İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ SENSÖR AĞLARINDA VERİMLİ KİMLİK DOĞRULAMA METODU TASARIMI VE UYGULAMASI

a

YÜKSEK LİSANS TEZİ

MEHMET BAYAR

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Temmuz 2022

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ SENSÖR AĞLARINDA VERİMLİ KİMLİK DOĞRULAMA METODU TASARIMI VE UYGULAMASI
a

YÜKSEK LİSANS TEZİ

MEHMET BAYAR
(504171279)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Sıddıka Berna Örs YALÇIN

Temmuz 2022

İTÜ, Fen Bilimleri Enstitüsü'nün 504171279 numaralı Yüksek Lisans öğrencisi MEHMET BAYAR, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "KABLOSUZ SENSÖR AĞLARINDA VERİMLİ KİMLİK DOĞRULAMA METODU TASARIMI VE UYGULAMASI a" başlıklı tezini aşağıdaki imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Sıddıka Berna Örs YALÇIN** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Sıddıka Berna Örs YALÇIN** İstanbul Teknik Üniversitesi	.....
	Doç. Dr. Şerif BAHTİYAR İstanbul Teknik Üniversitesi	.....
	Doç. Dr. Ali Emre PUSANE Boğaziçi Üniversitesi	.....

Teslim Tarihi : **3 Haziran 2022**
Savunma Tarihi : **19 Temmuz 2022**

Eşime,

ÖNSÖZ

Başta çalışmalarımda danışmanlığımı üstlenen, tecrübelerini paylaşan ve desteğini hiçbir zaman esirgemeyen değerli hocam Prof. Dr. Sıddıka Berna Örs YALÇIN'a,

Her zaman yanımda olan ve tüm zorluklara karşı beraber göğüs gerdiğim Elif Yürekli BAYAR'a, bizleri yetiştirip bugünlere gelmemiz için her türlü fedakarlığı yapan annelerim Naciye BAYAR ve Songül YÜREKLİ'ye, babalarım Hüseyin BAYAR ve Ziya YÜREKLİ'ye, ablam Burcu KOZ'a, enişte Halil KOZ'a ve kardeşlerim Emel, Pınar, Gökhan, Yasemin'e,

Ailem gibi sevdiğim tüm dostlarıma ve çalışma arkadaşlarıma,

Son olarak Aselsan Akademi programı ile eğitim süresince her konuda yardımcı olan işverenim ASELSAN A.Ş'ye,

Sevgi, saygı ve minnetlerimi sunar ve teşekkür ederim.

Temmuz 2022

MEHMET BAYAR
(Elektronik ve Haberleşme Mühendisi)

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **vii**
İÇİNDEKİLER ..... **ix**
KISALTMALAR ..... **xi**
ÇİZELGE LİSTESİ ..... **xiii**
ŞEKİL LİSTESİ ..... **xv**
ÖZET ..... **xvii**
SUMMARY ..... **xix**
1. GİRİŞ **1**
1.1 Tezin Akışı 2
2. TEKNİK ARAŞTIRMALAR VE GELİŞTİRME ORTAMI **5**
2.1 Düşük Güçlü Kablosuz Sensör Ağları 5
2.1.1 Kullanım Alanları 5
2.1.1.1 Çevre Ölçümü 5
2.1.1.2 Sağlık Takibi 6
2.1.1.3 Akıllı Evler 7
2.1.1.4 Askeri Uygulamalar 7
2.1.2 Ağın Yapısı 8
2.1.2.1 Trafik Modelleri 10
2.1.2.2 Kablosuz Ağ Oluşturma 11
2.1.2.3 Kablosuz Ağlarda Yönlendirme 13
2.1.3 Kablosuz Sensör Ağları Yönlendirme Protokolleri 14
2.1.3.1 Yönlendirme Protokollerinin Standartlaşması 15
2.1.3.2 RPL 16
2.1.3.3 6LowPAN 16
2.2 Kablosuz Sensör Ağları Protokol Katmanları 17
2.2.1 Fiziksel Katman 17
2.2.2 Medya Erişim Katmanı 18
2.2.3 Uyumlandırma Katmanı 19
2.2.4 Ağ Katmanı 19
2.2.5 Ulaşım Katmanı 20
2.2.6 Uygulama Katmanı 20
2.3 Kriptografi 20
2.3.1 Simetrik Kriptografi 20
2.3.2 AES 21
2.3.3 Asimetrik Kriptografi 21
2.3.4 RSA 22
2.3.5 Eliptik Eğri Kriptografisi 22
2.3.6 Hibrit Kriptografi 24

2.4 Geliştirme Ortamı ... 24
2.4.1 Contiki ... 24
2.4.2 Cooja ... 25
3. RPL YÖNLENDİRME PROTOKOLÜ ... 29
3.1 Ağ Topolojisi ... 29
3.1.1 Yukarı Yönlü Yönlendirme ... 30
3.1.2 Aşağı Yönlü Yönlendirme ... 31
3.2 Yönlendirme Metrikleri ... 31
3.2.1 Minimum Hop Sayısı ... 31
3.2.2 Beklenen Gönderim Sayısı ... 31
3.2.3 Enerji ... 31
3.3 RPL Kontrol Mesajları ... 32
3.3.1 DIO ... 33
3.3.2 DIS ... 34
3.3.3 DAO ... 34
3.3.4 DAO-ACK ... 35
3.4 Görev Fonksiyonu ... 36
3.5 Trickle Zamanlayıcısı ... 36
3.6 DODAG Oluşumu ... 37
4. KABLOSUZ SENSÖR AĞLARINDA GÜVENLİK VE GELİŞTİRİLMİŞ YÖNTEMLER ... 41
4.1 Kablosuz Sensör Ağlarında Güvenlik ... 41
4.1.1 Mesaj Gizliliği ... 41
4.1.2 Mesaj Bütünlüğü ... 41
4.1.3 Mesaj Kullanılabilirliği ... 42
4.1.4 Kimlik Doğrulama ... 42
4.1.5 Karşılıklı Kimlik Doğrulama ... 43
4.1.6 Mesaj Güncelliği ... 43
4.1.7 İleri ve Geri Yönlü Gizlilik ... 43
4.2 RPL Güvenlik Mekanizmaları ... 44
4.2.1 RPL Güvenli Mesajlar ... 46
4.3 RPL Güvenli Ağa Katılma ... 50
4.3.1 Önyüklü Modda Güvenli Ağa Katılma ... 50
4.3.2 Kimliği Doğrulanmış Modda Güvenli Ağa Katılma ... 50
4.3.2.1 Yaprak Olarak Katılma ... 51
4.3.2.2 Yönlendirici Olarak Katılma ... 51
4.4 LİTERATÜR ARAŞTIRMALARI ... 52
5. KİMLİK DOĞRULAMA MODU İÇİN GELİŞTİRİLEN ANAHTAR YÖNETİMİ METODU ... 59
5.1 Geliştirilen Anahtar Yönetimi Metodu ... 60
5.2 Ağa Katılma Süreci ... 63
5.3 Simülasyon Çalışmaları ... 67
5.3.1 Performans Metrikleri ... 69
5.4 Simülasyon Sonuçları ... 70
6. SONUÇLAR VE GELECEK ÇALIŞMALAR ... 73
KAYNAKLAR ... 75
ÖZGEÇMİŞ ... 83

KISALTMALAR

6LowPAN : IPv6 over Lowpower Wireless Personal Area Network
AES : Advanced Encryption Standart
DAG : Directed Acyclic Graph
DODAG : Destination-Oriented DAG
DIS : DODAG Information Solicitation
DIO : DODAG Information Object
DAO : Destination Advertisement Object
DAO-ACK : Destination Advertisement Object Acknowledge
ECC : Elliptic Curve Cryptography
RSA : Rivest Shamir Adleman
ICMPv6 : Internet Control Message Protocol Version 6
IETF : Internet Engineering Task Force
ROLL : Routing Over Low-power and Lossy Networks
SPIN : Sensor Protocols for Information Negotiation
OLSR : Optimized Link State Routing
FSK : Frequency Shift Keying
IP : Internet Protocol
IPv6 : Internet Protocol Version 6
RPL : Routing Protocol for Low Power and Lossy Networks
CoAP : Constrained Application Protocol
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
KSA : Kablosuz Sensör Ağları
WSN : Wireless Sensor Network
ROLL : Routing Over Low-power and Lossy Networks
OSI : Open Systems Interconnection
OF0 : Objective Function 0
MQTT : Message Queuing Telemetry Transport

ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1 : AES uygulamalarında anahtar ve blok uzunlukları **21**
Çizelge 4.1 : Geliştirilen Kimlik Doğrulama Metotları **54**
Çizelge 4.2 : Geliştilmiş Metotların Güvenlik Özellikleri Karşılaştırması **58**
Çizelge 5.1 : Anahtar yönetimi metotunda kullanılan terimlerin notasyonu ve açıklamaları **61**

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1 : Sıcaklık ve nem değerleri gerçek zamanlı ölçülen bir dağ [16] **6**
Şekil 2.2 : Kablosuz sensör ağlarının hasta takibi için kullanımı [23] **7**
Şekil 2.3 : Kablosuz sensör ağlarının askeri uygulamarda kullanımı [33] **8**
Şekil 2.4 : Bir noktadan bir noktaya iletişim **10**
Şekil 2.5 : Çok noktadan bir noktaya iletişim **11**
Şekil 2.6 : Bir noktadan çok noktaya iletişim **11**
Şekil 2.7 : Ethernet ağının yapısı **12**
Şekil 2.8 : Geçirgen olmayan kablosuz ağ yapısı **12**
Şekil 2.9 : Asimetrik yapıdaki kablosuz ağ **13**
Şekil 2.10 : Kablosuz sensör ağları ve TCP/IP için OSI katmanları **17**
Şekil 2.11 : 802.15.4 fiziksel katmanının çeşitleri [7] **18**
Şekil 2.12 : 802.15.4 fiziksel katmanında kullanılan kanallar [7] **18**
Şekil 2.13 : Simetrik Şifreleme [78] **21**
Şekil 2.14 : Asimetrik Şifreleme [78] **22**
Şekil 2.15 : ECC ve RSA anahtar uzunlukları **23**
Şekil 2.16 : ECC ve RSA enerji tüketimleri **24**
Şekil 2.17 : Cooja üzerinde çalışan veri toplama simülasyonu **26**
Şekil 2.18 : Cooja üzerinde incelenen kablosuz iletişimler **27**
Şekil 3.1 : Ağaç yapısı **30**
Şekil 3.2 : RPL kontrol mesajı [5] **32**
Şekil 3.3 : DIO mesajının yapısı [5] **33**
Şekil 3.4 : DIS mesajının yapısı [5] **34**
Şekil 3.5 : DAO mesajının yapısı [5] **35**
Şekil 3.6 : DAO-ACK mesajının yapısı [5] **35**
Şekil 3.7a : *Kök düğümü DIO mesajını gönderir* **39**
Şekil 3.7b : *DIO mesajını alan düğümler ebeveyn seçtikten sonra kendi DIO mesajlarını gönderir* **39**
Şekil 3.7c : *Bütün düğümler DODAG'a katılıncaya kadar DIO mesajları gönderilir* **39**
Şekil 3.7d : *Bütün düğümler DODAG'a katılmıştır* **39**
Şekil 3.7 : DODAG oluşum süreci. Çizikli oklar DIO mesajlarını gösterirken, tam oklar tercih edilen ebeveyn seçimlerini göstermektedir. **39**
Şekil 4.1 : AES-128 CTR ile CCM **44**
Şekil 4.2 : AES-128 CBC-MAC ile CCM **44**
Şekil 4.3 : Güvenli RPL kontrol mesajı [5] **46**
Şekil 4.4 : Security alanı [5] **47**
Şekil 4.5 : KIM tablosu [5] **48**
Şekil 4.6 : KIM değerine bağlı LVL Değerleri [5] **49**

Şekil 4.7 : Anahtar Belirleme Alanı [5] **49**
Şekil 4.8 : DODAG Yapılandırma Opsiyonu [5]..... **51**
Şekil 4.9 : Düşük Maliyetli Yöntemlerin Sınıflandırılması **57**
Şekil 5.1 : RPL Kimlik Doğrulama Modu Modeli..... **62**
Şekil 5.2 : Düğümlerin Kimlik Doğrulama ve İkinci Grup Anahtarını Alma Metotu **64**
Şekil 5.3 : Düğümlerin Alınan Kontrol Mesajlarını İşleme Süreci **66**
Şekil 5.4 : Yaprak düğümden yönlendirici düğüme geçiş süreci **67**
Şekil 5.5 : Kök düğümün ağ katılım listesinde olmayan düğümlere cevabı **68**
Şekil 5.6 : Düğümlerin Ortalama Ağ Kurulum Süresi **70**
Şekil 5.7 : Düğümlerin Ortalama Enerji Tüketimleri..... **71**
Şekil 5.8 : Düğümlerin Ortalama Mesaj Yükü..... **72**

KABLOSUZ SENSÖR AĞLARINDA VERİMLİ KİMLİK DOĞRULAMA METODU TASARIMI VE UYGULAMASI
a

ÖZET

Kablosuz sensör ağları teknolojilerinin gelişmesiyle birlikte uygulama alanları da hızlı bir şekilde artmaktadır. Kablosuz sensör ağlarında yer alan cihazlar kısıtlı işlem gücü, bellek alanı ve pil ömrüne sahiptir. Bütün bu kısıtlamalarla birlikte bu cihazları standart internet ağına bağlamak için çalışmalar yapılması planlanmıştır. Bu amaçla IETF (İnternet Mühendisliği Görev Grubu) grubu 6LowPAN (Düşük Güçlü Kişisel Alan Ağları Üzerinde IPv6) adında özelleştirilmiş uyumlandırma katmanı geliştirmiştir. Geliştirilen bu katmanla beraber her cihazın kendine ait bir IPv6 adresine sahiptir ve bu adres ile standart internet ağına bağlantı sağlanmıştır. Aynı çalışma grubu IPv6 ile uyumlu RPL (Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü) yönlendirme protokolünü de geliştirmiştir.

Tez kapsamında yapılan çalışma RPL protokolünün temel eksiklerinden birisi olan güvenliği ele almaktadır. Kablosuz sensör ağlarındaki güvenliği sağlayabilmek için ağın dış ve iç kaynaklı ataklara karşı direncinin artırılması gerekmektedir. Tez kapsamında RPL protokolünün tanımladığı güvenlik modlarından biri olan kimlik doğrulama modu kullanılarak yeni bir anahtar yönetim metotu geliştirilmiştir. Anahtar yönetim metotu RPL standart dökümanında geliştirilmeye açık bir alan olarak belirtilmiştir. Geliştirilen metotta ECC (Eliptik Eğri Kriptografisi) ve AES (Gelişmiş Şifreleme Standartı) şifreleme yöntemleri kullanılmıştır. Ağa katılacak cihazlar anahtar isteği mesajı gönderir ve koşullar uygunsa anahtar sunucusundan anahtar cevap mesajı ile ağda kullanılacak ikinci grup anahtarını alır. Anahtar isteme mesajı ve anahtar cevap mesajlarında ECC ile şifreleme ve şifre çözme işlemi gerçekleştirilmiştir. Karşılıklı kimlik doğrulamayı sağlayabilmek için anahtar cevap alındı mesajı anahtar sunucusuna gönderilir ve süreç tamamlanmaktadır. Bu mesaj simetrik kriptografi metotlarından biri olan AES ile şifrelenmektedir. Simetrik kriptografi metodları, ECC gibi asimetrik kriptografi metodlarına göre oldukça hızlıdır. Ağda oluşabilecek Man-in-the-Middle (Ortadaki Adam) ataklarına karşı önlem alınmıştır. Ayrıca ağda ikinci grup anahtarına sahip olmayan cihazlar ağdaki paketlerin şifresini çözemeyeceğinden ağ parametrelerine erişemeyecektir. Ağda yer alan bütün cihazlar geliştirilen anahtar yönetim metodu ile güvenli ağa katılım sağlar ve bu evreden sonra güvenli kontrol mesajlaşması gönderilerek ağın güvenliği artırılmaya çalışılmıştır. Bu çalışmalar RPL standartlarına uygun olarak yapılmıştır.

Geliştirilen anahtar yönetim metotu ve RPL kimlik doğrulama modunun uygulanması için gerçeklenmiş kablosuz sensör ağı işletim sistemine ihtiyaç duyulmuştur. Linux

kernel, TinyOS ve Contiki işletim sistemleri incelenmiştir. Linux kernel çok fazla belleğe ihtiyaç duymaktadır ve incelenen diğer işletim sistemlerine göre daha fazla enerji tüketmektedir. TinyOS ve Contiki kablosuz sensör ağlarında düşük güç tüketimli ve az bellek kullanan işletim sistemleridir. TinyOS NesC dilinde, Contiki ise C programlama dilinde yazılmıştır. C dilinin kullanılması, modüler yazılım mimarisi ve akademik çalışmalarda sıkça kullanılması nedeniyle yapılan tez çalışmasında Contiki işletim sistemi tercih edilmiştir. Ayrıca geliştirilen anahtar yönetimi metodunun ağ kurulum zamanına ve ağdaki düğümlerin enerji tüketimine etkisi gibi performans analizleri Cooja simulatörü kullanılarak yapılmıştır. Cooja Java dilinde yazılmış bir simülatördür. Simülatörde gerçeğe yakın sonuçlar alabilmek için Wismote cihazı kullanılmıştır.

Anahtar Kelimeler: RPL, Kablosuz Sensör Ağları, 6LowPAN, ECC, Anahtar Yönetimi, Kimlik Doğrulama, Güvenlik, Contiki, Cooja

Design An Efficient Authentication Scheme for WSN
a
a

SUMMARY

IoT systems have become increasingly popular lately. These systems consist of a combination of wireless sensor networks (WSN). Devices in wireless sensor networks have low processing power, memory space, and battery life. With all the restrictions, these devices had to be able to connect to the standard internet network. For this reason, a special adaptation layer and routing protocol needs to be developed. The IETF (Internet Engineering Task Group) group has started to work on solving these problems, and as a result of the work, it has come up with an adaptation layer called 6LowPAN (IPv6 over Low Power Wireless Personal Area Network). With this layer, each device in the network has its own IPv6 address and can be connected to the standard internet network with this address. This working group also developed a routing protocol called RPL (Routing protocol in low-power and lossy networks) compatible with the IPv6 protocol.

In order to ensure the reliability of WSNs, it is of great importance to increase the resistance of wireless networks to attacks. This thesis study covers the implementation of authentication mode, which is one of the security modes defined in the RPL protocol and design an efficient key management method. Key management methods are not specified in RPL standard document and that methods may vary depend on application. The key exchange procedure performed with ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption Standard) encryption methods. Any node will send a key request message to join the network. If all conditions are suitable, nodes will receive the key response message from the key server which contains the second group key to be used in the network. Encryption and decryption processes are performed with ECC in key request and key response messages. A key response acknowledgment message is sent to the key server for mutual authentication and the key management process is completed. This message is encrypted with AES, one of the symmetric cryptography methods. Symmetric cryptography methods are much faster than asymmetric cryptography methods such as ECC. In authenticated security mode, it provides security against man-in-the-middle attacks that may occur on the network. Also, any node in the network without the second group key can not decrypt network packets and they can not get network parameters. Every node in the network has joined the network with developed key management method. Secure control messages will be sent after the join phase. By using all these methods, the security of the network has been tried to be increased. These studies were carried out in accordance with RPL standards.

There is a need for operating system for implementation of the developed key management method and RPL authentication mode. Linux kernel, TinyOS and Contiki operating systems are examined. Linux kernel needs a lot of memory and consumes more energy than other operating systems examined. TinyOS and Contiki are operating systems with low power consumption and less memory in wireless sensor networks. TinyOS is written in NesC language while Contiki is written in C programming language. Contiki operating system was preferred in the thesis study due to the use of C language, modular software architecture and frequent use in academic studies. In addition, performance analyzes like network setup time and the energy consumption of the nodes in the network were made using the Cooja simulator. Cooja is a simulator written in Java. Wismote device was used to get realistic results in the simulator.

Keywords: RPL, Wireless Sensor Networks, 6LowPAN, ECC, Key Management, Authentication, Security, Contiki, Cooja

1. GİRİŞ

Kablosuz sensör ağları çok sayıda düğümün bir araya gelmesinden oluşur. Teknolojinin gelişmesi ile birlikte bu ağların kullanım alanı oldukça artmıştır. Çevre ölçümü, ortam izleme ve takibi, askeri, sağlık, ev otomasyonu alanlarında kullanımı oldukça yaygınlaşmaktadır. Ağda yer alan düğümler kısıtlı enerji, işlem gücü ve bellek kaynaklarına sahiptir. Kablosuz sensör ağları pille çalışan ve coğrafi olarak geniş alanlara yerleştirildiğinden tek tek pil değişimi mümkün olmamaktadır ve enerjisi tükenen düğüm devre dışı kalmaktadır. Kablosuz sensör ağlar için en önemli parametrelerden biri mesajların ne kadar verimli bir şekilde gönderildiğidir. Bunu sağlayabilmek için mesaj en az sayıda düğüm üzerinden iletilmelidir ve seçilen en verimli yol bu yol olmalıdır. Kablosuz sensör ağlarında iletilecek mesajlar için uygun yol kullanılacak yolun belirlenmesi amacıyla çok sayıda yönlendirme protokolü geliştirilmiştir. Bunlardan bazıları AODV [40], OLSR [41], SPIN [43], LEACH [44] gibi protokollerdir. Ancak bu yönlendirme protokollerinin patentli olması olması ve protokollerin sadece belirli uygulamalara özgü olması nedeniyle kablosuz sensör ağlarında kullanımı yaygın değildir. Kablosuz sensör ağlarının standartlaştırılması bir zorunluluk haline gelmiştir. *IETF (İnternet Mühendisliği Görev Grubu)* [1] *ROLL (Düşük Güçlü ve Kayıplı Ağlar Üzerinde Yönlendirme)* [2] ve *6LowPAN (Düşük Güçlü Kişisel Alan Ağları Üzerinde IPv6)* [3] adı altında 2 çalışma grubu kurarak kablosuz sensör ağlarında kullanılacak yönlendirme protokolü ve IPv6 adaptasyon yapısı oluşturmuştur. IPv6 tabanlı yönlendirme protokolü olan *RPL (Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü)* [5] bu çalışmanların sonucu olarak geliştirilmiştir ve RFC6550 numarası ile internet standartlarına eklenmiştir. RPL protokolü ağ içerisindeki aşağı ve yukarı yönlü yönlendirme tablolarını verimli bir şekilde oluşturup ağın sürekliliği sağlamaktadır.

Bu tez kapsamında RPL kimlik doğrulama modu için verimli bir anahtar yönetimi metotu geliştirilmiştir. Bu geliştirmeler yapılırken standart RPL mesaj yapısı değiştirilmememiştir. Ağa yeni katılacak düğüm ikinci grup anahtarını almak için

anahtar isteği gönderir ve eğer anahtar sunucusunda tanımlı bir düğümse anahtar cevap mesajı ile ikinci grup anahtarını alır. Ayrıca karşılıklı kimlik doğrulama için anahtar cevap alındı mesajı anahtar sunucusuna gönderilir. Anahtar istek ve anahtar cevap mesajlarının şifreleme işlemi asimetrik kriptografi yöntemlerinden biri olan ECC ile gerçekleşir. Anahtar cevap alındı mesajı ise simetrik kriptografi yöntemlerinden biri olan AES şifrelemesini kullanır. Böylece üç mesaj kullanılarak karşılıklı kimlik doğrulama işlemleri tamamlanmış olur. Ayrıca Man-in-the-middle (Ortadaki Adam) ataklarına karşı önlem alınmış olur. Düğümlerin güvenli ağa katılma süresi ve bununla birlikte enerji tüketimi artacaktır. Bu süreyi minimum tutmak için geliştirilen üç mesajlı yapı tercih edilmiştir. Güvenli ağ sayesinde anahtar sunucusunda tanımlı olmayan düğümler ağa katılamayacaktır ve ağ ile parametreler kötü niyetli dış kaynaklı düğümler tarafından elde edilemeyecektir.

Geliştirilen anahtar yönetimi metodu kablosuz sensör ağlarında sıkça kullanılan Contiki [9] işletim sistemini kullanarak gerçeklenmiştir. Kablosuz sensör ağlarında yer alan kısıtlar düşünülerek az kaynak tüketen ECC kütüphanesi Contiki yazılım paketine eklenmiştir. Contiki işletim sisteminde yer alan Cooja [10] simülatörü ile geliştirilen yöntem test edilmiş ve performans analizleri yapılmıştır. Düğümler güvenli ağa katılma evresinden sonra önyüklü modda çalışmaya devam ettiğinden enerji tüketimleri önyüklü moda oldukça yakındır ve uzun süreli kullanımlarda oldukça avantajlıdır.

1.1 Tezin Akışı

Bölüm 2'de tezin kapsamının anlaşılır olması için gerekli temel bilgiler anlatılacaktır. Bu temel bilgilerden ilk olarak kablosuz sensör ağlarının tanımına ve kullanım alanlarına değinilecektir. Devamında kablosuz sensör ağlarında kullanılan trafik modelleri ve ağ yapısının nasıl oluştuğu anlatılacaktır. Tez dahilinde kullanılan standart protokollere değinilecek ve kablosuz sensör ağlarında kullanılan protokol katmanları ve bu katmanın standart katmanlarla olan farkı anlatılacaktır. Ardından kablosuz sensör ağlarında kullanılan kriptografik şifreleme metotları anlatılacaktır. Bu bölümde son olarak tezde kullanılan geliştirme ve test ortamı gösterilecektir.

Bölüm 3'te ise kimlik doğrulama metodu desteği eklenecek olan protokolün yapısı anlatılacaktır. Bu protokolün kullandığı ağ yapısı çeşitleri, ağı oluşturmak için gereken kontrol mesajları ve mesajların ağda yer alan düğümler arasında iletilmesi için gerekli yönlendirmelerin hangi metriklere göre yapıldığı detaylı bir şekilde incelenecektir.

Takip eden Bölüm 4'te kablosuz sensör ağlarında güvenliği sağlamak için gereken gereksinimler anlatılacaktır. Güvenli ağın tanımı yapılacaktır. Ardından yönlendirme protokolüne ait modlardan detaylı olarak bahsedilecek ve bu modlara ait kontrol mesajları anlatılacaktır. Literatürde güvenli ağa katılma ve anahtar yönetimi ile ilgili geliştirilmiş kimlik doğrulama metotları incelenecektir. Bu metotları uygulamak için hangi kriptografik yöntemlerin kullanıldığı, avantajları ve dezavantajları belirtilecektir.

Bölüm 5'te tezin şimdiye kadar değindiği ağ yapıları ve kısıtlamaları göz önünde bulundurularak kimlik doğrulama modu için geliştirilen anahtar yönetimi metotu anlatılacaktır. Ağa güvenli olarak katılmak için geliştirilen metotun ağa katılım evresinin detayları ve bunu gerçekleştirmek için geliştirilen yeni mesajlar gösterilecektir. Ayrıca geliştirilen anahtar yönetimi metotunun simülasyon ortamında incelenmesi ve bu metotun performans analiz sonuçları yer alacaktır. Yönlendirme protokolünün diğer güvenlik modları ile performans metriklerinin karşılaştırması yapılacaktır.

Son olarak sonuç ve gelecek çalışmalar bölümü olan Bölüm 6'da simülasyon ortamında geliştirilen anahtar yönetimi metotunun performans analiz sonuçlarının değerlendirmesi yer alacaktır. Bunlara ek olarak geliştirilen anahtar yönetimi metotunun geliştirilebilir yönlerine değinilecek ve bunların hangi yöntemlerle yapılabileceğine ve gelecek çalışmalara dair öneriler sunulacaktır.

2. TEKNİK ARAŞTIRMALAR VE GELİŞTİRME ORTAMI

2.1 Düşük Güçlü Kablosuz Sensör Ağları

KSA'lar uygulama ve araştırma alanlarında yeni alanlara öncü olmuştur [11]. Farklı alanlarda yapılan geliştirmelerle yeni algoritmalar üretilmektedir. Teknolojinin de gelişmesiyle beraber bu algoritmalar yeni kullanım alanlarında kullanılmıştır. Farklı alanlarda kullanımından dolayı KSA'ların karakteristik özelliği oldukça değişebilmektedir. Fakat bu farklı özelliklerin içinde ortak özelliklerde yer almaktadır. KSA'lar rastgele dağılmış, çok sayıda küçük sensör düğümlerinden oluşur. Bu düğümler kaynak bakımından kısıtlıdır ve birbirleriyle düşük güçlü kablosuz iletişim ortamında haberleşir. Enerji, depolama alanı, işlem gücü ve hafıza gibi kısıtları bulunmaktadır. Kısıtlamalardan dolayı KSA'larda yer alan cihazlar çoklu atlamalı ağ kurabilmek için mesajları birden fazla cihaza gönderir. Böylece geniş kapsama ağı kurulmuş olur. Ayrıca enerji tüketimini azaltmak için düğümler ile kök düğüm arasında direkt iletişim kurulmasından kaçınılır.

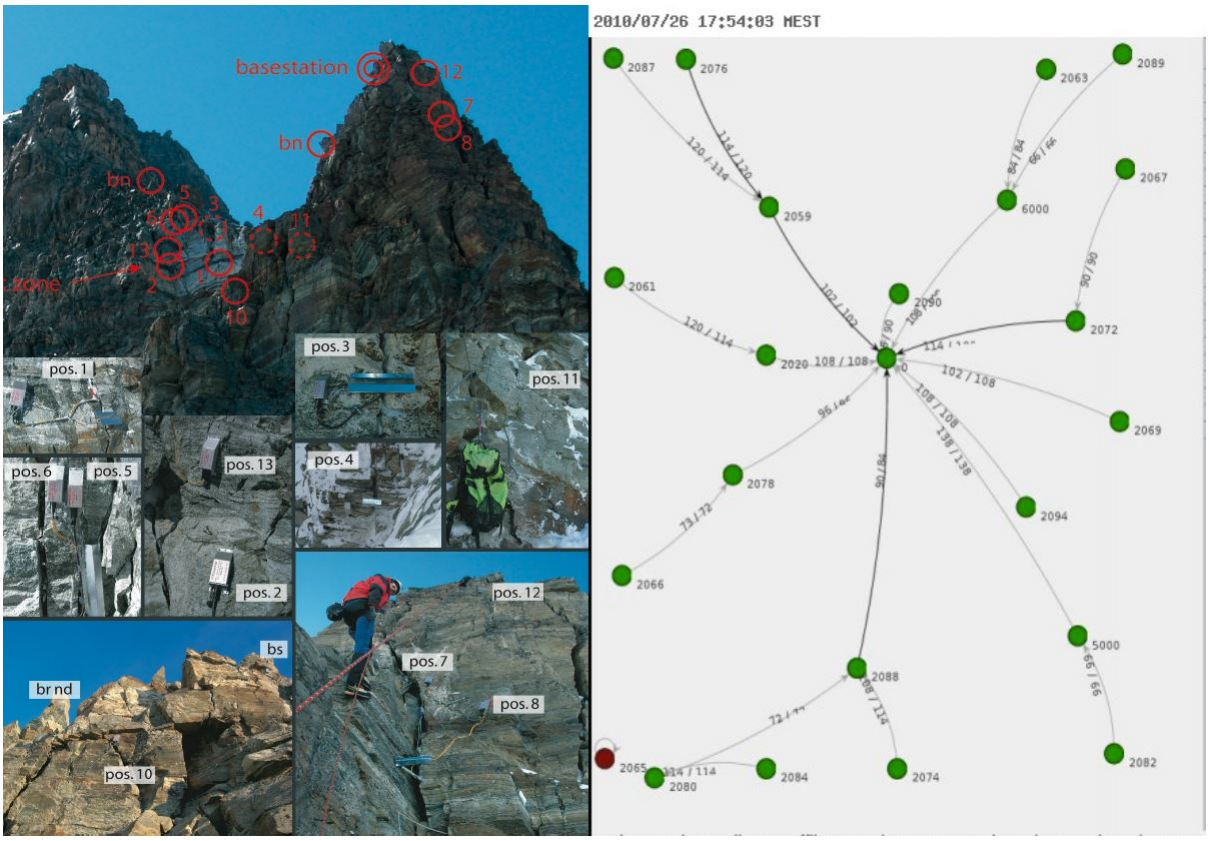
2.1.1 Kullanım Alanları

KSA'lar ölçüm ve algılama uygulamaları için bir temel oluşturur ve kullanım alanları gittikçe artmaktadır [12]. Günümüzde çevre ölçümü, ev otomasyonu, anlık sağlık takibi ve araç takibi alanlarında kullanılmaktadır.

2.1.1.1 Çevre Ölçümü

KSA'lar çevre ölçümünde önemli rol oynamaktadır. Hava, su, ve doğal afet olayları takip edilebilmektedir. Ayrıca zorlu doğa koşullarına sahip alanlardan bilgi edinmek için de kullanılmaktadır. Hava sıcaklığı, hava kalitesi, nem, toz, kirlilik miktarı ve su sıcaklığı gibi parametreler gerçek zamanlı incelenebilmektedir [13] [14] [15]. Şekil 2.1'te Alp dağlarına yerleştirilen kablosuz düğümler gösterilmektedir [16]. Düğümler aracılığı ile dağın farklı bölgelerinden toplanan sıcaklık ve nem verileri tepede bulunan

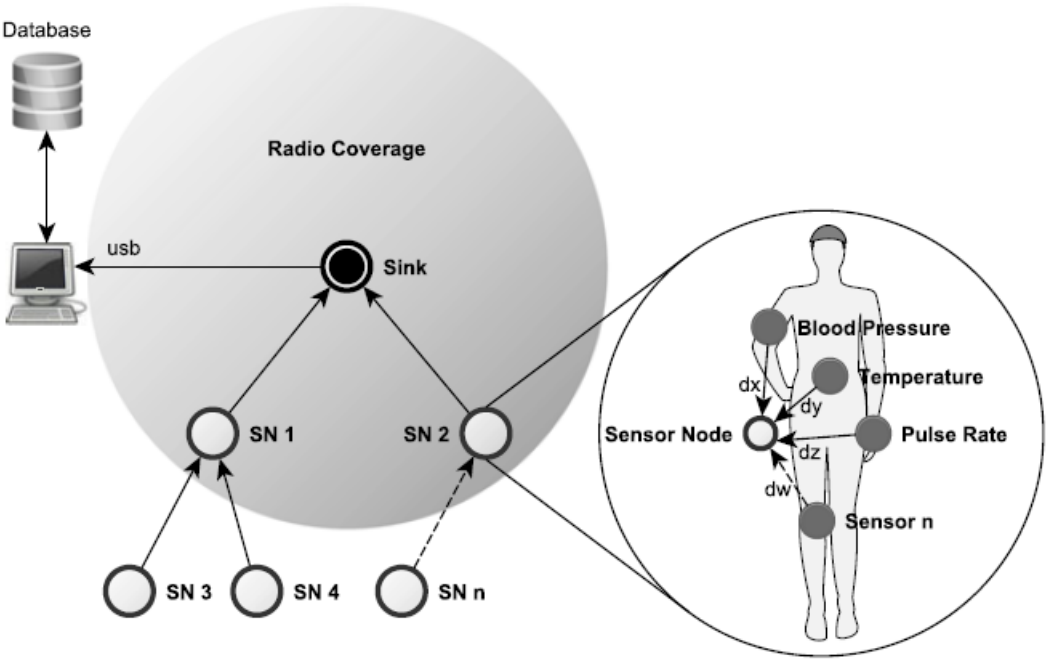
kök düğüme göndermektedir. Bu sayede dağın sıcaklık ve nem bilgilerine anlık ulaşılabilmektedir.



Şekil 2.1 : Sıcaklık ve nem değerleri gerçek zamanlı ölçülen bir dağ [16]

2.1.1.2 Sağlık Takibi

Günümüzde sağlık takibi uygulamalarında da kablosuz sensör ağları önemli yer almaktadır. Hastanelerde yoğun bakımlarında yer alan hastanın kalp hızı ve kandaki oksijen seviyesi ölçümü yapılmaktadır. [17] [18] [19] [20]. Ayrıca giyilebilir cihazlar sayesinde hastanın tansiyon, kan şekeri seviyesi, kalp hızı gibi kritik değerleri anlık olarak izlenebilmektedir [21] [22] [23]. Böylece hastaların hastaneye gitme oranı azaltılıp daha kolay hasta takibi yapılabilmektedir. Şekil 2.2'te KSA'ların sağlık alanındaki kullanımlarından biri görülmektedir.



Şekil 2.2 : Kablosuz sensör ağlarının hasta takibi için kullanımı [23]

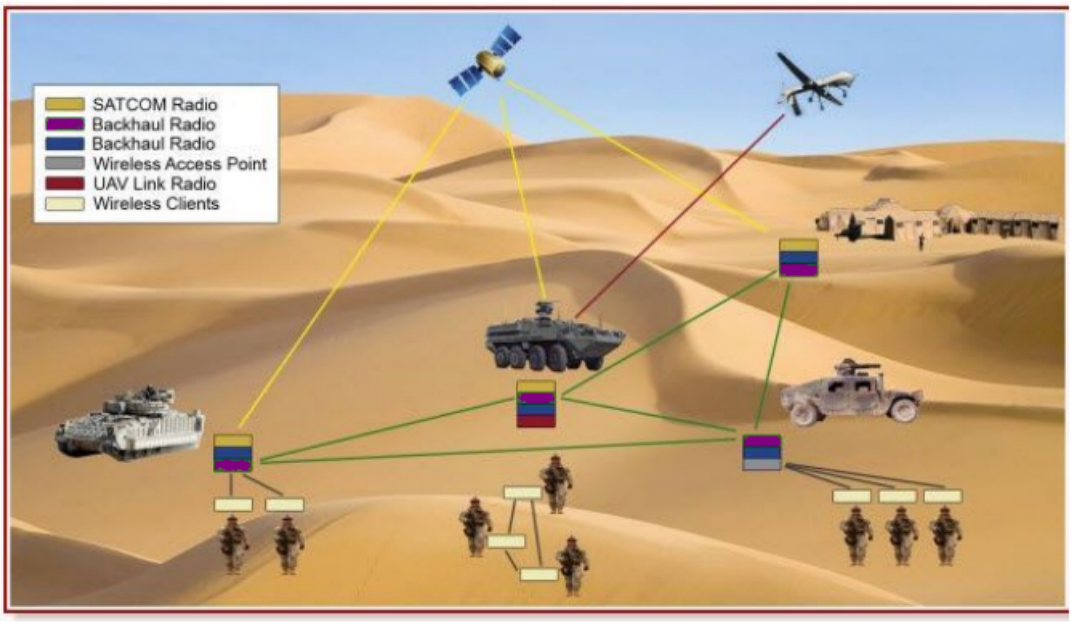
2.1.1.3 Akıllı Evler

Kablosuz sensör ağlarının evlerde kullanımı son zamanlarda gittikçe artmaktadır. Akıllı evler dediğimizde izlenebilen ve kontrol edilebilen bir ev sistemi düşünebiliriz. Evin içindeki kullanım alanlarına göre değişkenlik göstermektedir. Ev içindeki hava kalitesi, kablosuz prizlerin kontrolü, hareket takibi ve kapalı alanlarda konum belirleme gibi özelliklere sahiptir. Evlerde kullanılan elektronik cihazların güç tüketimi takibi ve uzaktan kontrolü gerçek zamanlı sağlanabilmektedir [24] [25] [26] [27]. Ayrıca biyometrik teknolojileri ile beraber kilit sistemi olarak kullanılabilmektedir.

2.1.1.4 Askeri Uygulamalar

Kablosuz sensör ağları askeri uygulamalar için de oldukça önem arz etmektedir. Akıllı toz isimli bir proje ile çok küçük boyutlarda bir cihaz üretip casusluk işlerinde kullanılmıştır. Günümüzde ise istihbarat, uzaktan savaş alanı gözetimi, anlık savaş takibi, hedef takip, alarm sistemleri gibi birçok alanda kullanılmaktadır [28]. Kara yer gözetimi ile ilgili kablosuz sensör ağları kullanılarak bir çalışma yapılmıştır [29]. Bu çalışmada düşük bütçeli sensörler tasarlanmıştır. Sensörler hareketli objelerden

gelen akustik ve manyetik sinyalleri algılamaktadır. Algılanan değerler arasındaki farkları kullanarak hareket eden cismin tipinin belirlenmesi hedeflenmektedir(Araç veya asker hareketliliği). Ayrıca savaş alanından ses, görüntü, ısı takibi yapılarak taktik üstünlük sağlamaya çalışılmaktadır [30] [31] [32]. Şekil 2.3'te sistem mimarisi gösterilmektedir.



Şekil 2.3 : Kablosuz sensör ağlarının askeri uygulamarda kullanımı [33]

2.1.2 Ağın Yapısı

Kablosuz sensör ağları çok farklı alanlarda kullanımlarına karşın, yazılım ve donanım mimarileri oldukça benzerlik içermektedir. Kablosuz sensör ağları yoğun şekilde yerleştirilmiş çok fazla düğümden oluşmaktadır. Kablosuz sensör ağlarında bir veya daha fazla kök düğümü yer alabilmektedir. Kök düğümler diğer düğümlerden gelen verileri toplar. Ayrıca verileri başka bir ağa göndermek için köprü görevi de görebilir. Düğümlerde kullanılan mikrokontrolcüler kilobaytlar cinsinden bellek ve hafıza alanına, düşük güçlü radyo özelliğine ve batarya tüketimi süresini maksimize edecek düşük güç tüketimi sistemlerine sahiptir. Kablosuz sensör ağları gözetim altında olmadan çalıştıkları için aşağıda belirtilen sorunları çözmek zorundadır:

- **Sınırlı Enerji Kaynağı**

  Kablosuz sensör ağlarında yer alan düğümler genellikle pille çalışmaktadır. Sayıca fazla olduklarından ve erişim imkanı zor olan yerlerde bulunduklarından pil

değişimi yapmak çok zordur. Bu duruma önlem olarak sensör düğümlerine güneş panellerinden sağlanan enerji ile veya nano boyutlu jeneratörler yardımıyla güç verilebilir. Kaynaktan bağımsız olarak pil tasarrufu kablosuz sensör ağlarında çok önemlidir. Ağın ömrü düğümlerin enerjisi ile doğrudan ilişkilidir. Bunun bir nedeni düğümlerin aynı anda veri göndermeye çalışıp kaynağa ulaşamaması ve tekrar aynı veriyi göndermek zorunda olmasıdır.

- **Sınırlı Bellek ve İşlem Gücü**

  Kablosuz sensör ağları çok sayıda cihazın bir araya gelmesinden oluştuğu için cihaz maliyeti çok düşük olmalıdır. Maliyet ve enerji tüketimini azaltmak için kilobaytlar mertebesinde bellek ve hafıza alanı ve işlem hızı düşük işlemciler yer almaktadır. Bu nedenle kullanılacak algoritmalar verimli olmalıdır.

- **Kendi Kendine Ağ Kurabilme**

  Kablosuz sensör ağları erişimi zor alanlarda çok sayıda yer almaktadır. Bu ağların kendi kendine bağlantı kurabilmesi, paketleri yönlendirebilmesi ve ağın devamlılığını sağlaması beklenmektedir. Herhangi bir değişikliğe karşı ağın kendi kendini onarması ve bu değişikliğe adapte olması gerekmektedir. Ayrıca birden fazla kök düğümü kullanmak ağı yönetmekte oldukça kolaylık sağlamaktadır.

- **Kayıplı Kablosuz Ortamda Çalışma**

  Kablosuz ortamda gönderilen veriler çevresel faktörlerden kaynaklı kayıp yaşayabilmektedir. Kullanılacak algoritmalar enerji, bellek, işlem gücü kısıtlarını gözeterek ve veri kaybını minimum yapacak şekilde tasarlanmalıdır.

- **Bilgi Güvenliği**

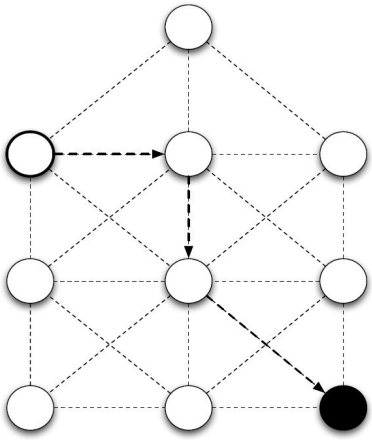
  Gönderilen bilgilerin güvenliği kablosuz sensör ağlarındaki en önemli parametrelerdendir. Kablosuz ortamda iletilen yayın ortamdaki herkes tarafından dinlenmektedir. Bunu engellemek için düşük işlem gücü ile simetrik ve asimetrik kriptolama işlemleri yapılabilir. Böylece ortamdaki paketler uçtan uca şifrelenmiş olup bilgi güvenliği sağlanmış olur.

2.1.2.1 Trafik Modelleri

KSA'lardaki asıl amaç ağ içindeki düğümlere verileri göndermek ve istenildiğinde o düğümlerden verileri alabilmektedir. Bunu gerçekleştirebilmek için bazı trafik modellerini kullanmaktadır.

- **Bir Noktadan Bir Noktaya İletişim**

  Önceden belirlenmiş gönderici ve alıcı arasındaki tek yönlü iletişim tipidir. Şekil 2.4 bu duruma örnek olarak gösterilmiştir. Ağda yer alan bir düğüm diğer düğümden veri isteyebilir. Eğer alıcı ile gönderici arasında direkt bir iletişim yoksa bu bilgi ara düğümler üzerinden gerçekleşir. [36]



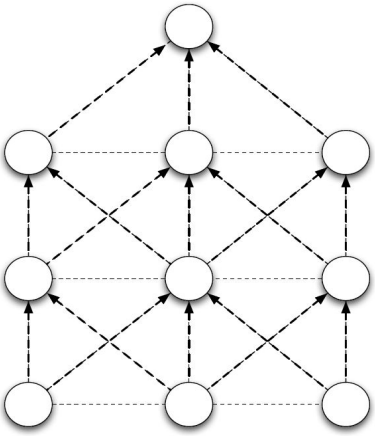
Şekil 2.4 : Bir noktadan bir noktaya iletişim

- **Çok Noktadan Bir Noktaya İletişim**

  Bu modelde çok sayıda düğüm elde ettiği bilgileri Şekil 2.5'te görüldüğü üzere tek bir alıcıya gönderir. Veri toplama prokollerinin güvenilir olmasına gerek yoktur [37]. Bu tür uygulamalarda çok sayıda düğümden veri alındığı için veri kaybolması sonucu çok etkilememektedir. Örneğin orman yangını engelleme sistemleri eşik tabanlı çalışan sistemlerdir. Sıcaklığın kaç derece arttığından ziyade sıcaklığın ani artış bilgisi daha önemlidir. Bu nedenle herhangi bir düğümden gelen yüksek sıcaklık bilgisi önem arz etmemektedir.

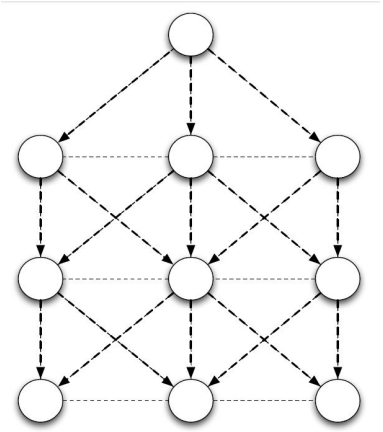
- **Bir Noktadan Çok Noktaya İletişim**

  KSA'larda yer alan düğümler yeniden programlanabilir olmalıdır. Örneğin, düğümde yer alan farklı bir sensör aktifleştirilebilir veya daha önceden belirlenen sınır değeri yeni ihtiyaçlara göre değiştirilebilir. Yeni parametrelerin kök



Şekil 2.5 : Çok noktadan bir noktaya iletişim

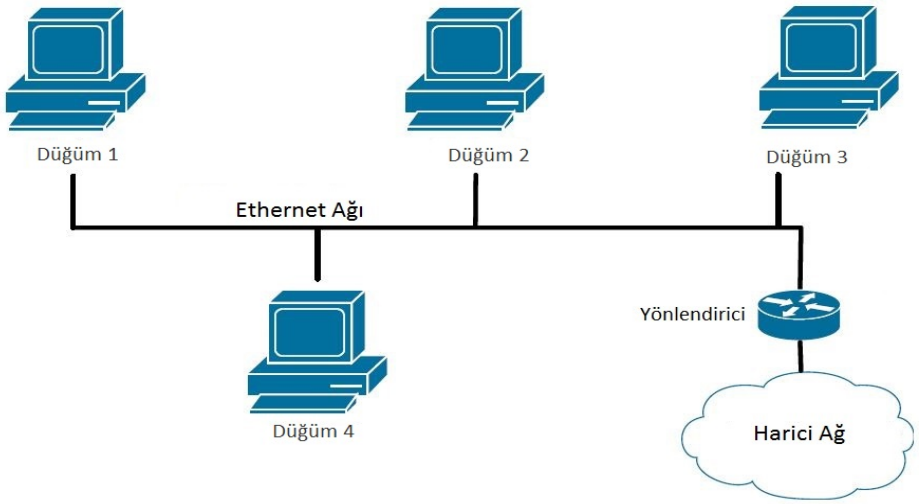
düğümünden başlayarak diğer tüm düğümlere iletilmesi gerekmektedir. Şekil 2.6 bu iletişim tipi detaylı bir şekilde gösterilmiştir. Çok noktadan bir noktaya iletişimin aksine veri gönderme protokollerinin veri güvenliği sağlamak zorundadır. Bunun nedeni ağ ile ilgili önemli parametre bilgilerinin gönderilmesidir. Bunu gerçekleştirmek için güvenli algoritmalar kullanılmaktadır. [38]



Şekil 2.6 : Bir noktadan çok noktaya iletişim

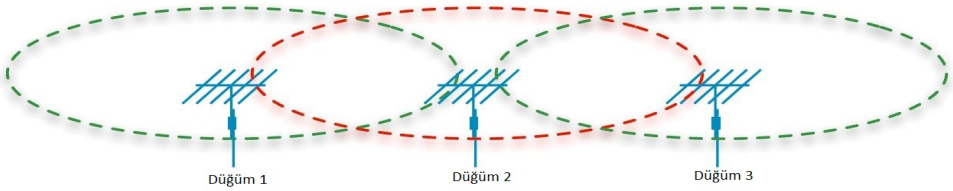
2.1.2.2 Kablosuz Ağ Oluşturma

Kablolu ağ sistemi olan Ethernet'te linke bağlı bütün düğümler bağlandığı hat ile ilgili bilgilere sahiptir. Bütün düğümler birbirlerinin komşularından haberdardır [39]. Bu nedenle ethernet ağ yapısına simetrik ve geçirgen ağ denilmektedir. Şekil 2.7 ile görüldüğü üzere 1 numaralı düğümün ilettiği mesajı 4 numaralı düğümü duyuyorsa, 2 ve 3 numaralı düğümlerde bu mesajı duymaktadır. Ağdaki herkes birbirine mesaj gönderip alabilir.



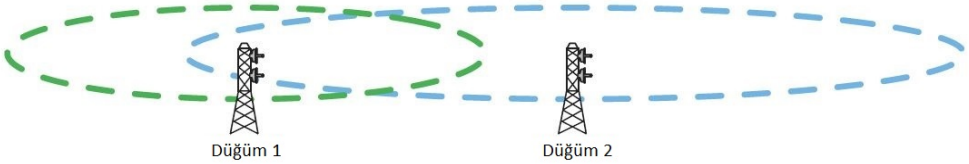
Şekil 2.7 : Ethernet ağının yapısı

KSA'lar ise geçirgen değildir. Şekil 2.8'te görüleceği üzere 2 numaralı düğüm 1 ve 3 numaralı düğümle haberleşebiliyorken, 1 ve 3 numaralı düğümler arasında bir iletişim yoktur. Her bir düğümün komşuları kendine aittir ve değişkenlik göstermektedir.



Şekil 2.8 : Geçirgen olmayan kablosuz ağ yapısı

Kablosuz ağlar kablolu ağların aksine simetrik olmayabilirler. Şekil 2.9'de görüldüğü üzere 1 numaralı düğüm 2 numaralı düğümün kapsama alanında iken, 2 numaralı düğüm 1 numaralı düğümün kapsama alanında değildir. 2 numaralı düğümün gönderdiği mesajlar 1 numaralı düğüme ulaşırken, 1 numaralı düğümün mesajları 2 numaralı düğüme ulaşamayacaktır. Bu duruma asimetrik iletişim denmektedir. Kablolu ağlarda genellikle değişim çok azdır. Cihazlar sabittir ve hareket çok azdır. Cihaz ağa ya bağlıdır ya da değildir. Bağlantı kalitesi yüksektir. Bunların aksine KSA'larda hava ortamı kablolu iletişimden oldukça farklıdır. Sinyal seviyesi ortamdan dolayı sürekli değişiklik gösterir ve ağdan kopup tekrar bağlanmalar meydana gelebilir. Gönderilen mesajların hepsi hedefine ulaşamayabilir. Bu nedenle ağ yapısı sürekli değişkenlik gösterir.



Şekil 2.9 : Asimetrik yapıdaki kablosuz ağ

2.1.2.3 Kablosuz Ağlarda Yönlendirme

KSA'larda yönlendirme kaynaktan hedefe doğru veri transferini sağlamaktır. Bu işlem iki adımda gerçekleşmektedir.

İlk adım ağ oluşturma evresidir. Gönderici ve alıcı birbirlerine komşu değillerse veri iletimi için ara düğümlerin bağlantısı olması gerekmektedir. Bu bağlantının hangi düğümler üzerinden gitmesi gerektiği belirlenmelidir. Yönlendirme algoritmaları ile en uygun yol seçilir. En iyi ifadesi birden fazla metrik ile açıklanmaktadır ve uygulamadan uygulamaya değişkenlik göstermektedir. Bu metrikler paket gönderimininde en az gecikme, hattı en yüksek bant genişliği ile kullanma, minimum hop sayısı, en kaliteli link veya minimum enerji tüketimidir.

İkinci adımda ise bakım evresidir. KSA'larda ağ yapısı sürekli değişebilmektedir. Bağlantı kalitesinin düşmesi, düğümlerin hareketliliği, düğümlerin pil ile çalışması gibi nedenlerden yönlendirme haritası geçersiz kalmaktadır. Bu nedenle yönlendirme protokolleri bu durumlarda yeni yollar bulmalıdır. Kontrol mesajları ile ağ dinamik tutulmaktadır. Bu işlemler veri gönderileceği zaman yapılabileceği gibi periyodik olarakta yapılabilir. Yönlendirme protokolleri bu nedenle 2 tipe ayrılır.

- **Reaktif Protokoller**

  Reaktif protokollerde yönlendirme tablosu veri göndermek gerektiğinde ve hedefe nasıl ulaşılacağı hakkında geçerli bir yol bilgisi olmadığında hesaplanır. Yeni yolları keşfetme süreci ağa paket göndermekle başlar. Hedef düğümden cevabın gelmesi için beklenir. Gelen cevaptan sonra yeni yol belirlenmiş olur ve düğüm ile hedef arasındaki bağlantı kurulmuş olur. Cevabın gelmesi ise paket iletiminden dolayı ağda gecikmeye neden olur. Ağda yer alan düğümler ağ ile ilgili bilgilerin sadece bir kısmına sahiptir. Bu kısım ise sadece verinin hangi hedefe gönderileceğidir. Reaktif protokollerdeki düğümlerin tüm ağa ait yönlendirme

tablosu tutmalarına gerek yoktur. AODV (İstek üzerine Mesafe Vektörü) [40] bir reaktif protokol örneğidir.

- **Proaktif Protokoller**

  Bu tip protokollerde ağdaki düğümler düzenli olarak bütün ağın yönlendirme tablolorını günceller. Ağ topolojisinde oluşabilecek tüm yolların önceden bilinmesi sağlanır. Böylece hedefe gönderilmek istenen paket reaktif protokollerin aksine direk ulaşır. Yol bilgileri önceden belli olduğu için mesajlaşma gecikmesi yaşanmaz. Ancak bu protokolde de yönlendirme tablolarını sürekli güncel tutabilmek ve ağda bilgi tutarlılığını sağlamak için kontrol mesajlaşması gerekmektedir. Ağda bulunan veri haberleşmesinden bağımsız olarak kontrol mesajlaşması her zaman gerçekleşmektedir. OLSR (Optimize Edilmiş Yol Durum Yönlendirmesi) [41] gerçeklemelerde kullanılan bir proaktif protokoldür.

2.1.3 Kablosuz Sensör Ağları Yönlendirme Protokolleri

Kablosuz sensör ağlarında kullanmak için birçok yönlendirme protokolü geliştirilmiştir [42]. Geliştirilen bu protokoller daha önce anlatılan (Bölüm 2.1.2) kısıtlamaları çözmeyi hedeflemiştir. KSA'larda bilgiyi göndermenin en kolay yolu ağ boyunca taşarak göndermektedir [42]. Bunun anlamı bilgiyi alan her düğüm o bilgi hedefe ulaşana kadar bütün komşu düğümlere gönderilmesidir. Birden fazla ebeveyne sahip olan düğüm aynı mesajı bütün ebeveynlerinden alacaktır. Bu durumu engellemek için bazı mekanizmalar geliştirilmiştir. Düğümler aynı mesajın daha önce alınıp alınmadığını kontrol edecektir. Ayrıca gönderilen paket kaç kere gönderilmesine izin verileceği ile ilgili bir bilgi de içerebilir. Bu önlemleri almak kolay olmasına rağmen taşma durumunun bazı olumsuz özellikleri bulunmaktadır. Düğümler aynı mesajı birden fazla kez alabilir. Bu durum yüksek enerji tüketimine neden olur ve bu mekanizmada enerji kullanımını kısıtlayıcı bir önlem bulunmamaktadır. Bu yöntem veri iletimini az sayıda yapacak sistemler için uygundur.

SPIN(Görüşme Tabanlı Algılayıcı Protokolü) [43] protokolü kablosuz sensör ağlarındaki bir düğümü seçmeden veri olup olmadığını sorgulama desteği getirmiştir. Ayrıca enerji tasarrufu desteği de eklemiştir. Bu protokolde veri iletişiminden önce düğümler arasında bir veri ile bağlantılı önbilgi mesajı paylaşılır. Bu mesajı alan düğümler önbilgiyi kontrol eder. Eğer bu veri istenen bir veriyse göndericiye istek

mesajı gönderir. Bu protokol enerji verimliliği açısından taşma prokolüne göre daha avantajlıdır. Ancak önbilgi formatı ile ilgili belirlenmiş bir format olmadığından her uygulama kendine ait bir format belirler. Ayrıca verinin gönderimini de garanti etmez. Hedefe doğru gönderilen pakette ara düğümler önbilgi ile ilgili veri ile ilgilenmiyorsa, hedef düğüm bu veriyi alamayacaktır. [43]

Kablosuz sensör ağlarında ölçülebilirlik ve enerjinin korunması sorunlarını çözmek için de LEACH (Düşük enerji Adaptif Gruplama Hiyerarşisi) [44] protokolü geliştirilmiştir. Bu protokolün amacı kök düğümlerin çok fazla mesaj alarak fazla yük altına girmesini engellemek ve toplam gönderilen mesaj sayısını azaltmaktır. Bunu gerçekleştirmek için düğümler bir araya gelip gruplanmıştır. Gruplanan düğümlerin grup başı bulunmaktadır. Gruptaki düğümler verileri grubun başkanına yönlendirilir. Böylece her bir düğüm kök düğüme tek tek mesaj göndermesi yerine grup başı toplu olarak mesajları gönderir. Böylece kök düğümlere gönderilen mesaj sayısı azaltılır ve enerji verimliliği de sağlanmış olur.

Enerji verimliliğini sağlayan kablosuz sensör ağları protokolü geliştirmek için düğümlerin uzaysal konumlarını kullanarak gerçekleşebilir. Eğer düğümlerin yerleştiği bölgeler biliniyorsa,istekler direkt olarak o bölgeye yoğunlaşabilir. Böylece gereksiz yere ağda haberleşme yükünü azaltır. Bu amaçla geliştirilem MECN (Minimum Enerji Haberleşme Ağı) ve GAF (Coğrafik Adaptif Doğruluk) protokolleri KSA'larda kullanılabilir.

KSA'larda enerji verimliliğini sağlamak için verilerin toplanması gibi yöntemler de kullanılmaktadır. Ara düğümler, komşu düğümlerden verileri toplar ve bu verilerin maksimum değer, minimum değer, ortalama değer hesaplama gibi işlemlere tabi tutar. Veri toplama yönteminin dezavantajlarından biri uygulamaya özel olmasıdır. Böylece farklı protokollerle uyumlu çalışamamaktadır. Bu nedenle kullanım alanları sınırlıdır.

KSA'ların kullanım alanı hem akademik hem de ticari olarak arttığından bu sistemleri diğer sistemlerle uyumlu olarak çalışması için entegre edilmesi gerekir. Bu da birbiriyle uyumlu ve birlikte çalışabilen protokollerin geliştirilmesi ihtiyacını ortaya çıkarmıştır. Böyle bir standartın olmaması nedeniyle KSA'larda kullanılan protokolleri standart hale getirmek için çalışmalar başlamıştır.

2.1.3.1 Yönlendirme Protokollerinin Standartlaşması

KSA'ların farklı alanlarda kullanım alanları görüldükçe endüstrinin ilgisi giderek artmıştır. Fakat bu sistemler kullanımda olan algoritmaların patentli olması nedeniyle ve uygulamalar arası uyumsuzluğun olması nedeniyle sorun teşkil etmektedir. Uyumluluğu sağlayabilmek için akademi ve endüstri bir arada çalışmıştır. Bu çalışmalarda KSA'ları IPv6 ağına taşıma fikirleri ortaya atılmıştır. Amaç KSA'ları IPv6 sistemine entegre ederek standart IP haberleşmesi ile paket göndermesi sağlamaktır. İlk olarak IPSO(Akıllı Objeler İçin IP) [4] grubu KSA'larda IP sistemini aktifleştirmek için çalışmalar gerçekleştirmiştir. Daha sonra IETF(İnternet Mühendisliği Görev Grubu) [1] tarafından oluşan ROLL [2] ve 6LowPAN [3] grubu da standartlaştırma ile ilgili çalışmalar gerçekleştirdi.

2.1.3.2 RPL

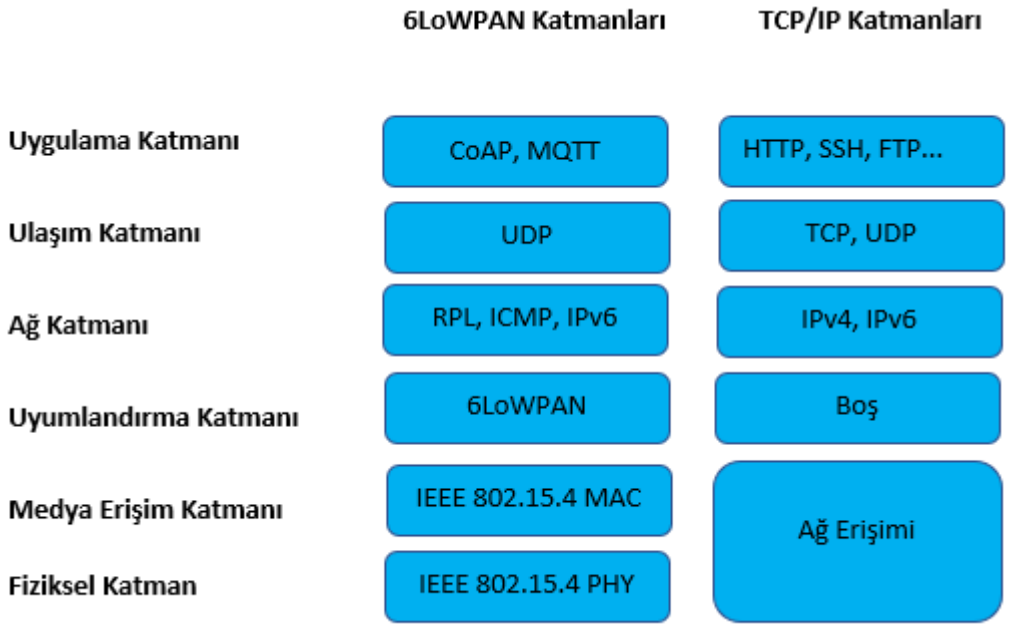
IETF tarafından oluşturulan ROLL çalışma grubunun amacı düşük güçlü, kısıtlı hafıza ve işlem gücü ve kayıplı ağlarda çalışabilen bir yönlendirme protokolü geliştirmektir. Bu protokol IPv6 ile çalışan ağlarla da uyumlu olmalıdır. ROLL çalışma grubu, endüstri istekleri doğrultusunda ev otomasyonu [45] [46], kırsal alan uygulamaları [48] ve endüstriyel uygulamalar [47] için gereksinimleri belirlemiştir. Çalışma grubunun çalışmaları neticesinde gereksinimleri karşılayan RPL(Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü) geliştirilmiştir. Bu protokol "RFC6550" [5] numarası ile standartlara girmiştir. RPL protokolü ile detaylı bilgi sonraki bölümlerde verilecektir.

2.1.3.3 6LowPAN

IETF 6LowPAN çalışma grubu kaynakları limitli olan Kablosuz Sensör Ağlarının standart IP haberleşmesine sahip IPv6 destekli cihazlarla uyumlu çalışabilmesi için 802.15.4 kanalını kullanarak bir uyumlandırma katmanı tasarlamak ve protokol geliştirmek üzere toplanmıştır ve yapılan çalışmalar sonucunda 6LowPAN protokolü ortaya çıkmıştır. Bu protokolde standart IPv6 paketlerini parçalara bölme ve tekrar birleştirme yapılmıştır. İlk olarak IPv6 ulaşım katmanı başlığı sıkıştırılmıştır. Ardından paketler uygun uzunluktaki parçalara ayrıldıktan sonra her parçaya 6LowPAN başlıkları eklenmiştir. 6LowPAN ağına katılan her düğüm IPv6 adresine sahip olacaktır ve bu adres ile diğer cihazlarla haberleşebilecektir. 6LowPAN katmanı "RFC6282" [6] dökümanı ile standart haline dönüşmüştür.

2.2 Kablosuz Sensör Ağları Protokol Katmanları

Geleneksel TCP/IP uygulamaları, hem kod alanı hem de bellek kullanımı açısından çok fazla kaynağa ihtiyaç duyar ve sınırlı kaynaklara sahip KSA'lar için kullanışlı değildir [2]. KSA TCP/IP yığını, standart TCP/IP yığınının yalnızca mutlak minimum özelliklerine sahip olacak şekilde tasarlanmıştır [8]. KSA'larda kullanılan 6LoWPAN yığını ve standart TCP/IP yığınının katmanları Şekil 2.10'te gösterilmiştir. 6LoWPAN altı katmanlı olmasına karşın standart TCP/IP beş katmanlıdır.



Şekil 2.10 : Kablosuz sensör ağları ve TCP/IP için OSI katmanları

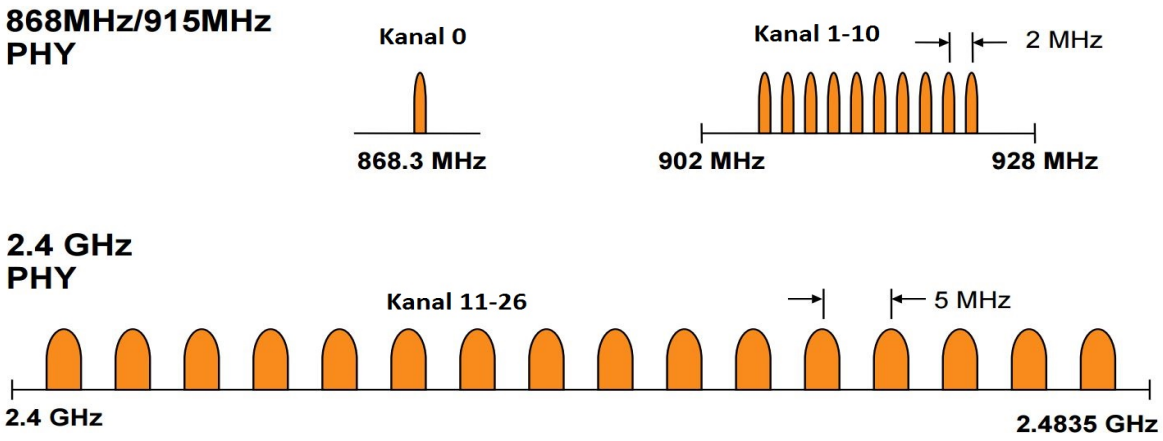
2.2.1 Fiziksel Katman

OSI katmanlarının ilk ve en alt kısmında yer alan bu katman ve cihazlar arasındaki fiziksel bağlantıyı sağlar. Bu katman veriyi gönderip almakla yükümlüdür. Gönderilecek verinin hangi ortamda iletileceği ve hangi modülasyon tekniğiyle gönderileceği bu katmanda belirlenmektedir. Gönderim ortamı elektriksel, mikrodalga veya ışık, gönderim modülasyon tipleri ise BPSK, QPSK, FSK olabilir. *"IEEE 802.11"*, *"IEEE 802.15.4"* vb. gibi farklı fiziksel katmanlar mevcuttur. Düşük güç ve kayıplı ağlarda kullanılan fiziksel katmana *"802.15.4"* denir ve standart haline dönüşmüştür. Bu standart, dünyanın farklı yerlerindeki farklı düzenlemeler nedeniyle üç farklı frekans aralığı kullanır. Amerika Birleşik Devletleri için 902-928 MHz, Avrupa için 868-868.8 MHz ve dünyanın geri kalanı için 2400-2448,3 MHz kullanır.

Hızlar, frekansa bağlı olarak 20 ila 250 kbit/s arasında değişir. *"802.15.4"* standardı ayrıca MAC katmanını da belirler. Bu standart iki tip MAC adresleme biçimini destekler: uzun (64 bit) ve kısa (16 bit). *"IEEE 802.15.4"*, iki tür modülasyon kullanır: ikili faz kaydırmalı anahtarlama (BPSK) ve dörtlü faz kaydırmalı anahtarlama (QPSK). Maksimum çerçeve boyutu (1 Bayt) MAC başlığı [11] dahil 128 bayttır. Fiziksel katmanın detayları Şekil 2.11 ve Şekil 2.12 ile gösterilmiştir.

Bant Genişliği (MHz)	Kanal Aralığı	Kanal Sayısı	Yonga Hızı Kyonga/saniye	Modülasyon	Bit Hızı Kb/saniye	Sembol Hızı Ksembol/saniye	Sembol Tipi
868-868.6	-	1	300	BPSK	20	20	İkili
902-928	2 MHz	10	600	BPSK	40	40	İkili
2400-2483,5	5 MHz	16	2000	O-QPSK	250	62,5	16'lı Ortogonal

Şekil 2.11 : 802.15.4 fiziksel katmanının çeşitleri [7]



Şekil 2.12 : 802.15.4 fiziksel katmanında kullanılan kanallar [7]

2.2.2 Medya Erişim Katmanı

Medya erişim katmanı kablosuz sensör ağlarındaki düğümlerin güvenli ve verimli bir iletişim kanalının kurulmasından ve enerji verimliliğinden sorumludur. 6LoWPAN için uyarlanmış bu katmana IEEE *"802.15.4"* MAC adı verilmiştir. Bu katman medyaya erişmek için CSMA/CA (Çarpışma Algılamalı Taşıyıcı algılama çoklu erişim) ve TDMA (Zaman Bölmeli Çoklu Erişim) olmak üzere iki tip olarak kategorize edilir. CSMA/CA protokolü, her düğümün paket göndermeden önce iletişim ortamını dinlediği ve eğer o an ortamda gönderilen paket yoksa paket gönderme üzerine kurulu olasılık teknikli bir yapıdır. Çoklu erişimden kastedilmek istenen birden fazla düğümün aynı anda ortama erişip veri gönderebilir ve aynı zamanda gönderilen

paketler çakışabilir. Bu çakışmalar bazı yöntemlerle çözülmektedir. Çarpışma tabanlı protokollerin aksine zaman bölmeli çoklu erişimli protokollerde bulunmaktadır. Bu yöntemde ise her bir düğüm için belirli bir zaman aralığı ayrılmıştır ve aynı anda veri göndermeyi engellenmeye çalışılmıştır. Ayrıca sürekli dinleme ve beklerken dinlemenin enerji tüketimine olan etkisini azaltır.

2.2.3 Uyumlandırma Katmanı

Kablosuz sensör ağlarındaki ihtiyaçlardan biri de cihazların IPv6 ağına bağlanabilmesidir. Kablosuz sensör ağlarındaki düğümlerin düşük işlem gücü, bant genişliği ve kısıtlı enerji sorunları olduğundan standart IP iletişimi ile haberleşmesi mümkün olmamaktadır. Standart IP iletişimini kablosuz sensör ağlarına getirmek için 6LowPAN isminde bir uyumlandırma katmanı geliştirilmiştir. Bu katmanda yapılan işler aşağıda belirtilmiştir.

- IPv6 paketinin minimum uzunluğu 1280 bayttır ancak 802.15.4 standartına göre gönderilebilecek maksimum veri uzunluğu 127 bayttır. Bu veri 25 bayt başlık, 21 bayt güvenlik ve 81 bayt ise data için ayrılmıştır. Standart IPv6 başlığı 40 bayttır bu alan 2 bayt olacak şekilde sıkıştırılmıştır.
- IPv6 paketinin sahip olduğu adres uzunluğu 128 bit iken, 802.15.4 standartının sahip olduğu adres uzunluğu 16 veya 64 bit olmaktadır. Bu adrese ağ katmanında yeni başlıklar eklenerek, standart IPv6 haberleşmesi yapılması sağlanır.
- Standart IPv6 cihazları mesajların iletilmesini dağıtıcılar üzerinden gerçekleştirirken, kablosuz sensör ağlarında bütün düğümlerin mesajları dağıtması gerekir. Bu nedenle gerekli olan yapıları tanımlar.

2.2.4 Ağ Katmanı

Standart haberleşmelerde de kullanılan ağ katmanı verilerin gönderici birimden alıcı birime iletimini sağlar. Eğer mesaj lokal ağdan başka bir dış ağa gönderilecekse yönlendirme tabloları ile gitmesi gereken hedeflere ulaşır. Kablosuz sensör ağlarında ise Bölüm 3'te anlatılan RPL bu katman için geliştirilmiştir. RPL protokolü kontrol mesajlarını kullanarak ağın topolojisini oluşurur ve düğümler arası iletişim için komşuları belirler. Kontrol mesajları ağ ile ilgili parametreleri de içermektedir. Her bir

düğüm mesajı komşu düğümlere iletmekle sorumludur. Paketin gönderildiği hedefe direkt erişim yok ise gerekli hoplama işlemleri gerçekleştirilir.

2.2.5 Ulaşım Katmanı

Bu katmanda UDP(Kullanıcı Veri Birimi Protokolü) ve TCP(Geçiş Kontrol Protokolü) olmak üzere iki tip protokol bulunmaktadır. Paketin geçerliliğini kontrol etmek için CRC işlemi yapılır ve belirtilmiş port numarası ile mesajı uygulama katmanına iletir. TCP bağlantısında ise port numarası kontrol edilir ve aktif bağlantı var ise mesaj uygulama katmanına iletilir. Eğer aktif bağlantı yoksa tanımlı diğer portları kontrol eder. Kablosuz sensör ağlarında ise kullanım kolaylığından UDP tercih edilir.

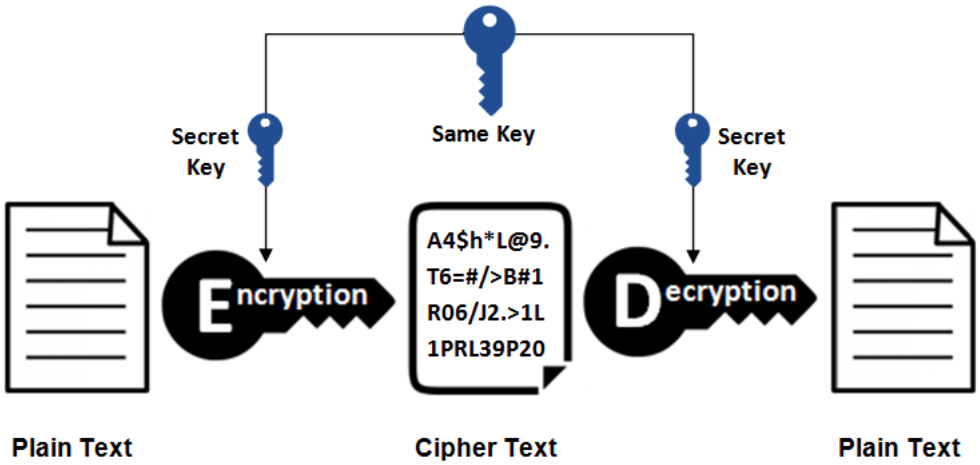
2.2.6 Uygulama Katmanı

Uygulamalar için API katmanı sağlamaktadır ve alt katman hakkında bilgi sahibi olmadan ağ üzerinde uygulama geliştirilen katmandır. Standart internet haberleşmesinde HTTP, FTP gibi prokoller kullanılmaktadır. Kablosuz sensör ağlarının düşük işlem gücü ve bellekten dolayı bu protokolleri mümkün değildir. Bunların yerine CoAP(Kısıtlanmış Uygulama Protokolü) ve MQTT(Telemetri Mesajları Sıralama Protokolü) gibi kaynak gereksinimi az olan uygulamalar kullanılır.

2.3 Kriptografi

2.3.1 Simetrik Kriptografi

Gizli anahtar kriptografisi diye de bilinen simetrik kriptografide şifreleme ve şifre çözme işlemleri için aynı anahtar kullanılır. Bu anahtar sadece gönderici ve alıcı arasında kullanılan gizli bir anahtardır. Gizli anahtar kullanılarak veriyi şifreleme işlemi gerçekleştirilir. Sadece bu anahtara sahip olan düğümler şifrelenmiş veriyi çözebilir. Şekil 2.13'te örnek kullanımı gösterilmektedir. Simetrik algoritmalar şifreleme işlemlerinin karmaşıklığı daha az olduğundan asimetrik algoritmalara göre daha hızlıdır. Ancak coğrafi olarak geniş alana yayılmış ve ağa yeni düğümün eklenip veya başka bir düğümün ayrılma ihtimali olan KSA'larda bu anahtarı saklamak oldukça zordur. Ayrıca her bir düğümün bellekte tutması gereken anahtar sayısı çok fazla arttığından simetrik kriptografi ile ölçeklenebilirlik oldukça azalmaktadır [75]. AES, 3DES gibi yöntemler örnek olarak gösterilmektedir.



Şekil 2.13 : Simetrik Şifreleme [78]

2.3.2 AES

AES (Gelişmiş Şifreleme Standartı) simetrik blok şifreleyici algoritmasıdır. Mesajları şifreleme ve şifre çözme işlemlerini gerçekleştirir.Mesajı 128 bitlik bloklara ayırır ve 128 bit, 192 bit veya 256 bitlik anahtar kullanarak şifreleme işlemini gerçekleştirir. AES algoritması anahtar uzunluğuna göre isimlendirilmektedir ve Çizelge 2.1'te gösterilmiştir. Blok şifreleyici olması nedeniyle orijinal mesaj ile şifrelenmiş mesajın uzunluğu aynıdır ve 128 bit uzunluğundadır. Ayrıca AES algoritmasının ECB, OFB, CTR, CBC gibi farklı şifreleme modları bulunmaktadır.

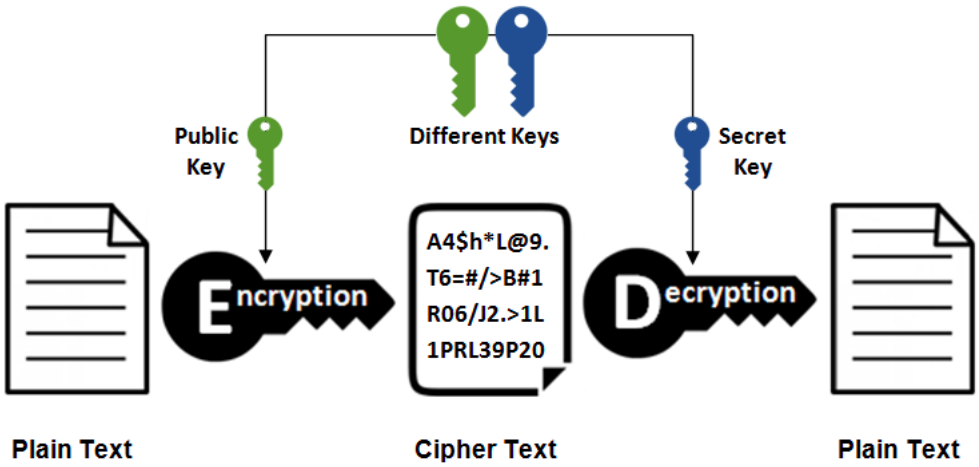
Algoritma	Anahtar uzunluğu	Blok Uzunluğu
AES-128	128 bit	128 bit
AES-192	192 bit	128 bit
AES-256	256 bit	128 bit

Çizelge 2.1 : AES uygulamalarında anahtar ve blok uzunlukları

2.3.3 Asimetrik Kriptografi

Açık anahtar kriptografisi diye de bilinen asimetrik kriptografide her düğümün kriptografik işlemleri gerçekleştirmek için açık anahtar ve gizli anahtar olmak üzere iki adet anahtar çifti bulunmaktadır. Her düğüm sadece kendisine ait gizli anahtarı bilmektedir. Açık anahtar ise bütün düğümlere dağıtılır. Böylece anahtar paylaşımında güvenlik riski bulunmamaktadır. Açık anahtar ile şifrelenen veriyi sadece ona uygun gizli anahtar çözebilir ve orijinal veriyi elde edebilir. Gizli anahtar ile şifrelenen

veriyi de sadece ona uygun açık anahtar çözebilmektedir. Şekil 2.14'te örnek kullanımı gösterilmektedir. Yüksek enerji tüketimi ve işlem gücü nedeniyle KSA'larda kullanımı yaygın değildir. Günümüzde ise düğümlerin hem işlemci gücü hem de bellek olarak daha güçlü olduklarından asimetrik kriptografi KSA'lar için uygunluğu ile ilgili çalışmalar yapılmaktadır. RSA, ECC gibi yöntemler asimetrik kriptografik algoritmalara örnektir. RSA ve ECC'nin karşılaştırılması Şekil 2.15 ve Şekil 2.16'te gösterilmektedir.



Şekil 2.14 : Asimetrik Şifreleme [78]

2.3.4 RSA

Asimetrik kripto sisteminin güvenliği bu anahtarları oluşturan çok büyük asal sayıların çarpanlarına ayrılmasının zorluğundan gelmektedir. 1977 yılında geliştirilmiş olan bu algoritmanın isminin ortaya çıkışı Ron Rivest, Adi Shamir ve Leonard Adleman'in isimlerinin baş harflerinin birleşimi ile ortaya çıkmıştır. Bu yöntemi kullanarak şifreleme ve imzalama işlemleri gerçekleştirilmektedir. Gizli anahtar paylaşımına gerek olmadan şifreleme işlemi yapılır. Gönderici gizli anahtarını kullanarak mesajı imzalar ve alıcı düğüme gönderir. Alıcı düğüm ise göndericinin açık anahtarını kullanarak mesajın imzasını doğrular. RSA'nın günümüzde kullanımı oldukça yaygındır. Güvenli bir RSA şifreleme işlemleri için minimum RSA-2048 önerilmektedir.

2.3.5 Eliptik Eğri Kriptografisi

Kriptografide kullanılan eliptik eğri sistemleri 1985 yılında Neal Koblitz ve Victor Miller tarafından önerilmiştir. ECC(Eliptik eğri kriptografisi), eliptik eğrilerin

matematiğine dayanan açık anahtar kriptografi yaklaşımıdır. RSA'da kullanılan çok büyük asal sayıların çarpımı yerine eliptik eğri denklemlerini kullanarak açık ve gizli anahtarını üretir. Şifre çözme ve dijital imza işlemlerini hızlı bir şekilde gerçekleştirir. ECC'nin asıl avantajı RSA gibi diğer açık anahtar yöntemlerinden daha küçük anahtar boyutu ile aynı seviyede veya daha yüksek koruma sağlamasıdır. 160 bitlik ECC anahtarının sağladığı güvenlik ile 1024 bit RSA anahtarı aynı derecede güvenlik sağlamaktadır. ECC bu anahtarı üretmek için eğri üzerindeki noktaları kullanır. Anahtar boyutunun kısa olması nedeniyle şifreleme işlemleri daha hızlı tamamlanır, daha az bellek kullanımı olur ve şifrelenmiş mesaj boyutunun kısalır. Diğer asimetrik kriptografi yöntemlerine göre bit başına daha fazla güvenlik sağladığından düşük işlem güçlü KSA'larda kullanılması uygundur.

RSA ve ECC açık anahtar kriptografi uygulamalarındandır. RSA sık kullanılan bir açık anahtar kriptografi yöntemidir ancak ECC daha kısa anahtar uzunluğu ile aynı güvenliği sağlamaktadır. Bu nedenle günümüzde endüstri ve akademik alanlarında kullanımı gittikçe artmaktadır. RSA-2048 kullanıldığı duruma karşılık gelen ECC anahtar uzunluğu 224 bit olarak hesaplanmıştır. Şekil 2.15'te RSA ile ECC'nin anahtar uzunluğu karşılaştırması, Şekil 2.16'te ise tüketilen enerjiler gösterilmiştir.

RSA/DSA	ECC	ECC:RSA/DSA
512	112	1:5
1024	160	1:6
2048	224	1:9
3072	256	1:12
7680	384	1:20
15360	512	1:30

Şekil 2.15 : ECC ve RSA anahtar uzunlukları

algorithm	signature		Key exchange	
	signature	verification	Client	Server
RSA-1024	304	11.9	15.4	304
ECDSA-160	22.82	45.093	22.3	22.3
RSA-2048	2302.7	53.7	57.2	2302.7
ECDSA-224	61.54	121.983	60.4	60.4

Şekil 2.16 : ECC ve RSA enerji tüketimleri

2.3.6 Hibrit Kriptografi

Simetrik anahtar algoritmaları ile anahtar dağıtımı işlemi yapılamamaktadır. Asimetrik kriptografi ile yapılan şifreleme işlemleri simetrik algoritmalara göre fazla işlem gücü gerektirdiğinden daha fazla enerji harcanmaktadır. Simetrik ve asimetrik kriptografinin avantajlı özellikleri birleştirilerek hibrit kriptografi modelleri geliştirilmiştir. Simetrik şifreleyiciler için rastgele gizli anahtar üretilir. Bu anahtar gönderici düğümde alıcının açık anahtarı ile şifrelenerek asimetrik kriptoloji şifreleyicisini kullanır. Gönderici mesajı simetrik şifreleyiciye ait gizli anahtarla beraber şifreler ve alıcı düğüme gönderir. Alıcı düğüm öncelikle aldığı mesajın şifre çözme işlemini kendine ait gizli anahtarı kullanarak gerçekleştirir ve simetrik gizli anahtara erişir. Elde edilen simetrik gizli anahtarı kullanarak mesajın şifresini çözer ve orijinal mesaja ulaşır.

2.4 Geliştirme Ortamı

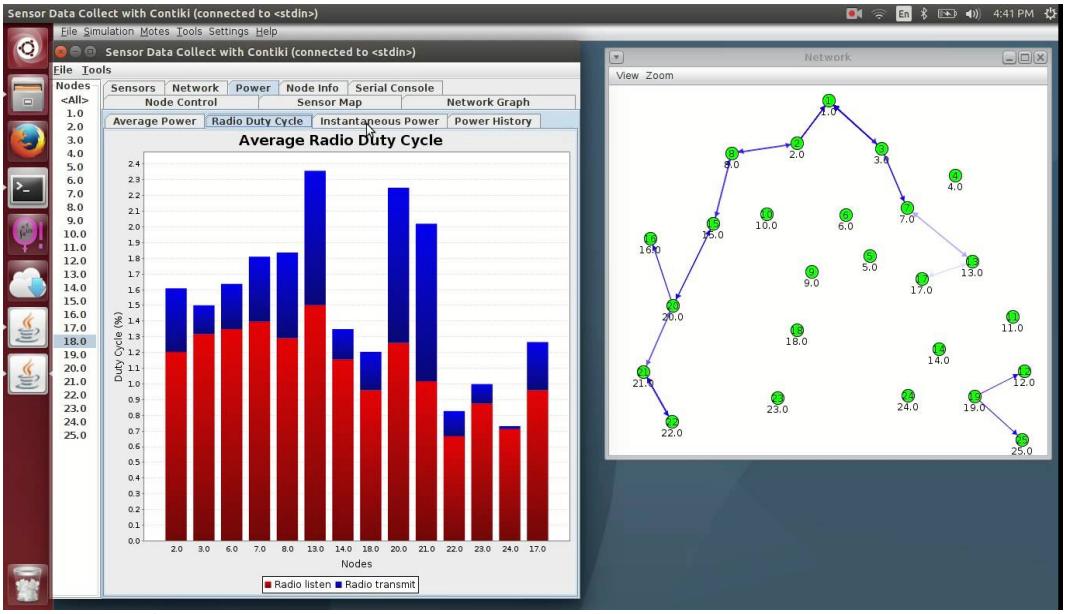
2.4.1 Contiki

Contiki [9] KSA'lardaki kısıtlamaları temel alınarak hazırlanmış, içerisinde çekirdek kütüphaneleri, program yükleyici ve bir dizi işlemi bulunduran bir işletim sistemidir. Ağ bağlantılı gömülü sistemlerde, akıllı nesnelerde ve KSA'larda kullanılır. Contiki akıllı nesne uygulamalarının programlanmasına yardımcı olan mekanizmalara sahiptir. İşletim sistemi C dili kullanılarak geliştirilmiştir ve içindeki tüm uygulamalarda C dilinde kullanılmıştır. Bu nedenle MSP430 gibi mimarilere kolayca port

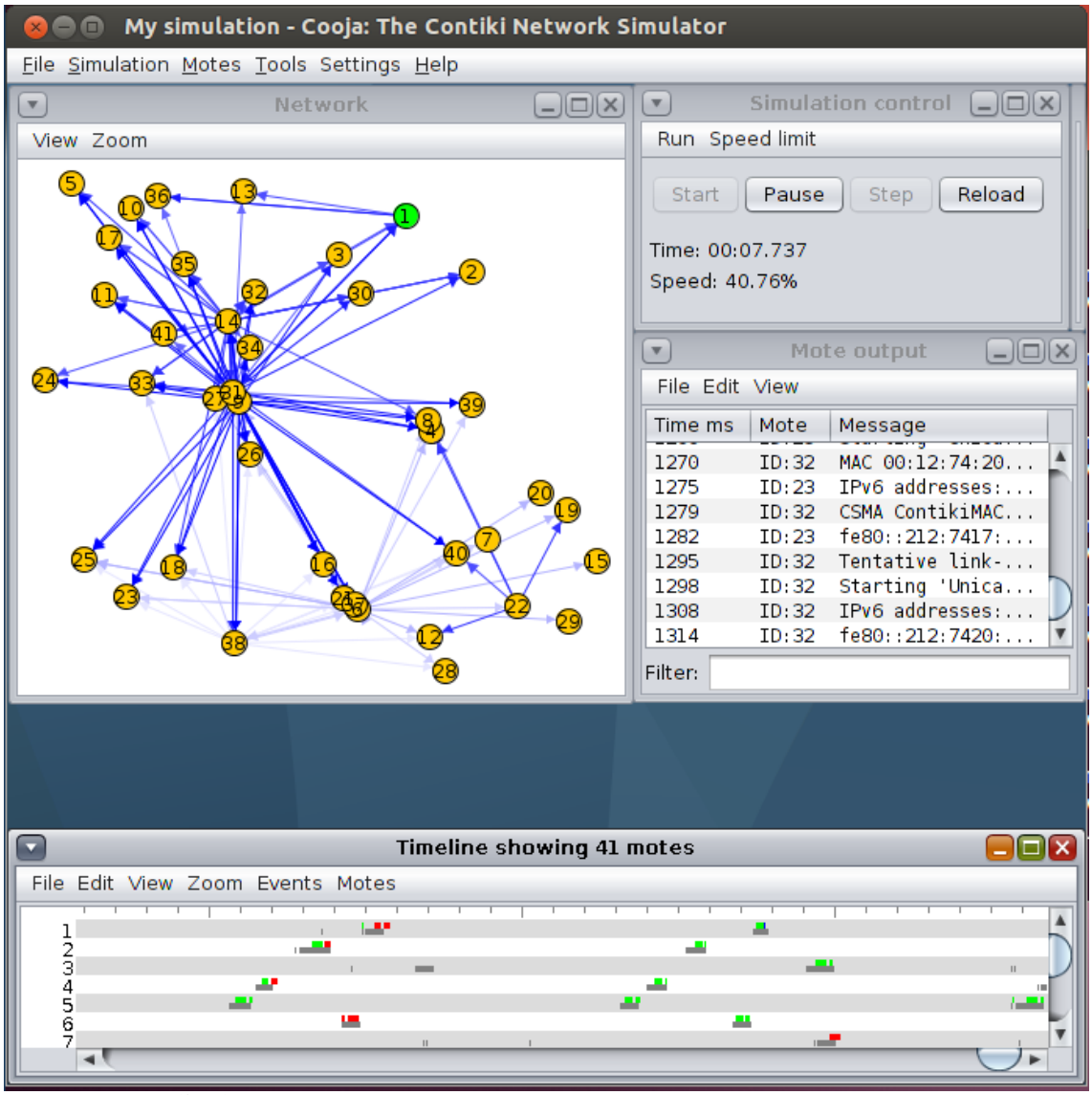
edilebilmektedir. KSA işletim sistemleri arasında IP iletişimini sağlayan ilk işletim sistemidir. Program yükleyici programları belleğe yükleme işlemini gerçekleştirir. Bu işlemi ana bilgisayarın kaynaklarını veya bağlı cihazın EEPROM hafızasını kullanır. Contiki işletim sistemi farklı katmanlar için farklı modüllere sahiptir. Yönlendirme modülleri "contiki/core/net/rpl" dizininde yer almaktadır. Bu dizinde yer alan dosyalar yaptıkları işlevlere göre isimlendirilmiştir. Örneğin, rpl-dag.c dosyası DAG(Yönlendirilmiş Döngüsel Ağaç) oluşturma işlevlerini içerir, rpl-icmp6.c dosyası ise ICMP(İnternet Kontrol Mesaj Protokolü) mesajlarının gönderme ve alma işlemlerini gerçekleştirecek arayüzü sahiptir. Bu çalışmada Contiki işletim sistemine ait bu dosyalar ve eklediğimiz ECC, AES ve anahtar dağıtımı ile ilgili dosyalar kullanılmıştır.

2.4.2 Cooja

KSA'lar çok sayıda düğümün bir araya gelmesinden oluştuğu için, geliştirme yapmak ve değişiklikleri test etmek zordur. Bu işlemi kolaylaştırmak için simülatörler kullanılmaktadır. Cooja, Contiki işletim sistemini kullanan KSA'ları simüle etmek için tasarlanmış Java tabanlı bir simülatördür [10]. Simülatör Java dilinde yazılmıştır ancak düğüm yazılımlarının C ile yazılmasına izin verir. Simülatör işletim sisteminde yazılmış programları ana bilgisayarda veya MSP430 simülatöründe derleyebilir. Cooja'da simüle edilmiş düğümlerle ilgili tüm etkileşimler Simulation Visualizer, Timeline ve Radio logger gibi eklentiler aracılığıyla gerçekleştirilir. Simülasyonu 'csc' (Cooja simülasyon konfigürasyonu) uzantılı bir xml dosyasında saklar. Bu dosya simülasyon ortamı, kullanılan eklentiler, düğümler ve konumları ve radyo ortamı vb. hakkında bilgiler içerir. Şekil 2.17 ve Şekil 2.18'te Cooja simülatörünün arayüzü görülebilir. Cooja simulatorü başka dizinde yer alan Contiki uygulamalarını çalıştırır ve RPL parametrelerini tek bir yerden değiştirme yeteneği sağlayan bir "project-conf.h" dosyası içermektedir.



Şekil 2.17 : Cooja üzerinde çalışan veri toplama simülasyonu



Şekil 2.18 : Cooja üzerinde incelenen kablosuz iletişimler

3. RPL YÖNLENDİRME PROTOKOLÜ

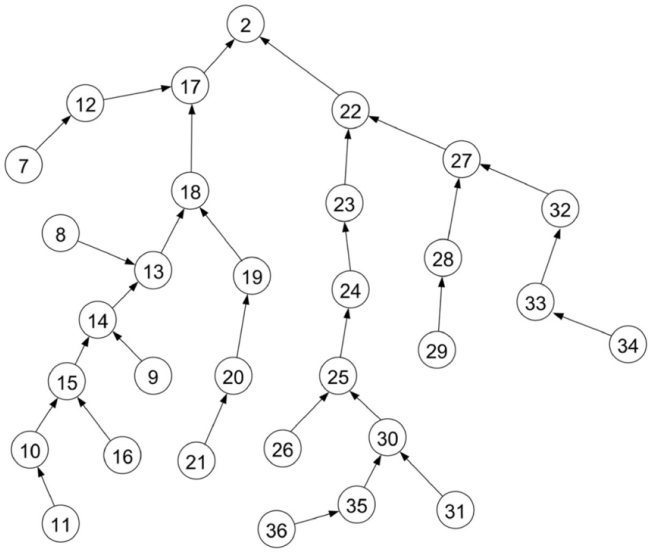
RPL(Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü) düşük güçlü ve kısıtlı kaynaklı KSA'lar için geliştirilmiş bir yönlendirme protokolüdür [5]. Bu protokol düğümler arası iletilen paketlerin akıllı bir biçimde iletilmesinden sorumludur. KSA'larda reaktif ve proaktif olmak üzere 2 tip yönlendirme protokolü vardır. RPL proaktif bir yönlendirme protokolüdür. RPL ağı kurulmaya başladığı anda düğümler arası yolları belirlemeye çalışır ve periyodik olarak ağ hakkında bilgi toplamaya devam eder. *DAG (Yönlendirilmiş Döngüsel Ağaç)* olarak da adlandırılan ağaç yapılarını kullanır. RPL *DODAG (Hedef Odaklı Yönlendirilmiş Döngüsel Ağaçlar)* şeklinde kurulur. Yani ağın diğer ağlar ile haberleştiği düğüm, DAG'ın kök düğümü gibi davranır. RPL ağında yer alan DODAG sayısı birden fazla olabilir ve bütün bu DODAG'ların birleşimine RPL olayı denir. Her RPL olayının kendine özgü bir kimliği vardır. Ağda aynı anda birden fazla RPL olayı bulunabilir ve her bir düğüm birden fazla RPL olayına bağlı olabilir. Ancak her bir düğüm RPL olayları için bir DODAG yapısına aittir [51].

RPL ağındaki her bir düğüm kendine bir ebeveyn düğüm seçer. Seçilen ebeveyn o düğüm için bir ağ geçidi gibi davranır. Eğer düğüme gelen paketin gönderileceği adres iletim tablosunda değilse, bu düğüm o paketi seçtiği ebeveyne gönderir ve paket bu şekilde gönderilmek istenen hedefe iletilir. RPL ağındaki tüm düğümler, kök düğümünden aşağı doğru yönlendirme tabloları vardır. Böylece kök düğümüne yakın düğümler daha büyük yönlendirme tablolarına sahiptir.

3.1 Ağ Topolojisi

KSA'lar önceden tanımlı bir topolojiye sahip olmadığından, RPL'in ilk olarak düğümler arası bağlantıyı kurması gerekmektedir.

RPL Şekil 3.1'te görüldüğü gibi protokolü ağaç yapısını en üstte yer alacak kök düğümünden başlar ve kenarlarda yaprak düğümlerle beraber ağaç topolojisini oluşturur. RPL'de genellikle tercih edilen bir ebeveyn olsa da o düğüm ile bağlantı



Şekil 3.1 : Ağaç yapısı

kaybolduğunda bağlanabilecek alternatif ebeveynlerin listesini tutmaktadır. Bu nedenle her bir düğüm için birden fazla yönlendirme yer almaktadır. [5]. RPL ağdaki mesaj trafiğin hareketlerini belirtmek için "aşağı yönlü" veya "yukarı yönlü" terimlerini kullanmaktadır. Yukarı yönlü mesajlar yaprak düğümlerden kök düğümüne doğru gönderilirken, aşağı yönlü mesajlar de kök düğümden yaprak düğümlere doğru gönderilmektedir.

3.1.1 Yukarı Yönlü Yönlendirme

Mesaj trafiğinin yukarı yönlü olabilmesi için DODAG bilgilerine ihtiyaç duymaktadır. DODAG bilgisinde düğümün tercih ettiği ebeveynler yer almaktadır. Böylece herhangi bir düğüm kök düğümüne mesaj göndermek istediğinde bu mesaj önce tercih edilen ebeveyne iletilir, daha sonra o düğüm kendi tercih ettiği ebevenye iletir. Bu süreç mesaj kök düğümüne iletilene kadar sürmektedir.

DODAG'da yer alan bir düğümün diğer düğümlere olan pozisyonunu belirlemek ve ağaç topolojinde oluşabilecek döngülerden kurtulabilmek için derecelendirme sistemi kullanılmaktadır. Dereceler 16 bitlik bir değerdir ve OF(Objektif fonksiyon)'e göre belirlenmektedir. Kök düğümü her zaman 0 derecesine sahiptir ve kökten uzaklaştıkça dereceler artmaktadır. Ebeveyn düğümün derecesi ona bağlı çocuk düğümden her zaman düşüktür.

RPL protokolü DODAG bilgilerini iletmek için DIO(DODAG Bilgi Mesajı) ve DIS(DODAG Bilgi İstemi) mesajlarını kullanır. DIO mesajını alan düğümler ağın parametreleriyle ilgili bilgilere sahip olur. Düğümler ağdan DIO mesajı almak istediklerinde DIS mesajı gönderirler. Mesajlarla ilgili detaylı bilgi ilerleyen bölümlerde anlatılacaktır.

3.1.2 Aşağı Yönlü Yönlendirme

Mesajların yönü ağdaki kontrol mesajlarının yönüne göre belirlenmektedir. RPL aşağı yönlü yönlendirme tablosunu güncel tutmak için DAO(Hedef Reklam Objesi) mesajını kullanır. Aşağı yönlü haberleşme denmesine rağmen DAO mesajları yukarı yönlü gönderilmektedir. DAO mesajları sadece düğümler arası DIO kontrol mesajlarının ardından gönderilmektedir. Bu mesaj kök düğümüne kadar iletilmektedir ve yol üzerindeki bütün düğümlerin mesajı yollayan düğüme nasıl erişeceği belirlenir.

3.2 Yönlendirme Metrikleri

KSA'larda düğümler arasında oluşacak bağlantıları kurmak ve ağaç yapısını oluşturmak için bazı metriklere ihtiyaç vardır. Bu metrikler düğümler arası hangi yolun seçileceği ve bağlantının kalitesine göre değişmektedir. Bu metriklerden en çok kullanılanlar beklenen gönderim sayısı, minimum hop sayısı ve tüketilen enerjidir.

3.2.1 Minimum Hop Sayısı

Yönlendirme protokollerinde kullanılan bu metrik kaynaktan hedefe gönderilen mesajın kaç adet hop işlemi yaptığını belirtir. Örneğin minimum hop sayısı 5 ise, kaynaktan gönderilen mesaj alıcıya ulaşana kadar 5 adet düğümden geçiyor demektir. Amaç bu sayıyı minimum tutup, ağ üzerindeki düğümlerin enerji tüketimini azaltmaktır.

3.2.2 Beklenen Gönderim Sayısı

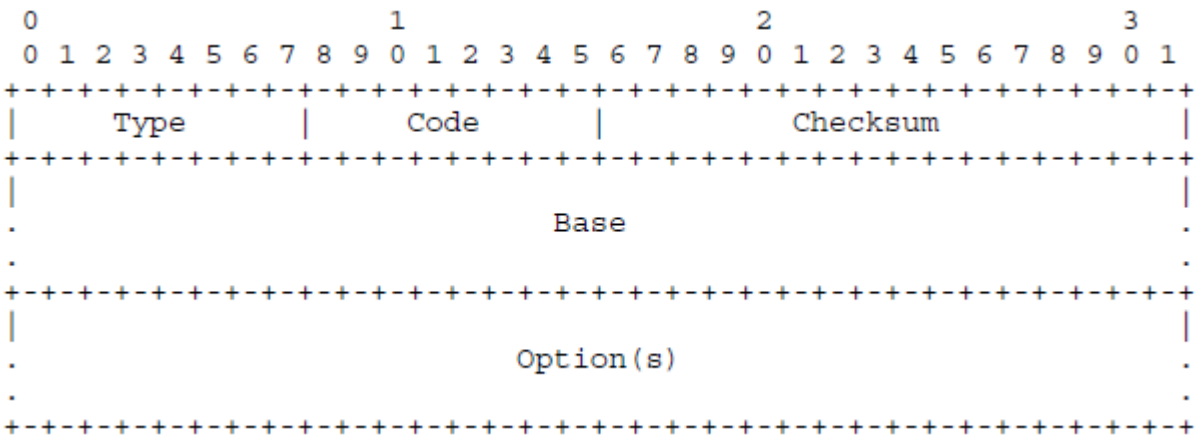
Belirli bir bağlantı üzerinden gönderilecek mesajı iki düğüm arasında iletmek için gereken gönderim sayısıdır. Bu değer hesaplanırken hatta kullanılan bütün bağlantıların Bu düğümler arası bağlantı kaliteli ise bu değer 1'e yakın olur.

3.2.3 Enerji

KSA'lardaki en önemli kısıtlardan birisi enerjidir. Bu nedenle düğümlerin enerji kullanımı kritik önem taşımaktadır.

3.3 RPL Kontrol Mesajları

RPL protokolü ağın topolojisini oluşturmak ve ağın sürekliliğini sağlamak için RPL kontrol mesajlarını kullanır. Şekil 3.2'te RPL kontrol mesaj yapısı görülmektedir.



Şekil 3.2 : RPL kontrol mesajı [5]

"Type" alanının RPL kontrol mesajlarına ait değeri 155'tir. "Code" alanı ile kontrol mesajlarının tipini belirlenir. "Base" kısmında mesaj tipine uygun veri alanı yer almaktadır. Bu alan her kontrol mesajı için farklılık içermektedir. Ayrıca kontrol mesajlarında kullanılmak üzere opsiyonel alanlar da bulunmaktadır. Standartta tanımlı RPL kontrol mesajları mesaj kodları ile beraber aşağıda listelenmiştir.

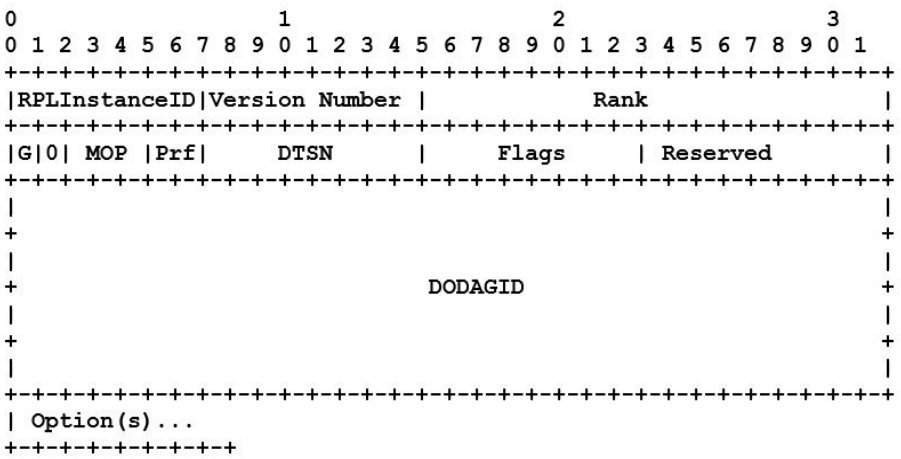
- 0x00: DIS
- 0x01: DIO
- 0x02: DAO
- 0x03: DAO-ACK
- 0x80: Secure DIS
- 0x81: Secure DIO
- 0x82: Secure DAO

- 0x83: Secure DAO-ACK
- 0x8A: Consistency Check

Standart DIO, DIS, DAO, DAO-ACK mesajları aşağıda detaylı olarak anlatılacaktır.

3.3.1 DIO

DIO mesajı periyodik olarak gönderilen bir kontrol mesajıdır. Mesajı gönderen birimin bağlı olduğu DODAG ile ilgili bilgileri içerir. Mesajı alan çocuk düğüm DIO mesajındaki bilgileri kullanarak ağa katılır ve mesajı gönderen düğümü kendine ebeveyn olarak seçer. Şekil 3.3 ile ilgili bilgiler aşağıda belirtilmiştir.



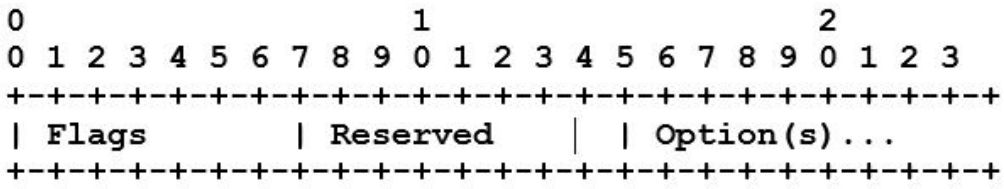
Şekil 3.3 : DIO mesajının yapısı [5]

- **RPLInstanceID:** 8 bit uzunluğundaki bu değer kök DODAG düğümü tarafından atanmıştır. RPL'in hangi gruba ait olduğunu belirtir.
- **Version Number:** 8-bit uzunluğundaki bu değer DODAG'a ait kök düğümünün versiyonudur. Ağda bir değişiklik olduğu zaman versiyon numarası 1 artar. Alınan her DIO mesajıyla güncel versiyona ait parametreler elde edilir.
- **Rank:** 16-bit uzunluğundaki bu değer DODAG'a ait düğümün derecesini belirtir. Bu derece kök düğüme olan uzaklığı belirtir.
- **Grounded (G):** DODAG'ın dışarıdaki ağlarla iletişim durumunu gösterir. Lokal bir ağda ise bu bayrak tanımlanır.

- **Mode of Operation (MOP):** Ağa katılacak düğümlerin çalışma modunu belirtir. Yönlendirici veya yaprak modu olmak üzere 2 çeşit çalışma modu bulunur. Yönlendirici olarak katılan düğümlerin yönlendirme tablosu tutması gerekmektedir.
- **DODAGPreference (Prf):** 3-bit uzunluğundaki bu değer aynı grupta yer alan DODAG kök düğümü ile diğer DODAG kök düğümleri arasındaki tercih sırasıdır.
- **DTSN:** 8-bit uzunluğundaki bu değer DIO mesajının tazeliğini garanti eder.
- **DODAGID:** 128-bit uzunluğunda olan bu değer kök tarafından belirlenen özgün IPv6 adresidir.

3.3.2 DIS

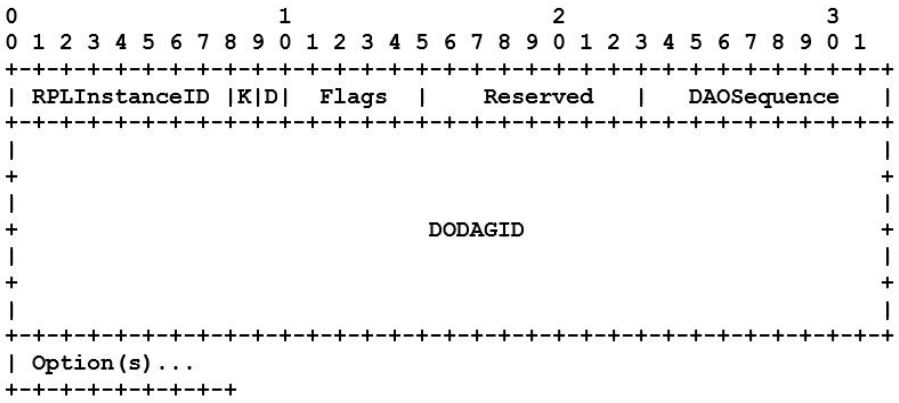
KSA'larda yer alan ve henüz DIO mesajı almamış bir düğüm ağa katılmak için veya periyodik DIO süresinini beklemeden ağ ile ilgili güncel parametreleri almak amacıyla komşu düğümlere DIS mesajı gönderir. Bu mesajı alan düğümler DIO mesajı ile cevap verir. Böylece DODAG hakkındaki bilgiler öğrenilir ve ağa katılım sağlanmış olur. Mesajın yapısı Şekil 3.4'te görüleceği üzere "flags" ve "options" alanlarından oluşmaktadır. Bu alanların aktif kullanımı yoktur ve ilerleyen zamanlarda kullanılmak için ayrılmıştır.



Şekil 3.4 : DIS mesajının yapısı [5]

3.3.3 DAO

DAO mesajı hedef düğüme ait yönlendirme bilgilerini DODAG boyunca taşımak için kullanılır. Kök düğümü hariç diğer bütün düğümler bu mesajı gönderir. DIO mesajını alan çocuk düğüm kendi ebeveynlerine DAO mesajı gönderir. Yukarı yönlü yönlendirme mesajıdır. DAO mesajı depolama modu ayarına bağlı olarak çocuk düğümden tercih ettiği ebeveynlere veya direkt olarak kök düğümüne gönderilir. DAO mesajının yapısı Şekil 3.5'te gösterilmiştir.

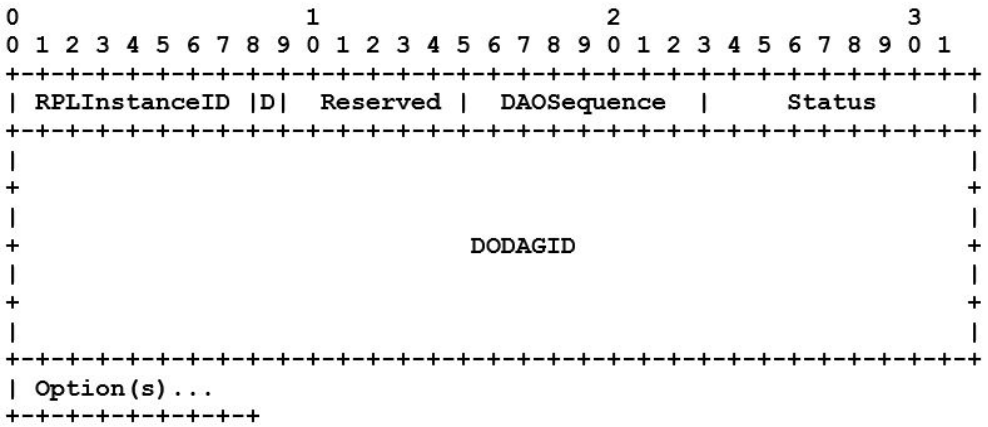


Şekil 3.5 : DAO mesajının yapısı [5]

- **RPLInstanceID:** DIO mesajında yer alan RPL grup değeridir.
- **K:** Alıcı düğümün DAO-ACK mesajı gönderip göndermeyeceğini belirtir.
- **D:** DODAGID alanının olup olmadığını belirtir.
- **DAOSequence:** Belirli düğümden gönderilen özgün her DAO mesajında artırılır.
- **DODAGID (optional):** 128-bit uzunluğundaki bu değer DODAG kökü tarafından tanımlanmıştır ve DODAG'ın kimliğini belirtir. Bu alan sadece D bayrağı tanımlanmış ise geçerlidir.

3.3.4 DAO-ACK

DAO mesajını alan düğüm opsiyonel olarak DAO-ACK mesajıyla cevap gönderebilir. Böylece DAO mesajının iletildiği bilgisi ve alınan DAO mesajının doğruluğu garanti edilmiş olur. Şekil 3.6'te mesaj yapısı gösterilmiştir.



Şekil 3.6 : DAO-ACK mesajının yapısı [5]

- **RPLInstanceID:** DIO mesajında yer alan RPL grup değeridir.
- **D:** DODAGID alanının olup olmadığını belirtir.
- **DAOSequence:** Alınan DAO mesajındaki değeri göndericiye tekrar gönderir. Alınan DAO mesajı ile gönderilen DAO mesajı arasındaki korelasyonu belirtir.
- **Status:** DAO mesajının kabul edilip edilmediğini belirtir. Bu değer 0 ise alınan DAO mesajı direkt kabul edilmiştir. 1-127 arasında ise DAO-ACK mesajı kabul edilmiştir fakat gönderen düğüme daha iyi bir ebeveyn seçmesi için tavsiye edilir. 127-255 arasındaki değerler ise DAO mesajının reddedildiğini gösterir[8].

3.4 Görev Fonksiyonu

Görev fonksiyonu KSA'larda yer alan düğümlerin ebeveyn seçmek ve derecelerini belirlemek için kullandığı yöntemlerin bütünüdür. Bu yöntemler minimum hop sayısı, harcanılan enerji, en az gecikmeli yol gibi yöntemlerdir. Bütün bu yöntemlerin amacı düğümlerin derecelerini en uygun şekilde belirlemek içindir. Güç kaynağına bağlı sistemler ile pile bağlı KSA sistemlerinin gereksinimleri birbirinden farklıdır. KSA'lar için en önemli parametrelerden biri düşük güç kullanımıdır.
Contiki işletim sisteminde OF0(Görev fonksiyon 0) ve ETX (Beklenen gönderim sayısı) olmak üzere iki tip görev fonksiyonu bulunmaktadır. OF0 yöntemi hop sayısını minimum sayıda tutmayı hedeflerken, ETX fonksiyonu düğümler arası en uygun yolu belirleyerek mesaj gönderim oranının iyileşmesini hedeflemektedir. RPL protokolünde objektif fonksiyonlar farklı katmanda geliştirildiği için gereksinimlere özgü görev fonksiyonu geliştirilebilir.

3.5 Trickle Zamanlayıcısı

KSA'larda ağın devamlılığını ve sürekliliğini sağlamak için periyodik olarak DIO mesajları gönderilir. Gönderilen bu mesajın sıklığı enerji tüketimini etkilemektedir. Bu DIO mesajların periyodu *Trickle* zamanlayıcısı ile belirlenir. Gönderilen her DIO mesajından sonra bu zamanlacının periyodu 2 katına çıkar. Böylece uzun süreli kullanımlarda enerji tüketimi azalmış olur [38]. Eğer ağda bir tutarsızlık tespit edilirse (Örneğin Seçilen ebeveynin ortamdan ayrılması, ağa yeni bir düğümün katılması vb...) *Trickle* zamanlayıcısı minimum'a çekilir ve ağda tamir süreci hızlı bir

şekilde gerçekleşir. *Trickle* zamanlayıcısının ayarlanabilir 3 parametresi vardır ve bu parametreler aşağıda açıklanmıştır.

- **Imin:** İki DIO mesajı arasındaki minimum süredir. Gönderilen her DIO mesajından sonra bu değer 2'ye katlanır. RPL protokolünde "DIOIntervalMin" parametresi ile tanımlanmıştır. Contiki ise RPL_DIO_INTERVAL_MIN tanımıyla bu değeri belirlemektedir. Bu tanımın karşılığı 10 ise Imin değeri $2^{10} = 1024$ ms olmaktadır bu da 1 saniyeye eşittir. Eşitlik 3.1 ile Imin değerinin nasıl hesaplanacağı gösterilmiştir.

$$I_{min} = 2^{MINIMUM\ DIO\ ARALIGI} \tag{3.1}$$

- **Imax:** İki DIO mesajı arasındaki maksimum süredir. Gönderilen her DIO mesajından sonra katlanan sürenin maksimum değeridir. RPL protokolünde "DIOIntervalDoublings" olarak tanımlanmıştır. Contiki ise RPL_DIO_INTERVAL_DOUBLINGS tanımıyla bu değeri belirlemektedir. Bu tanımın karşılığı 10 ise Imax değeri $1024 * 2^{10} = 104857$ ms olmaktadır bu da 17.5 dakikaya eşittir. Eşitlik 3.2 ile Imax değerinin nasıl hesaplanacağı gösterilmiştir.

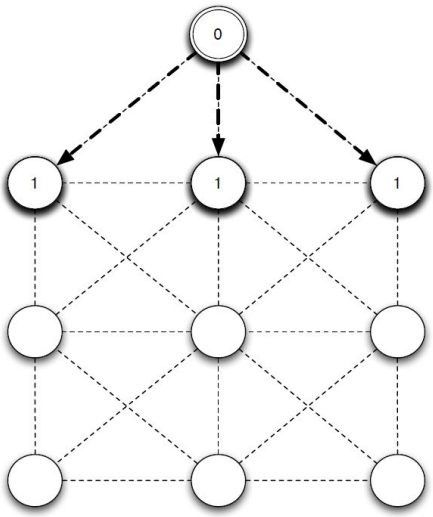
$$I_{max} = I_{min} * 2^{DIO\ KATLAMA\ ARALIGI} \tag{3.2}$$

- **Artık sabit:** 0'dan büyük bir sayıdır ve DIO gönderimini azaltır. Stabil hale gelen ağda kaç adet mesajdan sonra DIO mesajı gönderilmeyeceğini belirler. Ayrıca bütün düğümlerin her periyotta sürekli olarak veri göndermesi ağda trafiğe neden olur. Bu yaklaşım bütün düğümlerin aynı anda periyodunu sıfırlamasına neden olacağı için tehlikelidir. Bu değer genellikle 1-5 arasında seçilmektedir. Bu değer aralığında ağ trafiği ve düşük güç tüketimi arasında iyi bir denge sağlanır.

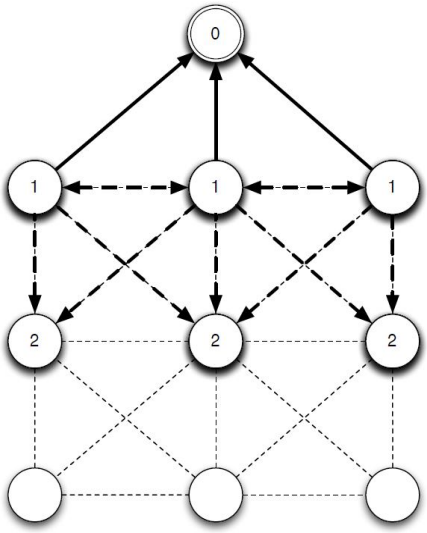
3.6 DODAG Oluşumu

RPL protokolünde DODAG oluşumu kök düğümden başlar. Kök düğümü DODAG konfigürasyon parametrelerini ve ağ ile ilgili bilgileri DIO mesajıyla gönderir. Şekil 3.7a'te bu gönderim gösterilmiştir. Bu mesajı alan komşu düğümler ağ ile ilgili bilgileri alır ve verileri işler. DIO mesajları bu şekilde sırayla iletilmeye başlanır.

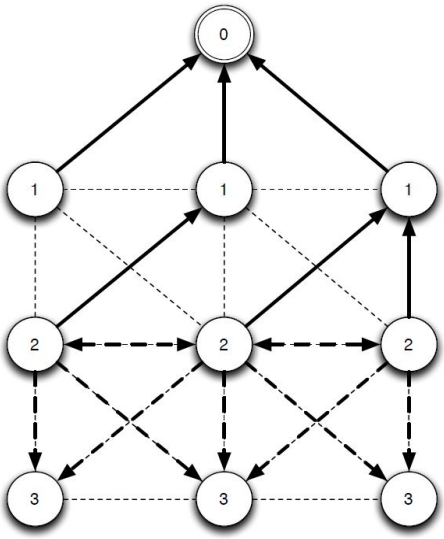
Herhangi bir DODAG'a bağlı olayan düğüm, gönderici düğüm ile bağlantı kalitesini hesaplar ve ağa katılıp katılmama kararını verir. Komşu düğüm DODAG'a katılırsa kök düğümüne doğru bağlantı oluşturur ve kök düğüm DODAG kökü ebeveyn olarak seçilir. Kendi DIO mesajını diğer düğümlere iletir. Şekil 3.7b'te bu durum belirtilmiştir. Daha sonra bu DODAG içerisindeki derecesini hesaplar ve DAO mesajı ile ağa katıldığı bilgisini ebeveynine iletir. Herhangi bir DIO mesajı almamış ve ağa katılmamış bir düğüm komşularına periyodik DIS mesajı göndererek DODAG bilgilerini isteyebilir. Bütün düğümler ağa katılana kadar bu süreçler Şekil 3.7c ve 3.7d de görüldüğü gibi gerçekleştirir. Katılım tamamlandıktan sonra *Trickle* [38] algoritması ile kontrol mesajları gönderim periyotları ayarlanır. Böylece ağ içindeki stabillik sağlanır.



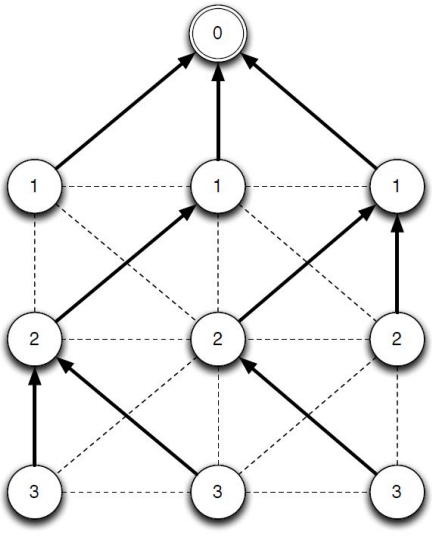
Şekil 3.7a : *Kök düğümü DIO mesajını gönderir*



Şekil 3.7b : *DIO mesajını alan düğümler ebeveyn seçtikten sonra kendi DIO mesajlarını gönderir*



Şekil 3.7c : *Bütün düğümler DODAG'a katılıncaya kadar DIO mesajları gönderilir*



Şekil 3.7d : *Bütün düğümler DODAG'a katılmıştır*

Şekil 3.7 : DODAG oluşum süreci. Çizikli oklar DIO mesajlarını gösterirken, tam oklar tercih edilen ebeveyn seçimlerini göstermektedir.

4. KABLOSUZ SENSÖR AĞLARINDA GÜVENLİK VE GELİŞTİRİLMİŞ YÖNTEMLER

4.1 Kablosuz Sensör Ağlarında Güvenlik

KSA'larda güvenli ağ iletişimini sağlamak oldukça önemlidir. Ağa katılan bütün düğümler ağ parametreleri ile ilgili kritik bilgilere sahiptir. Bu durum güvenlik açıklarına neden olabilmektedir. Bu durumda asıl amaç kötü niyetli düğümlerin tespit edilip ağ ile ilgi kritik öneme sahip parametrelere erişimi engellenmelidir. Standart güvenlik önlemleri yüksek işlem gücü ve kaynak gerektirmektedir. Kısıtlı işlem gücü ve pile sahip olan KSA'lar için kriptografik işlemler yapmak daha maliyetlidir. KSA'lardaki güvenlik gereksinimleri aşağıda detaylı olarak anlatılacaktır. Ayrıca güvenlik gereksinimlerini sağlayabilmek için hangi yöntemlerin kullanılabileceği de belirtilmiştir.

4.1.1 Mesaj Gizliliği

Yetkisi olmayan düğümlerin ağda iletilen mesajlara erişmemesi için gereken bir güvenlik gereksinimidir. KSA'larda gönderilen mesajlar çok fazla düğüme iletilmektedir. Bu durumda yetkisi olmayan düğümler gönderilen mesajı kolayca elde edebilir. Bu duruma ağ ile ilgili önemli parametreler şifrelenerek önlem alınabilir. Diffie-Hellman anahtar değişimi, anahtar dağıtım mekanizmaları ve açık ve gizli anahtara sahip asimetrik kriptografi kullanılarak şifreleme ve şifre çözme işlemleri gerçekleştirilebilir. KSA'larda kullanılan şifreleme işlemleri simetrik ve asimetrik olmak üzere iki çeşittir. Simetrik şifrelemeler enerji tüketimi ve işlem gücü olarak daha hızlı olduğu için daha çok tercih edilmektedir, ancak şifrelemenin gücü daha zayıftır. Asimetrik şifreleme işlemleri daha güçlü şifreleme vadeder fakat daha enerji tüketmektedir.

4.1.2 Mesaj Bütünlüğü

Kimliği doğrulanmayan düğümlerin ağda iletilen mesajların içeriğini değiştirmesini engellemek için gerekli olan güvenlik gereksinimidir. Ağda iletilen mesajların içeriği değiştirilirse mesajın güvenilirliği azalır ve ağ topolojisini bozulabilir. Bu nedenle mesaj bütünlüğü çok önemlidir. Genellikle uçtan uca kimlik doğrulama yapılarak bu işlem gerçekleştirilir. Uçtan uca ifadesi ile gönderici düğüm ile alıcı düğüm arasındaki iletişim kastedilmektedir. Mesaj bütünlüğünün doğruluğu gönderilen ve alınan mesajın MAC ve imza gibi hash değerleri karşılaştırılarak teyit edilir.

4.1.3 Mesaj Kullanılabilirliği

Kimliği doğrulanmış düğümlerin herhangi bir engel olmadan sorunsuz bir şekilde haberleşmesi bir güvenlik gereksinimidir. Ağda yer alan düğümlerle istenildiği zaman haberleşme yapılmalıdır. KSA'larda yer alan düğümler kaynak olarak oldukça kısıtlıdır. Kullanılabilirlik özelliği kaynak yönetimi ile yakından ilgilidir.DoS(Hizmet Engelleme) atağı ve düğümün ağdan çıkarılması kullanılabilirliği etkileyen olaylara örnek olarak gösterilebilir. Hedef düğüme yapılacak DoS saldırıları alıcı düğümü sürekli meşgul eder ve kısıtlı kaynaklarını tüketir. Bu durumdan kurtulmak için ağdaki düğümlerin yüklerinin dengelenmesi, kimliği doğrulanmayan düğümlerin ağa katılmasının engellenmesi gerekir. Bu yöntemler kullanılsa bile ağda gönderilen mesaj sayısının artacağından enerji tüketimi artacaktır.

4.1.4 Kimlik Doğrulama

KSA'larda kimlik doğrulama işlemi kullanıcı kimliği doğrulama ve mesaj doğrulama olmak üzere iki çeşittir.

- **Kullanıcı Kimliği Doğrulama:** KSA'larda yer alan düğümlerin ağa hangi amaçla ağa katıldığı bilinmediğinden bu düğümlerin kimliğinin doğrulanmış olması önemlidir. Ağdaki düğümlerin kötü niyetli bir düğüm mü yoksa kayıtlı bir düğüm mü olduğu belirlenmelidir. Güvenliği sabit altyapılarda bu işlemi gerçekleştirmek göreceli olarak daha kolaydır. Coğrafi olarak dağıtılmış düğümlerin bir arada olduğu KSA'larda ise uygulanması daha zordur. Ağ içinde meydana gelebilecek ataklara karşı önceden belirlenmiş sınır değerleri veya öğrenilmiş veri setleri ile önlem almak için çalışmalar yapılmıştır. Ayrıca araştırmacılar

ABIM(Anormal Davranış Belirleme Mekanizması) yöntemleri geliştirmek için çalışmalar yapmaktadır.

- **Mesaj Doğrulama:** Mesaj güvenliğinin sağlanması için gönderici düğümün göndereceği mesajın sadece alıcı düğümde okunup işlenmesi gerekmektedir. MAC ve dijital imza yöntemleri bu amaç için kullanılabilir. Gönderici düğüm gizli anahtarı kullanarak MAC değerini hesaplar, mesaja ekler ve alıcı düğüme gönderir. Alıcı düğüm de aynı anahtarla MAC değerini hesaplar ve aldığı değerle karşılaştırır. Böylece mesajın doğruluğundan emin olur.

4.1.5 Karşılıklı Kimlik Doğrulama

KSA'larda yer alan düğümlerin karşılıklı olarak birbirlerine kayıtlı ve haberdar olma durumudur. Düğümler ağa katılım aşamasında düğümler birbirlerinin kimliğini doğrular ve bu aşamadan sonra normal haberleşmelerini gerçekleştirir. İstemci sunucu arasındaki ilişki örnek olarak gösterilebilir.

4.1.6 Mesaj Güncelliği

Mesaj güncelliği, ağda iletilen mesajların her zaman güncel olması ve iletilen mesajların mesaj tekrarı içermemesi durumu olarak tanımlanabilir. Mesaj tekrarlama atakları KSA'larda gerçekleştirilen ataklardan biridir. Kötü niyetli düğüm ağda iletilen mesajlardan birini alır ve ileri bir zamanda bu mesajı tekrar gönderir ve ağ topolojisini bozmaya çalışır. Buna önlem almak amacıyla mesaj tekrarlarını tespit edebilecek mekanizmalar kurulmalıdır. Mesaj tekrarı tespit edildiğinde ise mesaj işlenmemelidir. Ayrıca gönderilen mesajlara o anın zaman damgası eklenerek önlem alınabilir.

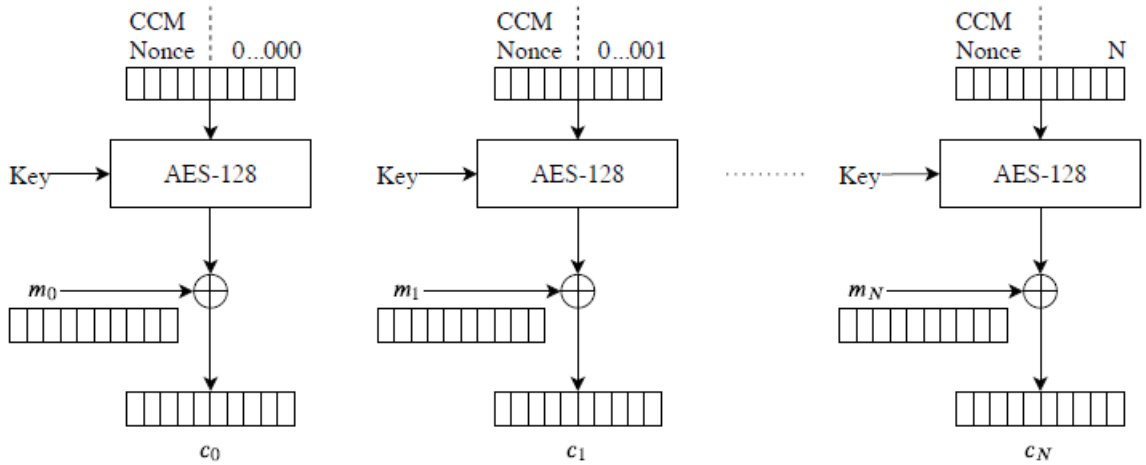
4.1.7 İleri ve Geri Yönlü Gizlilik

Mesaj gizliliğini sağlamak için ileri ve geri gizliliğin de sağlanması gerekmektedir.

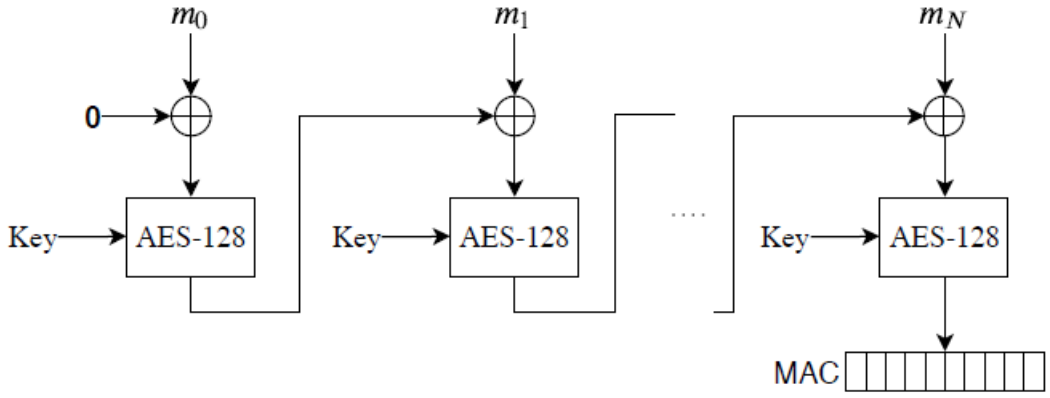
- **İleri Yönlü Gizlilik:** Ağdan ayrılan bir düğüm için ağ ile ilgili parametrelere ve anahtarlara erişememe durumudur.
- **Geri Yönlü Gizlilik:** Ağa yeni katılan düğümün ağda önceden gönderilen mesajlar hakkında bilgi sahibi olmamasıdır.

4.2 RPL Güvenlik Mekanizmaları

RPL protokolü sadece AES-128 ile CCM yapısını desteklemektedir. CCM(CTR ile CBC-MAC) 128 bitlik şifreleyici blokların bir sayaç değeri ile şifrelenip mesajda gizlilik ve güvenlik sağlaması için kullanılan bir yöntemdir. CTR terimi sayaç olarak kullanılan bir değişkendir. Şekil 4.1'te AES-128 CTR ile CCM, Şekil 4.2'te ise AES-128 CBC-MAC ile CCM kullanımları gösterilmiştir. CBC-MAC ile üretilen MAC değeri Security alanındaki LVL değişkenine bağlı olarak 32 veya 64 bit olmaktadır. MAC değeri mesajın bütünlüğünü garanti etmektedir. Kontrol mesajlarında yer alan güvenlik alanının sonundan başlayarak paketin kalan tüm baytları şifrelenmektedir. Böylece mesaj bütünlüğü ve gizliliği sağlanmış olur. Ayrıca RPL mesaj koduna bakarak bir mesajın güvenli olup olmadığı anlaşılabilmektedir.



Şekil 4.1 : AES-128 CTR ile CCM



Şekil 4.2 : AES-128 CBC-MAC ile CCM

RPL protokolünde güvenlik ile ilgili tanımlanmış 3 mod bulunmaktadır. Bu modlar aşağıda detaylı olarak açıklanmaktadır.

- **Güvenli olmayan:** RPL protokolünün varsayılan güvenlik modudur. RPL kontrol mesajları açık ve herhangi bir güvenlik alanı olmadan gönderilmektedir.

- **Önyüklü:** RPL protokolü sadece AES-128 ile CCM yapısını desteklemektedir.Bu modda gönderilecek RPL mesajları güvenli olmalıdır. Ağa katılmak isteyen düğüm önceden yüklenmiş anahtara sahip olmalıdır. Bu anahtar kullanılarak simetrik kriptolama işlemi yapılır. Böylece verinin bütünlüğü, gizliliği gibi güvenlik gereksinimleri sağlanmış olur. Ayrıca bu anahtara sahip olan düğümler yönlendirici veya iletici olarak ağa katılır. Yönlendirici olarak katılan düğümler ağ ile ilgili kritik parametrelere sahip olduğu için anahtarın mümkün olduğunca gizli tutulması gerekmektedir. Eğer bu anahtar ele geçirilirse ağ güvenliği tehlikeye girer ve kötü niyetli düğümler ağ ile ilgili bilgileri ele geçirebilir.

- **Kimliği Doğrulanmış:** RPL mesajları önyüklü modda olduğu gibi güvenli mesajları kullanmalıdır ve ağa katılmak isteyen düğüm önceden yüklenmiş anahtara sahip olmalıdır. Düğümler bu anahtarla verinin bütünlüğü, gizliliği gibi güvenlik gereksinimlerini de sağlar. Fakat bu anahtar ile sadece yaprak düğüm olarak katılabilir. Yönlendirici olarak ağa katılmak için düğüm ikinci bir anahtara ihtiyaç duymaktadır. Bu anahtarı anahtar otoritesinden alması gerekmektedir. Bu otorite isteği yapan düğüme eğer izin verildiyse ikinci anahtarı gönderir. Önyüklü mod ile tek farkı anahtarların düğümlere dağılma biçimidir. Bunun dışındaki güvenlik gereksinimleri ortaktır. Asimetrik kriptografinin yüksek bellek ve işlem gücü ihtiyacından dolayı KSA'larda uygulanmasında zorluklar vardır. IETF çalışma grubu RPL'de düğümlerin doğrulanması ile ilgili yeni bir çalışma grubu çağrısı yapmıştır. Anahtar dağıtma işlemleri simetrik kripto algoritmaları ile gerçekleştirilemez. RPL sadece simetrik algoritmaları desteklemektedir. Düğümlere anahtarların dağılımı, hangi şifreleme yöntemi ile gerçekleştirileceği ve bu modun uygulanması geliştirmeye açık alan olarak belirtilmiştir.

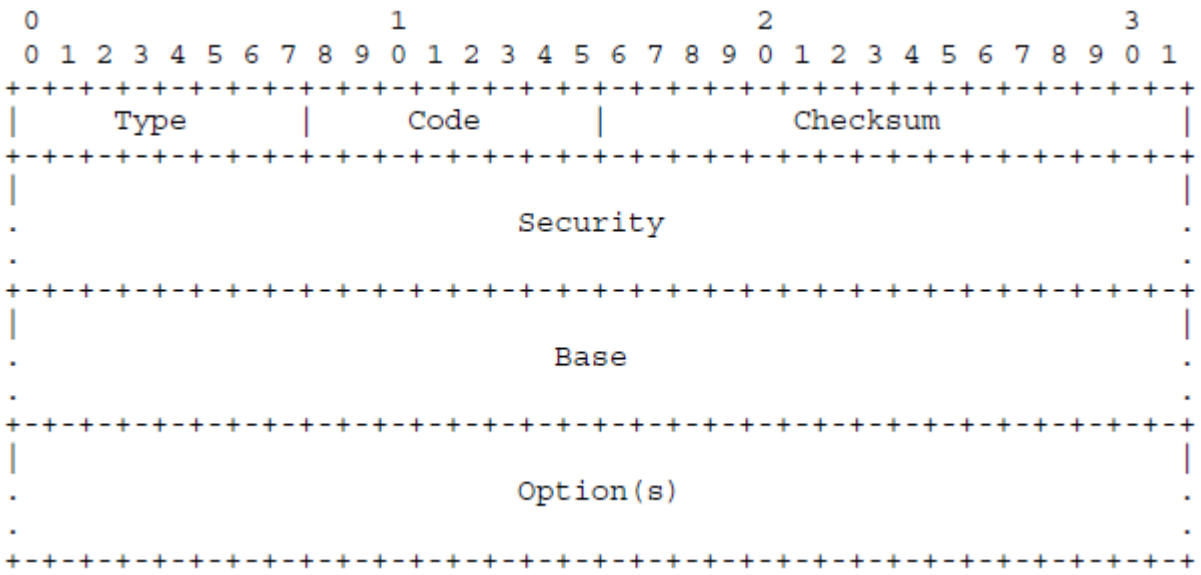
RPL protokolü güvenlik gereksinimleri olarak aşağıda belirtilen özellikleri belirlemiştir.

- **Veri Gizliliği:** Kontrol mesajlarının sadece hedef düğümde işlenmesidir. Diğer düğümlerin okudukları veriden ağ ile ilgilileri öğrenmemesi amaçlanmaktadır.

- **Veri Orijinalliği:** Gelen kontrol mesajlarının güvenilir bir kaynaktan gelip gelmediğini doğrular. Böylece alınan mesajın önceden tanımlanmış bir düğüm olup olmadığı anlaşılmaktadır.
- **Tekrarlama Koruması:** Kötü niyetli düğümlerin daha önce kullanılmış bir kontrol mesajını kullanarak ağ ile ilgili bilgileri almasını engellemek için gereklidir.

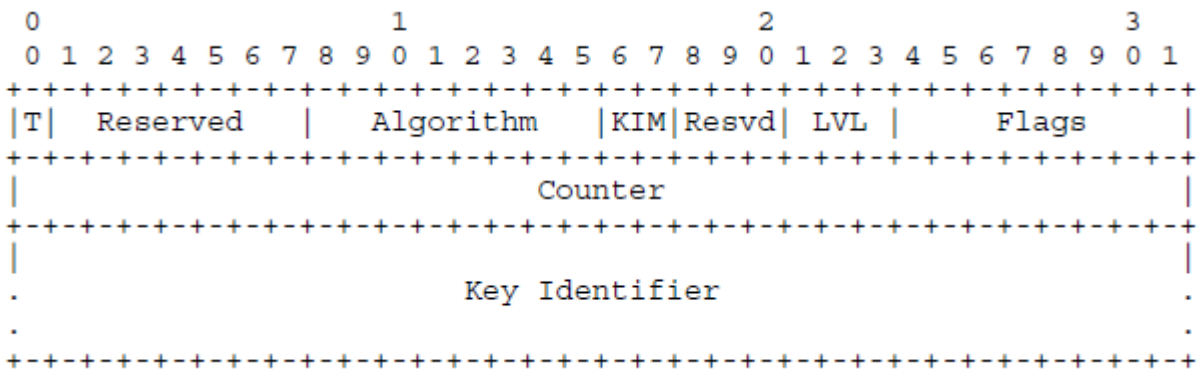
4.2.1 RPL Güvenli Mesajlar

DODAG'da yer alan düğümler güvenli modu kullanarak haberleşiyorsa, bütün RPL mesajları da güvenli olmalıdır. Her bir RPL mesajının güvenli versiyonu da bulunmaktadır.RPL mesajlarının güvenli olup olmadığı ICMP mesajlarının başlık alanındaki kod alanı ile belirlenmektedir. Güvenli DIS mesajı 0x80, güvenli DIO mesajı 0x81, güvenli DAO mesajı 0x82 ve güvenli DAO-ACK mesajı 0x83'tür. Güvenli RPL mesaj yapısı Şekil 4.3'te görülmektedir. Güvenli RPL kontrol mesajları standart mesajların aksine "Security" alanı içermektedir. Bunun dışında standart mesaj alanları ortaktır.



Şekil 4.3 : Güvenli RPL kontrol mesajı [5]

Security için ayrılmış alan Şekil 4.4'te detaylı olarak gösterilmiştir.



Şekil 4.4 : Security alanı [5]

- **T:** Bu alanın zaman damgası mı yoksa artan sayaç mı olduğunu belirtir.
- **Algorithm:** Ağda kullanılacak şifreleme, imza ve kimlik doğrulama tipini belirler.
- **KIM:** 2 bit uzunluğundaki bu değer ağdaki mesajlarda kullanılacak anahtarın kaynağının tipini gösterir. Bu değişkenin alabileceği değerler Şekil 4.5'te gösterilmiştir. '3' değeri için özel bir durum bulunmaktadır. Eğer LVL alanında şifreleme ile ilgili bir opsiyon seçilmiş ise "Key Identifier" alanı 9 byte veri içermelidir aksi halde bu alan boş bırakılmalıdır.
- **LVL:** 3 bitlik bu değer seçilecek KIM değerine karşılık gelen meesaj koruma sistemini belirler. Veri gizliliğini, orijinalliğini sağlayacak sistemin tipini belirtir. Bu değerin yüksek olması ağın daha iyi korunduğu anlamına gelmez. Şekil 4.6'te bu alanın alabileceği değerler gösterilmiştir. Ayrıca 4.6'te görülen "MAC" özelliği mesaja ait MAC değerinin uzunluğunu belirtir. ENC özelliği mesajın şifreli olup olmadığını, "Sign" ise imzanın uzunluğunu belirtir.

Mode	KIM	Meaning	Key Identifier Length (octets)
0	00	Group key used. Key determined by Key Index field. Key Source is not present. Key Index is present.	1
1	01	Per-pair key used. Key determined by source and destination of packet. Key Source is not present. Key Index is not present.	0
2	10	Group key used. Key determined by Key Index and Key Source Identifier. Key Source is present. Key Index is present.	9
3	11	Node's signature key used. If packet is encrypted, it uses a group key, Key Index and Key Source specify key. Key Source may be present. Key Index may be present.	0/9

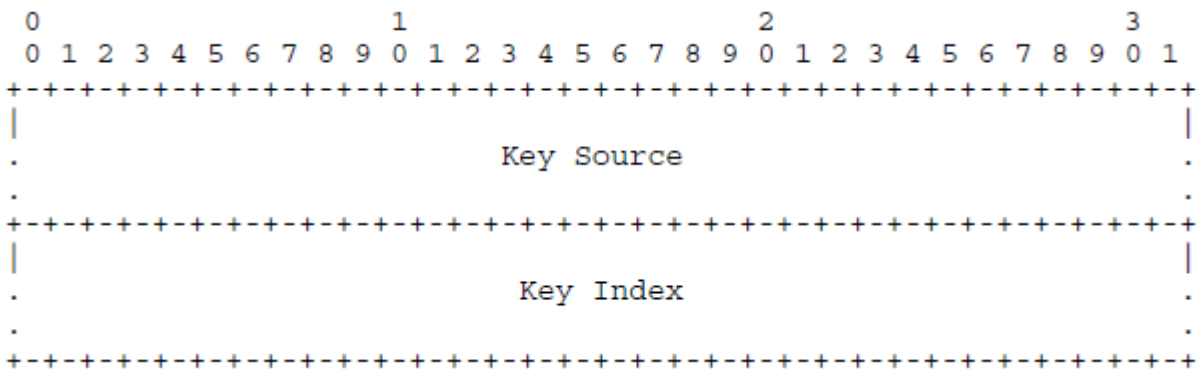
Şekil 4.5 : KIM tablosu [5]

- **Counter:** Kriptografik işlemlerde kullanılacak değerdir. 4 bayt uzunluğundadır.
- **Key Identifier:** Kriptografik işlemlerde hangi anahtarın kullanılacağını belirtir. Düğümlerin kendi arasında, grup içinde veya imza işlemlerinde hangi anahtarları kullanacağını belirtir. "Key Source" ve "Key Index" olmak üzere iki farklı alan içermektedir. Bu alanların detayları Şekil 4.7'te belirtilmiştir.
- **Key Source:** 8 bayt uzunluğundaki bu alan geçerli olduğunda grup anahtarının hangi kaynaktan geldiğini belirtir.

KIM=0,1,2		
LVL	Attributes	MAC Len
0	MAC-32	4
1	ENC-MAC-32	4
2	MAC-64	8
3	ENC-MAC-64	8
4-7	Unassigned	N/A

KIM=3		
LVL	Attributes	Sig Len
0	Sign-3072	384
1	ENC-Sign-3072	384
2	Sign-2048	256
3	ENC-Sign-2048	256
4-7	Unassigned	N/A

Şekil 4.6 : KIM değerine bağlı LVL Değerleri [5]



Şekil 4.7 : Anahtar Belirleme Alanı [5]

- **Key Index:** Aynı kaynakta birden fazla anahtar bulunabilmektedir. Bu anahtarların hangisinin o an kullanılan anahtar olduğunu belirten 1 bayt uzunluğundaki bir değerdir. ’0’ değeri önyüklü mod için ayrılmıştır. Farklı bir anahtar kullanılacaksa bu alanın değeri 0’dan farklı olmalıdır.

4.3 RPL Güvenli Ağa Katılma

Önyüklü veya kimliği doğrulanmış moduna sahip ağlar güvenli ağlar olarak tanımlanmıştır. Güvenli ağa katılmak isteyen düğümün önceden belirlenmiş bir anahtara sahip olması gerekmektedir. Bu anahtar ile komşu düğümlerle ve kök düğümle haberleşmektedir. Güvenli ağa katılmak isteyen düğüm güvenli DIO mesajını dinler. Eğer ağa trickle zamanlayıcısının periyodunu beklemeden katılmak istiyorsa güvenli DIS mesajı gönderip güvenli DIO mesajını tetikler. Standart DIO/DIS mesajlarının aksine güvenli modlarda kullanılan DIO/DIS mesajları için bazı değişiklikler yapmak gerekmektedir.

4.3.1 Önyüklü Modda Güvenli Ağa Katılma

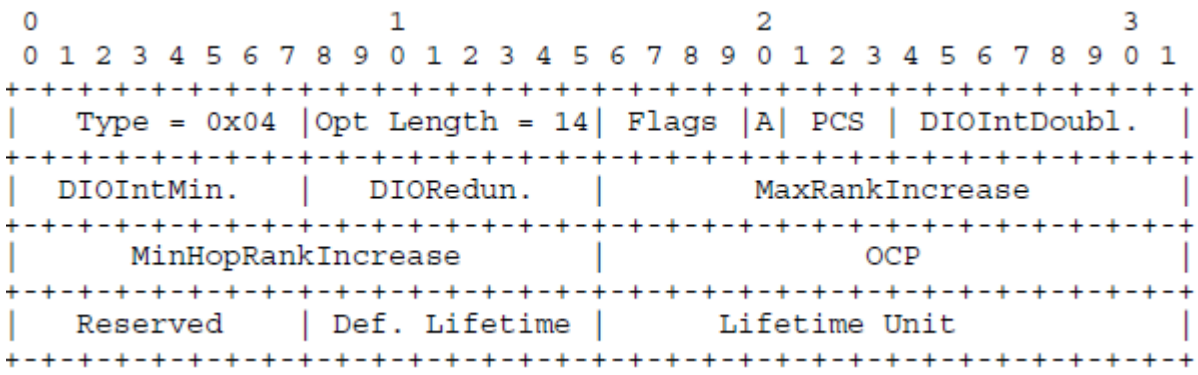
Önyüklü modda güvenli ağa katılmak için Şekil 4.8'te DODAG Yapılandırma opsiyonundaki 'A' bitinin 0 olması gerekmektedir. Ayrıca standartta tanımlı kurallar aşağıda belirtilmiştir.

- Gönderilen ilk DIS mesajının KIM(Anahtar Belirleme Modu) değeri 0 ve LVL değeri de 1 olmalıdır. Anahtar önceden belirlenmiş grup anahtarı olmalıdır. Bu nedenle Anahtar İndeksi 0 olmalıdır.
- Güvenli DIS mesajına cevap verildiğinde Trickle zamanlayıcısı sıfırlanmaktadır. Bir sonraki gönderilecek DIO mesajı güvenli DIS mesajı ile aynı güvenlik parametrelerini içermelidir. Eğer düğüm birden fazla güvenli DIS mesajı alırsa, gönderilecek DIO mesajı alınan son DIS mesajı ile aynı güvenlik parametrelerine sahip olmalıdır.
- Tek yönlü güvenli DIS mesajlarına gönderilecek DIO mesajları güvenli DIO mesajı olmalıdır.

4.3.2 Kimliği Doğrulanmış Modda Güvenli Ağa Katılma

Bu modda güvenli ağa katılmak için önyüklü modundaki kurallar uygulanarak ağa katılım sağlanır. Ağa katılan düğümün 4.8'te görülen DODAG Yapılandırma opsiyonundaki 'A' biti 1 olmalıdır. Böylece düğümün ağa yönlendirici olarak katılmadan önce anahtar otoritesi ile haberleşmesi gerektiğini belirtir. Kimliği

Doğrulanmış modda haberleşen düğümlerin yukarıda belirtilen kurallara ek olarak yeni kurallar tanımlanmıştır. Bu kurallar aşağıda belirtilmiştir.



Şekil 4.8 : DODAG Yapılandırma Opsiyonu [5]

- Ağdaki düğüm göndereceği güvenli DIO mesajında yer alan derecesi sonsuz olmalıdır. Eğer bir düğüm anahtar indeksi 0 olan bir DIO mesajı alırsa bu mesajın derecesinin sonsuz olmasını beklenir.
- Gönderilecek güvenli DAO mesajı RPL hedef opsiyonunda sadece kendi adresini içermelidir. Önyüklü modda kullanılan anahtarla alınan güvenli DAO mesajlarında RPL hedef opsiyonunda yer alan adres ile göndericinin IPv6 adresi aynı olmalıdır.

Kimliği Doğrulanmış modda yukarıda belirtilen kurallar anahtar indeksinin 0 olduğu durumda geçerlidir. Bu kuralları uygulayarak ağa katılan düğümler sadece yaprak olarak katılabilmektedir.

4.3.2.1 Yaprak Olarak Katılma

Önyüklü modda ağa katılmak için gereken kurallarla beraber kimliği doğrulanmış modda ağa katılma kuralları uygulanır. Böylece düğüm ağa yaprak olarak katılmış olur. DODAG dereceleri sonsuz olduğu için bu düğümler ebeveyn olarak seçilemezler. Bu nedenle kendisine başka düğümler bağlanamaz.

4.3.2.2 Yönlendirici Olarak Katılma

Kimliği Doğrulanmış modda ağa katılan düğümün yönlendirici düğüm olarak çalışabilmesi için anahtar otoritesinden ikinci anahtarı alması gerekmektedir. Standart IP mesajları kullanılarak anahtar sunucusuna bağlanır ve ikinci simetrik anahtarını alır.

RPL protokolü anahtar alma mekanizması için spesifik bir yöntem önermemiştir ve bu alan gelişime açıktır. Önerdiğimiz yeni anahtar alma mekanizması Bölüm 5'te detaylı olarak anlatılacaktır.

4.4 LİTERATÜR ARAŞTIRMALARI

KSA'larda kullanılabilecek kimlik doğrulama metotları geliştirmeleri son zamanlarda hız kazanmıştır. Bu metotlar kullandığı kriptografi yöntemine göre simetrik, asimetrik veya bu yöntemlerin birleşiminden oluşan hibrit yöntem olabilir. Çizelge 4.1'te şimdiye kadar geliştirilmiş kimlik doğrulama methodları gösterilmiştir ve aşağıda detaylı olarak anlatılacaktır.

Araştırmacılar	**Şifreleme Tipi**	**Kullanılan Teknikler**	**Detaylar**	**Uygulanan Güvenli Mod Tipi**
Chang, Zhang ve Qin (2010)	Asimetrik	Kimlik doğrulama metodu XKAS anahtar alma şemasına göre ECC kullanılarak yapılmıştır.	Bu yöntem 2007'de yayınlanan önceki kimlik doğrulama sistemini geliştirerek bir düğüm kimlik doğrulama aşamasını geliştirdi. Düğüm yalnızca özgün kimlik değerini saklar, böylece bellek alanı tüketimini azaltır.	Kimlik Doğrulama Modu
Liu ve Yan (2013)	Simetrik	Dışlama Esaslı Sistem ve özel şifre üretme fonksiyonları kullanmıştır.	Bu yöntem periyodik veya talebe dayalı anahtar yenileme ile beraber düğümlerin kimlik doğrulama işlemlerini gerçekleştirir.	Önyüklü Mod
Porambage ve diğerleri (2014)	Simetrik ve Asimetrik	AES ve ECC kullanılmıştır.	Bu yöntem uç cihazlar ve son kullanıcılar için kriptografi kimlik bilgileri gerektirir ve böylece karşılıklı iletişimin doğrulanması sağlanır.	Önyüklü Mod
Guicheng ve Zhen (2014)	Asimetrik	ECC kullanılmıştır	RFID kimlik doğrulamasını ve düğüm kimlik doğrulamasını, ECC kullanarak gerçekleştirdi.	Kimlik Doğrulama Modu
Shivraj, A, Singh (2015)	Asimetrik	Düşük maliyetli kimlik tabanlı ECC işlemlerini Lamport'un OTP algoritmasına uygun şekilde düzenlemiştir.	OTP'nin(Tek Zamanlı Parola) daha kısa anahtar uzunluğu ile aynı derecede güvenliği sağlamıştır.	Kimlik Doğrulama Modu
Santoso ve Vun (2015)	Simetrik ve Asimetrik	2 adımlı kimlik doğrulama yöntemi kullanır. ECC ve ECDH kullanarak şifreleme işlemlerini gerçekleştirir.	Kullanıcının IoT'nin cihaz kimlik bilgilerini mobil cihaza yüklemesi gerekir. Daha sonra ayrıntılar aynı yöntem kullanılarak ağ geçidine eklenecektir.	Kimlik Doğrulama Modu

Rghioui, Abdmeziem, Bouchkaren ve Bouhorma (2015)	Simetrik	Uzakta yer alan sunucuyu kimlik doğrulama için ve IOT sistemler için güvenli anahtar yönetimini gerçekleştirmiştir.	Bir uzak sunucunun kontrolüne dayanan ve ayrıca ağda anahtarların paylaşılmasını önlemek için dahili cihaz anahtarı üretimine dayanan hibrit anahtar yönetim şeması	Önyüklü Mod
Banerjee, Chatterjee ve DasBit (2015)	Simetrik	Düşük maliyetli hesaplama işlemi kullanır. Anahtarlar dinamik olarak üretilir.	Bu yöntem enerji açısından verimli düğüm kimlik doğrulaması ile düşük ek yük üretti.	Önyüklü Mod
Saleh ve Sourour (2015)	Simetrik	Ağ kurulma evresinde düğümler arası ortak anahtarları öğrenmeye dayalı bir yöntemdir. Düğümler arası ortak bir anahtar yoktur.	Bu yöntem yönlendirme protokollerinden biri olan SPIN ile entegre edilmiştir, böylece gereksiz protokol yürütmesini ortadan kaldırır.	Önyüklü Mod
Dey ve Hossain (2019)	Simetrik ve Asimetrik	Açık anahtar kriptolojisini kullanır. Diffie-Hellman anahtar değişimi yöntemi gerçeklenmiştir.	Bu yöntem akıllı ev ağlarında yer alan düğümlerin güvenli haberleşmesinde kullanılacak anahtarın belirlemek için yeni bir metot önermiştir. Diffie-Hellman anahtar değişimi yöntemini kullanmıştır.	Kimlik Doğrulama Modu
Shuai ve Ekibi (2019)	Simetrik ve Asimetrik	ECC kullanılarak kimlik doğrulama metotu geliştirilmiştir.	Akıllı ev ortamları için ECC kullanarak kimlik doğrulama metotu geliştirilmiştir. Kimlik Doğrulama metodu dört aşamadan oluşmaktadır.	Kimlik Doğrulama Modu

Çizelge 4.1 : Geliştirilen Kimlik Doğrulama Metotları

Chang ve ekibi [55] ECC kullanarak bir kimlik doğrulama methodu önermiştir. KSA'larda kullanılabilecek bu metot düğümlerin anahtar paylaşma evresi için XKAS anahtar yönetimi metodunu uygulamıştır. Asimetrik kriptografi kullanılması ve

kimlik doğrulama modunda yer alan anahtar yönetiminin uygulamaya spesifik olması nedeniyle RPL'de uygulanabilirdir. Böylece düğümler kimlik doğrulama modunda yönlendirici olarak ağa katılım sağlamıştır.

Saleh ve Sourour [63]'un önerdiği kimlik doğrulama protokolü kimlik doğrulama işlemlerini yönlendirme sürecinde simetrik kriptografi kullanarak gerçekleştirmiştir. Bu yöntemde kimlik doğrulama yönlendirme sürecinde gerçekleştiği için gereksiz mesaj gönderimi yoktur. Böylece kötü niyetli düğümlerin veri ağına katılması önlenmiştir. Mesajlaşma sayısı daha az olduğu için daha düşük enerji kullanmaktadır. Bu yöntem SPIN yönlendirme protokolünde kullanılmaktadır.

Banerjee ve ekibi [62] düğümlerin kimliğini doğrulamak için düşük maliyetli şifreleme yöntemi önermiştir. Her bir düğümde yapılacak işlemler az olduğu için düşük maliyetli terimi kullanılmıştır. Gönderici ve alıcı düğüm algoritması olmak üzere 2 çeşit algoritması vardır. Gönderici düğüm 32-bitlik özgün kimliğini şifreler ve 20 bitlik şifrelenmiş kimlik üretir. Bu kimlikle beraber gömülü bir anahtar ipucunu alıcı düğüme gönderir. Alıcı kısım mesajı çözebilmek için aynı algoritmayı kullanır ve gönderilen bilgiyi alır. Daha sonra komşu listesi ile eşleştirilmiş kimlik ile karşılaştırıp düğümü onaylar. Böylece kimlik doğrulama işlemi tamamlanır.

Porambage ve ekibi [58] son kullanıcı ve ara düğümler arasında bir kimlik doğrulama yöntemi önermiştir. İki adımdan oluşan kimlik doğrulama yöntemi son kullanıcı ve ara düğümler arasında güvenli bağlantılar sağlamayı amaçlamıştır. ECC kullanılarak bu işlem gerçekleştirilmiştir. Kimlik doğrulama için düğümlerin içine gömülü sertifikaların kullanılması nedeniyle düşük maliyetlidir.

Guicheng ve Zhen [57] kimlik doğrulama yönteminde ECC ile RSA'yı kıyaslayıp, ECC'nin daha iyi bir aday olduğunu göstermiştir. 162 bit anahtar uzunluğundaki ECC ile 1024 bit anahtar uzunluğundaki RSA'nın aynı güvenliği sağladığını göstermiştir. Bu nedenle ECC'nin RFID cihazlarına uygulanabilirliğini ve ECC'nin KSA'larda kimlik doğrulama yöntemi için uygun olacağını belirtmiştir.

Shivraj ve ekibi [59] OTP(Tek Seferlik Parola) yöntemini kimliğe dayalı ECC ve Lamport'un OTP algoritması ile birleştirmiştir. Lamport'un OTP algoritması ataklara karşı açık olduğundan bunun yerine kimlik doğrulamalı ECC'ye dayalı bir fonksiyon geliştirmişlerdir. Yazarın kullandığı metot önceki anahtarları kullanmadığı için

daha az bellek alanı kullanır ve anahtarları saklamaz. Günümüzde kullanılan OTP yöntemlerinin aksine daha küçük anahtar uzunluğu kullanır ve standart yöntemlerle aynı güvenlik seviyesini sağlar.

Santoso ve Vun [60] akıllı ev sistemlerinde kullanılmak üzere kimlik doğrulama yöntemi önermiştir. ECC kullanılmıştır ve ECDH yöntemi ile paylaşılmak üzere anahtar oluşturulmuştur. Kullanıcının gerekli bilgileri sürekli girmesi gerektiğinden kullanımı zordur. Bu yöntem mobil cihazlar ile kullanıcıların sistemi ayarlamasını sağlar. Önerilen metot içeriden ataklara karşı savunmasızdı bu nedenle kullanıcı gizliliği ve takip edilemezlik özelliklerini karşılayamadı.

Rghioui ve ekibi [61] 6LoWPAN ağları için güvenli anahtar yönetimi metodu önermiştir. Simetrik ve asimetrik şifreleme yöntemleri kullanıldığı için hibrit bir metoddur. Simetrik şifreleme daha az enerji kullandığı için tercih edilir. Asimetrik şifreleme de uçtan uca güvenliği sağlamaktadır. Böylece daha az enerji tüketimi ile ağ güvenliği sağlanmış olur.

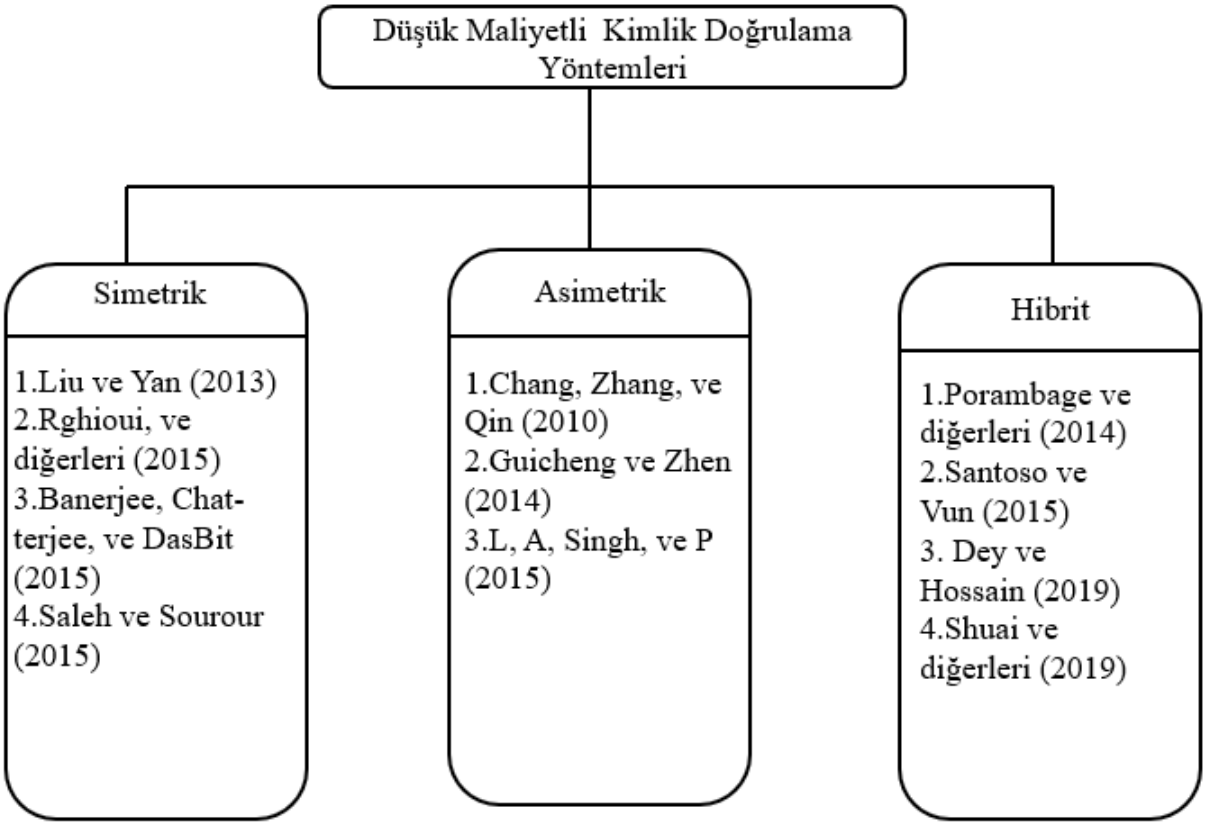
Liu ve Yan [56] farklı sensör ağları için anahtar yönetimi metodu önermiştir. Düğümlerin kimlik doğrulama işlemlerinin yanında anahtar yenileme işlemleri periyodik olarak gerçekleşmektedir. Anahtarlar aynı anahtarı üretmemek için özel bir fonksiyonla üretilmektedir ve sabit uzunluktadır. Düğümlerin ele geçirilmesi durumunda ise ağda kullanılan anahtarlar her bir düğüm için farklı olduğundan bu tip ataklara daha dayanıklıdır. Bu metod EBS(Dışlama Esaslı Sistem) ve basit simetrik şifrelemelerini kullanır. Dey ve Hossain [70] açık anahtar kriptolojisini kullanarak akıllı ev ağlarında düğümler arası kullanılacak anahtarı belirlemek için metot önermiştir. Diffie-Hellman anahtar değişimi yöntemini uygulamışlardır. Güvenilir servis sağlayıcı ağda yer alan bütün düğümlere ait güvenlik parametrelerine ve simetrik anahtarlara sahiptir. Güvenli ağ kurulmadan düğümler kimlik doğrulama işlemleri gerçekleştirip gerekli anahtarları almalıdır. Bu yöntem ağa yeni bir düğüm eklendiğinde buna ait anahtarların servis sağlayıcısına ekleme ihtiyacı olmadan kimlik doğrulama işlemlerini gerçekleştirir. Ayrıca önerilen yöntemi güvenlik analiz araçları ile doğrulanmıştır.

Shuai ve ekibi [71] ECC kullanarak akıllı ev ortamları için verimli bir kimlik doğrulama uygulaması önermiştir. Şu ana kadar bilinen aktif ve pasif ataklara önlem

almakla beraber ekstra fonksiyonu da bulunmaktadır. Bu metot açılış, kayıtlanma, kullanıcı girişi, kimlik doğrulama ve parola değiştirme olmak üzere 5 adımdan oluşmaktadır. Ayrıca önerilen yöntemi güvenlik analiz araçları ile test etmişlerdir.

Çizelge 4.1'te belirtilen yöntemleri inceledik. Bu metotlar RPL'de güvenli modları uygulamaya uygundur. Güvenlik yöntemleri birbirinden farklı olsa da asıl amaç güvenlik seviyesini artırmaktır. Her yöntemin uygulanması kullanıma özgüdür. RPL'de kaynak kısıtlı düğümlerden dolayı simetrik şifreleme desteği bulunmaktadır. Kimlik doğrulama modunda düğümlerin doğrulanması hala gelişime açık bir alandır.

Literatür araştırmalarına dayanarak, araştırmacıların RPL'in düğüm kimlik doğrulama modunu geliştirmek için kullandığı kimlik doğrulama yöntemlerinin sınıflandırılması Şekil 4.9'te ve geliştirilen metotların güvenlik özelliklerinin karşılaştırılması Çizelge 4.2'te gösterilmiştir.



Şekil 4.9 : Düşük Maliyetli Yöntemlerin Sınıflandırılması

Araştırmacılar	Şifreleme Tipi	Uygulanan Güvenlik Modu	Performans Analizi	Kimlik Doğrulama Süreci için Toplam Mesaj Sayısı	Yöntem Doğruluğu İspatı	Yöntem Doğruluğunun Araçla Onaylanması	Karşılıklı Kimlik Doğrulama	Tekrarlama Atakları	Man In the Middle Atakları	Kullanıcı Gizliliği	Senkronizasyon Bozma Ataklarına Dayanıklılık	Kimlik Taklidi Ataklarına Dayanıklılık
Chang vd. (2010) [55]	Asimetrik	Kimlik Doğrulama Modu	✗	4	✗	✗	✗	✓	✓	✓	✗	✗
Porambage vd. (2014) [58]	Hibrit	Kimlik Doğrulama Modu	✓	10	✗	✗	✓	✓	✗	✗	✗	✓
Guicheng ve Zhen (2014) [57]	Asimetrik	Kimlik Doğrulama Modu	✗	5	✗	✗	✓	✗	✓	✗	✗	✗
Shivraj vd. (2015) [59]	Asimetrik	Kimlik Doğrulama Modu	✓	4	✓	✗	✗	✓	✓	✗	✗	✗
Santoso ve Vun (2015) [60]	Hibrit	Kimlik Doğrulama Modu	✗	3	✗	✗	✓	✗	✓	✗	✗	✗
Kumar vd. (2016) [72]	Simetrik	Önyüklü Mod	✓	3	✓	✓	✗	✓	✓	✗	✓	✓
Wazid vd. (2017) [73]	Simetrik	Önyüklü Mod	✓	16	✓	✓	✓	✓	✓	✓	✗	✓
Li (2013) [74]	Asimetrik	Kimlik Doğrulama Modu	✓	12	✓	✓	✓	✓	✓	✓	✗	✓
Geliştirdiğimiz Metot	Hibrit	Kimlik Doğrulama Modu	✓	3	✓	✓	✓	✓	✓	✓	✓	✓

Çizelge 4.2 : Geliştilmiş Metotların Güvenlik Özellikleri Karşılaştırması

5. KİMLİK DOĞRULAMA MODU İÇİN GELİŞTİRİLEN ANAHTAR YÖNETİMİ METODU

Şu ana kadar yapılan RPL protokolü geliştirmeleri sadece güvenli olmayan modu desteklemektedir. RPL protokolünü destekleyen ve günümüzde çok sık kullanılan ContikiOS ve TinyOS bile bu güvenlik özelliklerinin desteğini eklememiştir. Perazzo [49] [50] RPL security modlarından önyüklü mod desteğini ve tekrarlama ataklarına karşı önlem mekanizmasını eklemiştir. Cooja simulatöründe de bu çalışmanın performans analizi yapılmıştır. RPL'e eklenen önyüklü modu desteği eklemek ağ kurulum zamanına, kontrol mesajlarının büyümesinden kaynaklı harcanan işlem gücü ve güç tüketimine etkisi çok azdır. Tekrarlama ataklarına karşı eklenen mekanizma ise ağ kurulum zamanına, kontrol mesajlarının büyümesinden kaynaklı harcanan işlem gücü ve güç tüketimine etkisi oldukça yüksektir. Düğüm sayısı arttıkça bu artış daha da artmaktadır.

Simetrik anahtarla gerçekleştirilen güvenlik desteği RPL ağını dışarıdan gelecek ataklara karşı korumaktadır [76]. Fakat kötü niyetli saldırganlar ağdaki bir düğüm üzerinden simetrik anahtarı elde edebilir ve bu anahtar ile ağa erişibilir ağın topolojisini değiştirebilir. Bu tip durumları engelleyebilmek için ağdaki düğümlere kimlik doğrulama yapılması gerekmektedir. Kısıtlı kaynaklı KSA'larda yer alan limitlerden bu yöntemlerin uygulaması azdır. Ayrıca RPL'de oluşabilecek atak çeşitleri mesajın gizliliği, veri bütünlüğü, erişilebilirlik ve kimlik doğrulama parametrelerine göre incelenmiştir. İncelenen parametrelerle beraber ataklara karşı nasıl müdahale edilmesi gerektiği ile ilgili önerilerde bulunulmuştur fakat RPL'de bu atakların nasıl gerçekleşeceği belirtilmemiştir.

Asimetrik kriptografinin KSA'larda uygulanması için yapılan araştırmalar Bölüm 4'te gösterilmiştir. Bu çalışmaların sonucu olarak asimetrik kriptografi kullanılarak Man-In-The-Middle(Ortadaki Adam) gibi güvenlik tehlikelerinden korunma sağlanmıştır. Ayrıca kimlik doğrulama işlemleri ile de ağ güvenliğini artırmaktadır. Günümüzde en çok kullanılan asimetrik kriptografi ECC'dir.

ECC anahtar uzunluğu diğer açık anahtar kriptografi yöntemlerine göre oldukça düşüktür. Bu işlemi aynı güvenlik seviyesinde gerçekleştirerek sağlamaktadır. 256 bitlik ECC anahtarı 3072 bitlik RSA anahtarı ile eşdeğer koruma sağlamaktadır. RSA anahtarı kullanılarak yapılacak kriptografi işlemleri kısıtlı bellek ve işlem güçlü düğümlerde oldukça zordur. Ayrıca, gönderilecek paket boyu arttığından önceden tek paket olarak gönderilen paketler artık birden fazla paket halinde gönderilecektir. Bu durum enerji tüketimini oldukça artırmaktadır. Bu dezavantajlarından dolayı KSA'larda RSA yerine ECC tercih edilmektedir.

Yaptığımız çalışmada bellek ve alan kullanımı az olan uECC(Mikro Eliptik Eğri Kriptografisi) [79] kütüphanesi Contiki yazılım paketine eklenmiştir. uECC gömülü sistemlerde ve kablosuz sensör ağlarında kullanımı oldukça yaygındır. Bu kütüphane yardımıyla anahtar çifti oluşturma işlemleri gerçekleştirilmiştir ve standart eğrileri desteklemektedir. Bu çalışmada *secp256r1* eğrisi kullanılmıştır.

RPL protokolünü iç ve dış kaynaklı ataklara karşı daha korunaklı yapabilmek için kimliği doğrulanmış mod ile geliştirmeler yapılmalıdır. Bu moddaki problemlerden biri anahtar yönetimidir. Anahtar otoritesinden ağda daha sonra kullanılacak anahtarı almak gereklidir. Bu anahtar ağdaki tüm düğümlere ulaşmalı ve daha korumalı bir yapı için periyodik olarak yenilenmelidir. Bu nedenle anahtar almak için haberleşmesi az olan ve güvenilir bir anahtar yönetimi protokolü gerekmektedir.

5.1 Geliştirilen Anahtar Yönetimi Metodu

RPL önyüklü güvenlik modu mesaj gizliliği, bütünlüğü ve güvenilirliği sağlar ve tekrarlama saldırılarına karşı da güvenlidir. Fakat bu modun güvenilirliği MAC mekanizmasına bağlıdır ve mesajın hangi kaynaktan geldiği hakkında bilgi içermez. RPL atakları incelendiğinde mesajın kaynağının güvenli olup olmadığı bilinirse atakların birçoğuna önlem alınabilir. Gönderilen mesajların şifre çözme işlemi sadece gerçek alıcı düğümde gerçekleşmelidir. Kötü niyetli düğümlerin ağ parametrelerine ve ağ ile ilgili diğer bilgilere erişim sağlamaması gerekir. Bu işlemi asimetrik kriptografi kullanarak gerçekleştirebiliriz. RPL standartı dijital imza ve asimetrik şifreleme işlemlerininin kullanımını önermiştir. Şifreleme işlemleri yüksek işlem gücü ve enerji tükettiğinden her bir kontrol mesajını şifrelemek verimli bir yöntem değildir. Bu nedenle bu işlemlerin sadece ağ kurulumu aşamasında gerçekleşmesi güç tüketimini

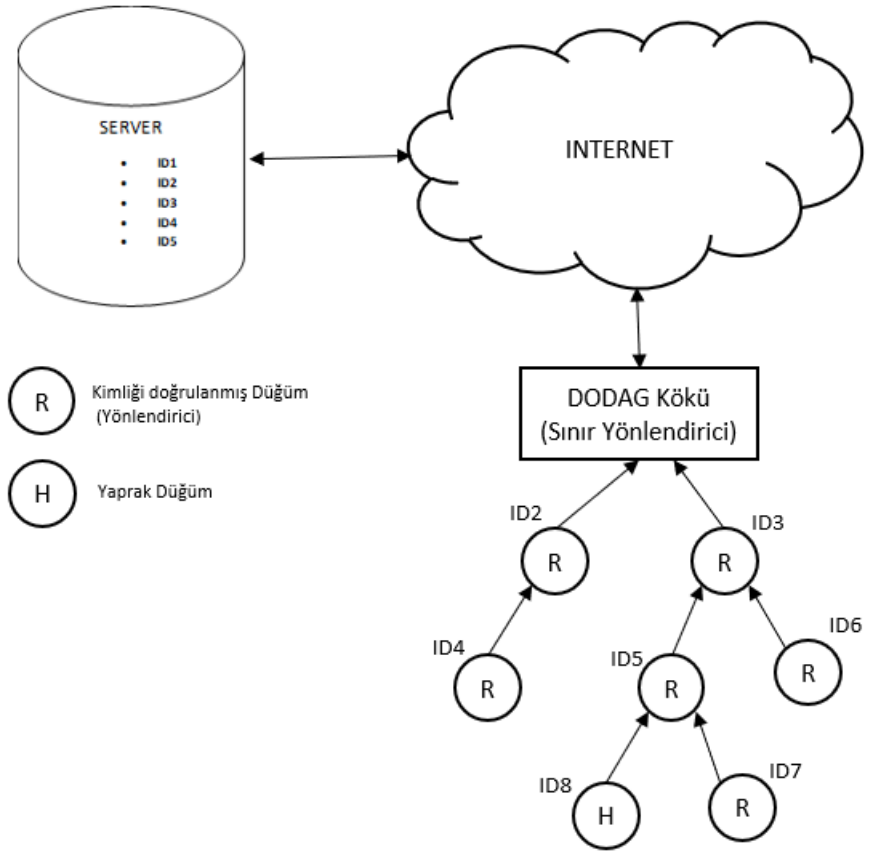
oldukça azaltacaktır. RPL standartı kimlik doğrulama modunu tanımlamıştır ve bu modla haberleşecek düğümler için bazı kurallar belirlemiştir. Anahtar yönetiminin nasıl yapılacağını tanımlamamıştır ve uygulamaya özel olarak belirtilmiştir. Bu çalışmada RPL'in kimlik doğrulama modu uygulanmıştır ve anahtar yönetimi için yeni bir metot önerilmiştir.

Şekil 5.1'te RPL kimlik doğrulama modunda kullanacağımız model görülmektedir. Bu modelde anahtar sunucusu, kök düğüm ve ağa yönlendirici veya yaprak düğüm olarak katılan düğümler yer almaktadır. Anahtar sunucusu yönlendirici olarak ağa katılacak düğümlerin listesini ve bu düğümlerin kullanacağı anahtarları saklar. Eğer anahtar isteyen düğüm geçerli bir düğümse anahtar bu düğüme kök düğüm aracılığı ile iletilir. Kök düğüm DODAG ağı kurulumunu başlatır ve yönlendirici veya yaprak düğümlerin ağa katılımı sağlanır. Ayrıca anahtar sunucusu ile haberleşerek sunucudan gelen anahtarı hedef düğüme iletir. Yönlendirici düğümler anahtar sunucusundan ikinci grup anahtarını alan yani ağa katılmasına izin verilen düğümlerdir. Yönlendirici düğümler DIO mesajları göndererek ağ kurulumuna yardımcı olur ve yaprak düğümler için ebeveyn olarak seçilebilirler. Yaprak düğümler ise ağa katılır ve sadece gönderilen veriyi iletir. DIO mesajı gönderemediği için ağ kurulumuna katkı sağlayamaz ve ebeveyn olarak seçilemez. Ayrıca ikinci grup anahtarına sahip olmadıkları için ağda gönderilen kontrol mesajlarını alsa bile mesajın şifresini doğru bir şekilde çözemez.

Notasyon	Açıklama
K	Önyüklü simetrik grup anahtarı
K_{priv_k}	Kök düğümün gizli anahtarı
K_{priv_i}	Diğer düğümlerin gizli anahtarı
K_{pub_k}	Kök düğümün açık anahtarı
K_{pub_i}	Diğer düğümlerin açık anahtarı
K_{second}	İkinci simetrik grup anahtarı
η_k	Kök düğümünün ürettiği rastgele sayı
η_i	Diğer düğümlerin ürettiği rastgele sayı
ID_i	Düğümlerin IPv6 adresleriyle ilişkilendirilmiş kimliği
K_{params}	İkinci simetrik grup anahtarına ait kaynak ve indeks bilgisi

Çizelge 5.1 : Anahtar yönetimi metotunda kullanılan terimlerin notasyonu ve açıklamaları

Önerdiğimiz metotta kullanılan terimler ve bu terimlerin açıklamaları Çizelge 5.1'te gösterilmiştir. Ayrıca önerilen yöntem için geçerli varsayımlar aşağıda belirtilmiştir.



Şekil 5.1 : RPL Kimlik Doğrulama Modu Modeli

- RPL kimlik doğrulama modunda ağa katılacak her düğüme önyüklü anahtar K önceden yüklenmiştir. Bu anahtarı kullanarak ağa yaprak düğüm olarak katılır.
- Ağdaki bütün düğümlerin kendilerine ait açık ve gizli anahtar çifti önceden yüklenmiştir. Kök düğüme ait açık anahtar K_{pub_k}, gizli anahtar K_{priv_k} olarak, diğer düğümler için ise açık anahtar K_{pub_i} ve gizli anahtar K_{priv_i}'dır.
- RPL kimlik doğrulama modunda K_{second} adında ikinci grup anahtarı vardır. Yönlendirici olarak ağa katılacak düğümler ikinci grup anahtarını almak için kök düğüme istek gönderir. Eğer koşullar uygunsa bu anahtar cevap olarak gönderilir ve isteği yapan düğüm ağa yönlendirici olarak katılır.
- Kök düğüm her zaman güvenilirdir. Anahtar sunucusu ile kök düğüm arasındaki iletişim kanalı güvenliği sağlanmış bir kanaldır ve önerdiğimiz şemada kök düğüm anahtar sunucusu olarak görev yapmaktadır. Ayrıca kök düğüm diğer düğümlerden daha yüksek işlem gücüne sahip ve depolama kapasitesi daha yüksektir.

- Kök düğüm ağa katılmasına izin verilen düğümlerin IPv6 adresleri ile ilişkilendirilmiş kimlik bilgileri listesine ve ağ oluşumunda kullanılacak ikinci grup anahtarına sahiptir. Ağdaki düğümlerin açık anahtarları burada saklanmamaktadır ve böylece ağa yeni bir düğüm katıldığında kök düğümde yer alan sadece kimlik bilgisini güncellemek yeterli olmaktadır. Ayrıca düğümlerin açık anahtarları saklanmadığı için depolama alanından kazanç sağlanmış olur.

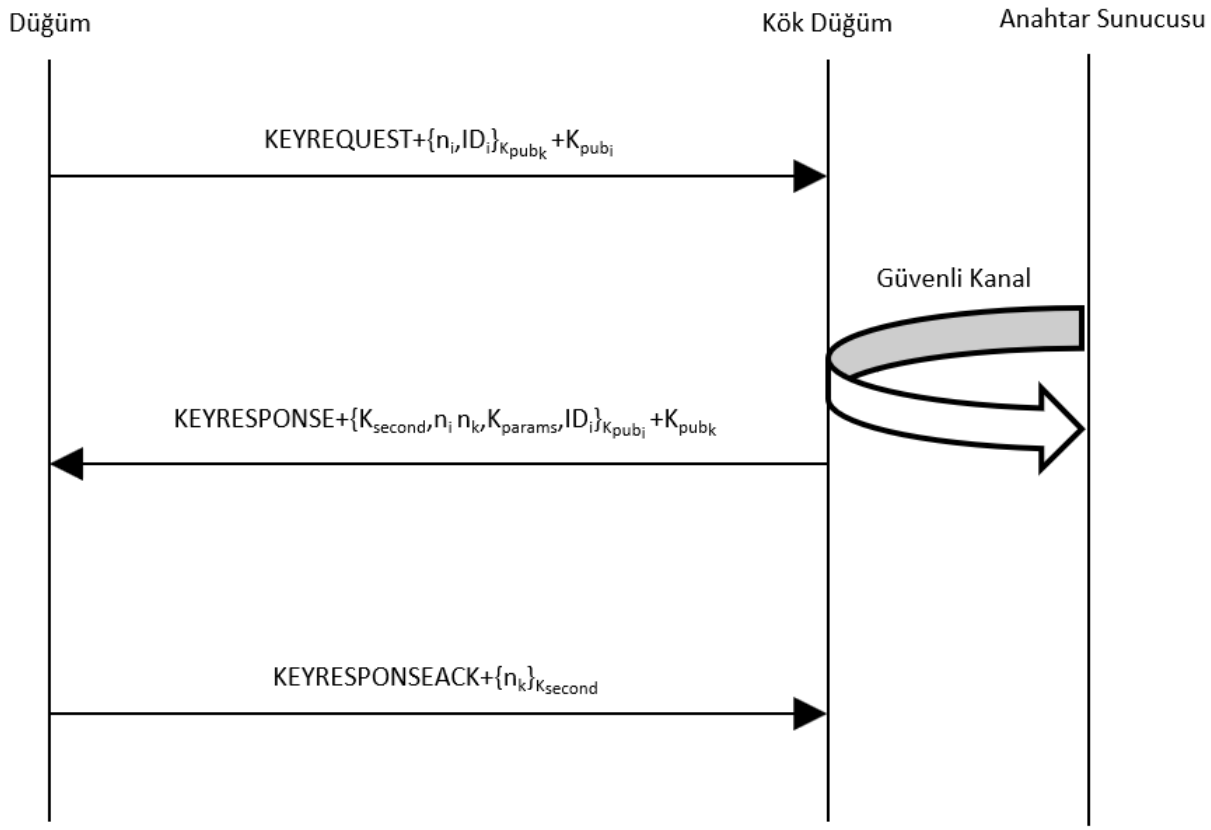
- Kötü niyetli düğümlerin daha önce kullanılmış bir kontrol mesajını kullanarak ağ ile ilgili bilgileri almasını engellemek için kimlik doğrulama işlemi gereklidir.

5.2 Ağa Katılma Süreci

RPL kimlik doğrulama modunda kök düğüm dışındaki tüm düğümler güvenli ağa yaprak düğüm olarak katılır. Yönlendirici olarak görev yapacak düğüm ikinci grup anahtarını almak için anahtar sunucusu tarafından kimliği doğrulanması gerekir. Güvenli DAO mesajı ebeveyn düğüme gönderilir ve o düğüm için ikinci grup anahtarını alma süreci başlar. Anahtar alma süreci başarılı bir şekilde tamamlanırsa düğümün kimliği doğrulanmış olur ve artık düğüm ikinci grup anahtarına sahiptir. Böylece yönlendirici düğüm olarak görev alır ve ağ oluşumuna katkı sağlar.

Kök düğüm ile ağdaki diğer düğümler arasında iletişimi sağlamak için yeni mesaj yapıları oluşturulmuştur. Bu mesajlar anahtar isteme, anahtar cevap ve anahtar cevap bilgilendirme mesajlarıdır ve başlık alanı ve veri alanından oluşmaktadır. Bu mesajların başlık alanı sırasıyla "KEYREQUEST", "KEYRESPONSE" ve "KEYRESPONSEACK" söz dizileri olurken bu mesajların veri alanları birbirinden farklıdır. Mesaj içeriğinin başlık alanı şifrelenmeden, veri alanının ise kritik bilgileri içeren kısımları şifrelenerek gönderilmiştir. Şekil 5.2'te ikinci grup anahtarını almak için geliştirilen anahtar yönetimi metotu gösterilmiştir ve aşağıda detaylı olarak anlatılacaktır.

Güvenli ağa yaprak olarak katılan düğüm anahtar istek mesajını kök düğüme göndermek için hazırlar. Mesaja ilk olarak "KEYREQUEST" başlığı eklenir ve bu alan şifrelenmez. Mesajı gönderen düğüm o an rastgele bir sayı üretir ve üretilen η_i değerini mesajın veri alanına ekler. Ardından düğümün IPv6 adresi ile ilişkilendirilmiş ID_i kimlik bilgisini K_{pub_k} ile 256 bit ECC kullanarak şifreler. Son olarak düğüm



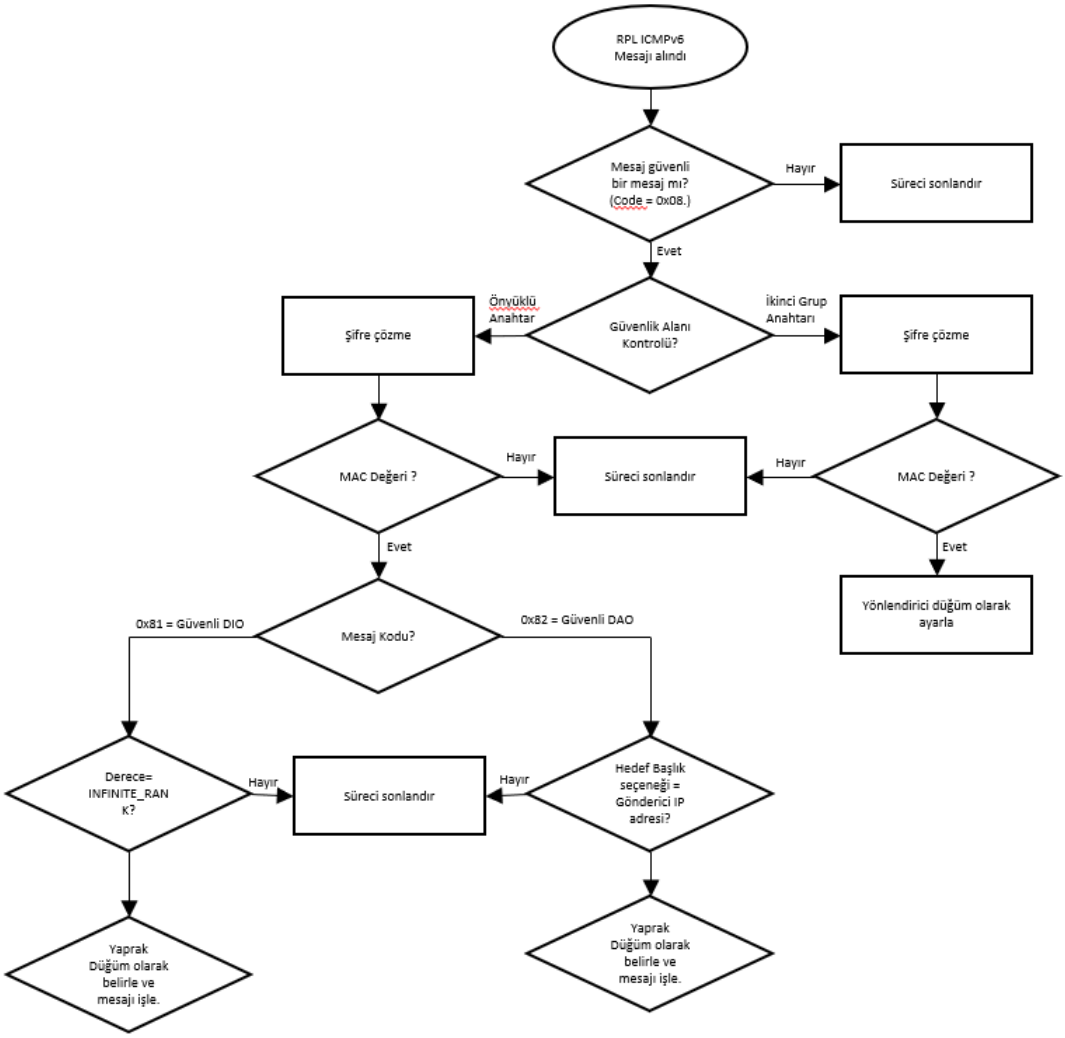
Şekil 5.2 : Düğümlerin Kimlik Doğrulama ve İkinci Grup Anahtarını Alma Metotu

kendi K_{pub_i} açık anahtarını şifreleme yapmadan mesaja ekler ve mesaj kök düğüme gönderilir.

Anahtar istek mesajını alan kök düğüm öncelikle göndericinin kimliğini kontrol eder. Eğer gönderici kimliği kök düğümde kayıtlı ise gelen mesajın başlık alanını kontrol eder. Başlık alanı "KEYREQUEST" ise mesajın şifrelenmiş kısmının şifresini K_{priv_k} anahtarını kullanarak çözer ve anahtar cevap mesajını hazırlar. İlk olarak "KEYRESPONSE" başlığı şifrelenmeden mesaja eklenir. Ardından ikinci grup anahtarı K_{second}, gönderen düğümün ürettiği rastgele sayı η_i, kök düğüm tarafından o an üretilmiş rastgele sayı η_k, ikinci grup anahtarının kaynağı ve indeksi K_{params} ve ID_i değeri cevap mesajına eklenir. Mesajın başlığı dışındaki kısımları gönderici düğümün K_{pub_i} ile 256 bit ECC şifrelenir. Rastgele üretilen değerin o an üretilmesi kriptografide verinin tazeliği açısından önemlidir. Bu değere meydan okuma değeri de denmektedir. Son olarak kök düğüm K_{pub_k} açık anahtarını şifreleme yapmadan mesaja ekler ve mesajı anahtar isteği yapan düğüme gönderir.

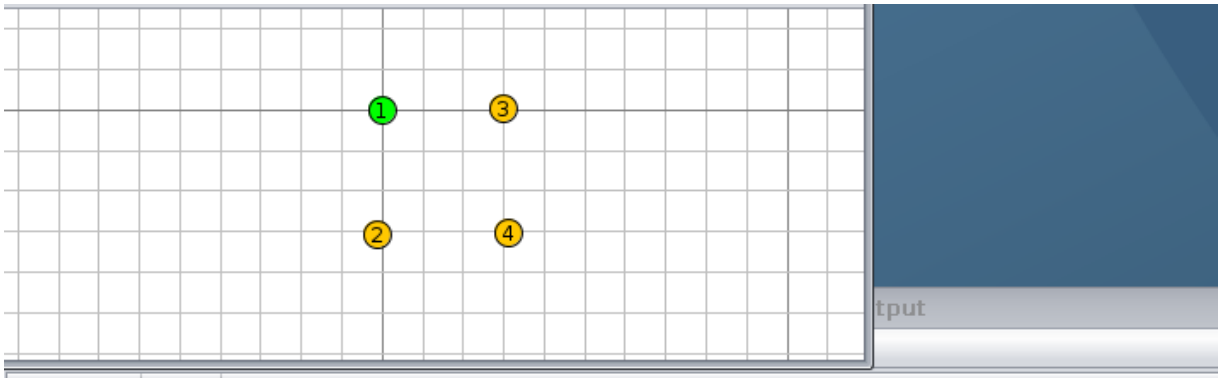
Anahtar cevap mesajını alan düğüm mesajın kök düğümden geldiğini kontrol eder. Başlık alanı "KEYRESPONSE" ise mesajın şifresini K_{priv_i}'yi kullanarak çözer. Anahtar istek mesajında gönderdiği rastgele değer ile anahtar cevap mesajında aldığı sayı aynı ise mesajın kök düğüme gönderildiğinden ve cevabın kök düğümden geldiğinden emin olur. Karşılıklı kimlik doğrulamayı gerçekleştirmek amacıyla kök düğüme mesajın alındığını bilgisinin iletilmesi gerekir. Bunun için anahtar cevap bilgilendirme mesajını hazırlar. "KEYRESPONSEACK" başlığı şifrelenmeden mesaja eklenir. Ardından anahtar cevap mesajında yer alan sayı mesaja eklenir. Mesajın başlığı dışındaki kısımları simetrik AES-128 algoritmasını kullanarak ikinci grup anahtarı ile şifrelenir ve gönderilir.

Anahtar cevap bilgilendirme mesajını alan kök düğüm mesajın şifresini AES-128 algoritmasını kullanarak ikinci grup anahtarı ile çözer. Anahtar cevap mesajında gönderdiği ve sadece kendisinin bildiği rastgele sayı ile alınan mesajda yer alan değer aynı olup olmadığını kontrol eder. Bu değere cevap değeri de denmektedir. Eğer değerler aynı ise anahtar cevap mesajının gönderici düğüme gönderildiğinden ve gelen mesajın gönderici düğümden alındığından emin olur ve karşılıklı kimlik doğrulama işlemi tamamlanır. Böylece kimliği doğrulanmış düğüm ikinci grup anahtarını kullanarak güvenli DIO mesajlarını gönderir ve ebeveyn olarak seçilebilir. Güvenli DAO mesajı göndererek kendi kimliğini ve kendine bağlı düğümlerin listesini de kendi ebeveyn düğümüne gönderir. Ağdaki bir düğümün önyüklü anahtarla ve kimliği doğrulanmış modda alınan kontrol mesajlarının süreci Şekil 5.3'te gösterilmiştir.



Şekil 5.3 : Düğümlerin Alınan Kontrol Mesajlarını İşleme Süreci

Ağ kurulum aşamasında bütün düğümler yaprak düğüm olarak katılır. İkinci grup anahtarını alıp kök düğüm tarafından onaylanan düğüm yönlendirici düğüm olarak görev almaktadır. DIO mesajları göndererek ağ kurulumuna yardımcı olur. Şekil 5.4'te düğümün yönlendirme düğümü olma süreci gösterilmiştir. Kök düğüm ağa katılacak düğümlerin listesini tutmaktadır. Listede yer almayan düğüm güvenli ağa katılma isteği gönderse bile kök düğüm anahtar cevap mesajını göndermeyecektir. Böylece ağ ile ilgili bilgilere erişim sağlayamayacaktır. Şekil 5.5'te 2x2 dizilimli ağda 4 numaralı düğüm bu duruma örnek olarak gösterilmiştir. Listede olan düğümler(2,3) ağdan ikinci anahtarları alıp DIO mesajlarını gönderebilirken, 4 numaralı düğüm gönderilen DIO mesajlarının şifresini çözemediği için ağ parametrelerini elde edememektedir. Böylece ağ dış kaynaklı düğümlerin neden olacağı ataklara karşı koruma sağlamaktadır.

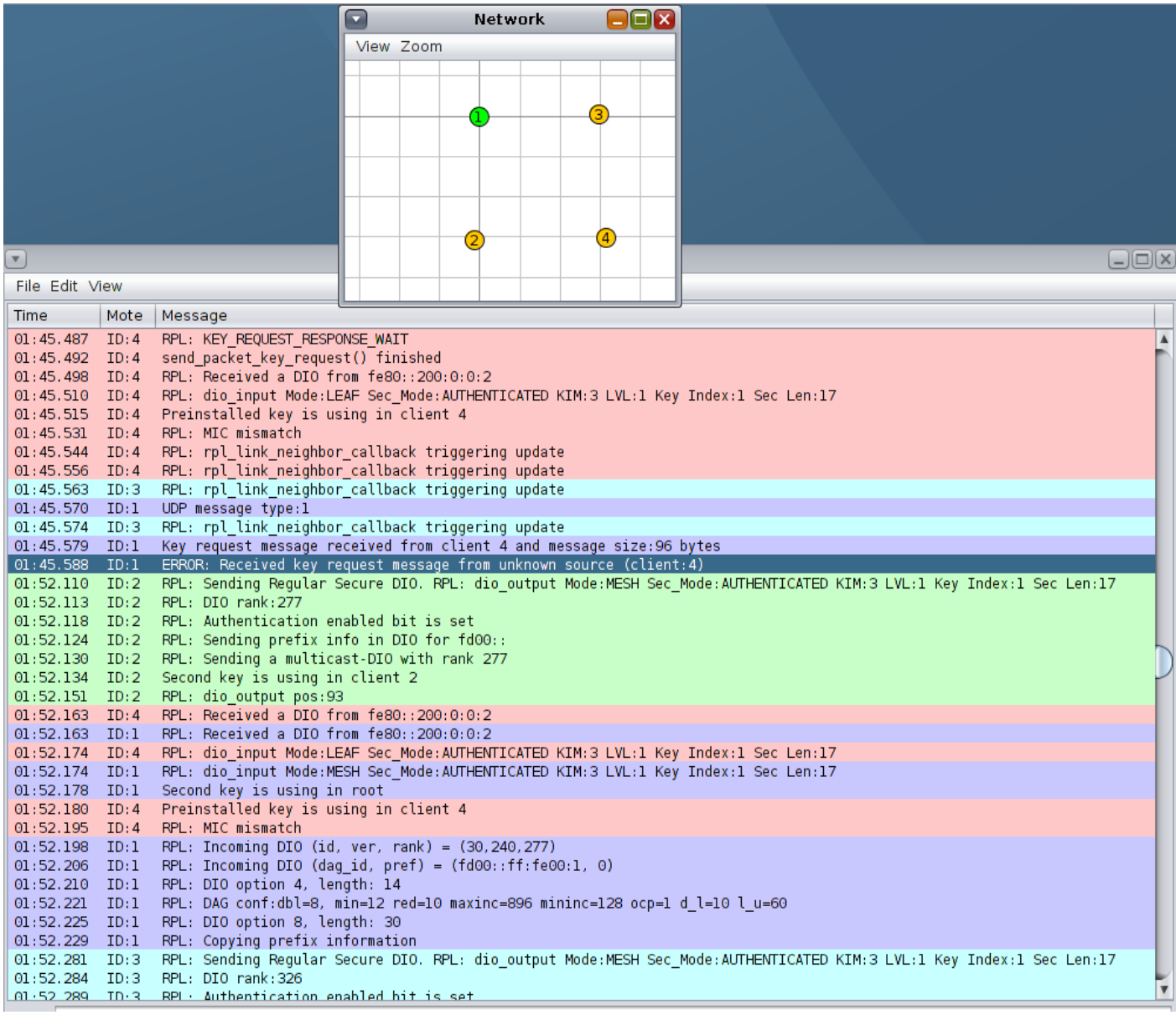


Time	Mote	Message
00:30.602	ID:1	Second key is using in root
00:30.618	ID:1	RPL: dio_output pos:93
00:30.637	ID:2	CLIENT: Received source ip index:1, server_ipaddr:1
00:30.640	ID:2	UDP message type:2
00:30.643	ID:3	RPL: Received a DIO from fe80::200:0:0:1
00:30.643	ID:2	ECC DECRYPT STARTED!
00:30.654	ID:3	RPL: dio_input Mode:LEAF Sec_Mode:AUTHENTICATED KIM:3 LVL:1 Key Index:1 Sec Len:17
00:30.660	ID:3	Preinstalled key is using in client 3
00:30.675	ID:3	RPL: MIC mismatch
00:35.005	ID:2	aesDecrypt length:49
00:35.013	ID:2	aes_key 57 5E 09 61 FD 15 02 80 22 41 0B E3 E7 3B 0A BA
00:35.023	ID:2	ECC DECRYPT FINISHED!
00:35.032	ID:2	Received key response message after decryption Length:49 bytes
00:35.043	ID:2	0xCC 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x0A 0x0B 0x0C 0x0D 0x0E 0xDD
00:35.054	ID:2	0xFF 0xFF 0xCB 0x8B 0xFF 0xFF 0xD5 0xDF 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
00:35.066	ID:2	0x01 0xFD 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xFF 0xFE 0x00 0x00
00:35.067	ID:2	0x01
00:35.072	ID:2	Received server challenge value:0xD5DF
00:35.076	ID:2	RPL: switching to mesh mode
00:35.083	ID:2	Sending key response ack before AES Length:18 bytes
00:35.094	ID:2	0x4B 0x45 0x59 0x52 0x45 0x53 0x50 0x4F 0x4E 0x53 0x45 0x41 0x43 0x4B 0xFF 0xFF
00:35.096	ID:2	0xD5 0xDF
00:35.099	ID:2	aesEncrypt input_size:16
00:35.107	ID:2	aes_key CC 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E DD
00:35.115	ID:2	Key response ack is sending to 1 with seq_id:0'
00:35.122	ID:2	RPL: uip_udp_packet_send NETSTACK_CONF_WITH_IPV6
00:35.127	ID:2	RPL: KEY_REQUEST_RESPONSE_RECEIVED
00:35.134	ID:2	RPL: Received a DIO from fe80::200:0:0:1
00:35.146	ID:2	RPL: dio_input Mode:MESH Sec_Mode:AUTHENTICATED KIM:3 LVL:1 Key Index:1 Sec Len:17
00:35.150	ID:2	Second key is using in client 2
00:35.170	ID:2	RPL: Incoming DIO (id, ver, rank) = (30,240,128)
00:35.178	ID:2	RPL: Incoming DIO (dag_id, pref) = (fd00::ff:fe00:1, 0)
00:35.182	ID:2	RPL: DIO option 4, length: 14
00:35.193	ID:2	RPL: DAG conf:dbl=8, min=12 red=10 maxinc=896 mininc=128 ocp=1 d_l=10 l_u=60
00:35.197	ID:2	RPL: DIO option 8, length: 30
00:35.202	ID:2	RPL: Copying prefix information

Şekil 5.4 : Yaprak düğümden yönlendirici düğüme geçiş süreci

5.3 Simülasyon Çalışmaları

Geliştirilen kimlik doğrulama modu ve anahtar yönetimi metotunun performans parametrelerinin incelenmesi amacıyla simülasyon çalışmaları gerçekleştirdik. RPL'de bulunan güvenli olmayan mod, önyüklü mod ve kimlik doğrulama modu olmak üzere üç mod karşılaştırılmıştır ve bu çalışma için Contiki paketinde yer alan Cooja simülatörü kullanılmıştır. Cooja emülatörü gerçekçi bir simülasyon ortamı



Şekil 5.5 : Kök düğümün ağ katılım listesinde olmayan düğümlere cevabı

hazırlamaktadır ve gerçek düğümlerde çalışacak yazılımı da üretmektedir. Bizim simülasyonlarımız Cooja simülatörü Wismote düğümlerini kullanacak şekilde ayarlanmıştır. Wismote düğümü IEEE 802.15.4 uyumlu CC2520 radyo birimine sahiptir. Bu düğüm ile ilgili detaylı bilgiler veri sayfasında yer almaktadır. Geliştirilen kimlik doğrulama modunun ağdaki performansını ölçmek için ızgara dizilimindeki 2x2, 3x3 ve 4x4 düğümler incelenmiştir. Düğümler arasındaki gönderim ve alma mesafeleri 30 metre, yayının karışmaya başladığı mesafe ise 60m olarak ayarlanmıştır. Sol üstte yer alacak düğüm kök düğüm olarak seçilmiştir. Simülasyonlar 30 dakika boyunca çalıştırılmıştır ve istatistiksel anlamda daha doğru sonuçlar almak için

simülasyon farklı başlangıç değerleriyle çok kez tekrarlanmıştır. Simetrik kriptografik işlemler Contiki-OS'ta yer alan AES-128 işlemleri ile, asimetrik kriptografik işlemler ise gömülü sistemlerde sıkça kullanılan uECC kütüphanesi kullanarak gerçeklenmiştir. RPL ile ilgili diğer ayarlar Contiki'nin varsayılan olarak seçtiği ayarlardır. Radyo görev döngüsü algoritması bütün düğümler için ContikiMAC olarak seçilmiştir.

5.3.1 Performans Metrikleri

RPL güvenli metotlarının ağ haberleşmesine olan etkilerini incelemek için aşağıdaki performans parametreleri incelenmiştir.

- **Ağ Oluşum Zamanı:** Simülasyonun başladığı andan itibaren son düğümün ağa katılıp kök düğüme erişim sağladığı anına kadar geçen süredir. Bu parametre ağın tamamen kurulup işlevsel hale geldiği zamanı belirtir. Gönderilen ilk DIO mesajı ile ağa katılan son düğümün aldığı DIO mesajı arasında geçen zaman farklı alınarak hesaplanmaktadır.

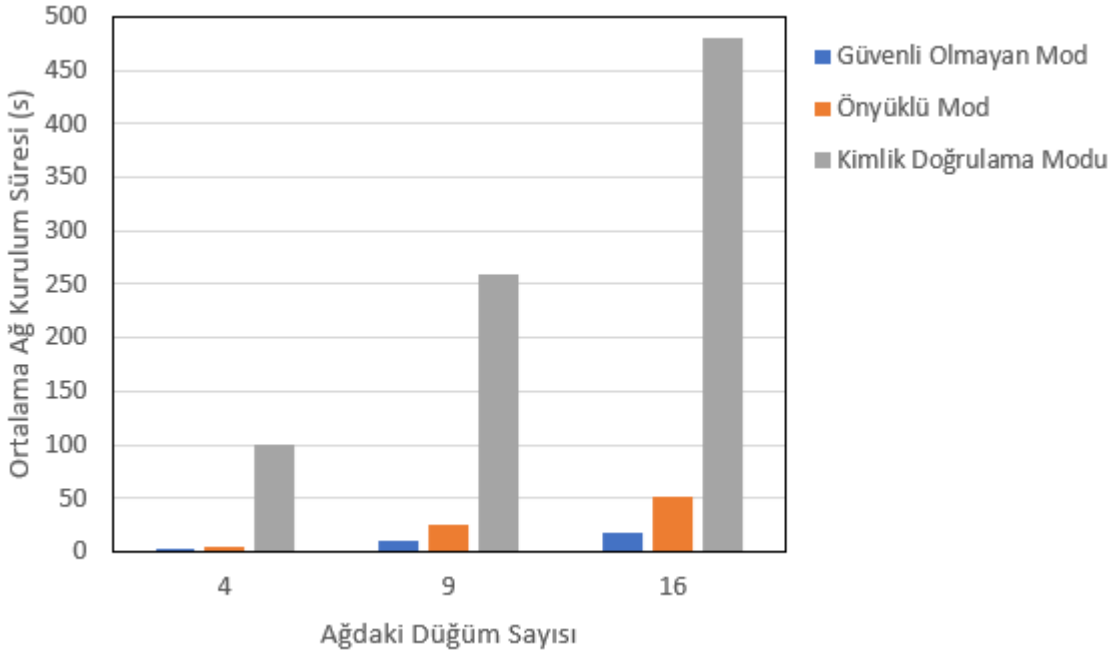
- **Enerji Tüketimi:** Ağdaki her bir düğümün güç tüketiminin ortalama değerini belirtir. Cooja simülatörüne ait powertrace aracı kullanılarak düğümün ortalama enerji tüketimi hesaplanmaktadır. Powertrace [77] aracı düşük güçlü kablosuz ağlarda yer alan düğümlerde işlemcini harcadığı gücü, mesaj gönderme ve alma için gereken güç değerlerini gerçeğe yakın bir şekilde hesaplar. Bu hesaplamaları işlemcinin uyku ve aktif modlarından ve radyo biriminin gönderme ve alma için harcadığı süreleri kullanarak hesaplar. Süre hesaplama işlemleri işlemcinin tik hesabı ile gerçekleştirilir. Mesaj gönderim ve alma için hesaplanan güç tüketimi radyo biriminin açık ve kapalı olduğu süreye göre değişmektedir ve en çok güç harcayan kısımdır. Bu araçla elde edilen bu bilgiler mesaj gönderme ve alma işlemlerini, mesajın işlem süresini ve mesajın şifreleme, şifre çözme sürecinin tamamını kapsar. Simülasyonda kullanılan Wismote düğümünün veri sayfası değerleri kullanılarak enerji tüketim hesapları yapılmıştır. Eşitlik 5.1'de enerji hesaplaması gösterilmiştir. Wismote düğümünün işlemci aktif modu, uyku modu, paket gönderimi ve paket alması için harcadığı akım değerleri sırasıyla 2.2mA, 0.00169mA, 33.6mA ve 18.5mA'dir. [80] [81]

$$Enerji = \frac{Deger * Akim * Voltaj}{Saniyedeki\ tik\ sayisi} \tag{5.1}$$

- **RPL Mesaj Ek Yükü:** Ağdaki düğümler tarafından gönderilen tüm RPL mesajlarının bayt cinsinden toplam boyutu olarak tanımlanır. Bu metrik, güvenlik özelliklerinin getirdiği mesaj boyutundaki ek yükü değerlendirmek için kullanılmıştır. Güvenli RPL modlarında güvenli olmayan mod kontrol mesajlarına ek olarak güvenlik alanı gönderilir ve alınır. Yapılacak kriptografik işlemler bu alandaki bilgilere göre değişiklik göstermektedir.

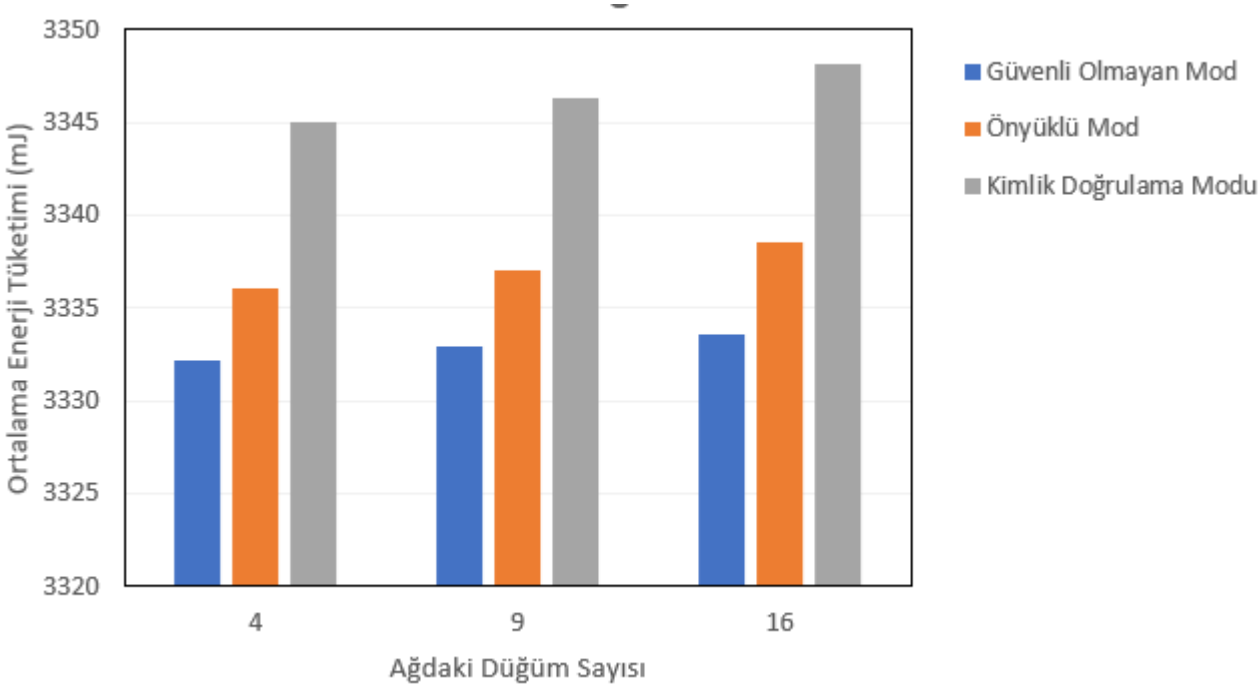
5.4 Simülasyon Sonuçları

Şekil 5.6'te ortalama ağ kurulum süresi gösterilmiştir. Ağdaki düğüm sayısı arttıkça ağın kurulum süresi artmaktadır ve bu beklenen bir sonuçtur. Önyüklü mod ile gönderilen güvenli RPL mesajlarının kullanılması ağ kurulum zamanını pek etkilememektedir. Kimlik doğrulama modunda ise ağa güvenli bir şekilde katılmak için ekstra mesajlaşma gerektiğinden ağ kurulum süresini oldukça artırmaktadır.



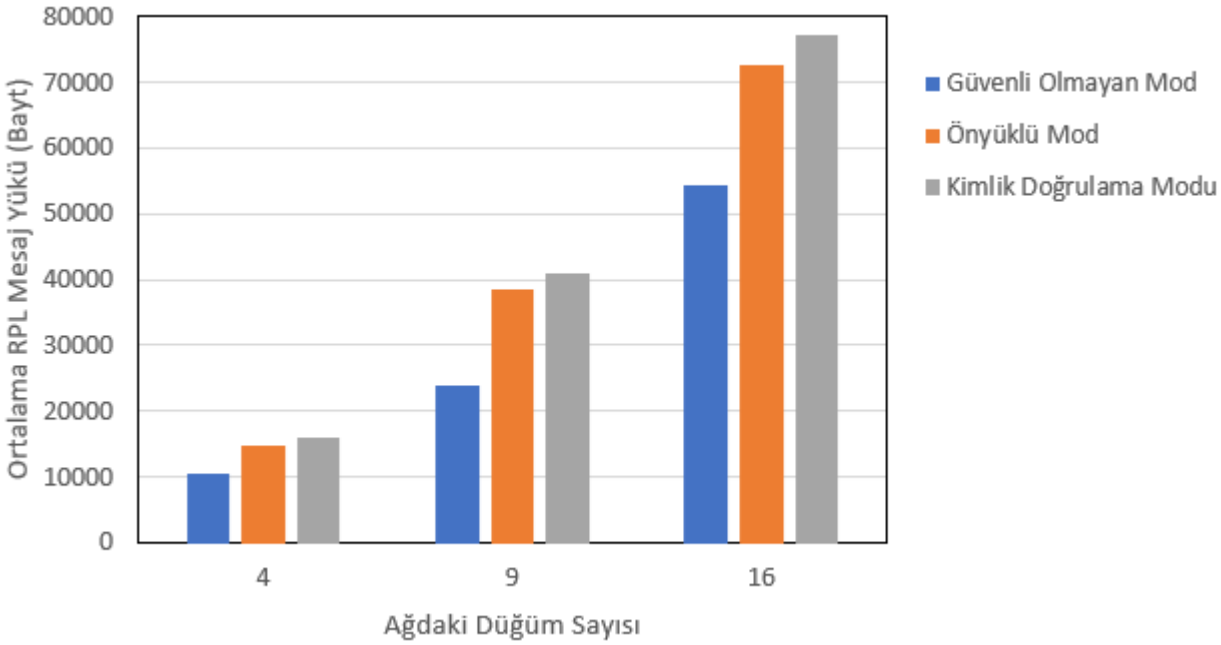
Şekil 5.6 : Düğümlerin Ortalama Ağ Kurulum Süresi

Şekil 5.7'te düğümlerin ortalama enerji tüketim değerleri gösterilmiştir. Beklenildiği üzere güvenli olmayan modda en düşük enerji tüketimi gerçekleşmiştir. Önyüklü modda enerji tüketimleri ise güvenli olmayan moda oldukça yakındır. Bunun nedeni güvenli mesajların uzunluğunun artmasına rağmen düğümlerde gerçekleşen simetrik kriptografi işlemlerinin hızlı olmasıdır. Kimlik doğrulama modunda ise ağa katılım sürecinde asimetrik kriptografi kullanıldığından önyüklü moda göre daha fazla enerji harcanmaktadır. Fakat düğüm ağa katıldıktan sonra simetrik kriptografi kullanıldığı için düğümlerin enerji tüketimlerinin ortalaması giderek azalmaktadır. Simülasyon daha uzun süre gerçekleştirildiğinde enerji tüketim değerleri önyüklü modun kullanımına yakın bir değer olacaktır. Ayrıca ağdaki düğüm sayısı arttıkça düğümler arası gönderilen mesaj sayısı artacaktır ve bu durum her düğüm için gönderilen ve alınan mesaj sayısını artıracaktır ve düğümlerin çalışma süresi artacağından enerji tüketimi de artacaktır.



Şekil 5.7 : Düğümlerin Ortalama Enerji Tüketimleri

Şekil 5.8'te RPL mesajlarının ortalama ek yükü gösterilmiştir. Önyüklü modda yer alan güvenli DIS ve DIO mesajlarının ek yükü ve kimlik doğrulama modunda ikinci anahtar alma sürecindeki mesaj fazlalığının yanında güvenli DIS ve DIO mesajlarının ek yükü belirtilmiştir. Şekilde görüldüğü ve beklendiği üzere en düşük ek yük güvenli olmayan modda gerçekleşmektedir. Önyüklü modda yer alan güvenli RPL mesajlarındaki güvenlik alanı nedeniyle ek yük biraz artmaktadır. Kimlik doğrulama modu ise önyüklü moda oldukça yakındır. Bunun nedeni düğümlerin güvenli ağa katıldıktan sonra DIO ve DIS mesajlarının yapısının önyüklü modla aynı olmasıdır. Ayrıca ağdaki düğüm sayısı arttıkça ağda iletilen mesaj sayısı artacağından mesajların ortalama ek yükü de artmaktadır.



Şekil 5.8 : Düğümlerin Ortalama Mesaj Yükü

6. SONUÇLAR VE GELECEK ÇALIŞMALAR

Bu tezde Contiki işletim sisteminde yer almayan kimlik doğrulama modu gerçeklenmiştir ve bu mod için yeni bir anahtar yönetimi metodu önerilmiştir. Bu metot Contiki işletim sisteminde gerçeklenmiştir. Bunun yanında Cooja simülatörü kullanılarak performans parametreleri gözlemlenmiştir ve elde edilen sonuçlar RPL'in diğer güvenlik modları ile karşılaştırılmıştır.

Simülasyon sonuçlarına göre kimlik doğrulama modunda ağ kurulum süreleri diğer modlara göre oldukça uzun sürmektedir. Düğüm sayısı arttıkça ağ kurulum süreleri de oldukça artmaktadır. Bu durumun aksine ortalama enerji tüketimi ve mesaj yükü ise önyüklü moda oldukça yakındır. Ağ kurulum aşamasından sonra sistem önyüklü mod gibi çalışacağından uzun süreli kullanımlarda kısıtlı enerjisi bulunan KSA'lar için enerji tüketimi önyüklü modda elde edilen sonuçlara yakın değerlere yaklaşacaktır.

Geliştirilen anahtar yönetimi metodu için bazı geliştirmeler yapılabilir. Kimlik doğrulama modunda kullanılan ikinci grup anahtarı ağ kurulum aşamasından itibaren hep aynı kalmaktadır. Yeni bir yöntemle veya mesaj tanımlaması yapılarak bu simetrik anahtar periyodik olarak güncellenip ağdaki tüm düğümlere dağıtılabilir. Böylece ağ güvenliği artırılmış olur ve ağdaki bir düğüm ele geçirilse bile anahtar periyodik olarak güncelleneceğinden ağ ile ilgili bilgiler ele geçirilmesi oldukça zorlaşır. Ayrıca düğümlerde yapılan asimetrik kriptografik işlemler başka bir anahtar sunucusunda gerçeklenebilir ve böylece limitli kaynaklı düğümler daha az enerji harcayarak kimlik doğrulama işlemini gerçekleştirebilir.

Başka bir gelecekte yapılacak çalışma olarak performans değerlendirmesinin gerçek donanımla yapılan deneyleri de içerecek şekilde genişletilmesi ve simülasyon sonuçlarıyla karşılaştırılması ile yapılan çalışmanın gerçekte ne kadar etkili olduğu

gözlemlenebilir. Ayrıca farklı ağ topolojileri ile çalışmalar yapılarak kimlik doğrulama yöntemi için hangi ağ topolojisi için daha uygun olduğu belirlenebilir.

KAYNAKLAR

[1] **IETF**, The Internet Engineering Task Force IETF, `https://www.ietf.org/`, Erişim: 28.05.2022

[2] **ROLL** Charter of the ROLL working group. IETF, Description of Working Group, `https://datatracker.ietf.org/wg/roll/about/`, Erişim: 28.05.2022

[3] **6LoWPAN** The 6LoWPAN Design Team. Charter of the 6LoWPAN working group. IETF, Description of Working Group, `https://datatracker.ietf.org/wg/6lowpan/about/`, Erişim: 28.05.2022

[4] **IPSO Alliance**, IP for Smart Objects (IPSO) Alliance https://github.com/OpenMobileAlliance/lwm2m-registry, Erişim: 29.05.2022

[5] **Winter, T.**, **Thubert, P.**, **Brandt, A.**, **Hui, J.**, **Kelsey, R.**, **Levis, P.**, **Pister, K.**, **Struik, R.**, **Vasseur, J.P. ve Alexander, R.**, (2012) RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550 (Proposed Standard).

[6] **Hui, J. ve Thubert, P.**, (2011) Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282.

[7] **IEEE 802.15.4 Standard** (2006) Wireless Medium Access Control (MAC) and physical layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), Part 15.4.

[8] **Vasseur, J.P. ve Dunkels, A.**, (2010) Interconnecting Smart Objects with IP: The Next Internet. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

[9] **Dunkels, A.**, **Gronvall, B. ve Voigt, T.**, (2004) Contiki - a lightweight and flexible operating system for tiny networked sensors, Local Computer Networks, 29th Annual IEEE International Conference, pp. 455–462.

[10] **Osterlind, F.**, **Dunkels, A.**, **Eriksson, J.**, **Finne, N. ve Voigt, T.**, (2006) Cross-Level Sensor Network Simulation with COOJA, pp. 641–648,

[11] **Romer, K. ve Mattern, F.**, (2004) The design space of wireless sensor networks. Wireless Communications, IEEE, 11(6):54-61.

[12] **Yick, Y.**, **Mukherjee, B. ve Ghosal, D.**, (2008) Wireless sensor network survey. Journal of Computer Networks, Volume 52(Number 12):292-2330.

[13] **Wener-Allen, G.**, **Lorincz, K.**, **Ruiz, M.**, **Marcillo, O.**, **Johnson, J.**, **Lees, J. ve Walsh, M.**, (2006) "Deploying a wireless sensor network on an active volcano. data-driven applications in sensor networks," IEEE Internet Computing, vol. 2, pp. 18–25.

[14] **Liu, G.**, **Tan, R.**, **Zhou, R.**, **Xing, G.**, **Song, W. ve Lees, J.M.**, (2013) Volcanic earthquake timing using wireless sensor networks, Proceedings of the 12th international conference on Information processing in sensor networks, pp. 91–102, ACM.

[15] **Song, W.**, **Huang, R.**, **Xu, M.**, **Ma, A.**, **Shirazi, B.**, **ve LaHusen, R.**, (2009) Air-dropped sensor network for real-time high-fidelity volcano monitoring, Proceedings of the 7th international conference on Mobile systems, applications, and services, pp. 305–318, ACM.

[16] **Hasler, A.**, **Talzi, I.**, **Beutel, J.**, **Tschudin, C. ve Gruber, S.**, (2008) Wireless sensor networks in permafrost research-concept, requirements, implementation and challenges. 9th International Conference on Permafrost, volume 1, pages 669-674.

[17] **Alemdar, H. ve Ersoy, C.**, (2010) Wireless sensor networks for healthcare: A survey, Computer Networks 54, 2688–2710.

[18] **Brennan, T.**, **Leape, L.**, **Laird, N.**, **Hebert, L.**, **Localio, A.**, **Lawthers, A.**, **Newhouse, J.**, **Weiler, P. ve Hiatt, H.**, (1991) Incidence of adverse events and negligence in hospitalized patients, New England journal of medicine 324, 370–376.

[19] **Gao, T.**, **Greenspan, D.**, **Welsh, M.**, **Juang, R. ve Alm, A.**, (2006) Vital signs monitoring and patient tracking over a wireless network, Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the, pp. 102–105.

[20] **Martinho, J.**, **Prates, L. ve Costa, J.**, (2014) Design and Implementation of a wireless multi parameter patient monitoring system, Procedia Technology, 542-549.

[21] **Darwish, A. ve Hassanien, A.E.**, (2011) Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring and Sensors. MDPI AG.

[22] **Baig, M. ve Gholamhosseini, H.**, (2013) Smart health monitoring systems: an overview of design and modeling. J Med Syst 37: 1–14.

[23] **Abreu, C.**, **Miranda, F.**, **Ricardo, M. ve Mendes, P.M.**, (2014) QoS-based management of biomedical wireless sensor networks for patient monitoring, SpringerPlus vol. 3 239.

[24] **Huiyong, W.**, **Jingyang, W. ve Min, H.**, (2013) Building a smart home system with WSN and service robot, Measuring Technology and Mechatronics Automation (ICMTMA), 2013 Fifth International Conference on, pp. 353–356, IEEE.

[25] **Waide, P.**, **Ure, J.**, **Smith, G. ve Bordass, B.**, (2013) The scope for energy and CO2 savings in the EU through the use of building automation technology final report, Waide Strategic Efficiency.

[26] **Jaafar, K. ve Watfa, M.K.**, (2013) Sensor networks in future smart rotating buildings, Consumer Communications and Networking Conference (CCNC), IEEE, pp. 962–967.

[27] **Suryadevara, N.K.**, **Mukhopadhyay, S.C.**, **Kelly, S.D.T. ve Gill, S.P.S.**, (2014) WSN-Based Smart Sensors and Actuator for Power Management in Intelligent Buildings, IEEE/ASME Transactions on Mechatronics

[28] **Ishfaq, A. ve Khalil, S.**, (2016) Military Applications using Wireless Sensor Networks: A survey, International Journal of Engineering Science and Computing 7039-7043 ISSN: 23213361.

[29] **Bokareva, T.**, **Hu, W.**, **Kanhere, S.**, **Ristic, B.**, **Gordon, N.**, **Bessell, T. ve Jha, S.**, (2006) Wireless sensor networks for battlefield surveillance. In Proceedings of the Land Warfare Conference, Brisbane, Australia, 24–27 October 2006; pp. 1–8.

[30] **Cannon, P.S. ve Harding, C.R.**, (2007) Future military wireless solutions, Ch. 8 Wireless Communications: The Future, Editor William Webb, John Wiley and Sons.

[31] **Winkler, m.**, **Tuchs, K.**, **Hughes, K. ve Barclay, G.**, (2008) Theoretical and practical aspects of military wireless sensor networks In Journal of Telecommunications and Information Technology, pp. 37-45.

[32] **Grilo, A.**, **Silva, R.**, **Nunes, P.**, **Martins, J. ve Nunes, M.**, (2007) Wireless sensor networking support to military operations on urban terrain, 12th International Command and Control Technology Symposium (ICCRTS), Command and Control Research Program (CCRP).

[33] **Srivastava, S.**, **Singh, M. ve Gupta, S.**, (2018) Wireless Sensor Network: A Survey, International Conference on Automation and Computational Engineering (ICACE), IEEE, pp. 159-163.

[34] **Ramson, S.R.J. ve Moni, D.J.**, (2017) Applications of Wireless Sensor Networks – A Survey, International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICIEEIMT), IEEE.

[35] **Kandris, D.**, **Nakas, C.**, **Vomvas, D. ve Koulouras, G.**, (2020) Applications of Wireless Sensor Networks: An Up-to-Date Survey, Applied System Innovation 3, no. 1: 14. https://doi.org/10.3390/asi3010014

[36] **RFC6997** Reactive Discovery of Point-to-Point Routes in Low Power and Lossy Networks. https://datatracker.ietf.org/doc/rfc6997/, Erişim: 02.06.2022.

[37] **Levis, P.**, **Brewer, E.**, **Culler, D.**, **Gay, D.**, **Madden, S.**, **Patel, N.**, **Polastre, J.**, **Shenker, S.**, **Szewczyk, R. ve Woo, A.**, (2008) The emergence of a networking primitive in wireless sensor networks", Communications of the ACM, Volume 51(Number 7), pp. 99-106.

[38] **Levis, P.**, **Clausen, T.**, **Hui, J.**, **Gnawali, O. ve Ko, J.**, (2011) The Trickle algorithm, RFC 6206.

[39] **Frazier, H.**, (2002) The 802.3 z gigabit Ethernet standard. Network, IEEE, 12(3), pp. 6-7.

[40] **Perkins, C.E. ve Royer, E.M.** (1999) Ad-hoc on-demand distance vector routing. In wmcsa, page 90. Published by the IEEE Computer Society.

[41] **Clausen, T.**, **Jacquet, P.**, **Adjih, C.**, **Laouiti, A.**, **Minet, P.**, **Muhlethaler, P.**, **Qayyum, A. ve Viennot, L.**, (2003) Optimized link state routing protocol (OLSR), RFC 3626.

[42] **Akkaya, K. ve Younis, M.**, (2005) A survey on routing protocols for wireless sensor networks. Journal of Ad Hoc Networks, Volume 3(Number 3):325-349.

[43] **Heinzelman, W.R.**, **Kulik, J. ve Balakrishnan, H.**, (1999) Adaptive protocols for information dissemination in wireless sensor networks. In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pages 174-185. ACM.

[44] **Handy, M.J.**, **Haase, M. ve Timmermann, D.**, (2002) Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In Mobile and Wireless Communications Network, 4th International Workshop on, pages 368-372. IEEE.

[45] **RFC5867** Building Automation Routing Requirements in Low- Power and Lossy Networks, RFC 5867. https://datatracker.ietf.org/doc/rfc5867/ Erişim: 29.05.2022.

[46] **RFC5826** Home Automation Routing Requirements in Low-Power and Lossy Networks, RFC 5826. https://datatracker.ietf.org/doc/rfc5826/ Erişim: 29.05.2022.

[47] **RFC5673** Industrial Routing Requirements in Low-Power and Lossy Networks, RFC 5673. https://datatracker.ietf.org/doc/rfc5673/ Erişim: 29.05.2022.

[48] **RFC5548** Routing Requirements for Urban Low-Power and Lossy Networks, RFC 5548. https://datatracker.ietf.org/doc/rfc5548/ Erişim: 29.05.2022.

[49] **Arena, A.**, **Perazzo, P.**, **Vallati, C.**, **Dini, G. ve Anastasi, G.**, (2020) Evaluating and improving the scalability of RPL security in the Internet of Things, Comput. Commun., vol. 151, pp. 119–132.

[50] **Perazzo, P.**, **Vallati, C.**, **Arena, A.**, **Anastasi, G. ve Dini, G.**, (2017) An Implementation and Evaluation of the Security Features of RPL,16th Int'l Conf. on Ad Hoc Networks and Wireless, vol. 10517. Springer Int'l Pub., 2017, pp. 63–76.

[51] **Gaddour, O. ve Koubaa, A.**, (2012) RPL in a nutshell: A survey, Computer Networks (14) 3163-3178

[52] **Whiting, D.**, **Housley, R. ve Ferguson, N.**, (2003) Counter with CBC-MAC (CCM), RFC 3610.

[53] **Tsiftes, N.**, **Eriksson, J. ve Dunkels, A.**, (2010) Low-power Wireless IPv6 Routing with ContikiRPL 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 406-407.

[54] **Razali, M.F.**, **Rusli, M.E.**, **Jamil, N.**, **Ismail, R. ve Yussof, S.**, (2017) The authentication techniques for enhancing the RPL security mode: A survey, in Zulikha, J.N.H. Zakaria (Eds.), Proceedings of the 6th International Conference on Computing Informatics (pp 735-743).

[55] **Chang, Q.**, **Zhang, Y. ve Qin, L.**, (2010) A node authentication protocol based on ECC in WSN. Proceedings of the International Conference on Computer Design and Applications, Jin. 25-27, IEEE Xplore Press, Qinhuangdao, China, pp: V2-606-V2-609.

[56] **Liu, Y. ve Yan, Y.**, (2012) A lightweight and scalable key management scheme for heterogeneous sensor networks. Proceedings of the 5th International Conference on BioMedical Engineering and Informatics, Oct. 16-18, IEEE Xplore Press, Chongqing, China, pp: 1393-1397.

[57] **Guicheng, S. ve Zhen, Y.**, (2013) Application of elliptic curve cryptography in node authentication of internet of things. Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct. 16-18, IEEE Xplore Press, Beijing, China, pp: 452-455.

[58] **Porambage, P.**, **Schmitt, C.**, **Kumar, P.**, **Gurtov, A. ve Ylianttila, M.**, (2014) Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. Proceedings of the IEEE Wireless Communications and Networking Conference, Apr. 6-9, IEEE Xplore Press, Istanbul, Turkey, pp: 2728-2733.

[59] **Shivraj, V.L.**, **Rajan, M.A.**, **Singh, M. ve Balamuralidhar, P.**, (2015) One time password authentication scheme based on elliptic curves for Internet of Things (IoT). Proceedings of the 5th National Symposium on Information Technology: Towards New Smart World, Feb. 17-19, IEEE Xplore Press, Riyadh, Saudi Arabia, pp: 1-6.

[60] **Santoso, F.K. ve Vun, N.C.H.**, (2015) Securing IoT for smart home system. Proceedings of the International Symposium on Consumer Electronics, Jun. 24-26, IEEE Xplore Press, Madrid, Spain, pp: 1-2.

[61] **Rghioui, A.**, **Abdmeziem, R.**, **Bouchkaren, S. ve Bouhorma, M.**, (2015) Symmetric cryptography keys management for 6lowpan networks. J. Theoretical Applied Inform. Technol., 73: 336-345.

[62] **Banerjee, P.**, **Chatterjee, T. ve Dasbit, S.**, (2015) LoENA: Low-overhead encryption based node authentication in WSN. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Aug. 10-13, IEEE Xplore Press, Kochi, India, pp: 2126-2132.

[63] **Saleh, M.**, **El-meniawy, N. ve Sourour, E.**, (2015) Authentication in flat wireless sensor networks with mobile nodes. Proceedings of the IEEE 12th International Conference on Networking, Sensing and Control, Apr. 9-11, IEEE Xplore Press, Taipei, Taiwan, pp: 208-212.

[64] **Jiang, Q.**, **Ma, J.**, **Wei, F.**, **Tian, Y.**, **Shen, J. ve Yang, Y.**, (2016) An untraceable temporal-credentialbased two-factor authentication scheme using ECC for wireless sensor networks. J. Netw. Comput. Applic., 76: 37-48.

[65] **Bala, D.Q.**, **Maity, S. ve Jena, S.K.**, (2017) Mutual authentication for IoT smart environment using certificate-less public key cryptography. Proceedings of the 3rd International Conference on Sensing, Signal Processing and Security, May 4-5, IEEE Xplore Presss, Chennai, India, pp: 29-34.

[66] **Hammi, M.**, **Livolant, E.**, **Bellot, P.**, **Serhrouchni, A. ve Minet, P.**, (2017) A lightweight mutual authentication protocol for the IoT. Proceedings of the iCatse International Conference on Mobile and Wireless Technology, (MWT' 17), Kuala Lumpur, Thailand, pp: 1-10.

[67] **Li, N.**, **Liu, D. ve Nepal, S.**, (2017) Lightweight mutual authentication for IoT and its applications. IEEE Trans. Sustainable Comput., 2: 359-370.

[68] **Li, X.**, **Niu, J.**, **Bhuiyan, M.Z.A.**, **Wu, F. ve Karuppiah, M.**, (2017) A robust ECC based provable secure authentication protocol with privacy protection for industrial internet of things. IEEE Trans. Indus. Inform., 3203: 1-11.

[69] **Shen, J.**, **Chang, S.**, **Shen, J.**, **Liu, Q. ve Sun, X.**, (2018) A lightweight multi-layer authentication protocol for wireless body area networks. Future Generat. Comput. Syst., 78: 956-963.

[70] **Dey, S. ve Hossain, A.**, (2019) Session-Key Establishment and Authentication in a Smart Home Network using Public Key Cryptography." IEEE Sensors Letters.

[71] **Shuai, M.**, **Yu, N.**, **Wang, H. ve Xiong, L.**, (2019) Anonymous authentication scheme for smart home environment with provable security. Comput. Secur. 2019, 86, 132–146.

[72] **Kumar, P.**, **Gurtov, A.**, **Iinatti, J.**, **Iinatti, J.**, **Ylianttila, M. ve Sain, M.**, (2016) Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments. IEEE Sensors Journal, vol. 16, no. 1, pp. 254-264

[73] **Wazid, M.**, **Kumar, A.**, **Odelu, V.**, **Kumar, N. ve Susilo, W.**, (2017) Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 391-406

[74] **Li, y.**, (2013) Design of A Key Establishment Protocol for Smart Home Energy Management System. Fifth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 88-93

[75] **Akyildiz, I.F.**, **Weilian, S.**, **Sankarasubramaniam, Y. ve Cayirci, E.**, (2002) A Survey on Sensor Networks, IEEE Communications Magazine, 40, 102-114.

[76] **Tsao, T.**, **Alexander, R.**, **Dohler, M.**, **Daza, V.**, **Lozano, A. ve Ed, R. M.**, (2015) A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). Retrieved from Internet Engineering Task Force (IETF): https://www.rfc-editor.org/info/rfc7416

[77] **Dunkels, A.**, **Eriksson, J.**, **Finne, N. ve Tsiftes, N.**, (2011) Powertrace: Network level power profiling for low-power wireless networks.

[78] **Url-1**, `https://www.ssl2buy.com/wiki`, Erişim: 28.05.2022

[79] **Url-2**, `https://github.com/kmackay/micro-ecc`, Erişim: 03.06.2022

[80] **Url-3**, `https://www.ti.com/product/CC2520`, Erişim: 03.06.2022

[81] **Url-4**, `https://www.ti.com/product/MSP430F5437`, Erişim: 03.06.2022

ÖZGEÇMİŞ

Ad Soyad: Mehmet BAYAR

Doğum Yeri ve Tarihi: Altındağ/ANKARA - 01.10.1993

E-Posta: mbayar93@gmail.com

Adres: Aselsan A.Ş. Teknokent Yerleşkesi, ODTÜ Teknokent - ANKARA

ÖĞRENİM DURUMU:

- **Lise:** 2011, Mehmet Emin Resulzade Anadolu Lisesi
- **Lisans:** 2016, Hacettepe Üniversitesi, Elektrik-Elektronik Mühendisliği
- **Yüksek Lisans:** 2022, İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği

İŞ DENEYİMİ:

- 2016- ASELSAN A.Ş Gömülü Yazılım Tasarım Mühendisi

DENEYİM ALANLARI:

- ARM-Cortex-M yazılım tasarımı
- Düşük güçlü sistem tasarımı
- Embedded Linux
- Android Özelleştirme