurmak için zamanlayıcı sıfırlanır ve yönlendirme paket gönderimi sağlanır.
- Ebeveyn düğüm tarafından alınan bir veri paketinin içerisinde yer alan maliyet bilgisinin kendi maliyetinden daha düşük olması durumu rotada bir tutarsızlık olduğunu belirtir. Bu durumda komşuların güncellenmesi için yönlendirme paket iletimi gerçekleştirilir.

Protokol, düğümler arası veri iletimini sağlamak için uç düğümden kök düğüme doğru en düşük maliyetli rotayı tercih edecek şekilde ebeveyn seçimi gerçekleştirmektedir. Paket gönderimi Şekil 3.15 ile gösterilen veri çerçevesi şablonu ile belirli bir hedefe yönelik olarak gerçekleştirilir. Veri paketi yönlendirme ve iletim süreçleri veri düzlemi ve bu düzlemde yer alan iletilen birim tarafından gerçekleştirilir. Paketi alan ebeveyn, paketi gönderen düğüme alındı mesajı göndererek paketi aldığını bildirir. Bu bilgi, iletişim kalitesinin belirlenmesi kullanılır. Ebeveyn düğüm tarafından alınan paket, bir üst düğüme iletmek üzere gönderim kuyruğuna eklenir. Alındı mesajını belirli bir süre (bir milisaniye) içerisinde iletmeyen ebeveyn düğüm için aynı paketin gönderimi varsayılan olarak otuz kez tekrarlanabilir. Yapılacak gönderim sonucunda paket başarılı bir şekilde ebeveyn düğüme iletilemez ise o paket kuyruktan çıkarılır ve yeniden gönderilmez.

Protokolde, veri paketleri için alındı mesajının paketi alan ebeveyn düğüm tarafından önceki düğüme iletilmesi şarttır. İletişim kalitesinin düşük olduğu ağlarda alındı mesajları doğru bir şekilde düğümler tarafından elde edilemeyebilir. Bu durumda paket mükerrer olarak yeniden iletebilir. Aynı paketin yeniden gönderilmek üzere ebeveyn düğüme iletilmesi ağda mükerrer paket trafiği yarabilir. Bu nedenle her bir düğüm aldığı paketleri daha önce alıp almadığını kontrol eder. Bu paketler için alındı bildirimi gönderilir fakat gönderim kuyruğuna eklenmez. Ayrıca bu durum iletişim

### 3.1.3. Test Ortamı

KAA'ların akademik ve ticari amaçlı kullanımlarını sağlamak için donanım ve yazılım geliştirme ortamlarına ihtiyaç vardır. Günümüzde az sayıda üretici, bu ihtiyaca cevap verebilecek türde tümleşik donanımları pazara sürmüştür. Çalışmanın bu bölümünde kullanılan tümleşik donanım ve geliştirme ortamı hakkında bilgiler sunulmuştur.

#### 3.1.3.1 Donanımsal Bileşenler

Yapılan gerçek zamanlı uygulamalarda, MEMSIC firmasına ait IRIS isimli KAA bileşenleri kullanılmıştır. Bu bileşenler üç tanedir.

- **IRIS Ana Birimi**

Bu birim, algılayıcı düğümün ana bileşenlerinin üzerinde yer aldığı devredir. Birime ilişkin görsel Şekil 3.17'te verilmiştir. Birim üzerinde Atmel ATmega 1281 serisi 8 bit mimariye sahip tümleşik devre olan mikrodenetleyici yer almaktadır. Devre kartı üzerinde ayrıca iletişim birimi de bulunmaktadır. Bu iletişim birimi, 2.4 GHz IEEE 802.15.4 kablosuz iletişim standardını destekleyen Atmel AT86RF230 serisi bir tümleşik devreden oluşur.



Şekil 3.17. IRIS Ana Birimi

Çizelge 3.2. Memsic IRIS düğümlerin teknik özellikleri

|                            |          |  |
|----------------------------|----------|--|
| <b>İşlemci/Radyo Kartı</b> | XM2110CA |  |
|----------------------------|----------|--|

**Denetleyici**

|                              |                     |                       |
|------------------------------|---------------------|-----------------------|
| <b>Seri</b>                  | Atmel ATmega 1281   |                       |
| <b>Tür</b>                   | 7.37 MHz, 8 bit     |                       |
| <b>Program Flash Belleği</b> | 128K bayt           |                       |
| <b>Seri Flash</b>            | 512K bayt           | 100.000 Ölçüm         |
| <b>RAM</b>                   | 8K bayt             |                       |
| <b>Konfigürasyon EEPROM</b>  | 4K bayt             |                       |
| <b>Seri İletişim</b>         | UART                | 0-3V iletim seviyesi  |
| <b>ADC</b>                   | 10 bit ADC          | 8 kanal, 0-3V giriş   |
| <b>Diğer Arayüzler</b>       | Digital I/O,I2C,SPI |                       |
| <b>Çekilen Akım</b>          | 8 mA / 8 µA         | Aktif mod / uyku modu |

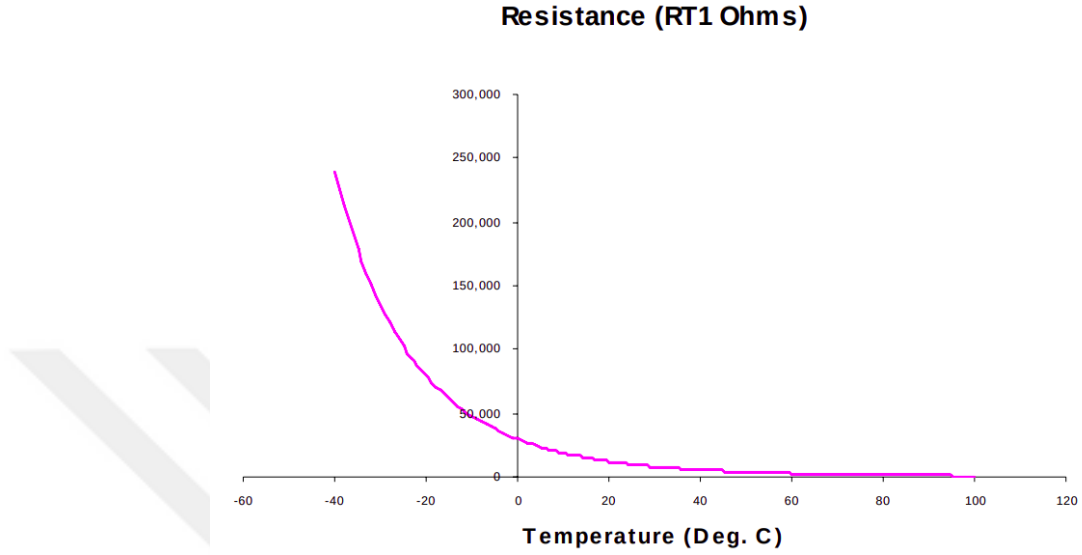
**RF Alıcı-Verici**

|                                |                                  |                                                      |
|--------------------------------|----------------------------------|------------------------------------------------------|
| <b>Seri</b>                    | Atmel AT86RF230                  | RF230                                                |
| <b>Frekans Bandı</b>           | 2405 MHz - 2480 MHz              | ISM bandı                                            |
| <b>Veri İletim Oranı</b>       | 250 kbps                         |                                                      |
| <b>RF Gücü</b>                 | 3 dBm (typ)                      |                                                      |
| <b>Alıcı Hassasiyeti</b>       | -101 dBm (typ)                   |                                                      |
| <b>Komşu Kanal Reddi</b>       | 36 dB<br>34 dB                   | + 5 MHz kanal aralığı<br>- 5 MHz kanal aralığı       |
| <b>Dış Mekan Kapsama Alanı</b> | >300 metre                       | ¼ dalga dipole anten, LOS                            |
| <b>İç Mekan Kapsama Alanı</b>  | >50 metre                        | ¼ dalga dipole anten, LOS                            |
| <b>Çekilen Akım</b>            | 16 mA<br>10 mA<br>13 mA<br>17 mA | Alıcı Modu<br>TX, -17 dBm<br>TX, -3 dBm<br>TX, 3 dBm |

**Elektromekanik**

|                           |               |                        |
|---------------------------|---------------|------------------------|
| <b>Batarya</b>            | 2 x AA pil    |                        |
| <b>Harici Güç</b>         | 2.7 V - 3.3 V |                        |
| <b>Kullanıcı Ara yüzü</b> | 3 LED         | Kırmızı, Yeşil ve Sarı |
| <b>Boyut (mm)</b>         | 58 x 32 x 7   |                        |
| <b>Ağırlık (gram)</b>     | 18            | Batarya hariç          |

direncinin azalmasının lineer olmayan bir eğri ile sıfır değerine yaklaştığı görülebilmektedir. Katalog değerleri dikkate alındığında değişimin -55 °C için 600kΩ ile 150 °C için 230Ω aralığında olduğu bildirilmiştir.



Şekil 3.21. Termistörün sıcaklık-direnç değişimi grafiği

10 bitlik A/D dönüştürücünün analog olarak almış olduğu gerilim değerini dijital bir sayı değerine dönüştürmesi sonucunda 0 ile 1023 aralığında ( $2^{10}$ ) bir değer elde edilir. Bu değer (ADC) ile (3.4), (3.5), (3.6) ve (3.7) bağıntı ve sabitleri kullanılarak sıcaklık değeri °C cinsinden hesaplanabilir (Crossbow, 2007).

$$\frac{1}{T(K)} = a + b * \ln(R_{thr}) + c * [\ln(R_{thr})]^3 \quad (3.4)$$

$$R_{thr} = \frac{R1 * (ADCFS - ADC)}{ADC} \quad (3.5)$$

$$R1 = 10k\Omega = 10000$$

$$ADCFS = 1023$$

$$a = 0.001010024 \quad (3.6)$$

$$b = 0.000242127$$

$$c = 0.000000146$$

$$T(C) = T(K) - 273.15 \quad (3.7)$$

Şekil 3.23 ile verilen ağ geçidi ana birimin güç gereksinimini karşılayabilecek şekilde üretilmiştir. Birim üzerinde bulunan ATMegal6L serisi denetleyici, ana birimin programlanma süreçlerini de yürütmektedir. USB seri portu üzerinden hem programlama hem de farklı platformlara veri aktarımı sağlanabilmektedir. Ayrıca birim üzerinde yer alan sıfırlama butonu (SW1) ile ana birimin yeniden başlatılması, JTAG konektörü ile devre içi hata ayıklama işlemleri gerçekleştirilebilmektedir.

### 3.1.3.2 İşletim Sistemi Çatısı

Birçok elektronik devrenin bir araya gelerek meydana getirdiği tümleşik bir devrenin programlanabilir olabilmesi ve çalışabilmesi için; sistemi yöneten bir merkezi işlem birimine, işlem ve süreçlerin donanımsal olarak yönetilmesini sağlayan komut seti mimarisine, yapılacak iş ve işlem sonuçlarının kalıcı ve geçici olarak depolanmasına imkân veren depolama birimlerine, dış dünya ile iletişim kurabilmek için I/O portlarına ve tüm bu süreçleri senkronize etmek için ortak bir tetikleme sinyaline ihtiyaç vardır. Komut seti mimarisi ile programlama süreçlerinin zorluğu, daha üst seviye dillerin doğmasına ve özelleşmesine neden olmuştur. Donanım kaynaklarının yönetiminin başlı başına daha karmaşık süreçler gerektirmesi, yazılım ve donanım arasında işletim sistemi adı verilen sistem yazılımlarının geliştirilmesini sağlamıştır. İşletim sistemi olarak anılan bu sistem yazılımının sağlamış olduğu servis ve bileşenler, üst seviye uygulamaların daha hızlı geliştirilmesine olanak sağlar. Algılayıcı ağlara ilişkin uygulamalarda kullanılmak üzere farklı donanımlara sahip gömülü sistemler için birçok işletim sistemi geliştirilmiştir. Örneğin; LiteOS, RT-Thread, Contiki OS, mbed OS, FreeRTOS, ThreadX, uC/OS, TinyOS, RIOT OS vb. işletim sistemleri tercih edilen sistemler arasındadır.

Algılayıcı ağlarda kullanılacak işletim sistemlerinde olması gereken temel gereksinimler;

- Sınırlı kaynağın verimli kullanımı
- Eşzamanlılık ile aynı anda farklı görevleri yerine getirebilme
- Esneklik ile yapının ölçeklenebilir olması
- Enerjinin verimli kullanımı

olarak ortaya konmuştur (Levis ve ark., 2005).

ve görevler oluşturabilir. Bileşen içerisinde yer alan görev mekanizması planlayıcı ile birlikte çalışan ve zamanlayıcı değeri küçük olan bir FIFO kuyruğundan oluşur. Kuyruk içeriğinin boş olması durumunda çevre birimler aktif kalmaya devam ederken işlemci uyku seviyesine geçebilmekte ve sistemin enerji verimliliğini artırılabilir. Görev mekanizması da düşük seviyeli komut mekanizmalarını tetikleyebilmektedir.

#### 3.1.4. KAA’larda Saldırı Türleri

KAA için iki saldırı kategorisinden bahsedilebilir. Bunlar pasif ve aktif saldırılardır (Butun ve ark., 2020). Saldırgan ağı dâhil olabilmek için ağ anahtarına ihtiyaç duyar. Ağ anahtarına sahip olmayan yetkisiz bir saldırgan verileri değiştirmeden iletişim kanallarını dinleyerek pasif saldırı gerçekleştirebilir. Böyle bir saldırganı tespit edebilmek zordur. Saldırgan daha çok ağı dinleyip kritik verileri elde etmeye çalışır. Bu kategoride yer alan saldırılar (Butun ve ark., 2020, Keerthika ve Shanmugapriya, 2021);

- **İzleme ve dinleme:** Bu saldırı ağın bütünlüğüne zarar vermez. Saldırgan iletişim kanalının gizliliğini ihlal eden davranışlar sergiler.
- **Trafik analizi:** Saldırgan ağın trafik düzenini takip ederek topoloji ve iletişim yapısı hakkında bilgi toplamaya çalışır. Toplanan bu bilgi, aktif saldırı için bir saldırı vektörü olarak kullanılabilmesine olanak sağlar.
- **Düğümün imhası:** Fiziksel olarak düğümün kullanılamaz hale getirilmesini amaçlar. Bu işlem; mühimmat, elektrik dalgalanması gibi yollarla gerçekleştirilebilir. Düğüm yeniden kullanılamaz.
- **Düşmanları kamuflej:** Saldırganlar normal düğümleri taklit ederek paketlerin farklı iletişim kanallarına yanlış yönlendirilmesine yol açar.

Aktif saldırılar ise; veri gizliliğinin yanı sıra veri bütünlüğünü de tehdit eden kötü niyetli eylemleri kapsamaktadır. Saldırgan, kaynakların yetkisiz kullanımını veya bir düğümün/ağın iletişiminin bozulmasını hedefleyebilir (Butun ve ark., 2020).

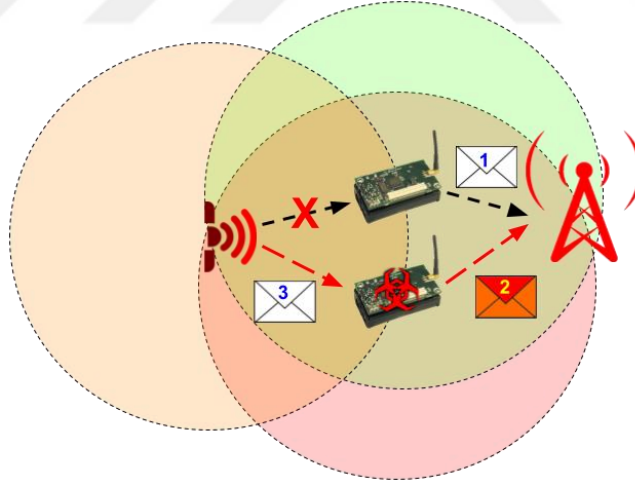
- **Fiziksel katman saldırıları:** Saldırganın aynı frekansta sinyal göndererek kanalı meşgul etmesine neden olan sıkışma (Jamming, DoS) saldırısı ve saldırganın

saldırısı gerçekleştirerek rota boyunca uçtan uca tüm düğümlerde aşırı trafiğe neden olarak kaynakları tüketmeyi hedefler.

KAA'lar için saldırı tespit sistemlerini tasarlayabilmek ve başarıları ölçümleyebilmek için ağda çalışan kötü niyetli düğümlere ihtiyaç vardır. Bu nedenle yapılan çalışmalarda kullanılan saldırı modelleri bu bölümde detaylandırılacaktır.

#### 3.1.4.1 Çıkış Deliği Saldırısı

Çıkış deliği (sinkhole) saldırısında kötü niyetli düğüm, sahte kontrol paketlerini sıradan komşu düğümlerine ileterek kendisinin en iyi rota seçimi olacağı (düşük gecikme, düşük rota maliyeti, yüksek bant genişliği vb.) konusunda aldatmaya çalışır. Böylece yönlendirme paket trafiğini kendi üzerinden geçirerek paketlerin izlenmesine, değiştirilmesine ve iletimine yetki kazanmış olur (Ngai ve ark., 2006). Birçok saldırının gerçekleştirilmesinde çıkış deliği saldırısı kritik bir öneme sahiptir. Paket trafiğinin kötü niyetli düğüm tarafından yönlendirilmesi ile birlikte paket kaybı, içerik değişikliği vb. gibi birçok saldırı kötü niyetli düğüm tarafından uygulanabilir hale gelir.



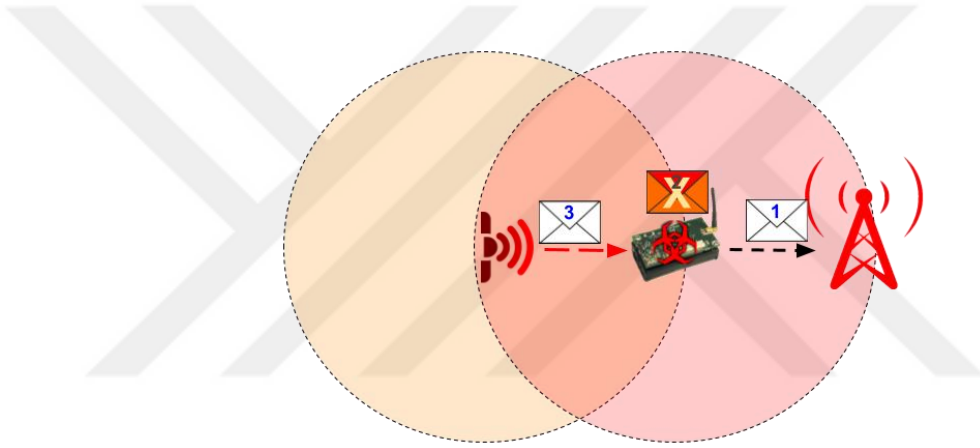
Şekil 3.25. Çıkış deliği saldırısı

Şekil 3.25 ile verilen görselde; algılayıcı düğüm, baz istasyonu ve biri kötü niyetli olmak üzere iki adet yönlendirici düğüm ve bu düğümlere ait kapsama alanları verilmiştir. Baz istasyonu, algılayıcı düğümün kapsama alanı içerisinde yer almamaktadır. Bu nedenle de paket gönderiminin gerçekleşebilmesi için yönlendirici düğümlerin paket

iletilmez ve paket kaybı meydana gelir. Saldırganın tespiti için ağ trafiğinin gözlemlenmesi gerekir. Düğümlerce alınan ve iletilen paket sayıları dikkate alınarak saldırı tespiti yapılabilir.

#### 3.1.4.3 Seçici Yönlendirme Saldırısı

Seçici yönlendirme (selective forwarding, grayhole) saldırıları, karadelik saldırılarına benzese de saldırıgan tüm paket trafiğini bloke etmek yerine sadece kendisine iletilen belirli özellikte paketlerin iletimini bloke eder. Böylece kritik veri taşıyan paketlerde veri kaybına neden olur (Karlof ve Wagner, 2003).



Şekil 3.27. Seçici yönlendirme saldırısı

Şekil 3.27 ile verilen görselde algılayıcı düğümün göndermiş olduğu bir dizi paket kötü niyetli düğüme ulaşmıştır. Seçici yönlendirme saldırı düzenleyen kötü niyetli düğüm paket içeriğini analiz ederek bu paketlerden bazılarını baz istasyonuna iletmeyerek bloke etmiş ve veri kaybına yol açmıştır. Karadelik saldırısında olduğu gibi saldırı tespiti için ağdaki paket trafiğinin izlenmesi gerekir. Düğümün aldığı ve ilettiği paket sayılar dikkate alınarak düğümün davranışı ile ilgili karara varılabilir.

#### 3.1.4.4 Veri Değiştirme Saldırısı

Veri değiştirme (data alteration) saldırıları, kötü niyetli düğüm tarafından iletilecek olan paket içeriğinin değiştirilmesi esasına dayanmaktadır. Paket içeriğinin

- **Davetsiz misafirin türü:** Ağa erişim şekline göre saldırganlar iki farklı şekilde sınıflandırılabilir. Saldırgan; ağa ulaşmak için farklı araçlar kullanıyorsa harici (external intruder), daha önce ağın üyesi olan ve güvenliği ihlal edilmiş bir düğüm üzerinden saldırılar gerçekleştiriliyorsa dâhili davetsiz erişim (internal intruder) olarak sınıflandırılır.
- **Saldırı türü:** Saldırganın ağa yetkisiz girişimi (attempted break-in), sahte kimlik kullanımı (masquerade), ağdan istenmeyen bilgi sızıntısı (leakage), yetkisiz erişimin elde edilmesi (penetration), ağ kaynaklarının bloke edilmesi (DoS), ağ kaynaklarına zarar verme (malicious use)
- **Algılama yaklaşımları:** İstatistik verilerine dayalı anomali tabanlı (anomaly based), yanlış kullanıma/suistimale dayalı (misuse based), davranış tabanlı teknik özelliklere dayalı (specification based)
- **Denetim verisinin kaynağı:** Ağ tabanlı (network-based) sistemlerde ağdaki paket aktarımlarının dinlenmesi ve incelenmesi ile, düğüm tabanlı (host-based) sistemlerde düğümün sistem ve hizmet etkinlik ve günlüklerinin takibi ile melez (hybrid) sistemlerde ise araçların hem ağ hem de düğüm verilerinin birlikte kullanılması şeklinde elde edilir.
- **Değerlendirme mekanizmasının konumu:** Merkezi (centralized) sistemlerde önceden belirlenmiş merkezi bir cihaz ile tüm ağ verisi üzerinden, Bağımsız (stand-alone) sistemlerde her düğüm bağımsız olarak topladığı bilgiler üzerinden, Dağıtık ve işbirlikçi (distributed and cooperative) sistemlerde her düğüm elde ettiği bilgileri diğer düğümlerle paylaşarak veya paylaşılan bilgi ve yanıt üzerinden, Hiyerarşik (hierarchical) sistemlerde küme başkanları tarafından küme içerisindeki üye düğüm verileri üzerinden, Mobil Aracı tabanlı (mobile Agent based) sistemlerde ise görevi üstlenen aracı düğümler elde ettikleri veriler üzerinden karar alırlar.
- **Altyapı:** İki farklı yapı tercih edilebilmektedir: düğümün ağ içerisindeki görev ve yeteneklerinin eşit olduğu düz (flat) yapı ile düğümlerin bir kümede gruplandığı ve kümede merkezi cihazın bulunduğu kümelenmiş (clustered) yapı.
- **Kullanım sıklığı:** Saldırı tespit sistemi, sürekli/anlık (continuous) ve periyodik (periodical) olarak belirli zaman dilimlerinde olmak üzere ağı iki farklı şekilde izleyebilir.

paketleri almaktadır. Fakat paket gönderimi belirli bir hedefe yönelik (unicast) olarak gerçekleştirildiğinden B ve C düğümleri bu paketleri filtreleyerek işlemez. A düğümünün baz istasyonuna yönelik yapmış olduğu paket gönderimleri, algılayıcı düğüm tarafından da alınır fakat aynı gerekçe ile işlenmez. Komşu düğümün izlenmesine dayalı saldırı tespiti, aynı kapsama alanı içerisindeki paket trafiğinin izlenmesine ve paketlerin analizine dayanmaktadır. Ayrıca düğümler tarafından alınan her paket belirli bir sinyal gücü yoğunluğuna sahiptir. Buna, alınan sinyal gücü (Received Signal Strength Indicator, RSSI) adı verilmektedir. Bu güç değeri; kapsama alanı içerisinde düğüme uzaklık, ortam koşulları gibi faktörlere bağlı olarak değişiklik gösterebilir.

Çalışmada, CTP mimarisi üzerinde çalışabilen komşu izleme tabanlı saldırı tespit ve yanıt sistemi tasarımı gerçekleştirilmiştir. CTP, ağdaki topolojik değişimleri dikkate alarak az sayıda kontrol paketi trafiği ile düğümlerin uykuda kalma sürelerini uzatarak ağ ömrünün artmasını ve ağ trafiğini azalmasını hedeflemektedir. Protokol yapısı gereği saldırılara karşı bir koruma sağlamayı hedeflemez. Bu nedenle protokol için saldırı tespit ve yanıt sistemlerinin tasarımı önemli bir odak noktasıdır. Tasarlanan sistem ile saldırıların etkilerini azaltmak amaçlanmıştır. Düğümler elde ettikleri veriler doğrultusunda kendi karar mekanizmalarını işletirler. Tasarlanan sisteme ilişkin blok diyagram Şekil 3.29 ile verilmiştir. Yapılan tasarım dört bileşenden oluşmaktadır. Bu bileşenler; ana birim, ağ izleme birimleri, işbirliği/kalıtım birimi ve akış onarım birimi başlıkları altında toplanabilir.

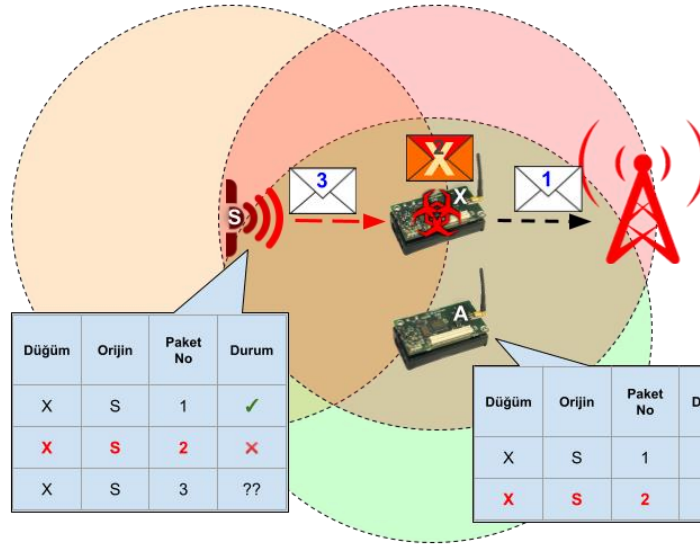
### 3.2.1.1 RENMIDER Ana Birimi

RENMIDER (Neighbor Monitoring-Based Intrusion Detection and Response in Real-Time WSNs, Gerçek Zamanlı Kablosuz Algılayıcı Ağlarda Komşu İzleme Tabanlı Saldırı Tespiti ve Yanıtı) ana birimi; komşu düğüm istatistiklerin tutulduğu, düğümlere ilişkin ceza değerlerinin tespit edilip atandığı, saldırı sebepli rota değişimi vb. gibi kararların verildiği (yanıt sistemi) ve diğer bileşenlerin koordinasyonunun sağlandığı birimdir. Ana birim bünyesinde *LIST* isimli bir alt bileşen bulundurmaktadır. Bu bileşen diğer birimlerin çalışabilmesi için ortak listeleri (paket listesi, düğüm istatistikleri ve yerel rota maliyet listesi) barındırmaktadır.

*LIST* alt bileşeni tarafından sağlanan listeler;

- **Paket listesi:** Düğümlerin paket trafiği özetlerini tutar. Böylece bir düğümün göndermesi gereken paketlerin gönderilip gönderilmediği tespit edilebilir. Ayrıca bu listede yer alan paket özet bilgisi ile veri üzerinde yapılacak kötü niyetli değişiklikler (data alteration) tespit edilebilecektir.
  - Paketi iletecek düğüm adresi
  - Paketin oluşturan düğüm adresi
  - Paket numarası (Oluşturan düğüm tarafından atanan)
  - Düğümün rota maliyeti (gerçek)
  - Sayaç
  - Paket özeti (CRC16)
- **Düğüm istatistikleri:** Komşu düğümlerin paket trafiğine katkılarının istatistiksel olarak tutulduğu listedir. Listede komşu düğümün;
  - Adresi
  - Ebeveyn adresi
  - Aldığı paket sayısı
  - İlettiği paket sayısı
  - İlettiği takip dışı paket sayısı
  - İlettiği ACK sayısı
  - Tetiklediği düşük seviyeli anomali sayısı
  - Tetiklediği yüksek seviyeli anomali sayısı
- **Yerel rota maliyetleri:** Komşu düğümler için düğüm tarafından belirlenen ceza değerleri bu listede tutulmaktadır. Listede komşu düğümün;
  - Adresi
  - Ceza katsayısı ( $PCX_{ij}$ )
  - Yerel rota maliyeti

Ana birim, CTP ile tümleşik olarak çalışır. Protokol, baz istasyonundan uç düğüme kadar bağlantı maliyetlerinin hesaplanması süreçlerini ve en uygun rota seçimini gerçekleştirirken, ana birim ise protokolün bu birime sağlamış olduğu verilerin işlenmesi sonucunda yeni komşuların listelere eklenmesi, mevcut komşuların seviye ve maliyet bilgilerinin güncellenmesi gibi süreçleri yürütür. Farklı yollarla elde edilen paket trafiği istatistikleri, diğer birimlere iletilerek gerekli değerlendirme süreçleri yürütülür. Tespit



Şekil 3.30. Komşu izleme tabanlı paket takibi

Şekil 3.30 ile verilen örnekte algılayıcı düğümden (S) kötü niyetli düğüme (X) doğru gerçekleşen bir paket trafiği verilmiştir. Algılayıcı düğüm ve kötü niyetli düğüm, A düğümünün kapsama alanı içerisinde. Kötü niyetli düğümün, 1 numaralı paketi baz istasyonuna ilettiğini ama 2 numaralı paketi ise iletmediğini varsayalım. A ve S düğümleri, komşulara ilişkin paket trafiğini takip edecek şekilde geliştirilmiştir. Bu nedenle S düğümünden X düğüme iletilen bir paket baz istasyonuna iletildiğinde S ve A düğümleri bu iletişimden haberdar olurlar (kapsama alanı sebebiyle). Kötü niyetli X düğümü 1 numaralı paketi aldığı anda S ve A düğümleri paket ile ilgili bilgileri kendi tablolarına işler (düğüm tarafından alınan paket sayısı istatistiği de artırılır) ve bu paketin iletilmesini beklemeye başlar. X tarafından paket iletimi gerçekleşirse düğümler gönderilen paketi kendi tablo verileri ile karşılaştırıp onay sürecini tamamlar. Böylece gönderilen paket sayısı da artırılmış olur. Paketin birden fazla kez alınmış veya gönderilmiş olması istatistiklerde mükerrer kayıtların oluşmasının da önüne geçer. Paketleri izleme amaçlı olarak kullanılan Paket Listesi (LIST alt bileşeni içerisinde yer almaktadır) 10 adet paketi tutabilecek uzunluğa sahiptir. Her paket listesi girişi üç yeni paket süresi (paket bazlı tetikleme) boyunca listede tutulup bu sayım sonunda silinmektedir. Böylece listenin paketlerle tamamen dolmasının önüne geçilmiş olur. Paket izleme süreci ile ilgili algoritmaya ilişkin kaba kod Şekil 3.31 ve akış diyagramı ise Şekil 3.32 ile verilmiştir.



Çalışmada kullanılan polinomal fonksiyon (3.8) ile verilmiş olup, bu fonksiyon CRC 16-CCITT ismi ile bilinmektedir (Witzke ve Leung, 1985). Üreteç polinomun katsayıları 0x11021 (desimal: 4129) sayısına karşılık gelmektedir. CRC, verinin ikilik karşılığının polinomal fonksiyon katsayısına bölümünden kalan olacak şekilde hesaplanır.

Tespit sistemi, paket izleme sistemi ile birlikte çalışarak daha az döngü ile süreci tamamlayabilecek şekilde en iyileştirilmiştir. Tespit sistemi bileşeni isteğe bağlı olarak aktif edilmektedir. Bileşen aktif edildiğinde paket özetlerinde tespit edilen tutarsızlıklar yanıt sistemi için bir girdi oluşturacak şekilde eylem tetikler. Tespit sistemine ilişkin akış diyagramı Şekil 3.32 ve kaba kodu ise Şekil 3.33 ile verilmiştir. Paket alımı sırasında veriye ilişkin olarak hesaplanan CRC16 özetleri listedeki veri özeti ile karşılaştırılmaktadır. Böylece özet değerler sadece bir kez hesaplanarak kullanılır/saklanır.

**Giriş:** Palinan: Düğüm tarafından tespit edilen yeni paket

Pliste: İmzaları eşleşen listedeki paket girdisi

**Çıkış:** durum: Tespite ilişkin sonuç; *true: ihlal var, false: ihlal yok/izlenmiyor*

**function PCHANGE(Palinan, Pliste)**

1: **if** !aktifPCHANGE **then**

2:     **return** false

3: **end if**

4: **if** Palinan.ozetCRC16 = Pliste.ozetCRC16 **then**

5:     **return** false

6: **end if**

7: Göndericinin CRC ihlal sayısını artır

8: Kontrol fonksiyonlarını tetikle

9: **return** true

Şekil 3.33. Veri değişikliği tespit sistemine ilişkin kaba kod

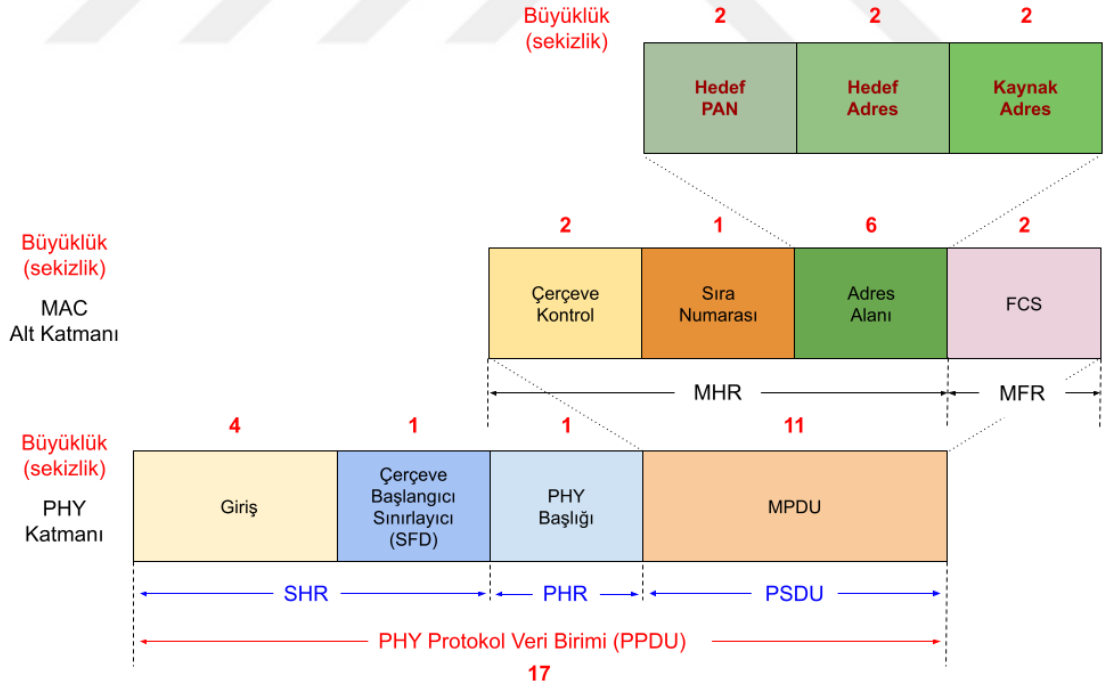
#### • Alındı Mesajı Takip Sistemi

Veri iletişiminde, düğümlerin ilettikleri paketler alıcı tarafından alındı geribildirim ile onaylanmaktadır. Bu geribildirim iletişim protokolü mimarisine göre alındı çerçevesi ile gerçekleşmektedir. Çerçeve yapısı Şekil 3.9 ile gösterilmektedir. Paket gönderimi sırasında bir düğüm, alındı mesaj bildirimi talebinde bulunmak istiyorsa veri paket

A düğümünden baz istasyonuna iletilen paketleri izleyebilmektedir. Algılayıcı düğümünden A düğümüne iletilen 1 numaralı veri paketi başarılı bir şekilde alındığı anda A düğümü alındı mesajını oluşturup iletişimin başarılı bir şekilde gerçekleştiğini duyurur. Fakat haberleşme protokolünde tanımlı olan standart gereği gönderilen alındı bildirimleri sadece paket numarasını barındırmaktadır ve bu nedenle de herhangi bir adres bilgisi içermez. Alındı bildirimi; A düğümünün kapsama alanı içerisindeki diğer tüm düğümler tarafından alınır, fakat sadece algılayıcı düğüm (veri paketini gönderen düğüm) tarafından işlenir.

Komşu izleme tabanlı saldırı tespit sistemi için ACK çerçevelerini izlemek, birçok saldırının tespit edilerek önlenmesi için önemli bir veri kaynağı olarak kabul edilebilir. Örneğin paket almadığı halde paket iletimi gerçekleştiren kötü niyetli düğümlerin tespiti ile paket kayıplı saldırılarda ACK mesaj sayısının takibi ile tespit yapılabilir.

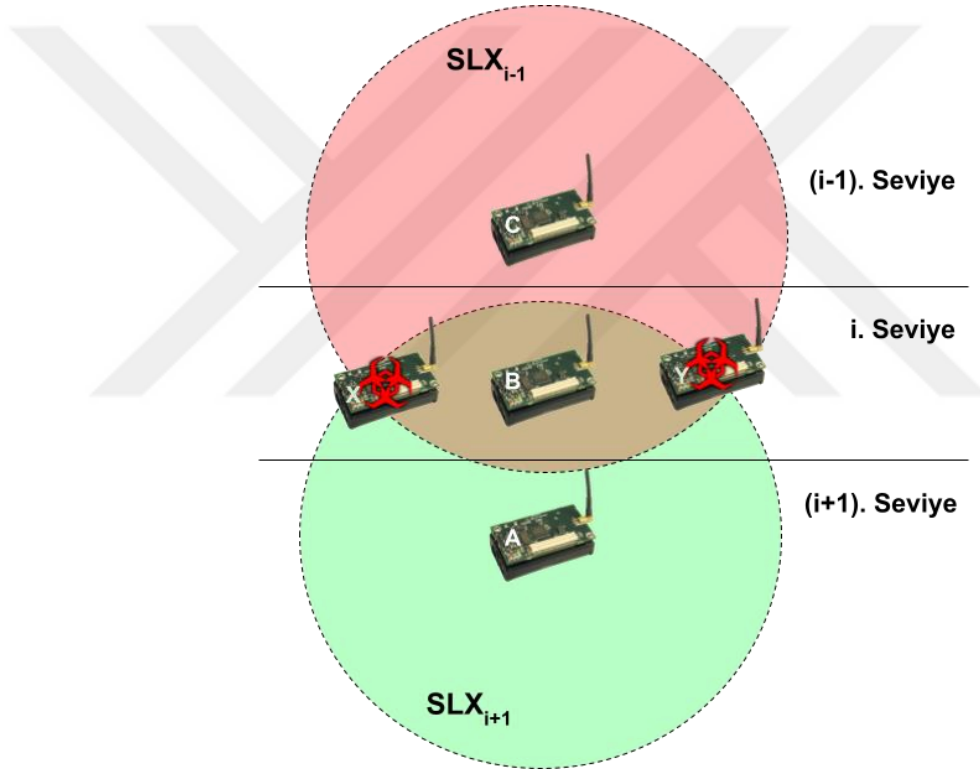
Çalışma kapsamında IEEE 802.15.4 haberleşme protokolü tarafından standart olarak kullanılan alındı çerçevesine altı bytelık adres alanı eklenerek Şekil 3.35 ile verilen iyileştirme yapılmıştır.



Şekil 3.35. Alındı çerçevesi için yapılan düzenleme

### 3.2.1.3 İşbirliği/Kalıtım Sistemi

Sınırlı kapsama alanına sahip düğümlerin izleyebileceği düğümler de sınırlıdır. Paket izleme yoluyla saldırı tespiti yapılabilmesi için düğüme iletilen paketler ile düğümün ilettiği paketlerin kıyaslanmasına ihtiyaç vardır. Bu nedenle topolojideki her saldırgan düğüm, aynı kapsama alanı içerisindeki diğer düğümler tarafından saldırgan olarak sınıflandırılmayabilir. Bunun sonucunda ise olası rota değişimlerinde tercih edilecek ebeveynin daha önce saldırı düzenlemiş ve rota dışına çıkarılmış bir düğüm olma olasılığı oraya çıkar. Bu nedenle düğümler arasında optimize edilmiş bir bilgi paylaşım sistemi, saldırganların yeniden devreye girmesinin önüne geçebilir.



Şekil 3.37. Kapsama alanı kesişimlerindeki ortak saldırganların tespiti

Şekil 3.37 ile verilen örnek topolojide X ve Y saldırgan düğümlerine paket gönderen A düğümü aynı kapsama alanı içerisinde olduğu için B düğümü tarafından da izlenebilmektedir. X ve Y düğümlerinin gerçekleştireceği kötü niyetli girişimler hem A hem de B düğümleri tarafından tespit edilebilmektedir. Fakat C düğümü A ile aynı kapsama alanı içerisinde yer almadığından A düğümüne trafiğine ilişkin X ve Y düğüm davranışlarını analiz edemez. Bu nedenle de C düğümü X ve Y düğümlerine paket trafiği

Mevcut problemi gidermek için çalışmada PCOLLAB isimli bileşen tasarlanmış olup bu bileşen; Şekil 3.38 ile gösterildiği gibi işbirliği paket iletimi ile düğümler arasında tek yönlü bilgi paylaşımını sağlamayı hedeflemiştir. Böylece aktif rotada yer alan düğümler ebeveyn düğümlerine, kendi komşu düğüm istatistiklerini aktarabileceklerdir. Bu işlem sadece aktif rotadaki düğümler tarafından gerçekleştirilebilecektir. Bu sayede paket trafiği minimum seviyede gerçekleştirilecektir. Gönderilen istatistiksel bilgiler, tüm komşu düğümler tarafından alınıyor olsa da sadece aktif rotadaki ebeveyn düğüm tarafından dikkate alınacaktır. Bilgi paylaşımı iki farklı süreç için tekrarlanabilir;

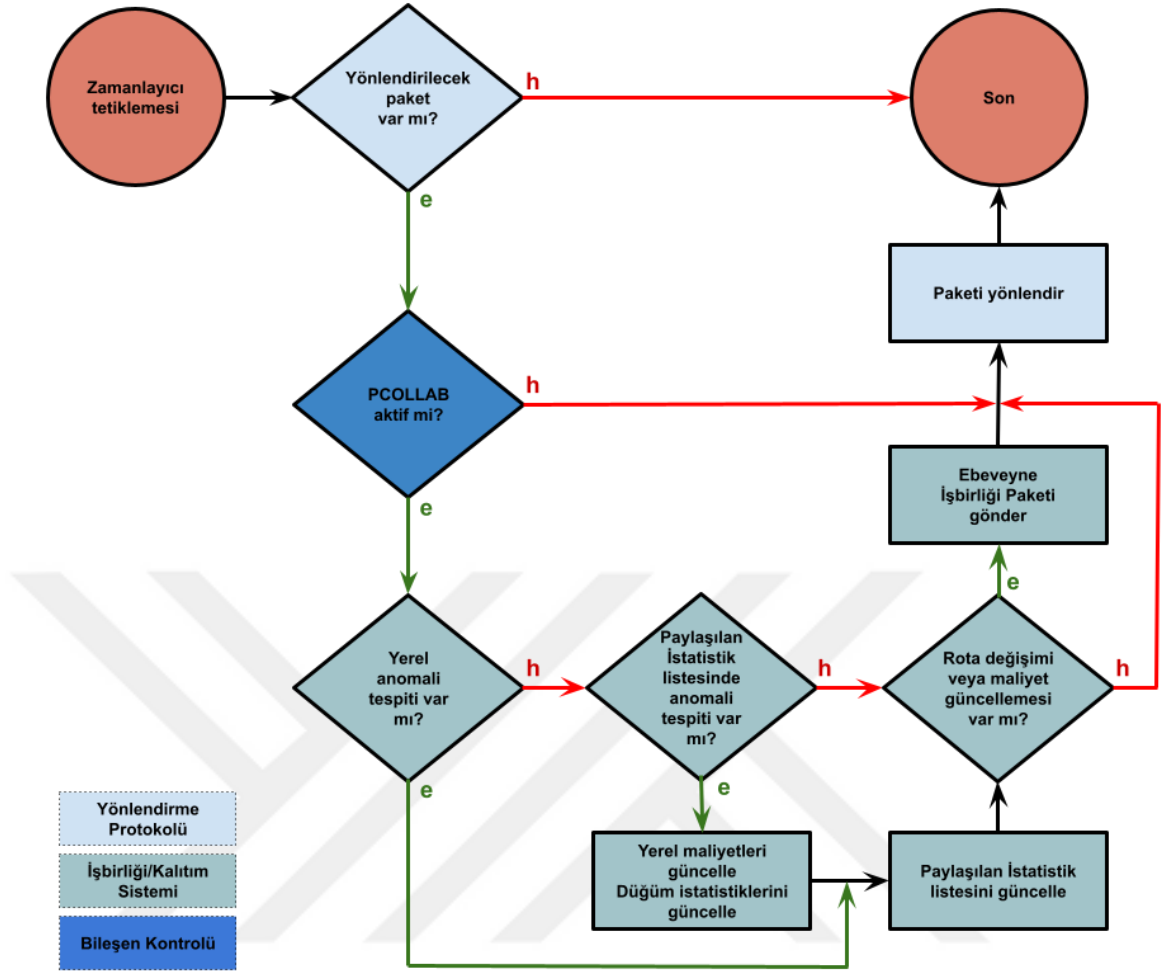
- Yeni ebeveyn düğüm seçimi sonunda, ilk paketin gönderiminden önce
- Saldırgan istatistikleri güncellendiğinde (saldırı tespiti)

Alınan işbirliği paketi, düğümler tarafından geçici bir yerel listeye kaydedilir ve sadece ebeveyn düğüm seçimi ile paket iletişimi başladığında kullanılmaya başlanır. Böylece başka düğümlerden gelen sahte istatistikler dikkate alınmaz.

|                       |   |              |   |   |   |   |   |                |   |   |   |   |   |   |   |
|-----------------------|---|--------------|---|---|---|---|---|----------------|---|---|---|---|---|---|---|
| 0                     | 1 | 2            | 3 | 4 | 5 | 6 | 7 | 8              | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| P                     | C | Rezerve Alan |   |   |   |   |   | [Ebeveyn..     |   |   |   |   |   |   |   |
| .. Ebeveyn]           |   |              |   |   |   |   |   | [ETX..         |   |   |   |   |   |   |   |
| ..ETX]                |   |              |   |   |   |   |   | Liste Uzunluğu |   |   |   |   |   |   |   |
| [Komşu Düğüm Listesi] |   |              |   |   |   |   |   |                |   |   |   |   |   |   |   |

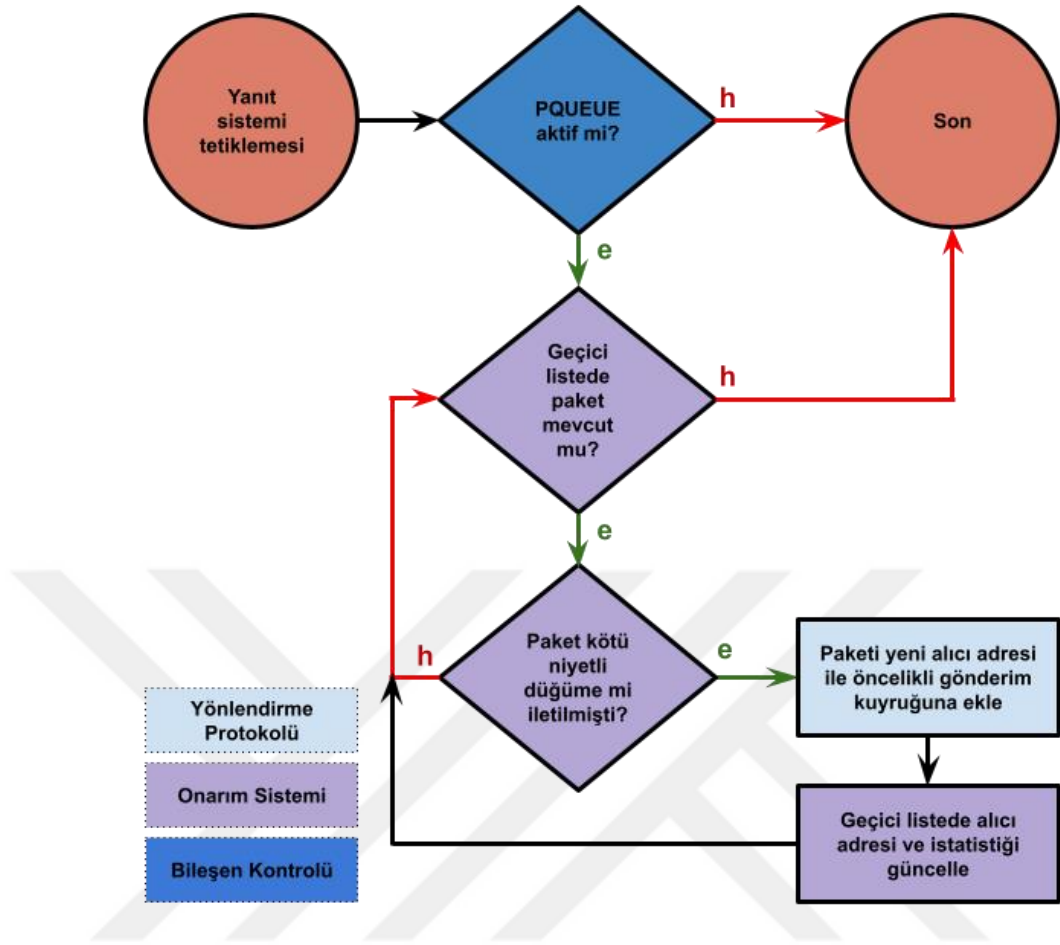
Şekil 3.39. İşbirliği çerçeve şablonu

İşbirliği sırasında kullanılan çerçeve şablonu Şekil 3.39 ile verilmiştir. Şablon içerisinde yer alan komşu düğüm listesi alanına ilişkin veri formatı ise Şekil 3.40 ile verilmiştir. Şablon içerisinde istenilen sayı kadar düğüme ilişkin bilgi paylaşımı yapılabilmektedir. Paylaşılan bilgi adedi çerçeve içerisinde yer alan “Liste Uzunluğu” alanı ile düğüme bildirilir. Çalışmada anomali sayısı sıfırdan büyük olan en yüksek beş düğüm istatistiğinin paylaşımı sağlanmıştır. Düğüm tarafından hiçbir anomali tespiti yapılmamış ise paket gönderimi gerçekleşmez.



Şekil 3.41. Paket gönderim sürecinde paylaşılmış istatistiklerin kullanımı

İşbirliği paketini alan düğümler tarafından işletilen süreçler Şekil 3.42 ile gösterilmiştir. Alınan paket içeriği “Paylaşılan İstatistikler” listesine kaydedilir veya kayıt varsa daha sonra kullanılmak üzere güncellenir.



Şekil 3.43. Onarım sisteminde paketlerin geçici listeden gönderim süreci

Şekil 3.32 ile verilen akış diyagramında izlenen paketlerin gönderilip gönderilmediği tespit edilerek geçici listeden kaldırılması veya yeniden kuyruğa eklenmesi süreçleri gösterilmektedir. Geçici listeye veri girişinin gerçekleşebilmesi için düğümün aktif olarak paket iletimi gerçekleştiriyor (paket sahibi) olması gerekir. Geçici listeden paketin yeniden gönderim süreci ise Şekil 3.43 ile verilen akış diyagramı ile gerçekleştirilmektedir. Aktif rotada yer alan ve paket iletimi gerçekleştiren bir düğüm, ebeveyninin saldırgan özellik gösterdiğini tespit ettiğinde yeni bir rota üzerinden geçici listede yer alan ve bu düğüme iletmış olduğu paketleri öncelikli olarak yeni ebeveyne iletir.

CTP, veri ve ağ trafiğinin iyileştirilmesi konusunda çeşitli mekanizmaları içerisinde barındırmaktadır. Verilerin tekrarlı gönderimin engellenmesi için gönderilen paket listesinin tutulması, gönderilen paketlerdeki rota maliyeti bilgisinin paketi alan düğüme

değer eklenerek komşu düğümler arasında en yüksek maliyetli rota değerine ulaşılır. Elde edilen bu yüksek maliyet değeri ile de düğüm cezalandırılır. Fonksiyonlar, saldırı tespit sisteminden elde edilen sonuçlara göre saldırı yanıt sistemi tarafından işletilir. Tasarlanan yanıt sistemi, kötü niyetli düğümü tümüyle ağdan çıkarmak yerine yüksek bir maliyet değeri ile cezalandırmayı sağlar. Böylece hatalı olarak sınıflandırılmış bir düğümün ağa yeniden kazandırılması mümkün hale gelir.

$$L\_ETX_{ij} = L\_ETX_{ij} + 1 \quad (3.11)$$

$$L\_ETX_{ij} = \max(L\_ETX_i) + ETX_{penalty} \quad (3.12)$$

$$PCX_{ij} = \frac{L\_ETX_{ij} - ETX_i}{hLevel_i} \quad (3.13)$$

- Paket kayıplı saldırılarda (karadelik ve seçici yönlendirme), saldırı kararı RENMIDER ana biriminde yer alan “Düğüm İstatistikleri” listesi dikkate alınarak tespit edilmektedir. Her bir komşu düğüme ilişkin olarak Alınan Paket Sayısı (APS) ve İletilen Paket Sayısı (IPS) olmak üzere;
  - **(APS – IPS) > 2** ise yerel maliyet hesabı;
    - Tıkanıklılık veya ETX değişimi varsa; düşük seviyeli kabul edilir ve (3.11) nolu eşitlik kullanılarak yapılır.
    - Değişim yok ise; yüksek seviyeli kabul edilir ve (3.12) nolu eşitlik kullanılarak yapılır.
    - İstatistiklerde yer alan anomali sayısı (düşük veya yüksek seviyeli) bir artırılır.
- Veri değiştirme saldırılarında ise aktif rotada yer alan komşu düğümün almış olduğu pakete ilişkin imza ile iletmış olduğu pakete ilişkin imza uyuşmazlığında (PCHANGE) düğümün yerel maliyet hesabı (3.12) nolu eşitlik kullanılarak hesaplanır. Düğüm istatistiklerinde yer alan yüksek seviyeli anomali sayısı bir artırılır.
- Alındı mesaj takibi (PACKB); paket göndericisinin kapsama alanı dışında yer aldığı ve gönderilen paketlerin tespit edilemediği durumlarda saldırı tespiti için

Saldırı tespitinin ardından ana bileşendeki “Düğüm İstatistikleri” listesinde ilgili düğüme ait istatistikler (Aldığı paket sayısı, İlettiği paket sayısı, İlettiği takip dışı paket sayısı, İlettiği ACK sayısı) sıfırlanır. Düğüme ilişkin değerlendirmelerin yapıldığı fonksiyona ait kaba kod Şekil 3.44 ile, yerel maliyetlerin hesaplanmasına ilişkin fonksiyona ait kaba kod ise Şekil 3.45 ile verilmiştir.

Şekil 3.46 ile verilen topolojide CTP kullanılarak elde edilmiş bir rota örneği verilmiştir. Baz istasyonu (B) ve algılayıcı düğüm (S) arasında iki farklı rota söz konusudur. 2 nolu düğüm rota maliyetini komşularına kontrol mesajı ile 22 ETX olarak duyururken, 3 nolu düğüm ise rota maliyetini 10 ETX olarak duyurur. 1 nolu düğüm ile 2 nolu düğüm arasındaki bağlantı kalitesi 12 ETX, 3 nolu düğüm ile de bu değer 10 ETX’tir. Bu durumda 1 nolu düğüm 3 nolu düğümü ebeveyn olarak kabul ettiğinde rota maliyeti 20 ETX, 2 nolu düğümü ebeveyn olarak kabul ettiğinde ise bu maliyet 34 ETX olarak hesaplanır. En düşük maliyetli rotanın ebeveyn olarak kabul edilecek olması sebebiyle 1 nolu düğüm 3 nolu düğümü ebeveyn olarak seçerek rota maliyetini komşularına 20 ETX olarak duyurur. Algılayıcı düğümün (S) 1 nolu düğümü ebeveyn olarak kabul etmesi ile birlikte bu düğümün rota maliyeti 30 ETX olur. Algılayıcı düğüm ile 1 nolu düğüme ilişkin komşuluk tabloları görsel üzerinde verilmiştir.

**Giriş:** dugum: İşlenecek komşu düğüm adresi  
anomaliseviyesi: İhlalin ceza değeri seviyesi

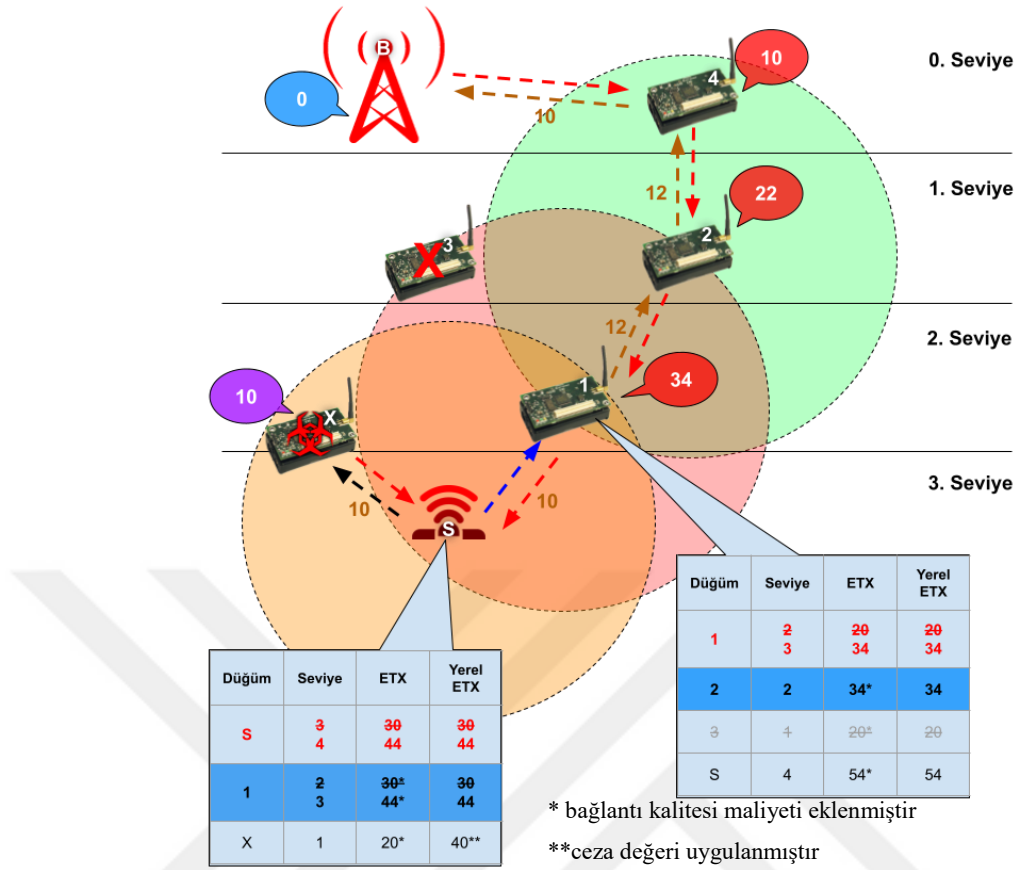
**function RenmiderIDRSPostProc(dugum, anomaliseviyesi)**

```

1: yeniYereLETX = dugum.yereLETX
2: if anomaliseviyesi = 0 then
3:   yeniYereLETX = yeniYereLETX + minETXpenalty
4: else if anomaliseviyesi = 1 then
5:   maksETX = Komşu düğümlerin en büyük yerel maliyet değeri
6:   adresDugum = Yerel maliyeti en yüksek olan komşu düğümün adresi
7:   if adresDugum != dugum.adres then
8:     yeniYereLETX = maksETX + maksETXpenalty
9:   end if
10: end if
11: dugum.yereLETX = yeniYereLETX
12: dugum.PCXlow=(yeniYereLETX-dugum.ETX) mod hLevel
13: dugum.PCX=(yeniYereLETX-dugum.ETX-dugum.PCXlow)/hLevel

```

Şekil 3.45. Komşu düğümün yerel maliyet güncellemesine ilişkin kaba kod



Şekil 3.47. Rota değişimi sonucu güncellenen komşuluk tabloları ve rota maliyetleri

Bu durumda 1 nolu düğümün rota maliyeti 34 ETX değerine yükselir ve bu bilgi komşu düğümlerle de paylaşılır. Algılayıcı düğüm (S), 1 nolu düğümden gelen kontrol paketini aldığı anda komşuluk tablosunu ve rota maliyetini günceller. Bu güncellemeyi komşularına kontrol paketi ile duyurur. Algılayıcı düğümün maliyet değerinin artması, kötü niyetli X düğümünden daha yüksek bir değere ulaşmasına neden olmuştur. Bu durum sonucunda ebeveyn değişimi için yeterli bir fark değerine ulaşılamamış olsa da daha yüksek seviyeli değişimlerde saldırgan düğümün yeniden seçilmesine neden olabilir. Bu problemi giderebilmek için dinamik ölçekli ceza katsayısının kullanımı önerilmiştir.

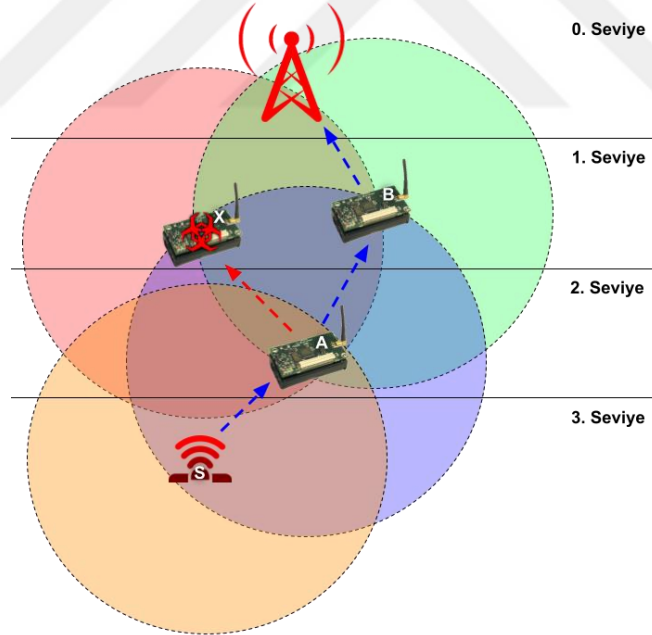
Dinamik ölçekli ceza katsayısı, ceza değeri uygulanmış yerel ETX değerinin topolojik değişimlerle birlikte ölçeklenmesini amaçlar. Bu sayede yüksek seviyeli bir topolojik değişimde (bağlantı kalitesinde yüksek değişimler hariç) saldırgan düğümlerin yeniden ağı hâkim olmaları önlenirken, bağlantı kalitesinden kaynaklanan değişimlerde yanlış sınıflandırılmış düğümlerin ağıya yeniden kazandırılması ve ebeveyn olarak kullanılması sağlanmış olur. Ceza katsayısı (3.13) ile verilen fonksiyon aracılığı ile

#### 4. ARAŞTIRMA BULGULARI ve TARTIŞMA

Yapılan çalışma kapsamında tasarlanan saldırı tespit ve yanıt sisteminin performans analizini gerçekleştirmek için farklı topolojilere ve saldırı türlerine sahip ağ yerleşimleri gerçek zamanlı ortamlarda test edilmiştir. Kullanılan aygıtlarla ilgili bilgiler “*Donanımsal Bileşenler*” bölümünde açıklanmıştır. Çalışmaların tamamında yönlendirme protokolü olarak CTP tercih edilmiştir.

##### 4.1. Yönlendirme Saldırı Modelleri ve Saldırı Tespit Sistemi Performans Analizleri

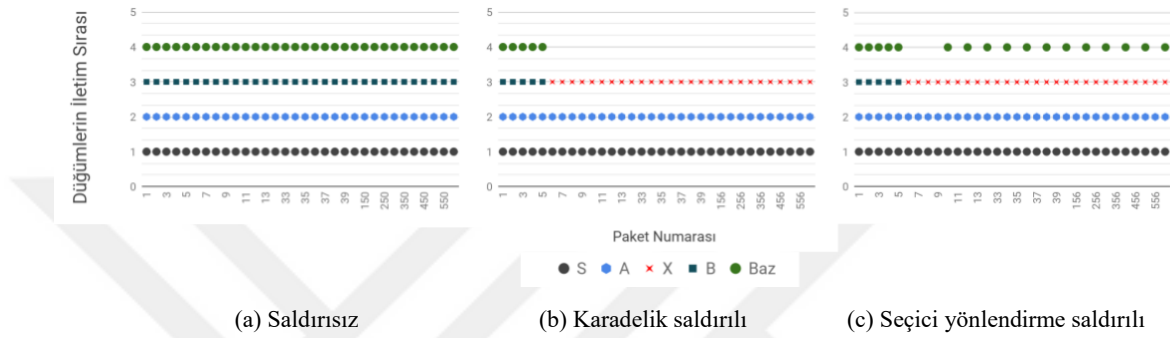
Gerçek zamanlı olarak gerçekleştirilen çalışmada saldırılar, teorik olarak önceden modellenmiş ve donanıma uygulanmıştır. Saldırgan düğüm ile ilgili testler Şekil 4.1 ile verilen topoloji kullanılarak gerçekleştirilmiştir (Ofrazoglu ve Abasikeles Turgut, 2020).



Şekil 4.1. Saldırı analizinde kullanılan topoloji

Şekil 4.1 ile verilen topolojide; algılayıcı düğüm (S), iki ara düğüm (A ve B düğümleri), saldırgan düğüm (X) ve baz istasyonu yer almaktadır. Düğümlerin kapsama alanı görsel üzerinde yer almaktadır. Gerçek zamanlı çalışma sistemini sağlayabilmek

düğümlemlerince iletilerek baz istasyonuna ulaşmıştır (600 adet paket). Algılayıcı düğümden baz istasyonuna iletilen paketlere ilişkin detaylı grafik Şekil 4.3 (a) ile verilmiştir. Bu grafikte, paketin hangi düğümler tarafından yönlendirildiği gösterilmektedir. Topolojide aktif rota üzerinde bulunan düğümler, herhangi bir paket kaybı olmadan tüm paketleri baz istasyonuna iletmışlerdir. Sayısal istatistikler Şekil 4.4 ile verilen grafikte yer almaktadır.

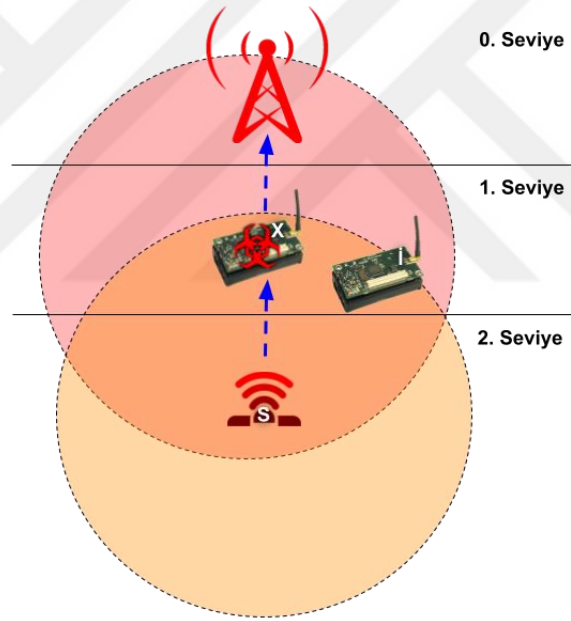


Şekil 4.3. Düğümlere ilişkin paket iletimleri

Çalışmanın sonraki bölümünde saldırgan düğüm aktif edilmiştir. Düğüm öncelikle çıkış deliği (sinkhole) saldırısı ile paket trafiğini ele geçirmeye çalışır. Bunun için komşu düğümlere en düşük maliyet bilgisine sahip olduğunu duyurmak için bilgilendirme mesajı (beacon) yayınlar. Bu yayın ile kendi rota maliyetini baz istasyonundan sonraki en düşük olabilecek değer olarak duyurur (1 ETX). Saldırı öncesi aktif rota üzerinde bulunan A düğümü, B düğümü üzerinden baz istasyonuna bağlıdır. Bu nedenle sahip olabileceği en düşük rota maliyeti 20 ETX'tir (iki seviye boyunca en iyi bağlantı kalitesinin olduğu durum için). Bu çalışmaya özgü olarak CTP'deki rota değişimi için gerekli olan eşik değeri 5 ETX olarak güncellenmiştir. Saldırganın 1 ETX'lik rota maliyetini duyurması ile birlikte A düğümü, B düğümü yerine daha düşük toplam maliyete (11 ETX) sahip saldırgan düğümü (X) seçer. Böylece saldırgan düğüm trafiği B düğümü üzerinden kendi üzerine almış olur.

Çalışmada çıkış deliği saldırısı ile birlikte trafiği üzerine alan saldırgan düğüm, sırasıyla karadelik ve seçici yönlendirme saldırılarını uygulamıştır. Karadelik saldırısının uygulandığı ilk durumda saldırgan, paket trafiğini üzerine aldıktan sonra tüm paketleri bloke ederek baz istasyonuna ulaşmasını engellemeye çalışmıştır. 600 paket için

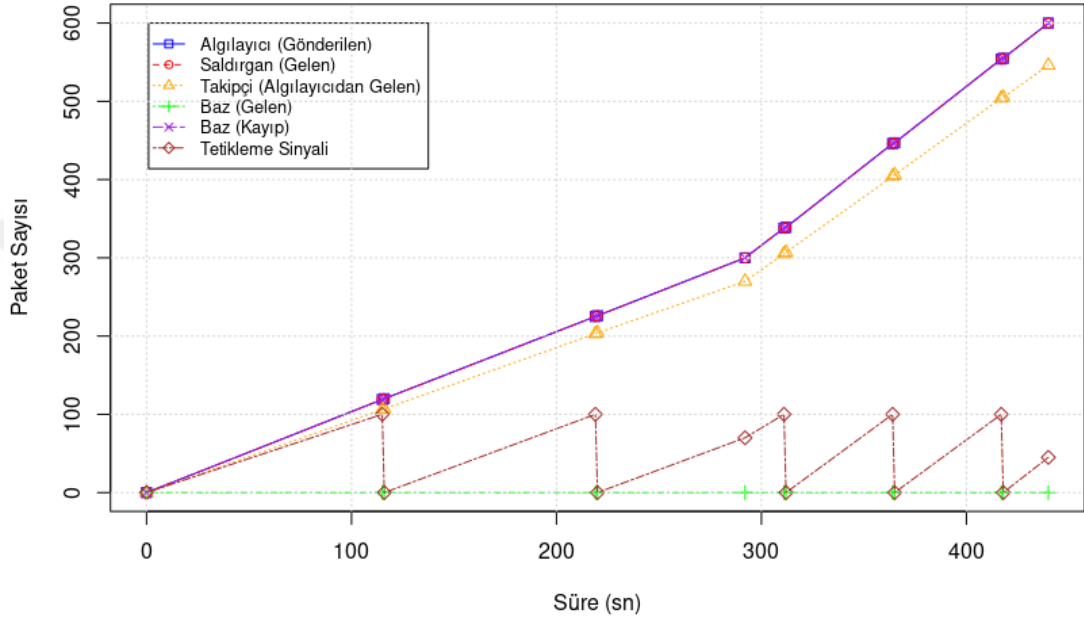
varyasyonudur. Bu çalışmada elde edilen veriler ışığında algoritma sonraki çalışmalar için güncellenmiştir. Kullanılan bu algorithma izlenen paketlerin takip listesindeki yaşam ömrü için bir sınırlama eklenmemiştir. İzlenen paketlerin tutulacağı liste uzunluğu ise 50'dir. Listenin aşılması durumunda listenin ilk verisinden itibaren veri ekleme süreci yeniden başlar. Çalışmada, saldırısız ve saldırılı (karadelik ve seçici yönlendirme) durumlar ayrı ayrı analiz edilmiştir. Kullanılan yeni düğüm yerleşimi Şekil 4.5 ile verilmiştir. Yerleşimde algılayıcı düğüm (S), saldırgan düğüm (X), izleyici/takipçi düğüm (İ) ve baz istasyonu yer almaktadır. İzleyici düğüm, algılayıcı ve saldırgan düğümlerin kapsama alanı içerisinde yer alacak şekilde ve sadece paket trafiğini izlemek amaçlı olarak konumlanmıştır. İzleyici düğüm, bu çalışma boyunca kendisini diğer düğümlere tanıtım mesajı ile duyurmadığı için herhangi bir paket trafiği gerçekleştirmez.



Şekil 4.5. Saldırıların gözlemci bir düğüm ile tespiti için kullanılacak düğüm yerleşimleri

Saldırgan düğümün saldırı düzenlemediği, paketleri normal bir ara düğüm gibi ilettiği duruma ilişkin zamana göre paket sayıları Şekil 4.6 ile gösterilmiştir. Grafikte, algılayıcı düğüm tarafından gönderilen ve baz istasyonu tarafından alınan paket sayılarının yanı sıra takipçi/izleyici düğüm tarafından izlenebilen paket sayıları da yer almaktadır. Çalışmanın ilk 300 adet paketi algılayıcı düğüm tarafından birer saniye

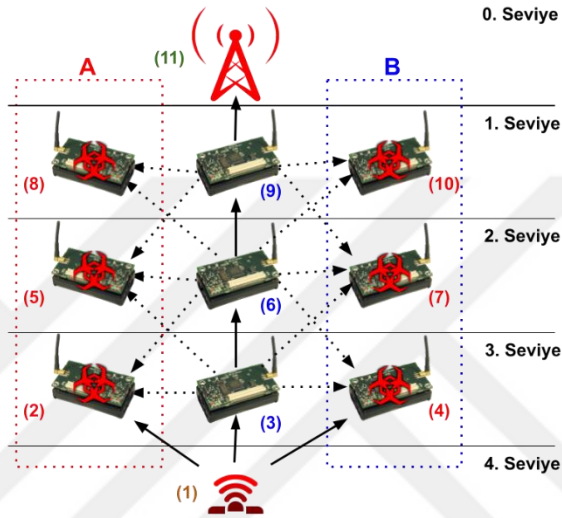
konumlandırılmıştır. İzleyici düğüm, saldırgan düğüm tarafından iletilmediğini tespit ettiği her yüz adet paket için bir alarm üreterek sayaçlarını sıfırlamıştır. Elde edilen sonuçlara ilişkin grafik Şekil 4.7 ile verilmiştir. Sonuçlara göre izleyici düğüm konumu gereği algılayıcı düğümünden iletilen bazı paketleri algılayamadığı için izleme sürecini %91 oranında bir başarı ile gerçekleştirebilmiştir (Ofllazoglu ve Abasikeles Turgut, 2020).



Şekil 4.7 Karadelik saldırısının gerçekleştirildiği süre içerisinde düğümler tarafından iletilen toplam paket sayılarının zamana göre değişimi

Saldırgan düğümün seçici yönlendirme saldırısı yaptığı bu uygulamada ise diğer uygulamalara benzer şekilde paketler, 1 ve 0.5 saniye aralıklarla 300'er adet olmak üzere algılayıcı düğümünden ağı iletilmiştir. Paket iletiminden önce saldırgan düğüm aktif hale getirilmiş ve yönlendirilecek olan paketleri %50 kayıpla iletmeleri sağlanmıştır. İzleyici düğüm, kötü niyetli düğüm tarafından iletilemeyen her yüz adet paket için bir alarm üreterek sayaçlarını sıfırlamıştır. Önceki uygulamalardan farklı olarak izleyici düğümün konumu daha iyi bir kapsama alanı içerisine yer alabilmesi bakımından bir miktar değiştirilerek algılayıcı düğümünden iletilen paketleri daha fazla alabilmesi sağlanmıştır. Bu çalışmaya ilişkin olarak zamana göre toplam paket sayılarındaki değişim Şekil 4.8 ile gösterilmiştir. Elde edilen sonuçlara göre izleyici düğüm algılayıcı ve saldırgan düğüme

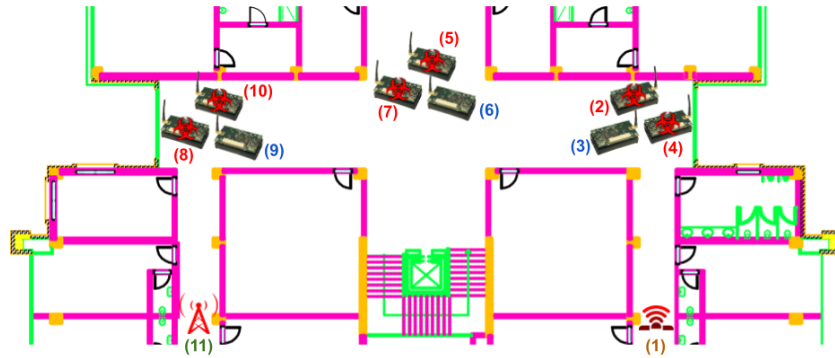
ettiği bilgiler ile saldırı tespitine ilişkin performans analizleri yapılmıştı. Bu çalışmada ise, aktif rotadaki düğümler dâhil olmak üzere tüm düğümlerin hem izleyici hem de aktif yönlendirici olarak yer aldığı ve çok sayıda kötü niyetli düğümün bulunduğu bir topolojideki saldırı tespiti ve bu saldırılara karşılık olarak düğümlerin vereceği yanıtlar incelenecektir. Çalışmada kullanılan gerçek zamanlı ortama ilişkin topoloji Şekil 4.9, düğümlerin bina içerisindeki yerleşimleri ise Şekil 4.10 ile gösterilmiştir.



Şekil 4.9. Düğümlerin topolojik gösterimi

Topolojide yer alan düğümler:

- Algılayıcı düğüm: **(1)**
- Ara düğüm: **(3), (6), (9)**
- Kötü niyetli düğümler: **A grubu: (2), (5), (8); B grubu: (4), (7), (10)**
- Baz istasyonu: **(11)**



Şekil 4.10. Düğümlerin bina içerisindeki yerleşimleri

vb. gibi veriler SQLite veritabanı aracılığı ile sonradan işlenmek üzere kayıt altına alınmıştır. Cihazlar arasındaki zaman eşzamanlılığının sağlanabilmesi için kayıt aygıtlarında ortak NTP sunucusu kullanılmış ve zaman eşitlemesi gerçekleştirilmiştir.

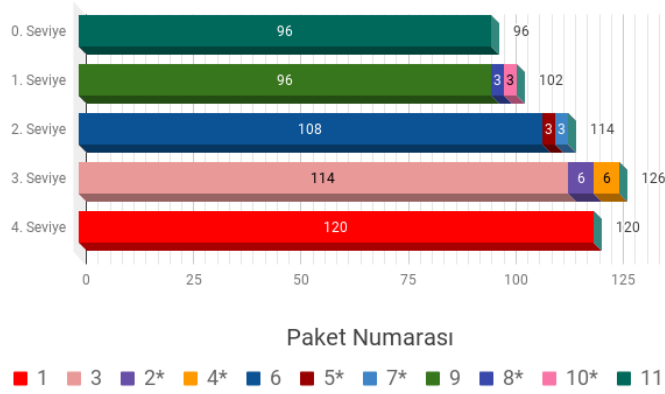
|                |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0              | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| Paket Numarası |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| ETX            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Seviye Bilgisi |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Güç            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Sıcaklık       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Işık Şiddeti   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

Şekil 4.11. Çalışmaya özgü olarak iletilmek istenen veri içeriği

#### 4.2.1. Sadece A Grubu Saldırgan Düğümlerin Aktif Edildiği Ağa İlişkin Sistem Başarımı

Bu çalışmanın ilk aşamasında, Şekil 4.9 ile verilen görselde yer alan A grubu saldırgan düğümler, baz istasyonu ve algılayıcı düğüm aktif edilmiştir. A grubu kötü niyetli düğüm numaraları; (2), (5) ve (8)'dir. Çalışmanın ikinci aşamasında ise, algılayıcı düğümden 79. paketin iletimi sonrasında B grubu saldırgan düğümlerin devreye girmesi sağlanmıştır. B grubu kötü niyetli düğüm numaraları ise; (4), (7) ve (10)'dur.

A grubu saldırgan düğümlerin devreye girmesi ile birlikte (1), (3) ve (6) numaralı ara düğümler ebeveyn olarak saldırgan düğümlere bağlanırlar. Aktif olan saldırgan düğümler tarafından duyurulan rota maliyetleri aynı olacağı için ara düğümlerin hangi saldırgan düğümü ebeveyn olarak seçtiği önceden bilinemez. Şekil 4.12 ile gösterilen grafikte algılayıcı düğüm (2) nolu saldırgan düğümü ebeveyn olarak kabul etmiştir. Algılayıcı düğümün göndermiş olduğu paketler (2) nolu saldırgan düğüm tarafından alınır ve iletilmez. Paket iletim grafiği incelendiğinde ilk 3 paket kaybından sonra algılayıcı düğüm ebeveyn değişikliğine giderek (3) numaralı düğümü yeni ebeveyni olarak seçmiştir. Yeni ebeveyn; algılayıcı düğüm ile (2) numaralı saldırgan düğüm ile aynı kapsama alanı içerisinde yer aldığından, saldırgan düğümün gerçekleştirmiş olduğu saldırıyı tespit etmiştir. Bu nedenle de düşük bir ETX değerine sahip olan (2) numaralı



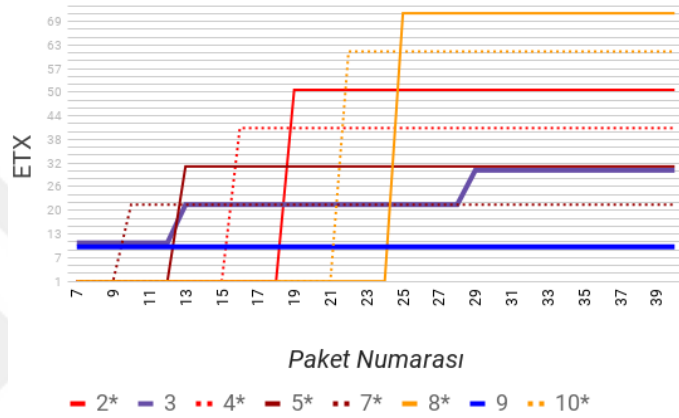
Şekil 4.13. Her seviye için düğümler tarafından alınan/iletilecek paket sayıları

Şekil 4.13 ile verilen görselde her bir seviye için düğümlerin almış/iletmiş oldukları paket sayıları verilmiştir. Algılayıcı düğümden iletilen 120 adet paketin 96 adedi baz istasyonuna ulaşmıştır. Çalışmada, saldırganın tespiti için 3 adet paket kaybı yeterlidir. Fakat kapsama alanı sebebi ile düğüme gönderilen paketlerin tespit edilemediği (2) ve (4) numaralı düğümlerde üçer adet paket kaybı olmak üzere fazladan 6 adet paket kaybı meydana gelmiştir. Geliştirilen tespit ve yanıt sisteminde fazladan paket kaybına neden olan durum, sisteme eklenen iki farklı ek bileşen ile giderilmiş ve bu konuya ilişkin analizlere sonraki bölümlerde yer verilmiştir.

#### 4.2.2. A ve B Grubu Saldırgan Düğümlerin Birlikte Aktif Edildiği Ağ İçin Performans Analizleri

Yapılan bu çalışmada ise Şekil 4.9 ile verilen görselde yer alan tüm saldırgan düğümler eş zamanlı olarak aktif edilmiştir (A ve B grupları). Önceki test ortamına benzer şekilde saldırgan düğümlerce iletilmeyen paketler üçe ulaştığında ağda rota değişikliği gerçekleştirmiştir. Düğümlerin paket iletimlerine ilişkin görsel Şekil 4.14 ile verilmiştir.

Çalışmada ayrıca, algılayıcı düğüm ile (6) numaralı düğüme ilişkin yerel rota maliyet listeleri de incelenmiştir. Şekil 4.16 ile verilen grafik, (6) numaralı ara düğüme ait yerel maliyet listesindeki değişimleri göstermektedir. Şekil 4.14 ve Şekil 4.16 birlikte incelendiğinde, 9. paketin (7) numaralı düğüm tarafından bloke edilmesi ile birlikte ara düğüm, saldırgan düğüme yüksek bir ceza değeri uygulamıştır. Benzer şekilde ara düğüm ile aynı kapsama alanı içerisinde yer alan diğer saldırgan düğümlerin de (sırasıyla (5), (4), (2), (10) ve (8)) yerel maliyet değerlerinde artış kademeli olarak gerçekleşmiştir.

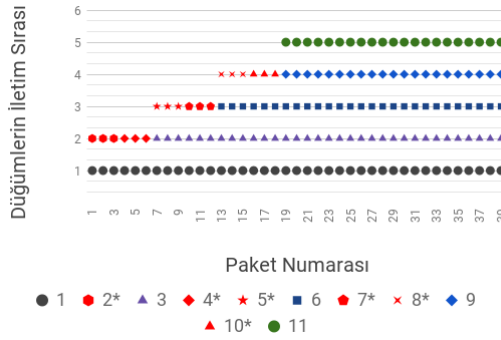


Şekil 4.16. (6) numaralı düğümün yerel rota maliyet listesindeki değişimler

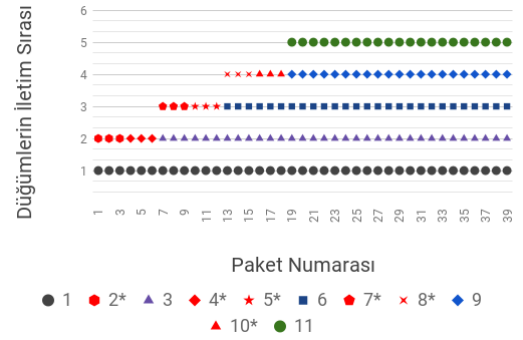
Şekil 4.16 ile verilen grafikte yer alan diğer bir durum ise (3) numaralı ara düğümün rota maliyetinde gerçekleşen artıştır. 12. paketin bloke edilmesi ile birlikte (3) numaralı ara düğümün de maliyet değerinde bir artış gerçekleşmiştir. Bu değişimin sebebi (3) numaralı düğümün ebeveyn olarak (6) numaralı düğümü tercih etmesi ve rota maliyet değerinin değişmesidir. Benzer şekilde 29. paketin iletimi sırasında da bir artış söz konusudur. (6) numaralı düğümün (9) numaralı düğümü ebeveyn olarak tercih etmesi ile beraber rota maliyet bilgisi güncellenmiş ve bu güncelleme bilgilendirme mesajı (beacon) ile diğer komşulara duyurulmuştur. Bilgilendirme mesajını alan komşu düğümler ise rota maliyetlerini yeniden hesaplamışlardır. Bu hesaplama sonucunda, ortaya çıkan fark değerinin 10 ETX değerini aşmıyor olması yeni bir bilgilendirme mesajı dağıtımını geciktirmiştir. Bu nedenle (3) numaralı düğüm bilgilendirme mesajını standart periyodu içerisinde göre diğer düğümlere duyurulmuştur.

#### 4.2.3. PACKB ve PCOLLAB Bileşenlerinin Tespit Sistemine Etkileri

İzleyici düğümlerin kapsama alanı dışında gerçekleşen paket trafiğini izleyememeleri, saldırıların doğru olarak tespit edilememesine neden olmaktadır. Çünkü geliştirilen paket izleme sistemi, alınan paketler ile gönderilen paketlerin eşleştirilmesi ve analizi esasına dayanmaktadır. Paket kayıplı saldırılarda alınan paketlerin düğüm tarafından gönderilmemesi durumunda anomali tespiti sağlanır. Saldırganı tespit edemeyen düğümler bu düğüme veri akışı sağlayarak saldırıların paketler üzerindeki hâkimiyetinin sürmesine devam edebilir. Fakat gönderici düğüm, izleyici düğümün kapsama alanı dışında olduğu koşullarda izlemenin gerçekleşmediği önceki test ortamlarında ortaya konmuştur. Bu durum daha fazla paket kaybına neden olmuştur. Bu test ortamında ise problemi ortadan kaldırabilmek için “Alındı Mesajı Takip Sistemi” ve “İşbirliği/Kalıtım Sistemi” iki farklı bileşen önerisi ayrı ayrı test edilecektir. Çalışma ortamı olarak yine Şekil 4.9 ile verilen topoloji kullanılacaktır. Topolojideki tüm saldırı düğümler paket iletişimi başlamadan önce aktif edilmiştir. Alındı mesajı takip sisteminde, düğümün ilettiği alındı mesaj sayısı (ACK) ve düğümden iletilen paket sayıları dikkate alınmıştır. Alındı mesaj sayısı ile iletilen paket sayısı arasındaki fark üçe ulaştığında eğer paket takip sistemi bir alarm üretmemiş ise bu bileşen tarafından düğümün yerel rota maliyet değeri güncellenir.



(a) Alındı mesajı takip sistemli



(b) İşbirliği/Kalıtım sistemli

Şekil 4.18. Ek bileşenlerle geliştirilmiş olan paket izleme sisteminin iletim başarımları

İşbirliği/Kalıtım sisteminde ise düğüm, rota değişimi veya saldırı tespitinde ilk paket gönderiminden önce tespit ettiği anomali sayısı ve düğüm adreslerini ebeveyn ile

(b) ile verilen grafikte, algılayıcı düğümden (2) ve (4) numaralı saldırganlara iletilen ve paket kaybı ile sonuçlanan iletişimin sonucunda (3) numaralı düğüm bu saldırıları tespit eder. Bu nedenle algılayıcı düğümün (3) numaralı düğüme iletmış olduğu bilgilendirme paketi bu düğüm tarafından işlenmeye değer bulunmamıştır. (3) numaralı düğümün, (5) ve (7) numaralı saldırgan düğümleri ebeveyn seçerek gerçekleştirmiş olduğu iletişim girişimi paket kaybı ile sonuçlanır. Bunun sonucu olarak (3) numaralı ara düğüm (6) numaralı düğümü ebeveyn olarak seçme kararı alır. (6) numaralı düğüm (5) ve (7) numaralı saldırgan düğümlerin paket kaybettiğinden aynı kapsama alanı içerisinde bulunduğu için haberdardır. Fakat (2) ve (4) numaralı düğümler için herhangi bir tespit işlemi gerçekleştirememiştir. İşbirliği sistemi gereği (3) numaralı düğüm; (5), (7) ve (6) numaralı düğümleri ebeveyn olarak seçip ilk paketi göndermeden önce;

- (5) nolu düğüm ebeveyn olarak seçildiğinde: (4), (2)
- (7) nolu düğüm ebeveyn olarak seçildiğinde: (5), (4), (2)
- (6) nolu düğüm ebeveyn olarak seçildiğinde: (7), (5), (4), (2)

numaralı düğümlere ilişkin bilgilendirme mesajı yayınlar. Bu mesajlar komşu tüm düğümler tarafından alınır ve sadece mesaj içeriğindeki saldırgan düğüm listesinden kapsama alanı içerisinde olanlar yerel listeye kaydedilir/güncellenir. Fakat bu istatistikler sadece veri iletimi gerçekleştiren düğümün ebeveyni tarafından veri paketi gönderimi öncesinde dikkate alınır. Bu nedenle (6) numaralı düğüm (2) ve (4) numaralı düğümden de haberdardır. 13. paketin (6) numaralı düğüme iletilmesi ile birlikte bu düğüm (3) numaralı komşusu tarafından paket öncesi aldığı istatistikleri yerel listesinden incelemeye ve işlemeye başlar. Listede daha önce işlenmemiş ve hali hazırda ebeveyn olmaya aday düğümler var ise bu düğümlere ceza değeri atanarak aday ebeveyn olma durumları sonlandırılır. Şekil 4.19 (b) ile verilen grafikte (2) ve (4) numaralı düğümlerin yerel rota maliyetlerindeki değişim ceza değerinin uygulanması sonucu ortaya çıkmıştır. Bu sayede, bu düğümlerin ebeveyn olmalarının da önüne geçilmiştir.

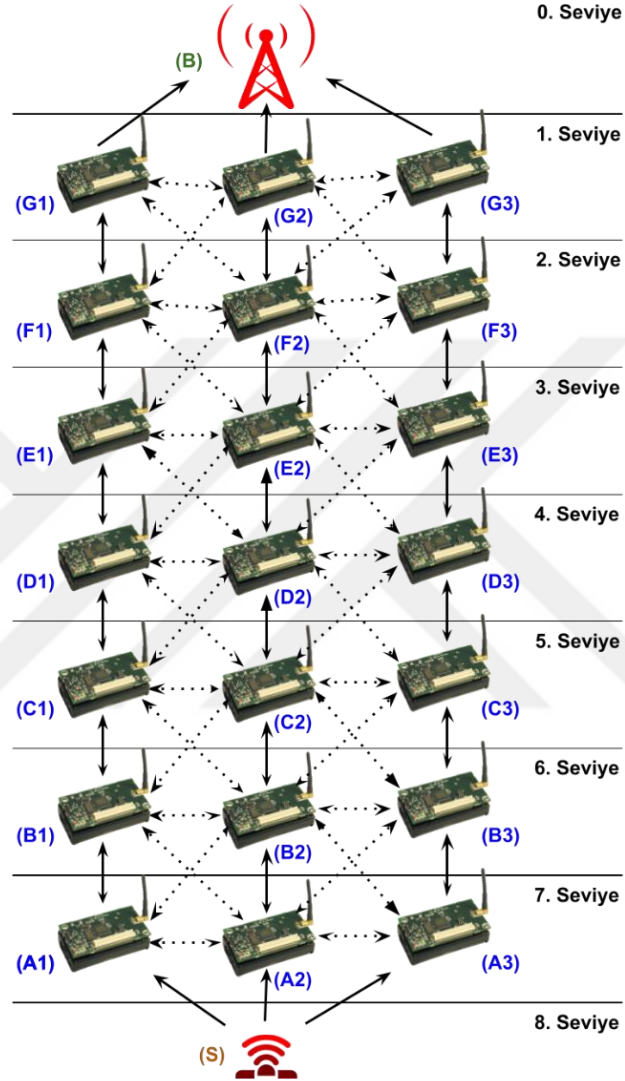
İşbirliği/Kalıtım sistemi, alındı mesajı takip sistemine göre ekstra paket gönderimine ihtiyaç duymaktadır. Fakat ağa yeni katılmış bir düğümün alındı mesajı takip sistemi ile önceden tespit edilmiş saldırgan düğümleri öğrenebilmeleri mümkün değildir. Bu noktada işbirliği sistemi bir kalıtım mekanizmasına dönüşür.

#### 4.2.4. Saldırganın Ağ Üzerindeki Konumunun Tespit Sistemine Etkisi

Çalışmanın bu bölümünde saldırgan düğümün topolojide bulunduğu konumun ağın yeniden kullanılabilir duruma gelmesi için harcanan süreye etkisi incelenmiştir. Düğüm yerleşimleri için Şekil 4.9 ile verilen topoloji kullanılmıştır. Önceki çalışmalardan farklı olarak ağda sadece bir adet saldırgan düğüm bulunmaktadır. Çalışma korumasız ve PLOST bileşeni ile korunmakta olan ağ aygıtları için ayrı ayrı gerçekleştirilmiştir. Saldırgan; verilen topolojide (2), (6) veya (10) numaralı düğümlerden birisi olabilmekte ve çıkış deliği + karadelik saldırıları yapabilmektedir. Çalışmada ağın korumalı ve korumasız olduğu durumların yanı sıra saldırının başlamasından itibaren baz istasyonuna iletilen ilk paketin iletim süresi (saldırganın aktif rotadan çıkarılması ve yeni rotanın kurulması için geçen süre) ve saldırısı sonrası paket akışının kararlı duruma gelmesi ile birlikte paketler arasındaki ortalama iletim süreleri incelenmiştir. Korumasız olan ağda, ağın yeniden kurulabilmesi ve geçen sürenin ölçülmesi için saldırgan düğüm belirli bir paket kaybından sonra (10 paket) devre dışı bırakılmıştır.

Çalışmaya ilişkin sonuçlar Çizelge 4.2 ile sunulmuştur. Korumasız bir ağ için 1. seviye düğüm olan (10) numaralı saldırgan düğüm devreden çıkarıldıktan sonra (10 paket kaybı sonunda) ağın yeniden ebeveyn seçerek sonraki paketi baza iletime süresi 371 ms olarak gerçekleşmiştir. Ağın tekrar kararlı duruma geçmesi ile birlikte paketlerin baza iletimi için ortalama geçen süre 103 ms olarak ölçülmüştür. Benzer süreçler 2. seviye ((6)) ve 3. seviye ((2)) düğümlerin saldırgan olarak seçilmesi ile devam etmiştir. Rota maliyetlerinin topolojinin alt seviyelerine ilerledikçe artıyor olması ve saldırgan düğümün çıkış deliği saldırısı ile daha fazla komşu düğüm rotasında değişikliğe neden olması, saldırı sonrasında ağın yeni rota üzerinden kurulmasını geciktirmiştir. PLOST bileşeni ile korunan bir ağda iletişimin bozulmasına neden olan faktörler (paket kaybı, vb. gibi) sonucunda ceza katsayısı güncellemeleri ile ebeveyn seçim süreci hızlandırılmış ve ağın daha hızlı bir şekilde kararlı duruma gelmesi sağlanmıştır. Özellikle 2. seviyede yer alan saldırgan düğüm için saldırı sonrası baza paket ulaşım süresi önemli ölçüde azalmıştır.

Topolojide çok sayıda düğüm ve seviyenin yer alması sebebi ile daha küçük bir alanda çalışabilmek için düğümlerin sinyal güçleri %20 seviyesine indirilmiş ve antenleri Şekil 4.20 gösterildiği şekilde çıkarılmıştır.



Şekil 4.21. Düğümlerin topolojik gösterimi

ETX eksikliğini komşularına kendi maliyeti olarak duyurmuş ve trafiği çıkış deliği saldırısı ile üzerine almıştır. Fakat bu işlem, paketin ebeveyn tarafından bloke edilmesine neden olur. Çünkü yönlendirilecek paketlerin içerisindeki ETX değerinin ebeveynin rota maliyetinden yüksek olması gerekir. Bu nedenle de iletilecek paketin ETX alanına yazılacak değere rota maliyetinin 2 ETX fazlası eklenmiştir. Böylece saldırgan düğüm, paket trafiğini %50 oranında bloke ederek kalan paketlerin uygun ebeveyn üzerinden baz istasyonuna ulaşmasını amaçlar.

#### **4.3.1. Korumasız Bir Ağ İçin Saldırı Analizi**

Bu çalışma ile saldırı tespit ve yanıt sistemi olmayan bir ağda, saldırgan düğümün devreye girmesi ve devreden çıkması durumları için algılayıcı düğümden iletilen paket sayıları ile baz istasyonuna ulaşan toplam paket sayıları analiz edilmiştir. Çalışmada, baz istasyonundan başlanarak düğümler sırası ile aktif edilmiş ve topolojinin stabil hale gelmesi beklenmiştir. Daha sonra 5. seviyeye yerleştirilen saldırgan düğüm; ilk önce çıkış deliği + karadelik, daha sonra da çıkış deliği + seçici yönlendirme saldırıları gerçekleştirmiştir. Her saldırı belirli bir süre gerçekleştirildikten sonra saldırgan düğümün enerjisi kesilerek ağdan çıkarılmış ve topolojinin yeniden ne kadar süre sonra kararlı duruma gelerek baz istasyonuna veri iletmeye başladığı gözlemlenmiştir.

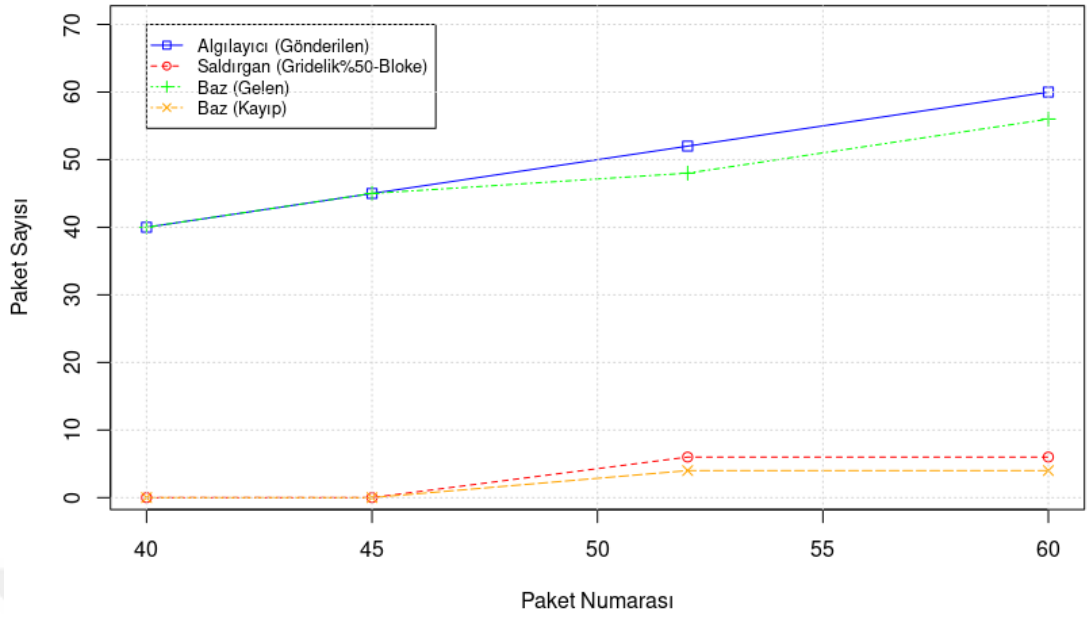
Şekil 4.23 ile verilen grafikte 75. paketin baza iletimi sırasında karadelik saldırısını düzenleyen saldırgan devreye alınmış ve 78. paket itibari ile saldırgan, ağ trafiğine dâhil olarak paketleri bloke etmeye başlamıştır. Uygulamada kullanılan düğümlerin tespit ve yanıt sistemi devre dışı bırakıldığı için düğümler, saldırganı ağdan çıkaramamıştır. 60 adet paketin saldırgan tarafından bloke edilmesinden sonra saldırgan düğümün enerjisi kesilmiştir. Saldırgan düğümü ebeveyn olarak kabul eden B2 düğümü bir süre daha saldırgan düğüme veri göndermeye çalışmış fakat alındı mesajlarını alamadığı için alternatif bir düğüm arayışına girmiştir.

Şekil 4.24 ile verilen grafikte ise savunmasız bir ağ içerisinde seçici yönlendirme saldırısı gerçekleştiren ve daha sonra devreden çıkan saldırgan bir düğüm için ağda gerçekleşen paket kaybı analiz edilmiştir. 5. seviyeye yerleştirilen saldırgan; 150. paketin baza iletilmesi ile birlikte devreye girmiş, 153. paket itibari ile de trafiği yönetmeye başlamıştır. Saldırı 100 adet paket için gerçekleştirilmiştir ve sonrasında saldırgan düğümün enerjisi kesilmiştir. Sonuçlara göre saldırgan düğümün paketlerin 50 adedinin baz istasyonuna yönlendirmesine izin verirken geri kalanını bloke etmiştir. Saldırganın enerjisinin kesilmesinin ardından B3 düğümü saldırgan düğüme paket gönderimine devam ederek alındı mesajı bilgisi alamadığı için rotayı değiştirmiştir. Bu süreç içerisinde bir adet paket kaybı daha gerçekleştirilmiştir. Baz istasyonunda gerçekleşen toplam paket kaybı 51 adettir. Saldırganın rota maliyetlerinin diğer düğüm maliyetlerine yakın olması sebebi ile ağda bir kararsızlık oluşmamış ve paket iletimi hızlıca olağan rotası üzerinden gerçekleşmeye devam etmiştir.

#### **4.3.2. PLOST ve PACKB Bileşenleri ile Koruma Altına Alınan Ağ İçin Performans Analizleri**

Bu test ortamında saldırı tespit ve yanıt sistemi aktif edilen düğümlerin; karadelik ve seçici yönlendirme saldırılarına karşı sistem performansları incelenmiştir. Çalışmada; “*Paket İzleme Sistemi*” ve “*Alındı Mesajı Takip Sistemi*” bileşenleri aktif edilmiştir.

Bu bölümde yapılan ilk çalışmada; karadelik saldırısı yapmak üzere programlanmış düğüm, Şekil 4.21 ile verilen topolojide 5. seviyeye yerleştirilmiştir. 65. paketin baz istasyonuna iletimi ile birlikte aktif edilen saldırgan, çıkış deliği saldırısına başlamış ve paket trafiğini üzerine almıştır. 67. paketten itibaren karadelik saldırısı gerçekleştiren saldırgan düğüm, ilk 3 adet paketi bloke ettiği anda komşu düğümler tarafından saldırgan olduğu tespit edildiğinden ceza değeri uygulanarak aktif rota dışına çıkarılmıştır. Algılayıcı düğümden gönderilen paket sayısı, baza ulaşan paket sayısı ve karadelik saldırısı tarafından bloke edilen paket sayısı Şekil 4.25 ile verilen grafikte gösterilmiştir.



Şekil 4.26. Saldırı tespit ve yanıt sistemi aktif edilmiş düğümlerde çıkış deliği + seçici yönlendirme saldırısının ağa etkisi

Saldırgan düğüm, çıkış deliği saldırısı ile trafiği üzerine alarak saldırıya 45. paket itibarı ile başlamıştır. %50 paket kaybı oranı ile gerçekleştirilen bu saldırıda, 3. paketin bloke edilmesi ile birlikte saldırı komşu düğümler tarafından tespit edilmiştir. Düğümün aktif iletişim rotasından dışlanması 52. paketin iletimi ile sağlanmıştır. Komşu düğümlerin; saldırgan düğüm dışında farklı bir ebeveyn seçmesi süreci, saldırganın rota maliyetinin 4. seviyedeki düğümlerle aynı olduğundan bu işlem sırasında fazladan bir paket kaybı yaşanmamıştır. Bu saldırı sırasında gerçekleşen toplam paket kaybı 3 adet olarak tespit edilmiştir.

Bu bölümde yapılan üçüncü çalışmada ise Şekil 4.21 ile verilen topolojideki farklı seviyelere yerleştirilen saldırganların ağ etkileri incelenmiştir. 2 ve 6. seviyeye farklı çalışma zamanları için yerleştirilen saldırgan düğümler karadelik ve seçici yönlendirme saldırıları gerçekleştirmiştir.

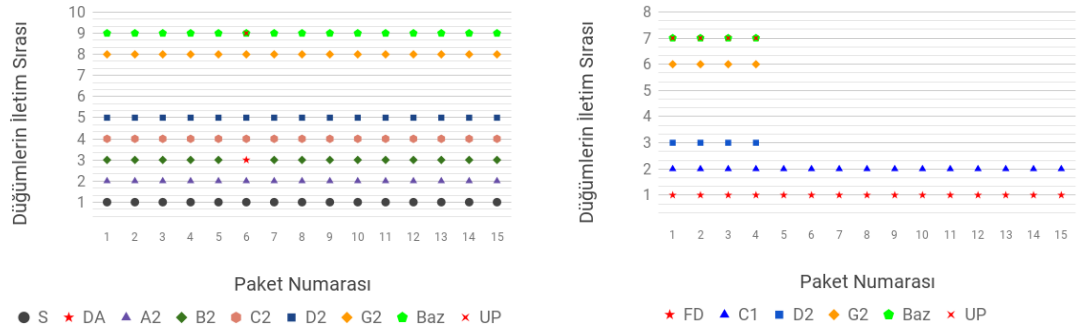
Yapılan çalışmalar göstermiştir ki, özellikle karadelik saldırısı olarak modellenen saldırının sabit bir seviye ve maliyet bilgisini komşu düğümlere duyurması, topolojinin alt seviyelerinde çok daha fazla düğümün rota maliyetlerinde değişikliğe yol açmıştır. Saldırgan düğümün tespit edilmesi sonrasında CTP algoritmasının yeni rota arayışı ve kararlı duruma geçmesi sırasında ek paket kaybı ortaya çıkmıştır. Çizelge 4.3 ile verilen tabloda 9-seviyeli topoloji için farklı sayıdaki saldırı düğümün PLOST ile PLOST+PACKB bileşenlerinin birlikte kullanımına ilişkin genel sonuçlar verilmiştir. Saldırgan düğümler, topolojinin merkezinden (ortası) başlayarak algılayıcı düğümün olduğu daha yüksek topoloji seviyelerine doğru yerleştirilmiştir. Her seviyede en az bir adet saldırı olmayan düğüm bulunmaktadır. Tabloda yer alan veriler saldırının başladığı ve tüm saldırı düğümlerin aktif rotadan çıkarıldığı ilk 100 pakete ilişkin istatistiklerdir. Saldırgan sayısının ağdaki miktarının artması ile birlikte ağdaki normal düğüm sayısı azalır.

Çizelge 4.3. PLOST ve PLOST+PACKB bileşenlerinin kullanımının 9-seviyeli topoloji için başarımları

| Yöntem      | Saldırı türü | Saldırgan sayısı | Düğüm sayısı | Paket iletim oranı |
|-------------|--------------|------------------|--------------|--------------------|
| SALDIRISIZ  | -            | -                | 23           | 0.97               |
| PLOST       | ÇD+KD        | 1                |              | 0.94               |
|             |              | 2                |              | 0.91               |
|             |              | 4                |              | 0.77               |
|             |              | 7                |              | 0.56               |
| PLOST+PACKB |              | 1                |              | 0.94               |
|             |              | 2                |              | 0.91               |
|             |              | 4                |              | 0.84               |
|             |              | 7                |              | 0.78               |

**Saldırı Türü:** Çıkış deliği (ÇD), Karadelik (KD)

Ayrıca saldırı tespitinden sonra kara listeye alınan saldırgan düğümden gelen paketler için alındı bilgisi yanıtı verilmez. Başarının ölçülmesi için baza ulaşan yabancı paket sayısı dikkate alınacaktır. Veri gönderimi 0.5 saniye aralıklarla gerçekleştirilmiştir.



(a) Veri değiştirme saldırısı

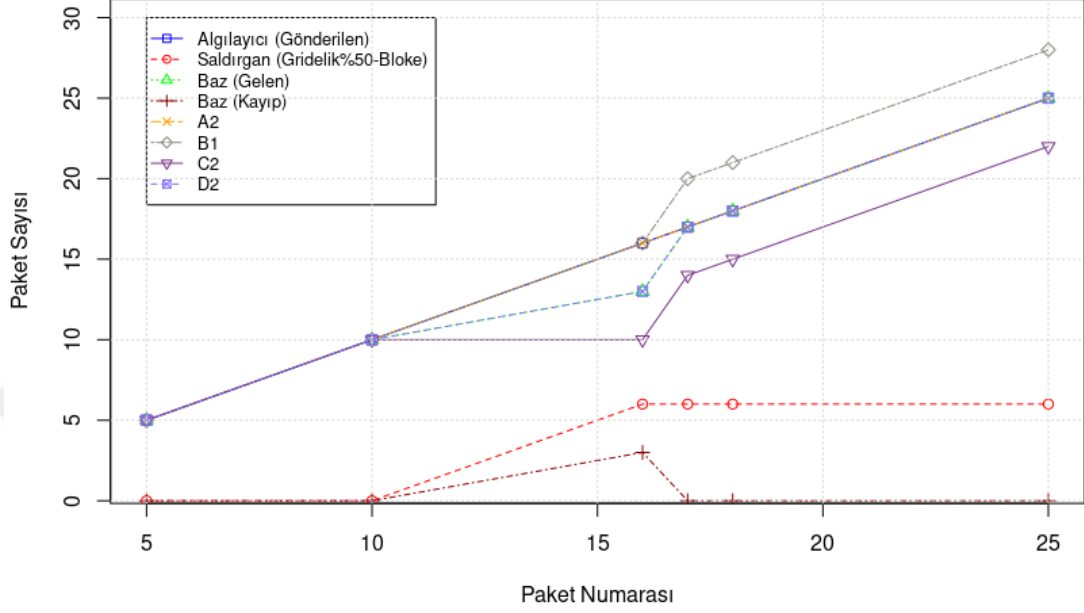
(b) Sel saldırısı

Şekil 4.28. Saldırlara karşı düğümlerin veri iletimi davranışları

Şekil 4.28 ile verilen grafiklerde veri değiştirme saldırısı (a) ve sel saldırısına (b) karşı düğümlerin vermiş olduğu yanıtlar görülebilmektedir. Grafiklerde verilmiş olan; “DA” olarak etiketlenen düğüm paket değişikliği gerçekleştiren saldırganı, “FD” ile etiketlenen düğüm sel saldırısı gerçekleştiren saldırganı ve “UP” ile etiketlenen veri ise istenmeyen paketleri temsil etmektedir.

Veri değiştirme saldırısı için saldırgan düğüm (DA); 4. paketin iletimi ile birlikte çıkış deliği saldırısına başlamış ve A2 düğümünden B2 düğümüne gelen trafiği üzerine almıştır. Şekil 4.28 (a) ile verilen grafikte de görüleceği üzere trafiği kendi üzerine alan saldırgan 6. paketin A2 düğümünden kendisine iletimi ile birlikte veri değişikliği gerçekleştirmiştir. Çıkış deliği saldırısının başarıya ulaşabilmesi için saldırgan, paket gönderimi gerçekleştirirken paket içerisinde yer alan rota maliyet bilgisini C2 düğümünden daha fazla olacak şekilde güncelleme yoluna gider. Değiştirilmiş paket sırasıyla C2 ve D2 düğümleri tarafından üst düğümlere iletilir ve baza ulaştırılır. Bu çalışmada, 6. ve 7. paket iletim sırasının hangi düğümler tarafından gerçekleştirildiği izlenmemiştir. Baza ulaşan veriler dikkate alındığında gelen paketin G2 düğümü üzerinden iletiliği görülmüştür. 6. paketin değiştirilerek iletilmesi 6. ve 7. seviye düğümleri tarafından algılanır ve saldırgan düğüme ceza değeri uygulanarak rota dışına

arkaya baz istasyonuna iletilmiştir. Saldırganın ağda etkilemiş olduğu cihaz sayısının sınırlı olması, ağda fazladan bir paket kaybına neden olmamıştır.



Şekil 4.29. Saldırı tespit ve yanıt sistemi ile birlikte aktif edilen akış onarım sisteminin çıkış deliği + seçici yönlendirme saldırısına etkisi

#### 4.4. Genel Değerlendirme ve Literatürdeki Benzer Çalışmalar

Yapılan çalışmalar kapsamında geliştirilen saldırı tespit ve yanıt sistemi bileşenlerinin farklı saldırı düğüm sayısı oranı ve saldırı modeli ile test edilmesi sonucu elde edilen performans özeti Çizelge 4.4 ile verilmiştir. Literatürde yapılan benzer çalışmalara ilişkin sonuçlar ise Çizelge 4.5 ile gösterilmiştir. Bu çalışmaların; test ortamı/donanımı, düğüm sayısı, saldırı modeli, kullanılan topoloji, yönlendirme algoritması, saldırıların topolojideki konumları gibi konularda farklılık gösteriyor olması, yapılan çalışmaların ancak yaklaşık olarak karşılaştırılmasına imkân sağlar.

Çizelge 4.5. Literatürdeki benzer çalışmalara ilişkin özet sonuçlar

| Literatür                                                           | Test ortamı | Saldırı türü | Saldırgan sayısı | Düğüm sayısı | Saldırganın düğüm sayısına oranı | Paket kaybı oranı | Paket iletim oranı |
|---------------------------------------------------------------------|-------------|--------------|------------------|--------------|----------------------------------|-------------------|--------------------|
| Midi ve ark. (2016)<br>* Zarar gören paketler yeniden iletilmiştir. | GZ          | SY%40        | 1                | 6x6          | 0.03                             | 0.0008            | -                  |
|                                                                     |             | ÇD+SY%20     |                  |              |                                  | 0.011             | -                  |
|                                                                     |             | ÇD+SY%20     |                  |              |                                  | 0.086             | -                  |
| Cui ve Yang (2014)<br>* Zarar gören paketler yeniden iletilmiştir.  | B           | SY%75        | 4                | 11x11        | 0.03                             | -                 | 1.00               |
|                                                                     |             | SY%50        | 6                |              | 0.05                             | -                 | 1.00               |
|                                                                     |             | SY%37.5      | 8                |              | 0.07                             | -                 | 0.99               |
|                                                                     |             | SY%30        | 10               |              | 0.08                             | -                 | 0.96               |
|                                                                     |             | SY%25        | 12               |              | 0.10                             | -                 | 0.95               |
| Cho ve Qu (2023)<br>* $TH=0.8$ , Hybrid                             | B           | SY%100 (KD)  | 1                | 50           | 0.02                             | -                 | 0.89               |
|                                                                     |             | SY%20        |                  |              |                                  | -                 | 0.96               |
|                                                                     |             | SY%60        |                  |              |                                  | -                 | 0.90               |

**Test Ortamı:** Gerçek zamanlı (GZ), Benzetim (B)

**Saldırı Türü:** Çıkış deliği (ÇD), Seçici yönlendirme (SY), Karadelik (KD)

Çizelge 4.5 ile verilen çizelgede, Midi ve ark. (2016) yaptıkları çalışmalara ait veriler ortalama 1500 veri paketi için elde ettikleri sonuçlara ilişkindir. Bu çalışmada ihlal sonucu hasar gören veri paketlerinin yeniden iletimi gerçekleştirilmiştir. Çalışmalarda saldırgan düğüm ve ebeveyn seçim süreçlerinden kaynaklı paket kayıplarının miktarı net olarak sunulmamıştır. Saldırının gerçekleşmesi ve saldırgan düğüme yapılan paket trafiğinin kesilmesinin ardından baza iletilemeyen paket sayıları dikkate alındığında elde edilen ortalama sonuçlar ( $\sim 0.049$ ) önerilen yöntem ile elde edilen sonuçlarla benzerlik

## 5. SONUÇ ve ÖNERİLER

Kablosuz iletişim teknolojileri, son yıllarda hızlı bir şekilde gelişen ve birçok alanda kablolu iletişimin yerini almaya başlamış önemli bir iletişim seçeneğidir. Kablosuz teknolojiler, daha önce kablolu iletişimde mümkün olmayan esneklik ve serbestliği sağlayarak cihazların birbirlerine bağlı kalmasını mümkün kılmaktadır. Kablosuz algılayıcılar, bu teknolojiyi kullanarak elde ettikleri hassas bilgilerin birbirleri üzerinden merkeze aktarılmasına olanak sağlayan bir teknolojidir. Özellikle gelişen ve küçük boyutlarda imal edilebilen gömülü sistem teknolojisi ile birlikte, çok düşük güçlerde çok uzun süreler işlev görecektir. Bu aygıtların yeni birçok alanda kullanılmaya başlanması bu teknolojilere olan talebi de artırmıştır. Fakat üretilen bu donanımların kısıtlı özelliklere sahip olması düşük üretim maliyetleri gibi avantajlara sahip olsa da kısıtlı işlem kapasiteleri karmaşık algoritmaların bu aygıtlarda işletilebilmesinin önündeki en büyük engel konumundadır. Özellikle bu aygıtların; kritik birçok görev için dış ortamda barındırılıyor olması, daha fazla tehdidin ortaya çıkmasına da neden olmaktadır. Tüm bu donanımsal kısıt ve riskler göz önüne alındığında uygulanabilir güvenlik algoritmalarının geliştirilmesi son derece önemlidir. Literatürdeki çalışmaların büyük bölümünün benzetim ortamında gerçekleştirilmiş olması, gerçek zamanlı test ortamlarından elde edilecek sonuçları önemli kılmaktadır. Çalışma kapsamında KAA'lar için CTP algoritması üzerinde gerçek zamanlı olarak uygulanabilir bir güvenlik sistemi önerisi sunulmuştur. Bileşen tabanlı gerçekleştirilen tasarımda, tasarım bileşenlerinin farklı topolojilerde ve saldırılardaki davranışları analiz edilmiştir.

Tez çalışması kapsamında;

1. Yönlendirme algoritması olarak kullanılan CTP'nin faydalarından yararlanan ve bu algoritmanın özelliklerini kullanarak onu daha güvenli bir algoritma konumuna getirmeyi hedefleyen komşu izleme tabanlı saldırı tespit ve yanıt sistemi geliştirilmiştir.
2. Geleneksel istatistiksel tabanlı paket izleme algoritmalarından farklı olarak düğümlerin aldıkları ve ilettikleri paketleri veri seviyesinde işler. Bu sayede

almaktadır. Bunun sonucu olarak paket kayıpları ortaya çıkabilmektedir. Geliştirilen tespit ve yanıt sistemi algoritması problemin etkilerini azaltıyor olsa da bu süreci daha iyi yöneten yönlendirme algoritmalarının verimi artıracığı söylenebilir. Önerilen sistem, düğümlerin kendi rotalarına karar verdiği ve paket iletişiminin tek bir rota üzerinden sağlandığı tüm yönlendirme protokolleri için kullanılabilir. Bu nedenle farklı yönlendirme protokollerinin bu sistemdeki saldırı performansları incelenebilir.

2. Önerilen saldırı tespit ve yanıt sistemi, bileşen tabanlı olarak tasarlanmıştır. Bu nedenle de daha fazla saldırıyı (sahte düğüm, solucan deliği saldırısı vb. gibi) algılayabilecek bileşenlerle sistemin desteklenmesi ve gerçek zamanlı donanımlara uygulanabilmesi mümkündür.
3. Önerilen saldırı tespit sisteminde, saldırı kararları için statik eşik değeri kullanılmıştır. Saldırının tespiti için saldırının eşik değerine ulaşacak kadar gerçekleştirmesi gerekir. Her ne kadar yanıt sistemi yeniden gönderim algoritması yürüterek etkileri azaltmaya çalışıyor olsa da bu süreci iyileştirmek için ağ dinamikleri ile orantılı bir eşik değeri kullanılabilir. Böylece daha az çaba ile sistemin çalışmasına ve performansın artmasına olanak sağlanacaktır.

- Cui, B., & Yang, S. J., 2014. NRE: Suppress Selective Forwarding attacks in Wireless Sensor Networks. **2014 IEEE Conference on Communications and Network Security**. <https://doi.org/10.1109/cns.2014.6997490>
- De Couto, D. S. J., Aguayo, D., Bicket, J., & Morris, R., 2003. A high-throughput path metric for multi-hop wireless routing. **MobiCom '03: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking**, 134–146. <https://doi.org/10.1145/938985.939000>
- Di Nuzzo, F., Brunelli, D., Polonelli, T., & Benini, L., 2021. Structural Health Monitoring System With Narrowband IoT and MEMS Sensors. **IEEE Sensors Journal**, 21(14), 16371–16380. <https://doi.org/10.1109/jsen.2021.3075093>
- Dunkels, A., Gronvall, B., & Voigt, T., 2004. Contikia lightweight and flexible operating system for tiny networked sensors. **29th Annual IEEE International Conference on Local Computer Networks**, 455–462. <https://doi.org/10.1109/LCN.2004.38>
- Edwards Murphy, F., Magno, M., Whelan, P., & Vici, E. P., 2015. b+WSN: Smart beehive for agriculture, environmental, and honey bee health monitoring — Preliminary results and analysis. **2015 IEEE Sensors Applications Symposium (SAS)**. <https://doi.org/10.1109/sas.2015.7133587>
- Fakhri, A. B., Sadik, K. G., Mohammed, S. L., & Zubaidi, Salah L., 2020. Measurement validation of patient vital signs monitoring system using wireless sensor network. **13th International Conference on Developments in ESystems Engineering (DeSE)**, 423–426. <https://doi.org/10.1109/DeSE51703.2020.9450765>
- Fonseca, R., Gnawali, O., Jamieson, K., Kim, S., Levis, P., & Woo, A., 2006. The collection tree protocol (CTP). **TinyOS TEP**, 123, Article 2.
- Fonseca, R., Gnawali, O., Jamieson, K., & Levis, P. A., 2007. Four-bit wireless link estimation. **HotNets**.
- Gay, D., Levis, P., von Behren, R., Welsh, M., Brewer, E., & Culler, D., 2003. The nesC language: : A holistic approach to networked embedded systems. **ACM SIGPLAN Notices**, 38(5), 1. <https://doi.org/10.1145/780822.781133>
- Ghugar, U., Pradhan, J., Bhoi, S. K., & Sahoo, R. R., 2019. LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system. **Journal of Computer Networks and Communications**, 2019(2054298), 1–13. <https://doi.org/10.1155/2019/2054298>
- Gnawali, O., Fonseca, R., Jamieson, K., Moss, D., & Levis, P., 2009. Collection tree protocol. **Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems**, 1–14. <https://doi.org/10.1145/1644038.1644040>
- Gogate, U., & Bakal, J., 2019. Refining healthcare monitoring system using wireless sensor networks based on key design parameters. In S. Chandra & A. Joshi (Eds.), **Information and Communication Technology for Intelligent Systems** (pp. 341–349). Springer Singapore. [https://doi.org/10.1007/978-981-13-1742-2\\_33](https://doi.org/10.1007/978-981-13-1742-2_33)
- Gunduz, M. Z., & Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. **Computer Networks**, 169(107094), 107094. <https://doi.org/10.1016/j.comnet.2019.107094>
- Gupta, S., Zheng, R., & Cheng, A. M. K., 2007. ANDES: an Anomaly Detection System for Wireless Sensor Networks. **2007 IEEE International Conference on**

- Luo, J., Chen, Y., Wu, M., & Yang, Y., 2021. A Survey of Routing Protocols for Underwater Wireless Sensor Networks. **IEEE Communications Surveys & Tutorials**, 23(1), 137–160. <https://doi.org/10.1109/comst.2020.3048190>
- Magana-Espinoza, P., Aquino-Santos, R., Cárdenas-Benítez, N., Aguilar-Velasco, J., Buenrostro-Segura, C., Edwards-Block, A., & Medina-Cass, A., 2014. WiSPH: A wireless sensor network-based home care monitoring system. **Sensors**, 14, 7096–7119. <https://doi.org/10.3390/s140407096>
- Markert, J., & Massoth, M., 2013. Honeypot framework for wireless sensor networks. **Proceedings of International Conference on Advances in Mobile Computing & Multimedia (MoMM '13)**, 217–223. <https://doi.org/10.1145/2536853.2536941>
- Mehetre, D. C., Roslin, S. E., & Wagh, S. J., 2018. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. **Cluster Computing**, 22(S1), 1313–1328. <https://doi.org/10.1007/s10586-017-1622-9>
- Memsic., 2010. Mote Processor Radio & Mote Interface Boards User Manual (Rev. A, Vols. 7430-002109). **Memsic Inc.**
- Merad Boudia, O. R., Senouci, S. M., & Feham, M., 2015. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. **Ad Hoc Networks**, 32, 98–113. <https://doi.org/10.1016/j.adhoc.2015.01.002>
- Midi, D., Sultana, S., & Bertino, E., 2016. A system for response and prevention of security incidents in wireless sensor networks. **ACM Transactions on Sensor Networks**, 13, Article 1. <https://doi.org/10.1145/2996195>
- Mir, A., & Khachane, A., 2018. Sensing Harmful Gases in Industries Using IOT and WSN. **2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)**. <https://doi.org/10.1109/iccubea.2018.8697380>
- Mohsin, A., & Yellampalli, S. S., 2017. IoT based cold chain logistics monitoring. **2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)**. <https://doi.org/10.1109/icpcsi.2017.8392059>
- Naz, P., Hengy, S., & Hamery, P., 2012. Soldier detection using unattended acoustic and seismic sensors. **SPIE Proceedings**. <https://doi.org/10.1117/12.920449>
- Ngai, H., Liu, J., & Lyu, M. R., 2006. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. **IEEE International Conference on Communications**, 8, 3383–3389. <https://doi.org/10.1109/ICC.2006.255595>
- Oflazoglu, Ç., & Abasikeles Turgut, İ., 2020. Gerçek-Zamanlı Kablosuz Algılayıcı Ağlarda Toplama Ağacı Protokolünün Yönlendirme Saldırılarına Karşı Dayanıklılığının Analizi ve Saldırı Tespit Sistemi Tasarımı. **Academic Platform Journal of Engineering and Science**, 8(2), 249–257. <https://doi.org/10.21541/apjes.617854>
- Ogundile, O., & Alfa, A., 2017. A Survey on an Energy-Efficient and Energy-Balanced Routing Protocol for Wireless Sensor Networks. **Sensors**, 17(5), 1084. <https://doi.org/10.3390/s17051084>
- Panatik, K. Z., Kamardin, K., Shariff, S. A., Yuhani, S. S., Ahmad, N. A., Yusop, O. M., & Ismail, S., 2016. Energy harvesting in wireless sensor networks: A survey. **2016 IEEE 3rd International Symposium on Telecommunication Technologies (ISTT)**. <https://doi.org/10.1109/istt.2016.7918084>

Zhou, Y., Fang, Y., & Zhang, Y., 2008. Securing wireless sensor networks: a survey. **IEEE Communications Surveys & Tutorials**, 10(3), 6–28. <https://doi.org/10.1109/comst.2008.4625802>

