İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

RPL SALDIRILARINA KARŞI STANDART UYUMLU VE KİMLİK DOĞRULAMALI RPL GÜVENLİK MODU TASARIMI

YÜKSEK LİSANS TEZİ

Arif Burak ORDU

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

HAZİRAN 2022

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

RPL SALDIRILARINA KARŞI STANDART UYUMLU VE KİMLİK DOĞRULAMALI RPL GÜVENLİK MODU TASARIMI

YÜKSEK LİSANS TEZİ

Arif Burak ORDU
(504171282)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. S. Berna ÖRS YALÇIN

HAZİRAN 2022

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

STANDARD COMPLIANT AND AUTHENTICATED RPL SECURITY MODE DESIGN AGAINST RPL ATTACKS

M.Sc. THESIS

Arif Burak ORDU
(504171282)

Department Electronics and Communication Engineering

Electronics Engineering Programme

Thesis Advisor: Prof. Dr. S. Berna ÖRS YALÇIN

JUNE 2022

İTÜ, Lisansüstü Eğitim Enstitüsü'nün 504171282 numaralı Yüksek Lisans Öğrencisi Arif Burak ORDU, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "RPL SALDIRILARINA KARŞI STANDART UYUMLU VE KİMLİK DOĞRULAMALI RPL GÜVENLİK MODU TASARIMI" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

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

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

Anne ve babama,

ÖNSÖZ

Çalışmalarımda danışmanlığımı üstlenen, tecrübelerini paylaşan ve desteğini esirgemeyen sayın Prof. Dr. Sıddıka Berna Örs YALÇIN'a,

Aselsan Akademi programı ile tüm imkanları bize sunan, çalışmakla gurur duyduğum şirketim Aselsan A.Ş'ye,

Aselsan Akademi sorumlularından İrem YÜKSEK ve İbrahim Halil GİDEN'e,

Çalışmalarım boyunca desteklerini esirgemeyen iş arkadaşlarım Mehmet Özgen ÖZDOĞAN, İsmail Çağdaş YILMAZ, Emre Kutlu KÖSE, Ahmet ADA ve Özkan YILMAZ'a, yöneticilerim Hüseyin Ertürk ÇETİN ve Ahmet EROL'a,

Yüksek Lisans programı boyunca ihmal ettiğim tüm arkadaşlarıma,

Hayatımın her anında desteklerini benden esirgemeyen canım annem Nuray ORDU, babam Mete ORDU, ablam Reyhan Şeyda KALAY, kardeşim İsmail Enes ORDU, dedem Musa ORDU ve babaannem Reyhan ORDU'ya,

Sevgi, saygı ve teşekkürlerimi sunarım.

Haziran 2022

Arif Burak ORDU
Elektronik Mühendisi

İÇİNDEKİLER

KISALTMALAR

6LBR : 6LoWPAN Border Routers
6LoWPAN : IPv6 over Low-Power Wireless Personal Area Networks
AES : Advanced Encryption Standard
BAN : Burrows, Abadi and Needham
BKE : Bilateral Key Exchange
BLE : Bluetooth Low Energy
CBC-MAC : Cipher Block Chaining Message Authentication Code
CC : Consistency Check
CCM : Counter with CBC-MAC
COAP : Constrained Application Protocol
CPU : Central processing unit
CTR : Counter
DAG : Directed Acyclic Graph
DAO : Destination Advertisement Object
DAO-ACK : Destination Advertisement Object Acknowledgment
DIO : DODAG Information Object
DIS : DODAG Information Solicitation
DODAG : Destination-Oriented DAG
DODAGID : DODAG Identifier
DSSS : Direct Sequence Spread Spectrum
DTLS : Datagram Transport Layer Security
ECC : Elliptic-curve cryptography
ETX : Expected Transmission Counts
EUI-64 : Extended Unique Identifiers - 64 bit
GHz : Gigahertz
GPS : Global Positioning System
GSM : Global System for Mobile Communications
H : Host
HTTP : Hypertext Transfer Protocol
ICMPv6 : Internet Control Message Protocol for IPv6
ID : Identity
IDS : Intrusion Detection System
IEEE : Institute of Electrical and Electronics Engineers
IETF : Internet Engineering Task Force
IoT : Internet of Things
IPv4 : Internet Protocol version 4
IPv6 : Internet Protocol version 6
ITU : International Telecommunication Union

kbps : Kilobit per second
KIM : Key Identifier Mode
KMS : Key Management Server
LLN : Low-power and Lossy Network
LoRaWAN : Long range wide-area network
LVL : Security Level
MAC : Media Access Layer
Mbps : Megabit per second
MHz : Megahertz
MOP : Mode of Operation
MP2P : Multipoint-to-point
MRHOF : Minimum Rank with Hysteresis Objective Function
MQTT : Message Queueing Telemetry Transport
MTU : Maximum Transmisson Unit
NB-IoT : Narrowband IoT
NFC : Near Field Communication
OCP : Objective Code Point
OF : Objective Function
OF0 : Objective Function Zero
O-QPSK : Offset-Quadrature Phase-Shift Keying
OSI : Open Systems Interconnect
P2MP : Point-to-multipoint
P2P : Point-to-point
PLC : Power Line Communication
R : Router
REST : Representational State Transfer
RF : Radio Frequency
RFC : Request for Comments
RFID : Radio-frequency identification
ROLL : Routing Over Low-Power and Lossy
RPL : IPv6 Routing Protocol for Low-Power and Lossy Networks
SFD : Start of Frame Delimiter
SPDL : Security Protocol Definition Language
SRPL : Secure RPL
TCA : Trusted Computing Architecture
TCP : Transmission Control Protocol
TLS : Transport Layer Security
TPM : Trusted Platform Module
TRAIL : Trust Anchor Interconnection Loop
UDP : User Datagram Protocol
VeRA : Version Number and Rank Authentication

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

RPL SALDIRILARINA KARŞI STANDART UYUMLU VE KİMLİK DOĞRULAMALI RPL GÜVENLİK MODU TASARIMI

ÖZET

İnternet Mühendisliği Görev Gücü (IETF) organizasyonu tarafından geliştirilen ve Açıklama İsteği (RFC) standartları ile tanımlı Düşük Güç ve Kayıplı Ağlar için IPv6 Yönlendirme Protokolü (RPL), düzinelerce ila binlerce sınırlı kaynak ve zayıf bağlantılara sahip kısıtlı yönlendiriciyi organize edebilen ve Düşük Güç ve Kayıplı Ağlar (LLNs) için optimize edilmiş standart bir yönlendirme protokolüdür. RPL protokolü, enerji verimli, ölçeklenebilir ve otonom yapısı ile LLN'ler için vazgeçilmez bir protokol olmasına rağmen, hassas veri ve mekanizmaları ile sayısız güvenlik saldırısına açık olarak kabul edilmektedir. Bu tez çalışmasında, ilk önce RPL mekanizmalarını ve literatürde yer alan RPL'e karşı yapılan güvenlik saldırılarını derinlemesine analiz ettik. Bu analizler sonucunda RPL güvenlik saldırılarının büyük oranda, RPL kontrol mesajlarının hassas veri içeriklerini kullanarak RPL'in dinamik mekanizmalarını hedef alan içerik saldırılarından oluştuğunu ve var olan saldırılar haricinde birçok yeni saldırının keşfe açık olduğunun fark ettik. Bu doğrultuda, Trickle zamanlayıcı parametre saldırısı adı verdiğimiz yeni bir RPL içerik saldırısı önerdik. Saldırgan modelimizi Contiki işletim sistemi RPL gerçeklemesi üzerinde modelledik ve bu saldırgan modelinin Cooja simülasyon aracında simülasyonunu yaparak RPL ağları üzerindeki yıkıcı etkisini gözlemledik. Daha sonra, literatürdeki RPL saldırına karşı geliştirilen saldırı önlemleri hakkında kapsamlı bir araştırma yaptık. Önerilen çözümlerin büyük bir çoğunluğunun RPL içerik saldırılarının tümünü engelleyecek nitelikte olmadığını veya RPL'e uygulanması halinde mevcut RPL mekanizmaların harcadığı kaynak miktarına kıyasla çok daha fazla işlem, hafıza ve enerji yükü doğurduğunu gözlemledik. Bu kapsamda, RPL içerik saldırılarına karşı bütüncül ve hafif bir karşı önlem mekanizması olacağını düşündüğümüz standart uyumlu RPL kimliği doğrulanmış güvenlik modunu inceleme altına aldık. Ancak, RPL kimliği doğrulanmış modu için birçok mekanizma RFC standartlarında eksik veya gelecek çalışması olarak bırakılmıştı. Bu eksiklileri gidermek amacı ile standardın önerilerine ve katı yasaklamalarına bağlı kalarak RPL protokol detaylarını, ağ elamanlarının davranışlarını, kontrol mesajı içeriklerini ve bir kimlik doğrulamalı anahtar değişim şemasını değerlendirerek kapsamlı bir RPL kimliği doğrulanmış güvenlik modu sistemi önerdik. Bu sistemde kullanılmak üzere, İkili Anahtar Değişimi (BKE) olarak bilinen karşılıklı kimlik doğrulamalı anahtar değişim protokolünü güven zinciri mekanizmasına dayalı bir yöntem ile genişleterek anahtar güncelleme prosedürünü de içeren kapsamlı bir kimlik doğrulamalı anahtar değişim protokolü tasarladık. Tasarlanan bu protokolü bir güvenlik protokolü resmi doğrulama aracı olan Scyther simülasyon aracı ile resmi doğrulamasını yaptık. Bu çalışmanın, araştırmacılara RPL güvenliğine ve standart uyumlu kimliği doğrulanmış RPL güvenlik moduna kapsamlı bir yaklaşım ile daha fazla katkıda bulunmalarına yardımcı olacağına inanıyoruz.

STANDARD COMPLIANT AND AUTHENTICATED RPL SECURITY MODE DESIGN AGAINST RPL ATTACKS

SUMMARY

The rapid development in the Internet of Things (IoT) applications has come up with systematic approaches and solutions for various edge devices and network technologies in the scope of many interoperability and managerial problems. At the beginning of this millennium, Internet Protocol Version 6 (IPv6) has been proposed and then developed by the Internet Engineering Task Force (IETF) to provide internetworking solutions for a growing number of devices connected to the internet. With the advent of the IoT technologies and their recent advances, an adaptation solution for transmission of IPv6 packets over IEEE 802.15.4 has been deployed to enable resource constraint devices to be accessed directly from the internet by using IPv6 and created the term IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). Routing Over Low-Power and Lossy (ROLL) networks Working Group analyzed the routing requirements in urban, industrial, home, and building automation applications and defined a dynamic and self-healing protocol IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) compliant with 6LoWPAN.

RPL's self-organization and self-recovery mechanisms make it open to abuse with poisonous data contents. Any malicious usage, modification, fabrication, or deficiency on these control messages and fields makes the nodes detract from their expected behaviors. In this direction, many research articles have already discussed RPL message forging attacks and possible countermeasures. However, any countermeasure step to prevent or detect RPL attacks most likely will consume extra resources (memory, process power, energy, bandwidth), which are already seen as constraints. For that reason, the methods that will be deployed on the system should be carefully managed in detail.

RPL has also its security features *pre-installed* and *authenticated* operation modes. As the pre-installed mode, employed with the static keys, has significant weaknesses the authenticated mode provides the infrastructure to solve this situation but with many shortcomings and is open to improvements.

In the scope of this thesis study, we intensely analyzed RPL working mechanisms and RPL security attacks in the literature. By gathering seven well-known RPL attacks (Rank, Local Repair, Version Number or Global Repair, Routing Table, Objective Function Parameter Manipulation, DAO Inconsistency, and DAG Inconsistency Attacks) under a single title, we came up with a new taxonomy that we call RPL content attack. As a result of these analyzes, we realized that RPL security attacks are mostly content attacks targeting the dynamic mechanisms of RPL by using sensitive data contents of RPL control messages, and many new attacks are open to discovery,

apart from existing attacks. In this direction, we have proposed a novel RPL content attack called Trickle timer parameter attack.

Trickle timer is the critical mechanism that makes RPL an adaptive and energy-efficient routing protocol by controlling the sending frequency of DIO control messages according to the stability of the network. DIO and the option messages attached to DIO contain information that defines the RPL network, as well as some important parameters that can be changed dynamically according to the state of the network. Three of these parameters are the DIO Interval Doubling Number (DIOIntDoubl.), Minimum DIO Interval (DIOIntMin), and Redundancy Coefficient (DIORedun.) fields carried in the DODAG Configuration option and affect the Trickle timer algorithm directly. The proposed attacker model maliciously manipulates these parameters, resulting in increased DIO sending frequency at nodes receiving manipulated DIOs. We modeled our proposed attacker model on the RPL implementation on Contiki operating system and observed its destructive effect on RPL networks by simulating this attacker model in the Cooja simulation tool. We deployed the attacker in different locations of the network. We observed that the effect of the attack increases as the location of the attacker is closer to the DODAG root from the edge of the network. Another noteworthy observation was that while we only expected an increase in the number of DIO messages, the increase in the number of DAOs also caught our attention.

Before proposing any countermeasure to RPL attacks, we first conducted comprehensive research on mitigation methods and Intrusion Detection Systems (IDSs) in the literature. Then, we have observed that the majority of the proposed solutions are not capable of preventing all RPL content attacks or that if applied to RPL, they cause much more processing, memory, and energy burden compared to the number of resources expended by existing RPL mechanisms. In this context, we have examined the standard-compliant RPL authenticated security mode, which we think will be a holistic and lightweight countermeasure mechanism against RPL content attacks. However, many mechanisms for the RPL authenticated mode were missing or left as future work in the Request for Comments (RFC) standards.

The RPL authentication mode mechanism requires a second symmetric group key for routers to operate the RPL mechanism. In order to address this shortcoming, we attached a comprehensive key management scheme with extending and adopting the BKE (Bilateral Key Exchange) protocol to help secure RPL with the key establishment and authentication mechanisms, including a re-keying process. We fully verified this designed security protocol with the Scyther simulation tool, which is a security protocol formal verification tool.

The proposed authentication and key exchange protocol includes hash functions and cryptological methods, includes both symmetric and asymmetric keys. The proposed protocol was designed in three stages. In the first stage, it was a 3-message protocol scheme designed to authenticate the node to join the network first and obtain the current second key of the network. When we used the Scyther tool to validate the protocol in the first stage, it failed. Scyther tool made us realize an attacker model that compromised the secrecy of the second key. In the second stage, this vulnerability was fixed, and the proposed protocol was updated and fully verified. In stage three, a

re-keying support was added by updating the entire protocol with a lightweight solution based on a trust chain mechanism and fully verified.

Then, we proposed a comprehensive RPL authenticated security mode system, adhering to the recommendations and strict prohibitions of the standard, evaluating the RPL protocol details, the behavior of network elements, control message contents, and our proposed authenticated key exchange scheme.

In the last part of the thesis, we mentioned the possible future studies for the proposed method and the details of the usage of the solution. We also explained that a cryptological method that will be carefully applied in 6LoWPAN networks would not create as much overhead as can be avoided and significantly contribute to the prevention of RPL content attacks. We believe this study helps both implementers and researchers to contribute more to RPL security and the standard-compliant Authenticated Mode of RPL with an extensive approach.

1. GİRİŞ

Nesnelerin İnterneti (IoT) uygulamalarında yaşanan hızlı büyüme, birçok birlikte çalışabilirlik ve yönetimsel sorununu beraberinde getirse de ağ ve uç cihaz teknolojileri için sistematik yaklaşımlar ve çözümler ortaya çıkarmıştır. İnternete bağlanan cihaz sayısındaki öngörülen artışın doğuracağı ağ yönetim problemine çözüm olarak İnternet Mühendisliği Görev Gücü (IETF) bu milenyumun başında İnternet Protokolü Sürüm 6 (IPv6)'yı geliştirmiştir [9,10]. IoT teknolojilerinin ortaya çıkışı ve son gelişmeleri ile birlikte, kaynak kısıtlı cihazlara IPv6 kullanılarak internetten doğrudan erişilebilmesini sağlamak amacıyla IPv6 paketlerinin IEEE 802.15.4 üzerinden iletilmesini sağlayan bir adaptasyon çözümü ile Düşük Güçlü Kablosuz Kişisel Alan Ağları üzerinden IPv6 (6LoWPAN) geliştirilmiştir [11,12]. Düşük Güç ve Kayıplı Ağlar Üzerinden Yönlendirme (ROLL) Çalışma Grubu kentsel, endüstriyel, ev ve bina otomasyonu uygulamalarındaki yönlendirme gereksinimlerini analiz ederek dinamik, kendi kendini onaran ve 6LoWPAN ağları ile uyumlu bir protokol olan Düşük Güç ve Kayıplı Ağlar için IPv6 Yönlendirme Protokolü (RPL)'i [20] geliştirmiştir.

RPL'in kontrol mesajlarıyla sağladığı kendi kendini organize etme ve onarma mekanizmaları, onu zehirli veri içerikleriyle kötüye kullanıma açık hale getirir. Bu kontrol mesajları ve alanlarındaki herhangi bir kötü niyetli kullanım, değişiklik, üretim veya eksiklik, RPL'i kullanan ağ düğümlerinin beklenen davranışlarından uzaklaşmasına neden olur. Bu doğrultuda araştırmacılar birçok RPL mesaj sahteciliği saldırısını ve olası karşı önlemlerini konu olarak ele almıştır. [32,33]. Bu çalışmalarda açıkça görülmektedir ki, RPL saldırılarını önlemeye veya tespit etmeye yönelik alınan herhangi bir önlem adımı, büyük olasılıkla zaten kısıtlı olarak görülen kaynaklar (bellek, işlem gücü, enerji, bant genişliği) üzerinde ek tüketime sebep olacaktır [32]. Bu nedenle bir sistem üzerinde konuşlandırılacak RPL saldırı karşı önlem yöntemlerinin dikkatli ve detaylı bir şekilde yönetilmesi gerekmektedir.

RPL'in kendi güvenlik önlemi olarak önden yüklenmiş mod ve kimliği doğrulanmış mod olarak iki farklı güvenlik modu mevcuttur [20]. Bu modlardan önden yüklenmiş mod statik değişmeyen simetrik kritpto anahtarı kullanması ile önemli bir güvenlik açığına sahip iken, kimliği doğrulanmış mod bu durumun aşılması için bir altyapıya sahip olmasına rağmen geliştirmeye açık birçok eksik tanımlamaya sahiptir. [33,48]

Bu tez çalışması kapsamında RPL mekanizmalarına, RPL güvenlik saldırılarına ve bu saldırılara karşı alınan güvenlik önlemlerine kapsamlı ve detaylı bir gözden geçirme yapıyoruz. Daha sonra yeni bir RPL içerik saldırısı olan Trickle zamanlayıcısı saldırısını öneriyor, bu saldırıyı Contiki [59] işletim sistemi RPL gerçeklemesi üzerinde modelleyerek Cooja [60] simülasyon aracında simülasyonunu yaparak RPL ağları üzerindeki yıkıcı etkisini gösteriyoruz. Daha sonra RPL içerik saldırılarına bütüncül bir çözüm olabilecek standart uyumlu RPL kimliği doğrulanmış güvenlik modu öneriyoruz. Önerilen bu yöntem için, bir anahtar güncelleme mekanizmasını da içeren karşılıklı kimlik doğrulama ve güven zinciri mekanizmalarına dayalı kimlik doğrulama ve anahtar değişim protokolü tasarlıyoruz. Tasarlanan protokolü bir güvenlik protokolü doğrulama simülasyon aracı olan Scyther [65] aracında resmi güvenlik doğrulamasını yapıyoruz. Tezin sonunda ise RPL saldırılarına karşı kriptolojik yöntemlerin kullanılmasının aslında kaçınıldığı kadar kaynak yükü bindirmeyeceğini aksine verimli olduğu durumların olacağını anlatıyor, önerilen çözüm için olası gelecek zaman çalışmalarından ve kullanım alanı detaylarından bahsederek araştırmacıları bu yönde RPL güvenliğine katkıda bulunmaya davet ediyoruz.

2. NESNELERİN İNTERNETİ

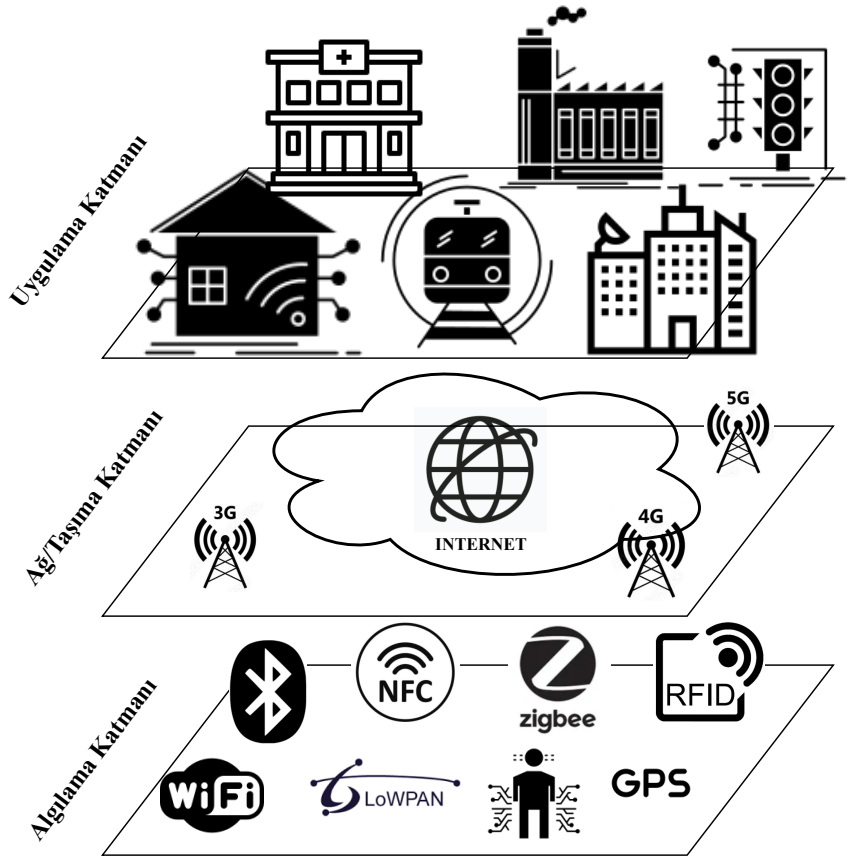
90'lı yıllarda ortaya atılan bir kavram olan "Nesnelerin İnterneti" ya da kısaltılmış hali ile IoT (Internet of Things), güncelliğini günümüze kadar koruyarak akademi ve endüstrinin odak noktası olmuş ve halen gelecek ağ ve cihaz teknolojilerini şekillendirmeye devam eden baskın bir teknoloji ve araştırma alanıdır. [2,3]. IoT isminin ortaya çıkışı 1999 yılında bir İngiliz teknoloji öncüsü ve MIT üniversitesindeki Auto-ID Laboratuvarının kurucularından biri olan Kevin Ashton'un RFID teknolojisini tedarik zincirinde kullanması ile olmuş daha sonra kısa sürede popüler hale gelmiş ve internetin Kablosuz Sensör Ağları (WSN) aracılığı ile fiziksel dünyaya bağlandığı bir haberleşme sistemi haline gelmiştir [1].

Günümüzde ise IoT, etrafımızdaki her şeyin akıllı cihazlara dönüşüp internete bağlanma yeteneği kazandığı, bu akıllı cihazların (nesnelerin) birbirleri ve insanlar ile her yerde ve her zaman iletişim kurmasını sağlayan bir olgu haline gelerek, sağlık sektörü, otomobil sektörü, akıllı bina uygulamaları, endüstriyel uygulamalar, spor, ulaşım, tarım, akıllı ölçüm sistemleri, lojistik, eğlence sektörü gibi sayısız alanda kullanılmaktadır [15]. IoT'nin bu şekilde yaygınlaşması insanlı veya insansız internete bağlanan cihaz sayısında inanılmaz bir artış olması sonucunu doğurmuştur.

Cisco'nun 2020 yılında yayınlamış olduğu bir araştırma raporuna göre internete bağlı cihaz sayısı 2018'de 18.4 milyar iken, 2023 yılında 29.3 milyara ulaşması beklenmektedir [4]. Bu artış beraberinde birçok ağ yönetim problemini de beraber getirecektir. Neyse ki İnternet Mühendisliği Görev Gücü (IETF) 2000'li yılların başında mevcut IPv4 adres yapısının internete bağlı cihazların biricik adresleri belirlemekte ve yönetmekte yetersiz kalacağını öngörerek IPv6'yı geliştirmiştir. Mevcut internet altyapısında kullanılan IPv4 adres yapısı 32 bit'lik bir adres alanını desteklerken IPv6 128bit'lik bir adres alanına sahiptir. IPv6 128bit'lik adres alanı ile internete direk bağlanabilen biricik kimlikli cihaz sayısının ulaşılması çok güç bir değere (yaklaşık $2^{128} \approx 3.4x10^{38}$) ulaşmıştır. [9,10]

2.1 Nesnelerin İnterneti Mimarisi

Nesnelerin İnterneti'ni, bileşenlerini, teknolojilerini, ihtiyaçlarını ve problemlerini anlamak için bir referans mimari ortaya koymak çok önemlidir. ITU, IoT Forum, IETF gibi kuruluşların yanında çok sayıda araştımacı, Nesnelerin İnterneti için bir mimari sunsa da henüz üzerinde hemfikir olunmuş ve standart haline gelmiş bir mimariye ulaşılamamıştır. [14]



Şekil 2.1 : Nesnelerin İnterneti üç katmanlı mimarisi

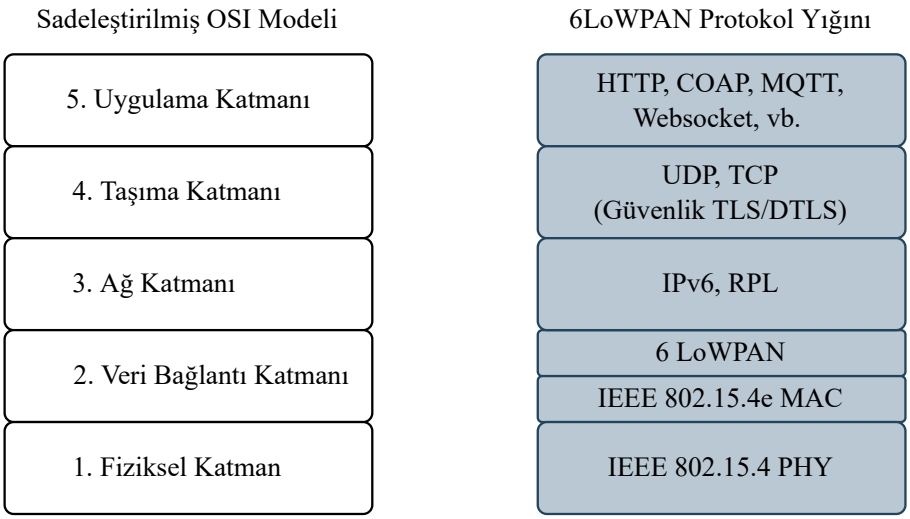
Önerilen mimarilerin en yaygın ve genel olanı; Algılama Katmanı, Ağ/Taşıma Katmanı ve Uygulama Katmanın'dan oluşan üç katmanlı olanıdır [15]. Algılama Katmanı; sensör arayüzleri ile dış dünyayı algılayabilen, gerektiğinde bir fonksiyonu gerçekleştirebilen, gerektiğinde bilgiyi işleyebilen ve kullanabilen göreceli kısıtlı kaynaklara sahip akıllı cihaz ve bu cihazların ağlarından oluşur. Ağ Katmanı, algı katmanındaki cihaz ve ağları çeşitli ağ geçitleri, kablolu kablosuz haberleşme ve ağ teknolojileri ile uç birim bileşenlerini ulaşılabilir kılan katmandır. Uygulama Katmanı

ise Nesnelerin İnterneti'nin kullanımına özel şekillenen aplikasyonların, servislerin, bilgi işleme ve yönetim birimlerinin yer aldığı ve uygulamanın amacı ile muhattap insanlı veya insansız birime kavuşturan katmandır.

Algılama Katmanınını aynı zamanda uç katmanı veya uç cihaz katmanı olarak, bu katmanda kullanılan her tür cihaz ve haberleşme teknolojisini ise uç katman teknolojileri olarak adlandırabiliriz. Uç katman cihazları birbirleri ile haberleşebilir, bir ağ kurabilir veya bir ağ geçidi aracılığı ile ağ katmanına ulaşabilirler. Uç katmanda kullanılan standartlaşmış haberleşme ve ağ tenolojilerine; Internet Protocol Version 6 over Low Power Wireless Personal Area Networks (6LoWPAN), ZigBee, Bluetooth Low Energy (BLE), Z-Wave, Near Field Communication (NFC) ve Radio Frequency Identification (RFID) gibi kısa mesafe teknolojilerini, LoRaWAN, Narrow Band (NB-IoT), Extended Coverage (EC)-GSM-IoT ve Sigfox gibi uzun mesafe teknolojilerini örnek gösterilebiliriz. [16,17]

2.2 6LoWPAN ve Standartlaşmış Protokol Yığını

IoT'nin bir parçası olan akıllı uç cihazlar her zaman yüksek donanımlara sahip cihazlar olmayıp limitli işlem gücüne, düşük hafızalı, kısa mesafe haberleşme yapan, düşük veri hızına sahip, kısıtlı enerjili veya batarya ile çalışan cihazlar olabilir. Bu cihazlar Uluslararası Haberleşme Birliği'nin (ITU) tanımına göre "Kısıtlı Cihazlar" olarak adlandırılmışlardır [5]. IPv6 ile tanımlanan bazı ağır ve maliyetli protokollerinin bu kısıtlı cihazlarda gerçeklenmesi de ayrı bir teknolojik zorluğu ortaya çıkartmıştır [1]. Bu tür zorluklara çözüm getirmek konusunda öncülük eden IETF bu durumun aşılması için bazı sıkıştırma ve parçalı gönderme yöntemleri ile IPv6 paketlerinin görece düşük bant genişliğine sahip IEEE 802.15.4 üzerinden kullanılmasını sağlayacak bir adaptasyon çözümü olarak güç-verimli, dayanıklı ve internete bağlanabilirlik özelliklerini sağlayan kablosuz haberleşme ağ teknolojisi olarak 6LoWPAN çözümünü getirmişlerdir. [11,12]. 6LoWPAN sayesinde cihazlar hem kendileri ile hem de dış IP ağları (örneğin internet) ile IPv6 kullanarak doğrudan haberleşebilme yeteneğine sahip olmuşlardır [15].



Şekil 2.2 : 6LoWPAN protokol yığını

6LoWPAN protokol yığını, haberleşme ağlarında en çok kabul görmüş ağ yapısı olan Open Systems Interconnect (OSI) katman yapısının beş katmanlı basitleştirilmiş haline benzer şekilde tarif edilebilir (Şekil 2.2) [19].

Birinci ve en alt katman olan Fiziksel Katman'da veri bitleri RF haberleşme sinyallerine dönüştürülür. Bu katmanda 2.4 GHz bandında çalışan IEEE 802.15.4 fiziksel katman tanımlamaları kullanıldığı gibi Sub1-GHz bandında çalışan ve daha fazla mesafe elde edilebilen düşük-güç RF, Bluetooth® Akıllı Güç Hattı Haberleşmeleri (PLC) ve düşük-güç Wi-Fi® gibi teknolojilerin de kullandığı IEEE 802.15.4g standardı da kullanılabilir. IEEE 802.15.4 fiziksel katman tanımlamaları; bina uygulmalarında kullanılabilecek büyüklükteki ağlar için enerji-verimliliği, mesafe ve veri hızı optimizasyonu sağlacak niteliktedir. [19]

IEEE 802.15.4 fiziksel katmanında 2 Mbps fiziksel veri hızına imkan sağlayan Ofset-Karesel Faz Kaydırmalı Anahtarlama (O-QPSK) modülasyonu kullanılmaktadır. Bu modülasyonda gönderici üzerindeki her 4 bit havaya 32 fiziksel bit olarak gönderilir. Dolayısıyla 2 Mbps veri hızının kullanıcıya yansıyan kısmı 250 kbps'ye düşmektedir. Ancak, Direct Sequence Spread Spectrum (DSSS) olarak adlandırılan bu teknik ile veri hızında düşüş olmasına karşı veri aktarım sağlamlığı kazanılmıştır. [18]

IEEE 802.15.4 fiziksel katmanda 2.4 GHz ile 2.480 GHz arasında 5 MHz aralıklar ile 16 farklı frekans kanalı tanımlamıştır. Bu frekans kanallarının genişliği 2 MHz

olarak belirlenip ortogonal yerleşim ile bir alt kanalın bir üst kanalın girişiminin önüne geçilmiştir. Göndermeç birimi bu kanalların herhangi birinden başlangıç sinyali (preamble) ve ardından bilinen sabit veri sıralamasına sahip Start of Frame Delimiter (SFD) yollar. Almaç birimleri ise başlangıç sinyalini farkettiği frekansa kurulup SFD sayesinde veri geleceğini doğrular. Bu katmanda bir seferde havaya basılabilecek maksimum veri boyu 1 byte'ı veriboyu bilgisi olmak üzere toplam 128 byte'tır. 127 Byte veri boyu IEEE 802.15.4 Maximum Transmisson Unit (MTU) değerini belirlemiş olmaktadır. [18]

İkinci katman olan Veri Bağlantı Katmanı, birbiri ile direk bağlantısı olan iki ağ düğümünün arasındaki bağlantının emniyetli (reliable) olmasını, fiziksel katmanda alma gönderme sırasında oluşabilecek hataların algılanmasını ve düzeltilmesini sağlayan katmandır. Bu katman aynı zamanda, taşıyıcı algılamalı çoklu erişim özelliğini içinde barındıran Ortama Erişim Katmanı'nı da içerir. (Media Access Layer, MAC). Çakışmayı Önleyici Taşıyıcı Algılamalı Çoklu Erişim (CSMA-CA) sayesinde bir ağ düğümü gönderim yapmadan önce havayı dinler ve başka gönderen yoksa gönderime geçer bu şekilde RF sinyallerin çakışması önlenmiş olur [18]. Ayrıca, IEEE 802.15.4e standardı IEEE 802.15.4'den farklı olarak zaman senkronizasyonu ve kanal atlama özelliği ile daha az güç tekitimi ve daha sağlam bağlantılar kurmayı başarabilmektedir. [18,19]

IPv6 paketlerinin tek seferde gönderilmesi gereken minumum maksimum veri boyu (MTU) 1026 Byte iken IEEE 802.15.4'nin 127 Byte'tır. IETF bu engeli aşmak için RFC 6282 dokümanı ile geliştirdiği sıkıştırma ve parçalı yollama metodları ile IPv6 paketlerinin IEEE 802.15.4 üzerinden yollanabilmesini sağlamıştır. Geliştirilmiş bu metodların yer aldığı ve 6LoWPAN adaptasyon katmanı olarak adlandırabileceğimiz bu katman yine veri taşıma katmanında yer almaktadır. [19]

IEEE ilk iki katmanında cihazın MAC (Media Access Control Address) adresinden türetilen iki farklı adres tipi kullanılır. Bu adreslerden biri 16 bit uzunluğundaki kısa adres, diğeri ise EUI-64 genişletilmiş adrestir. Bu adresler paket başlıklarındaki yükü azaltarak hafıza gereksinimini azaltmaktadır. [19]

Üçüncü katman olan Ağ Katmanı, verilerin adreslendiği ve ağa, gerekirse bir kaç düğüm ötesine yönlendirildiği katmandır. IETF, Routing Over Low Power and Lossy Netorks (ROLL) çalışma grubu RFC 6550 dokümanı ile RPL yönlendirme protokolünü önermiştir. [19]

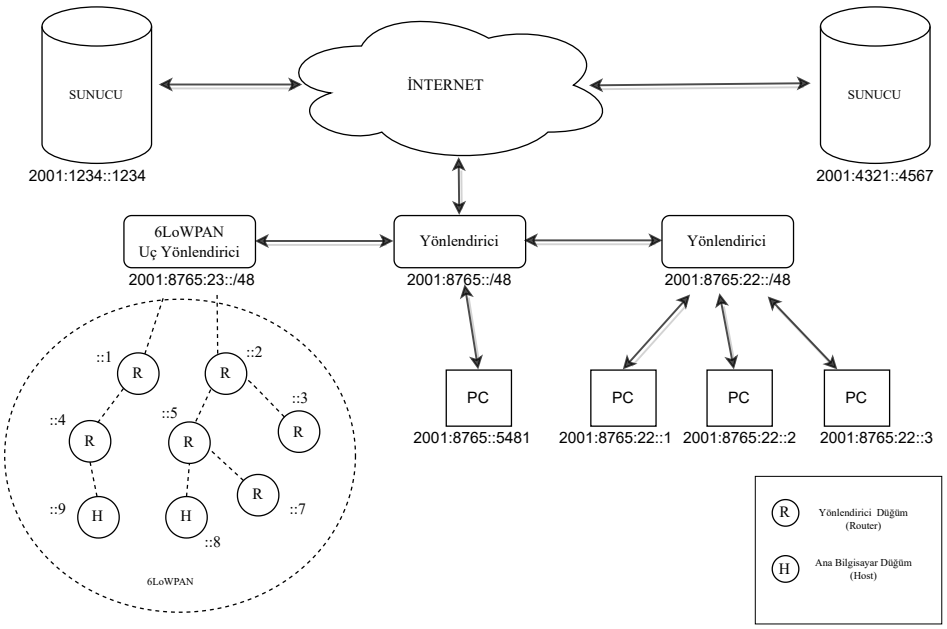
Dördüncü katman olan Taşıma Katmanı, cihazların üstünde koşan uygulamalar için haberleşme oturumların açıldığı katmandır. Bu oturumlar sayesinde aynı cihaz üzerinden birden fazla uygulama kendi haberleşme kanallarını oluşturmuş olur. Bu katmanda internet dünyasında yaygın kullanılan TCP protokolü ve TCP üzerine uygulanabilen TLS güvenlik protokolü kullanılsa bilem TCP'nin onaylı veri yapısından dolayı kullanılabilse de düşük güç tüketimi gerektiren uygulamalar için pek uygun değildir. Bunun yerine; UDP ve UDP ile kullanılabilen DTLS güvenlik protokolü enerji tüketimi için daha uygun bir seçenektir. [19]

Beşinci ve son katmanı ise uygulama verisinin biçimlendirildiği Uygulama Katmanı'dır. İmternet dünyasında yaygın şekilde kullanılan HTTP protokolü 6LoWPAN sistemleri için paket boyu ve enerji verimliliği için çok uygun olmadığından IETF RFC 7252 dokümanında HTTP gibi REST mekanizmasına sahip COAP protokolünü tanımlamıştır. Bunun yanında TCP üzerine koşan MQTT protokolü de 6LoWPAN sisteminde uygulama katmanı protokolü olarak kullanıbilir. [18,19]

Şekil-2.3 ile bir IPv6 ağına dahil olmuş 6LoWPAN ağı örneği verilmiştir.

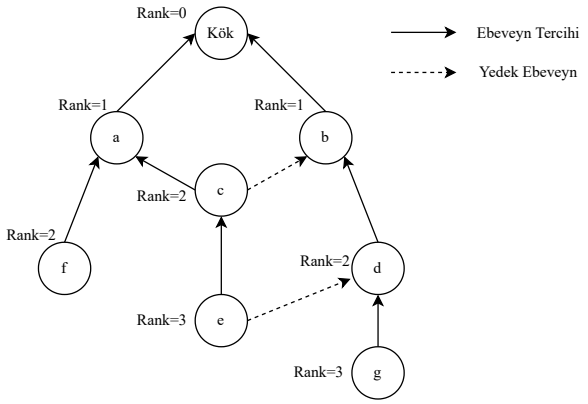
2.3 RPL

Kablosuz kısıtlı IoT uç cihazlarının karşılaştıkları bir başka zorluk ise bulundukları haberleşme ortamının yani ağın kısıtlı ve kayıplı olmasıdır. IETF Yorum İsteği (RFC) standartları Kısıtlı ve Kayıplı Ağı; kısıtlı çok sayıda ağ cihazının kayıplı ve kopabilen bir bağlantı ile birbirleri ile tek veya çok hedefli, çift yönlü iletişim kurduğu, değişken ve düşük paket teslim etme oranına sahip ağlar olarak tanımlamıştır [20]. RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks), düşük güçlü uç cihazların RF bağlantı kayıplarının olduğu bir ortamda (Low-Power and Lossy Networks, LLNs) otomatik şekilde ağ kurabilmesi ve kurulan bu ağda oluşan herhangi bir sorun karşısında yine otomatik şekilde organize olabilmesi için geliştirilmiş bir



Şekil 2.3 : Bir IPv6 ağına dahil olmuş 6LoWPAN ağı

yönlendirme protokolüdür. RPL'lin kurduğu topoloji, birden fazla Yönlendirilmiş Döngüsüz Çizelge'den (DAG) oluşan, kök (root) adı verilen bir noktada sonlanan ve Hedef Bazlı Yönlendirilmiş Döngüsüz Çizelge (DODAG) olarak adlandırılan yönlü ağ çizgeleri ile tanımlanabilir [20] . Daha iyi anlaşılması için DODAG yapısı Şekil2.4'te verilmiştir.



Şekil 2.4 : Hedef Bazlı Yönlendirilmiş Döngüsüz Çizelge (DODAG)

DODAG'ı oluşturan çizelgeler adından da anlaşıldığı üzere döngü oluşturmaz ve DODAG kökü (DODAG root) adı verilen düğümde sonlanırlar. Bir düğümün ağdaki

pozisyonu rank değeri ile belirlenir. Rank değeri DODAG kökünde en düşük değerde olup ağın derinlerine gittikçe düzenli bir şekilde artar. Daha yüksek rank'lı düğümler daha düşük rank'lı düğümlere bağlanarak kendilerine ebeveyn düğümü (preffered parent) seçerler. Rank değerinin hesaplanması ve ebeveyn düğüm seçimi RPL'in kullandığı Objektif Fonksiyon (OF, Objective Function) [21,22] ile belirlenir. Ağ kurulumunun başlatmatılması ve bakımı için RPL protokolünün işletilmesi DODAG kökünün sorumluluğundadır. Bir DODAG'ın bir kökü bulunur ve değeri DODAG kökünün global IPv6 adresi olan DODAGID alanı ile isimlendirilir. DODAG kökü aynı zamanda kablosuz kayıplı ağ ile kablolu veya kablosuz harici ağlar (Örneğin; internet) arasında köprü (Ağ Geçidi) görevini üstlenir. Bu tür senaryoda DODAG kökü 6LoWPAN Köprü Yönlendirici (6LoWPAN Border Routers, 6LBR) adını almaktadır. Bir RPL ağı aynı Objektif Fonksiyon'u kullanan birden fazla DODAG'tan oluşabilir, bu tür ağ yapısına da RPL Instance adı verilir. Bir ağ elamanı aynı anda iki RPL Instance'a hizmet verebilir, ancak bu tür kullanım senaryoları için RFC standardında [20] fazla detaya yer verilmemiştir.

RPL protokolü, ICMPv6 Tip:155 mesajlarının Code alanı ile özelleşen DIS, DIO, DAO, DAO-ACK gibi RPL kontrol mesajları ile sağlanır ve ağın tüm elemanları tarafından kullanılır. Bu kontrol mesajlarının kullanım sıklığı enerji verimliliğini de göz önünde bulunduran RPL protokolünde adaptif şekilde değişmektedir. Bu zamanlamalar Trickle Zamanlayıcısı (Trickle Timer) [23], DAO Gecikme zamanlayıcısı gibi zamanlayıcılar ile yönetilir. Örneğin, ağ kurulumu tamamlandıktan sonra ağ kararlı ise kontrol mesajı yayınlama sıklığı gittikçe azalır. Ağda bir problem algılanırsa (döngü algılanması, paket iletilememesi vb.) bu zamanlayıcılar tetiklenerek hatanın büyüklüğüne göre lokal (local repair) veya global onarım (global repair) mekanizmaları başlatılır.

RPL'in kurduğu ağlarda; çok noktadan bir noktaya (MP2P) , bir noktadan çok noktaya (P2MP) ve bir noktadan bir noktaya (P2P) haberleşme alt yapısı kurulabilmeketedir. MP2P için sadece yukarı yönlü yönlendirme (Upward Routing) yapısı kurulması yeterli iken, P2MP ve P2P haberleşme haberleşme altyapısı için yukarı yönlü yönlendirmenin yanında bir de aşağı yönlü yönlendirme (Downward Routing)

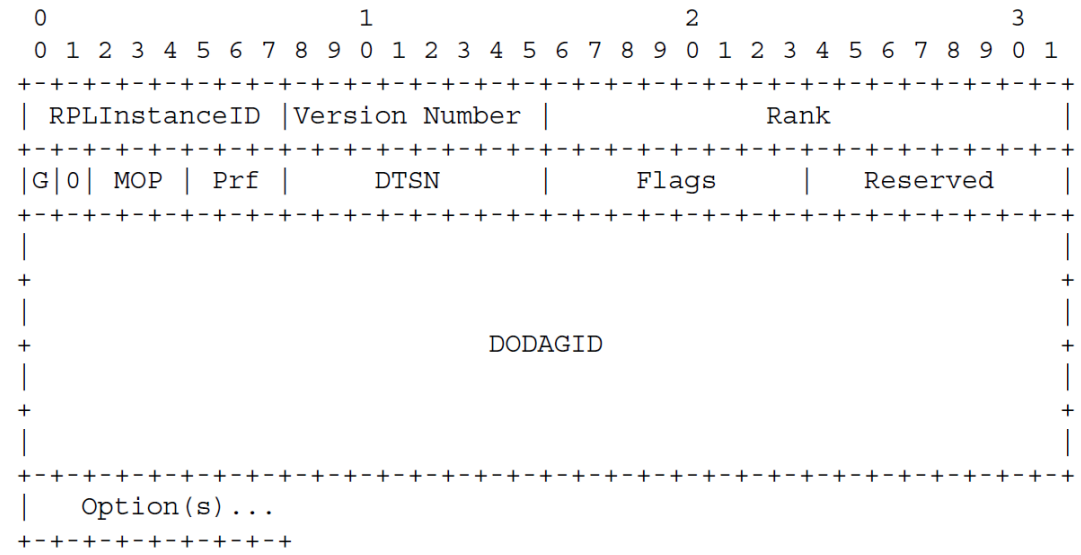
yapısının kurulması gerekmektedir. İlerleyen bölümlerde RPL'in adaptif ve tamir edeci özellikli mekanizmaları daha detaylı açıklanacaktır.

2.3.1 Yukarı yönlü yönlendirme

Tipik bir Kablosuz Algılayıcı Ağında (WSN) ağ cihazlarının ağ geçidi veya kök düğümü (DODAG root) olarak da adlandırılan ortak bir veri havuzuna periyodik olarak veri (örneğin sıcaklık ve nem ölçümleri) göndermesi standart bir kullanım senaryosudur. Bu kullanım senaryosu için 6LoWPAN ağında kurulması ve yukarı yönlü yönlendirme altyapısının kurulması ve idame ettirilmesi yeterlidir. Bu bölümde yukarı yönlü yönlendirme yapısının kurulmasını ve bu yapının kurulmasında kullanılann RPL kontrol mesajlarını inceleyeceğiz.

DIO mesaj yapısı

DIO (DODAG Information Object) ağ kurulurken ihtiyaç duyulan ve ağı tanımlayan bilgilerinin ana kaynağıdır. DIO, ICMPv6 başlık alınında bulunan Code alanı 0x01 olan kontrol mesajıdır. Başlık alanından sonra DIO mesajının gövdesi (Base Object) yer almaktadır. DIO mesajı gövde yapısı Şekil-2.5'te görülebilir.

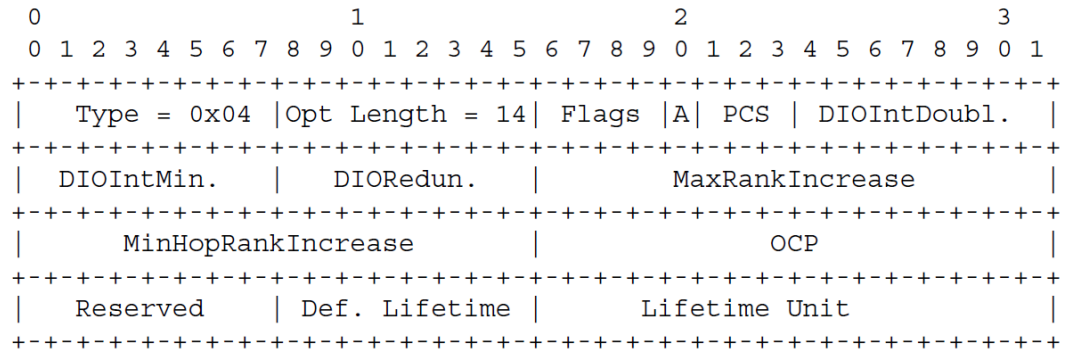


Şekil 2.5 : DIO mesaj yapısı

DIO mesajı daha önce bahettiğimiz şekilde bir DODAG'ı kimliklendiren RPL Instance ID ve DODAGID bilgilerini taşımaktadır. RPL Instance ID'den hemen sonra yerleştirilmiş olan Versiyon Numarası (Version Number) ise DODAG'ın versiyon

numarasını belirtir ve DODAG ilk kurulurken en düşük değeri alır. Bu değer sadece DODAG kökü tarafından daha sonra bahsedeceğimiz global onarım (Global Repair) sırasında arttırılır. Rank değeri ise yine daha önce bahsettiğimiz üzere bir düğümün ağdaki pozisyonunu belirler ve DIO mesajını gönderen düğümün rank değerini belirtir. Bir sonraki alan 'G' bayrağı alanıdır. Bu alan DODAG'ın belirlenmiş olduğu uygulamaya hizmet edip edemediğini bildirir ve sadece DODAG kökü (6LBR) tarafından değiştirilebilir. Eğer bu alanın değeri '0' ise bu ağ akışkandır (floating) ve DODAG kökünün başka bir ağ ile bağlantısı kopmuş demektir. Bir sonraki alan MOP (Mode of Operation) alanıdır ve DODAG'ın sadece yukarı yönlü yönlendirmeyi veya yukarı ve aşağı yönlü yönlendirmenin ikisini de destekleyip desteklemeyeceğini belirleyen alandır. Yukarı yönlü yönlendirmenin detaylarına ilerleyen bölümlerde bahsedilecektir. "Prf" alanı bir RPL Instance içindeki DODAG'ların tercih edilme önceliğini belirtir. Sıradaki alan olan DTSN (Destination Advertisement Trigger Sequence Number) alanı ise aşağı yönlüm yönlendirme prosedüründe mesajın tazeliğini için kullanılan bir alan olup ilerleyen bölümlerde anlatılacaktır. DIO içerisindeki diğer alanlar ise gelecekteki özellikler için rezerve edilmiş olup gönderici düğüm tarafından '0'lar ile doldurulmalı, alıcı düğüm tarafından da göz ardı edilmelidir.

DIO ona eklenen opsiyon mesajları ile kullanılabilir. Bunlardan en temel alanı Tip:4 DODAG Konfigürasyon (DODAG Configuration) Opsiyonu'dur ve içeriği Şekil-2.6'te gösterilmiştir. Bu alan içerisindeki bilgiler DODAG ağı ömrü boyunca sabit olur ve her DIO mesajıyla birlikte gönderilmesine gerek yoktur.



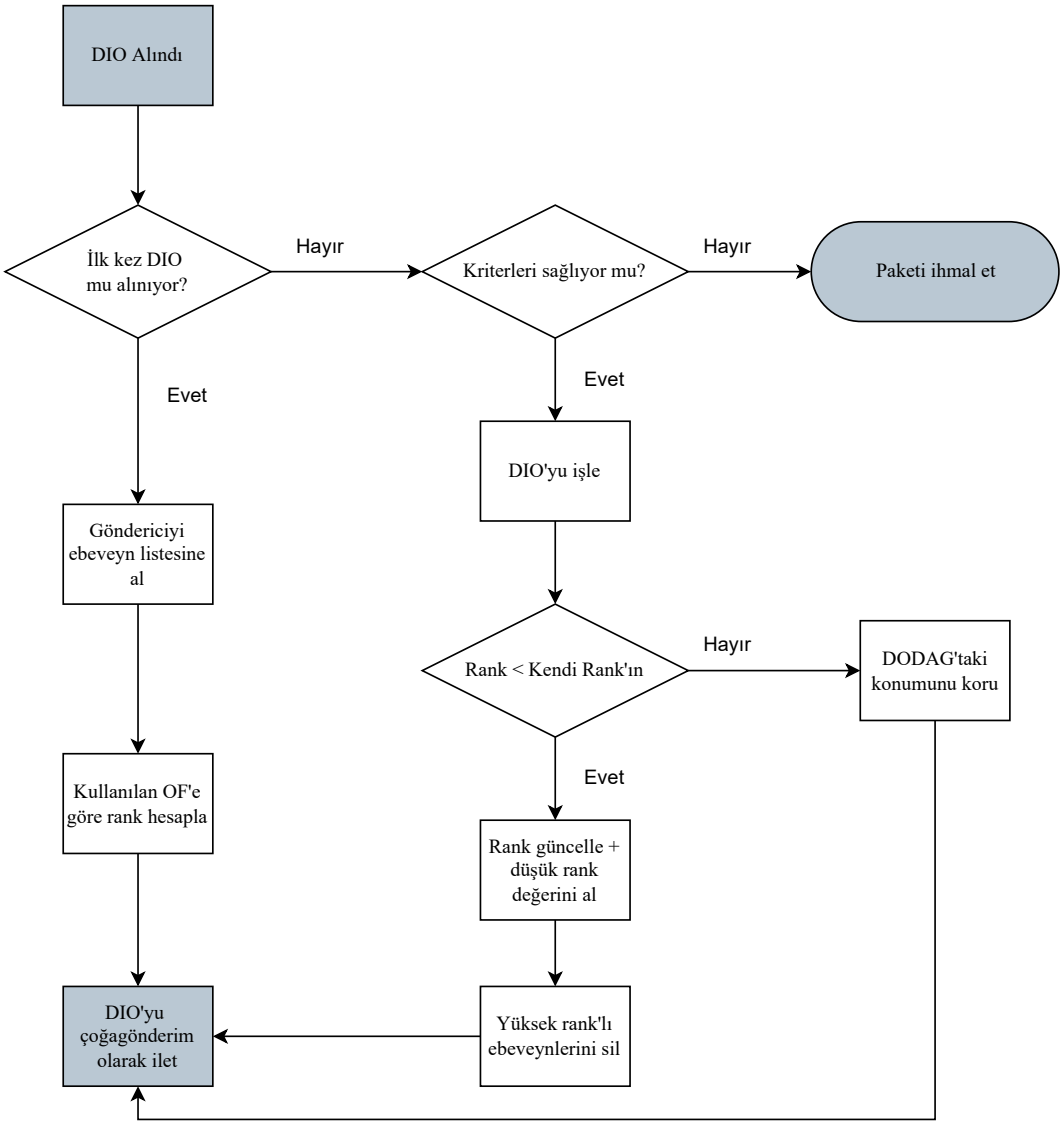
Şekil 2.6 : DODAG Konfigürasyon opsiyonu mesaj yapısı

Tip alanından bir sonraki alan opsiyon uzunluğu alanıdır ve opsiyon mesajının uzunluğunu belirtir. Sıradaki alan gelecek işlevler için rezerve edilmiş bayrakların alanıdır ve tüm bayrak alanına bir fonksiyon atanana dek '0' değeri yerleştirilir. Bir sonraki alan ise bu tez kapsamında konu olacak kimlik doğrulma aktif/aktif değil bayrağıdır. Eğer bu bayrak değeri '1' RPL güvenlik modlarından kimlik doğrulama modu (Authenticated Mode) aktif demektir. Kimlik doğrulama modundan ilerleyen bölümlerde daha detaylı şekilde bahsedilecektir. "DIOIntervalDoublings", "DIOIntervalMin" ve "DIORedundancyConstant"değerleri Trickle zamanlayıcı için gerekli parametreler olup ilerleyen bölümlerde anlatılacaktır. "MaxRankIncrease" alanı lokal onarım (local repair) işlemi sırasında rank değerinin ne kadar artabileceğinin belirten değerdir. "MinHopIncrease" alanı ise düğümün rank değeri ile herhangi bir ebeveyn düğümünün rank değeri arasındaki minimum rank artış değerini vermektedir. Bu değer sayesinde Objektif Fonksiyonu'nun hesapladığı 16 bit genişliğindeki rank değeri tam sayıya çevrilerek düğümün kaçıncı atlama (hop)'ta olduğu belirlenebilir. RPL için birden fazla Objektif Fonksiyonu vardır ve ileride sayıları daha da artabilir. OCP alanı ilgili RPL Instance'da hangi Obejktif Fonksiyonu'n kullanıldığı belirtir. Son olarak; "Default Lifetime" ve "Lifetime Unit" alanları birlikte bir yönlendirmenin ömür süresini saniye cinsinden belirler. Bu süre stabil bir ağda haftaları bulabilir.

Yukarı yönlü topolojinin kurulması

Bir RPL ağında üç tip düğüm vardır. Bunlardan birincisi kapı daha önce de bahsi geçen ve ağgeçidi yönlendiricisi (6LBR) olarak da adlandırılan kök yönlendiricidir. İkinci tip düğüm yönlendircilerdir (router). Üçüncü tip ise konakçı (host) düğümdür. Topoloji kurulumu yönlendiriciler arasında yapılırken, konakçı düğümler sadece kurulan ağa katılıp veri kanalı üzerinden ağı kullanan düğümlerdir. Ağ kurulumu kök düğümün göndermeye başladığı çoğagönderim (multicast) DIO mesajı ile başlar. Bu mesajı alan düğümler Objektif Fonskiyonu'nun belirlediği metrik ve kısıtlamala kurallarına göre rank değerlerini hesaplar ve kendilerine ebeveny düğüm seçerler. Bu düğümler hesaplanan rank değerlerini DIO mesajının içine güncelleyip onlar da güncellenmiş DIO mesajını çoğayayım olarak yayınlarlar. Eğer ağın içindeki bir düğüm belli bir süre DIO mesajını alamamış ise DIS (DODAG Information Solicitation) mesajı yayar. DIS

mesajını alan yönlendirici düğümler Trickle zamanlayıcını resetleyerek karşılık olarak DIO mesajı yayınlarlar. Bu işlem ağın son düğümüne ulaşana dek yayılır. Bu şekilde tüm düğümler kendine bir ebeveyn seçmiş, Hedef Bazlı Yönlendirilmiş Döngüsüz çizelge (DODAG) yapısı kurulmuş ve yukarı yönlü yönlendirme altyapısı kurulmuş olur (Şekil-2.4). Ağın tüm düğümleri bir ebeveyn seçtiği ve DODAGID sayesinde kök düğümün IPv6 adresini bildikleri için veri paketlerini kök düğüme ulaştırabilirler. Düğümler bir veriyi hedef adresi kök düğüm olarak gönderir, her düğüm kendine gelen veri paketini ebeveyn düğümüne iletir bu şekilde kök düğüme ulaşır. Şekil-2.7 [30] düğümlerin DIO mesajnı işleme alma akışını göstermektedir.



Şekil 2.7 : Düğümlerin DIO mesajını işleme alma akışı

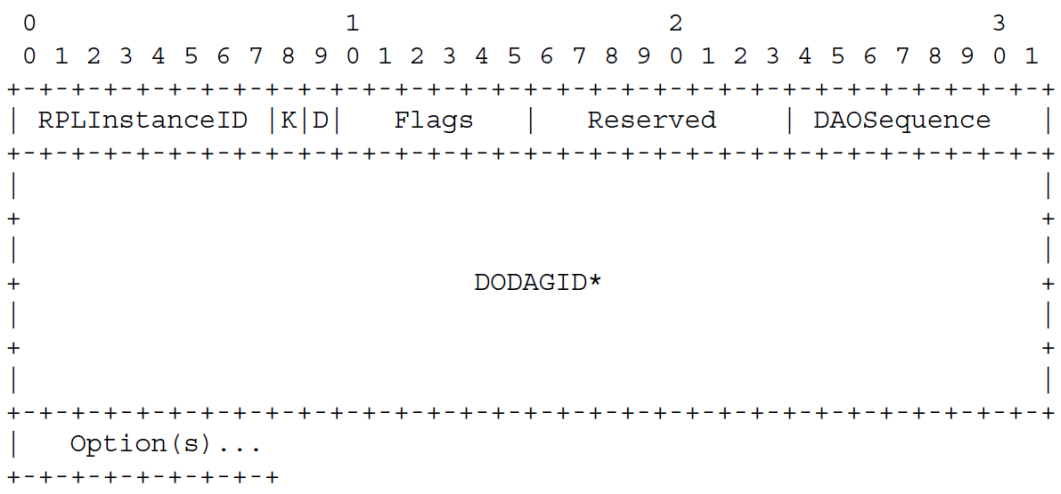
2.3.2 Aşağı yönlü yönlendirme

Aşağı yönlü yönlendirme desteği RPL protokolünün bir diğer önemli özelliğidir. Tek noktadan çok noktaya (P2MP) veri trafiği özelliğinin desteklemesi sayesinde ağ yöneticisinin uç birim cihazlarına ulaşması ve komut göndermesi sağlayabilme imkânı tanımıştır. Bu da büyük alanlara yayılmış ve ulaşılması güç uç birim çevreleri için büyük kolaylık sağlayacaktır. Sistem yöneticisi düğüm için bir parametre yükleme vb. işlem için uç birimin yanına gitmek zorunda kalmayacaktır. RPL standardı P2MP desteği için iki operasyon modu sunmaktadır. Bunlardan birincisi, IPv6 başlık yapısına göre kaynak yönlendirmesi (source routing) [24] yöntemini kullanan, depolama olmayan mod (storing mode)'dur. Bu modda her düğüm kök düğüme ebeveyn düğümlerini bildirir. Kök düğüm ise bu bilgiler ile bir düğüm için gerekli veri yolu haritasını çıkartır. İkincisi ise depolama modu (storing mode)'dur. Bu modda her yönlendirici düğüm, çocuk düğümlerini (child node) içeren bir yönlendirme tablosu tutar. Bu bölümde aşağı yönlü yönlendirme yapısının kurulmasını ve bu yapının kurulmasında kullanılann RPL kontrol mesajlarını inceleyeceğiz.

DAO mesaj yapısı

Destination Advertisement Object (DAO) mesajları, aşağı yönlü yönlendirme bilgisini yaymak için kullanır. DAO, ICMPv6 başlık alınında bulunan Code alanı 0x02 olan kontrol mesajıdır. Başlık alanından sonra DAO mesajının gövdesi (Base Object) yer almaktadır. DAO mesajı gövde yapısı Şekil-2.8'da görülebilir.

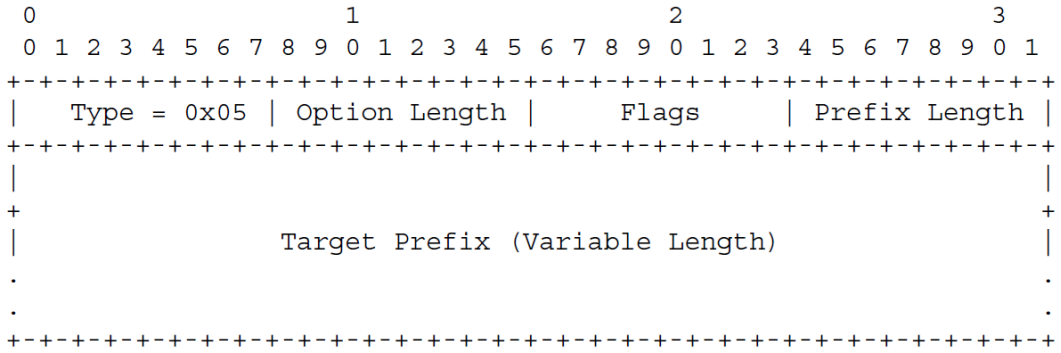
DIO mesajında olduğu gibi RPL Instance ID bilgisi taşınmaktadır. Bu bilgi DIO mesajından öğrenilen değer ile aynıdır. Sıradaki alan sadece ilk iki biti kullanılan bayraklar (flags) alanıdır. İlk bayrak olan 'K' gönderilen DAO mesajına karşılık bir alındı bilgisi mesajı (Code:0x03 DAO–Acknowledgement mesajı) beklenip beklenmediğini belirtir. Sıradaki alan 'D' bayrağıdır. Bu bayrak DAO mesajı içerisinde DODAGID bilgisinin yer alıp almadığını gösterir. Eğer 'D' bayrağının değeri bir ise, DAO gövde nesnesi ile opsiyon alanı arasında DODAGID bilgisi yer almaktadır. Bir düğüm birden fazla Instance'a ait olabileceği için, düğüm aşağı yönlü



Şekil 2.8 : DAO mesaj yapısı

yönlendirme kuracağı Instance'a ait kök düğümün yani DODAGID bilgisini ilgili Instance'ın DIO mesajından öğrendiği şekilde kullanmalıdır. Diğer bayrak bitleri gelecekte kullanılmak üzere rezerve bırakılmıştır ve 0 değeri ile doldurulmalılardır. DAO Dizi (DAO Sequence) alanı her gönderilen DAO mesajı ile artırılan sayaç değeridir. Bu alan DAO mesajının tazeliğinden emin olunmasını ve DAO iletildi bilgisinin takibinde kullanılır.

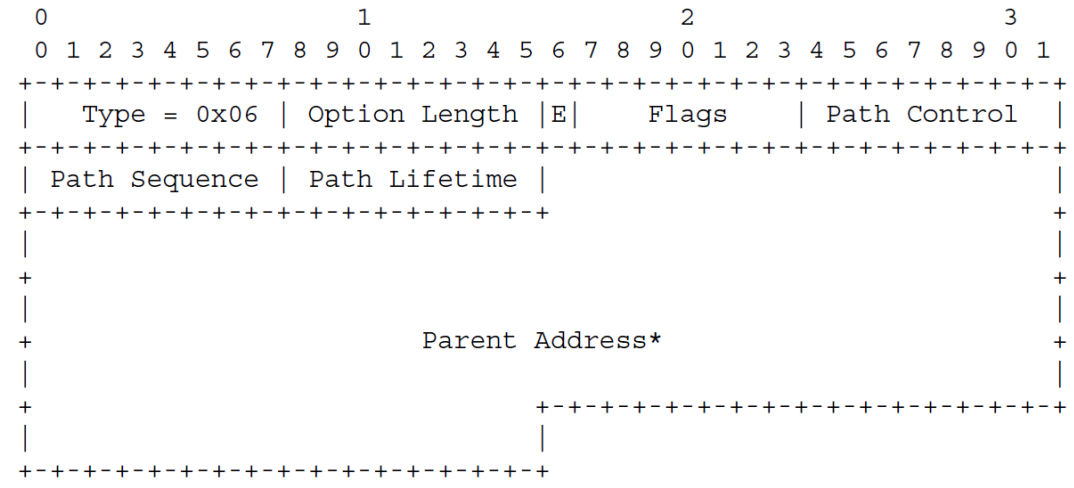
DAO mesajı ona eklenen opsiyonlar ile birlikte kullanılabilir. Bu tez kapsamında RPL Hedef (RPL Target) ve Transit Bilgisi (Transit Information) opsiyonlarını inceleyeceğiz. RPL Hedef opsiyonu, yönlendirme bilgisi olarak IPv6 adres bilgisi, ön ek (prefix) veya çoğa gönderim grup bilgisini içerir. Yönlendirme terminolojisinde bu adresler ulaşılabilirlik bilgisi için kullanılır. Hedef opsiyonu mesaj yapısı Şekil-2.9'de verilmiştir



Şekil 2.9 : RPL Hedef opsiyonu mesaj yapısı

RPL Hedef opsiyonunun ilk alanı Tip alanıdır ve değeri 0x05'tir. Bir sonraki alan ise opsiyon mesajının uzunluğunu belirtir. Bu uzunluk değeri Tip ve Opsiyon uzunluğu alanı haricindeki alanların toplam uzunluğunu verir. Bir sonraki alan ise ön ek uzunluğunu vermektedir. Son alan olan Hedef Ön ek (Target Prefix) alanında, bir düğüme veya tüm bir gruba ulaşılması için gerekli ortak ön en bilgisi yer almaktadır. Bayraklar alanı ise gelecek kullanım için rezervedir.

İkinci opsiyon olan Transit Bilgisi opsiyonunun Tip değeri 0x06'dır. Bu opsiyon bir veya daha fazla hedefe giden yolun niteliklerini belirtmek için kullanılır. Daha açık şekilde ifade etmek gerekirse, bir düğüm bu mesaj ile muhtemel ebeveyn adreslerini, ebeveyni ile ortak ata (ancestor) düğümüne bildirir. Bu sayede ata düğüm bu alanı gönderen düğüm için kaynak yönlendirme haritası oluşturabilir. Bu opsiyon depolama olmayan aşağı yönlendirme konfigürasyonunda kök düğüme yollanır. Depolama modunda ise ebeveyn alanının doldurulmasına gerek yoktur çünkü bu modda Transit Bilgisini her düğüm direk komşu olduğu ebeveynlerine gönderir. Transit Bilgisi opsiyonunun mesaj yapısı Şekil-2.10'de verilmiştir.



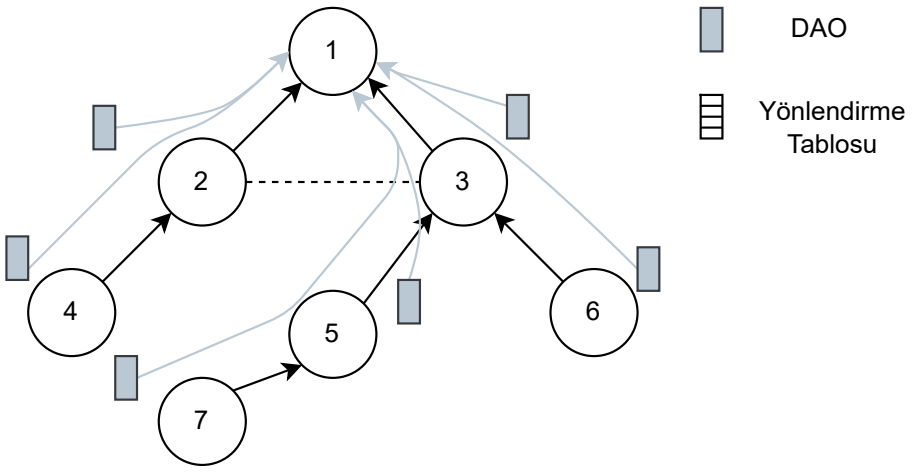
Şekil 2.10 : Transit Bilgisi opsiyonu mesaj yapısı

Tip alanından bir sonraki alan opsiyon uzunluğu alanıdır. Ebeveyn adresi belirtileceği durumlarda bu alan opsiyon mesajının Tip ve kendi alanı haricindeki alanların uzunluk bilgisini belirtmektedir. Sıradaki alan bayraklar alanıdır ve sadece ilk biti olan 'E' bayrağı kullanılmaktadır. Bu bayrak ebeveyn adresi alanında belirtilen ebeveynin RPL ağına mı yoksa harici bir ağa mı ait olduğunu gösterir. Bu bitin değeri 1 ise, ilgili ebeveynin harici bir ağa ait olduğu anlamına gelmektedir. Diğer bayrak alanları ise

gelecek kullanımlar için rezerve edilmiştir. Sıradaki üç alan ise ulaşılabilirlik kontrolü için kullanılmaktadır. İlki, DAO mesajının gönderileceği ebeveyn sayısını kısıtlayan Yol Kontrolü (Path Control) alanıdır. İkincisi, Hedef Opsiyonu alanında güncellenmiş bir bilgi var olup olmadığını belirten Yol Dizisi (Path Sequence) alanıdır. Üçüncü alan ise, hedef ön ekinin (prefix) ne kadar süre geçerli olduğunu belirten Yol Ömür Süresi (Path Lifetime) alnıdır. Ömür Süresi birimi gerçeklemeye dayalı değişebilir.

Depolama olmayan mod (Non-storing mode)

Depolama Olmayan Mod'da her düğüm bir DAO mesajı üretir ve DODAG kökünü gönderir. DAO gönderme sıklığı gerçekleme özelinde değişebilir. Ancak, RPL standardı DAO gönderme sıklığı Rank değeri ile ters orantılı değişecek şekilde olmasını önermiştir. Daha açık ifade etmek gerekirse, DODAG köküne uzak olan düğümler daha sık DAO mesajı gönderirken, yakın olan düğümler daha az sıklıkta DAO mesajı göndereceği anlamına gelmektedir. Ayrıca, her düğüm DAO mesajını, ebeveyn adres alanında ebeveyn IPv6 adresi olacak şekilde Transit Bilgisi opsiyonu ile kullanmak zorundadır. Bir düğümün birden fazla ebeveyni varsa her birini çoklu Transit Bilgisi opsiyonu ile DODAG köküne bildirmelidir. Oluşturulan DAO mesajları Yukarı Yönlü Yönlendirme yolu üzerinden DODAG köküne yollanır. Şekil-2.11 bu süreci göstermektedir.

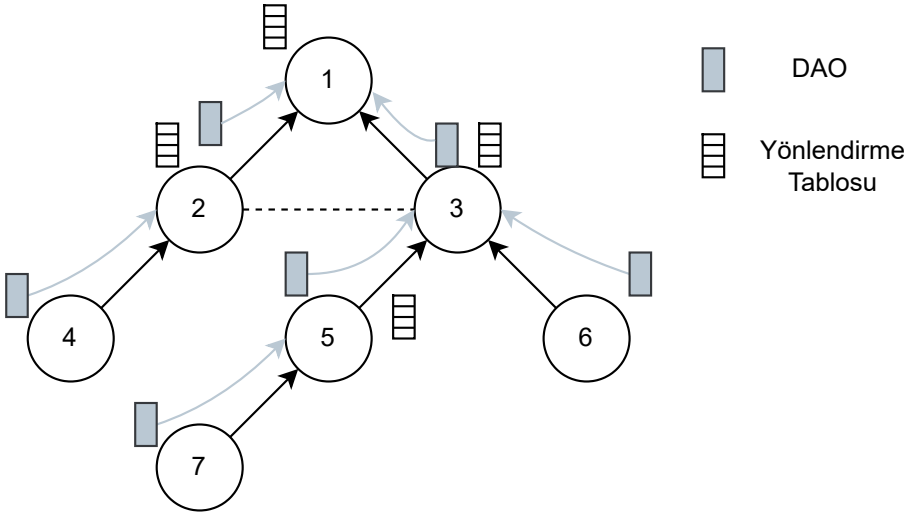


Şekil 2.11 : RPL Depolama Olmayan mod

DAO mesajlarının yukarı yönlü gönderimi sırasında, DAO'nun DODAG köküne ulaşmasına aracılık eden düğümler bu DAO mesajının dizi numarasını gözlemleyerek yönlendirme bilgisinin güncel mi yoksa bir eski mi olduğu bilgisine ulaşabilmektedir. DODAG kökü DAO'lar ile gönderilen yönlendirme bilgilerini kullanarak her bir düğüm için yönlendirme haritası çıkarır. Bu yönlendirme bilgileri IP paketlerinin kaynak yönlendirme (soruce routing) başlık yapısında kullanılır. Bu şekilde aşağı yönlü bir IP veri paketi atlama (hop) limiti 0 oluncaya kadar aşağıya yönlendirilir.

Depolama modu (Storing mode)

Depolama Olmayan Mod'da olduğu gibi Depolama Modu'nda da DAO mesajları kullanılır. DAO zamanlamaları da yine Depolama Olmayan Mod ile aynı mantık ile kullanılabilir. Ancak, Depolama Modu'nda DAO mesajları DODAG köküne değil de düğümün yukarı yönlü yönlendirme sırasında seçtiği ebeveyn düğümüne yollanır. Bu modda her bir ebeveyn düğüm kendi yönlendirme tablosunun tutar. Şekil-2.12 Depolama modunun işleyişini göstermektedir.



Şekil 2.12 : RPL Depolama modu

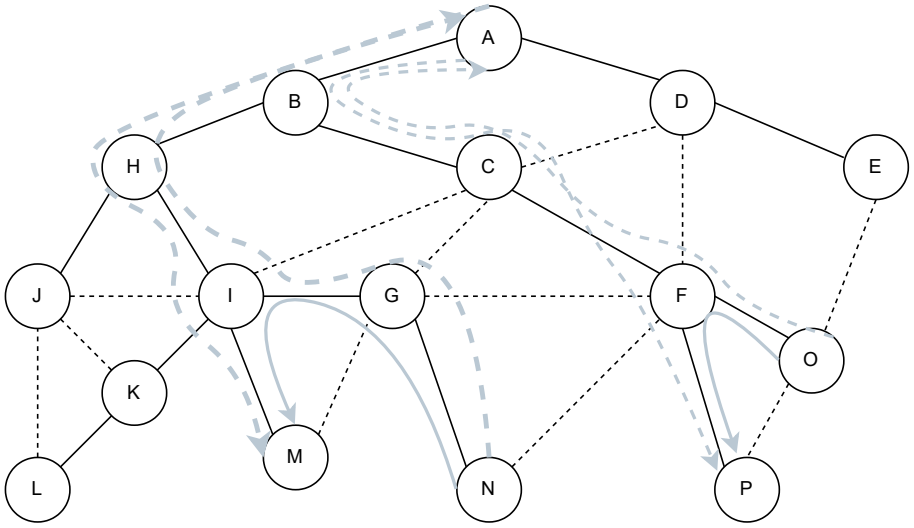
Düğüm DAO mesajını oluşturuken Transit Bilgisi opsiyonunda ebeveyn adresi alanını boş bırakır çünkü zaten ebeveynine yollayacaktır. Ancak, bu düğüm aracılığı ile ulaşılabilecek ön eklerin listesini ebeveyn düğümüne yollaması gerekir; bu işlemi de daha önce tanımlanan Hedef opsiyonu ile yapar. Eğer birden fazla ön ek bildirmesi gerekiyor ise birden fazla Hedef opsiyonundan oluşan DAO mesajı

hazırlamalıdır. DAO mesajlarının gönderme işlemi tamamlandıktan sonra her ebeveynin bir yönlendirme tablosu oluşmuş olacaktır. DODAG kökü üzerinden aşağıya doğru gönderilen bir paket her düğümde tabloya bakılarak aşağıya doğru yönlendirilir, ta ki atlama limiti sıfırlanana kadar.

Depolama Modu DODAG içi bir noktadan bir noktaya (P2P) haberleşmede daha kısa yoldan gidilmesini sağlar ve enerji tasarrufu sağlar. Depolama olmayan modda bir düğümden diğer düğüme atılan tüm paketler ilk önce kök düğüme kadar yukarı yönlü gönderilir. Sonra kök düğüm paketi hedef düğüme düğüme aşağı yönlü paketi yollar. Ancak, depolama modunda kaynak düğümün attığı mesaj, kaynak düğüm ile hedef düğümün ortak ata düğümüne ulaştıktan sonra hedef düğüme yani aşağıya doğru yönlendirilir. Depolama modunun sağladığı bu fayda aşağıdaki Şekil-2.13'de gösterilmiştir. Örneğin, RPL depolama olmayan modda 'O' düğümü 'P' düğümüne bir veri göndereceği zaman bu veri 'F' ve 'C' düğümleri üzerinden ilk önce kök düğüme gönderilecek, kök düğümünde yönlendirme haritasına bakılarak kaynak yönlendirmeli IPv6 başlığı ile 'B','C' ve 'F' düğümleri üzerinden 'P' düğümüne gönderilecektir. Oysaki depolama modunda 'O' düğümü veriyi 'F' düğümüne iletecek, 'F' düğümünde çocuk düğümlerin yönlendirme bilgisi olduğu için paketi kök düğüme yollamadan aşağıya 'P' düğümüne gönderecektir. Açıkça görüldüğü üzere depolama modunda veri yolu çok daha kısaltılarak enerji ve zaman kazancı sağlanmaktadır. Depolama modu bu avantajı sağlasa da büyük ağlarda ebeveyn düğümlerin sakladığı yönlendirme tablosunun büyüklüğü, düğümün hafızasında saklayacağı verinin büyümesi anlamına gelecektir, özellikle DODAG köküne yakın düğümlerde.

2.3.3 Objektif fonksiyonu ve yönlendirme metrikleri

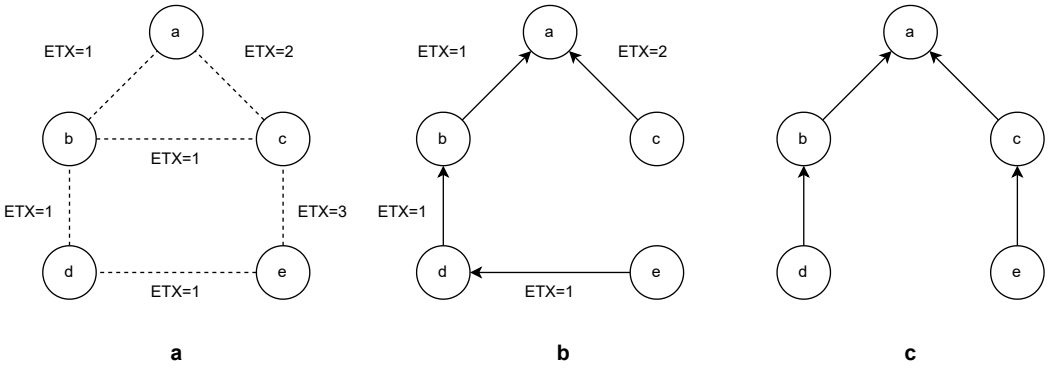
Objektif Fonksiyon'ları (OFs), bir RPL düğümünün yönlendirme yolunun (route path) nasıl optimize edileceğine ve ebeveyn tercihinin nasıl yapılacağına karar verirler. [20] Objektif Fonskiyon'lar bu işlemler için DAO veya DIO mesajıyla beraber kullanılabilen Tip:0x02 "DAG metric container" opsiyon mesajının içerdiği metrik ve kısıt bilgilerini [25] kullanırlar. RFC standartlarının üstünde durduğu iki temel Objektif Fonksiyonu'ndan birincisi olan Objective Function Zero (OF0) [21] atlama sayısı (Hop Count) metriğini kullanırken, ikinci ise Minimum Rank with Hysteresis



Şekil 2.13 : RPL Depolama modunun veri yollarını kısaltmasının gösterimi

Objective Function (MRHOF) [22] Expected Transmission Counts (ETX) metriğini kullanmaktadır.

Atlama sayısı metriği bir düğümün kök düğüme ulaşması için toplam gerekli düğüm atlama sayısı olarak basitçe ifade edilebilir. ETX metriğini ise kısaca, iki komşu arasında link kalitesini çift yönlü paket teslim oranına göre hesaplanmış bir değer olarak ifade edebiliriz. ETX metriğini kullanan düğümler kök düğümüne ETX toplamı en düşük yönlendirme yolundan gitmeyi tercih eder. ETX ve Hop Count metriklerinin kullanıldığı iki farklı Objektif fonksiyonunda ebeveyn seçiminin nasıl yapıldığı Şekil-2.14'te gösterilmiştir.



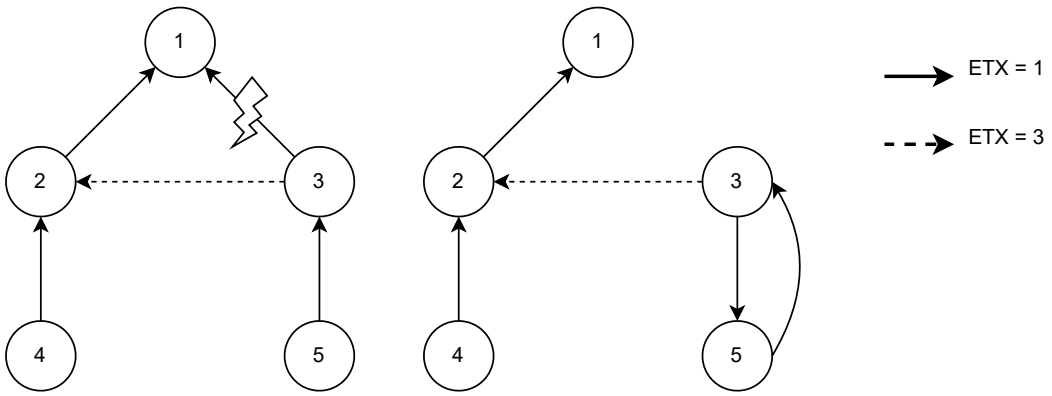
Şekil 2.14 : a) Komşu düğümler arası ETX değeri b) ETX metriği ile ebeveyn seçme (MRHOF) c) Hop Count metriği ile ebeveyn seçme (OF0)

2.3.4 Yönlendirme döngüleri

Yönlendirme döngülerinin oluşumu, her tür ağda yaygın bir sorundur. Bir hata veya hareketlilik (mobility) sebebi ile düğüm kendine yukarı yönlendirme seçeneği (ebeveyn düğüm) olarak yeni bir düğümü seçebilir. Seçtiği bu düğüm ast olan bir düğüm ise döngü oluşabilir. Bu durum ağda karışıklığa, paket kayıplarına, enerji kayıplarına ve paket gecikmelerine sebep olacaktır. Bir yönlendirme döngüsü her zaman bir ağ hatası veya düğüm hareketliği kaynaklı olmayabilir. Örneğin, bir düğümün anteninin yayılımındaki değişkenlik bile bir düğümün kök düğümden uzaklığını değiştirebilir [26]. Bu sebeple, kayıplı ağlar için geliştirilen bir yönlendirme protokolünün bu tür tutarsızlıkları hem algılamalı hem de olmaması için ek mekanizmalara sahip olmalıdır.

Döngüden kaçınma mekanizmaları

DIO mesajları çoğa gönderim ile yayınlanabilen bir mesajdır. Bazı durumlarda daha yüksek rank'a sahip çocuk düğümlerin DIO mesajının işleme alınması istenmeyen yönlendirme döngülerine sebep olabilir. Bu tür bir döngüden kaçınmak için RPL standardının açıkça belirttiği ilk kural, bir düğüm kendi rank'ından daha yüksek rank değeri içeren DIO mesajlarını rank hesabı için kullanmamasıdır. Şekil-2.15'teki [26] örneği inceleyerek bu durumu açıklayabiliriz. Bu ağ yapısı ETX metriğine göre kurulmuş bir ağ olsun. 3 numaralı düğümün bağlantısı düğüm 1 ile kopmuş olsun. Eğer düğüm 3, düğüm 5'i ETX (rank) değeri düğüm 2'nin ETX değerinden düşük diye ebeveyn düğüm olarak seçerse bir döngü oluşacağı açıkça görülmektedir. Bu tür bir durumda düğüm 3 kendini DODAG'tan koparmak için `INFINITE_RANK` değeri ile DIO yaymalıdır. Bu durumda onun çocuk düğümü de `INFINITE_RANK` değeri yayıp ağdan kopacaktır. Düğüm 3 ETX değeri en az olan düğümü ebeveyn olarak tercih edecektir. Ebeveyn seçen düğüm 3 hesapladığı yeni ETX (rank) değerini içeren DIO ile yayınım yapacak, düğüm 5 ise yeniden ebeveyn olarak düğüm 3'ü seçip yeni rank değerini hesaplayacaktır. Bu işlem RPL için lokal onarım (local repair) işlemi olarak adlandırılmaktadır.

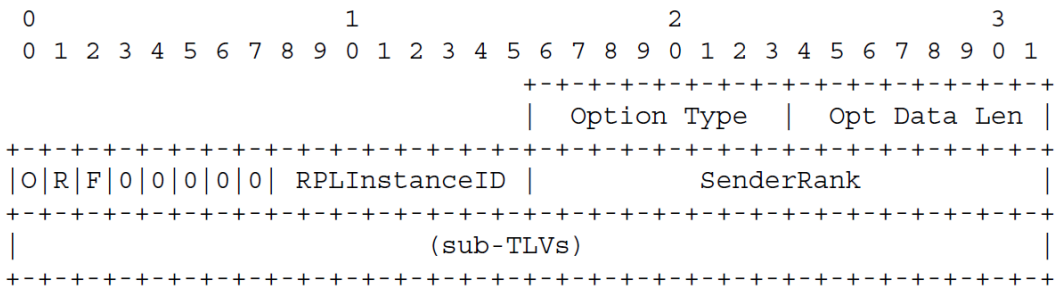


Şekil 2.15 : Bir döngü oluşum senaryosu

İkinci bir kural olarak RPL, bir DODAG versiyonu içerisinde bir düğümün değiştirebileceği rank değerini de sınırlamıştır. Rank değerinin azaltılması bir döngü riski içermese de rank değerinin azaltılması bir döngü riski doğurmaktadır. Bu sebeple RPL rank artışını "RankLowest + RankMaxInc" değeri ile sınırlamıştır. RankLowest değeri bir DODAG versiyonu içerisinde yayınlanabilecek minimum rank değeridir. "RankMaxInc" değeri ise DODAG konfigürasyon opsiyonu mesajı içerisinde yer almaktadır. Lokal onarım sırasında yayınlanan `INFINITE_RANK` bu kuralın dışındadır.

Döngü algılama mekanizması

RPL, döngü olup olmadığını algılamak için standart IPv6 veri paketlerin başlık yapısına ek olarak bulunan RPL Opsiyonu [27] alanındaki bilgileri kullanmaktadır. Bu alan veri paketleri her bir atlama düğümünde güncellenmektedir. RPL Opsiyon mesajı yapısı Şekil-2.16'de sunulmuştur.



Şekil 2.16 : IPv6 Veri paketi başlığı RPL Opsiyon mesajı yapısı

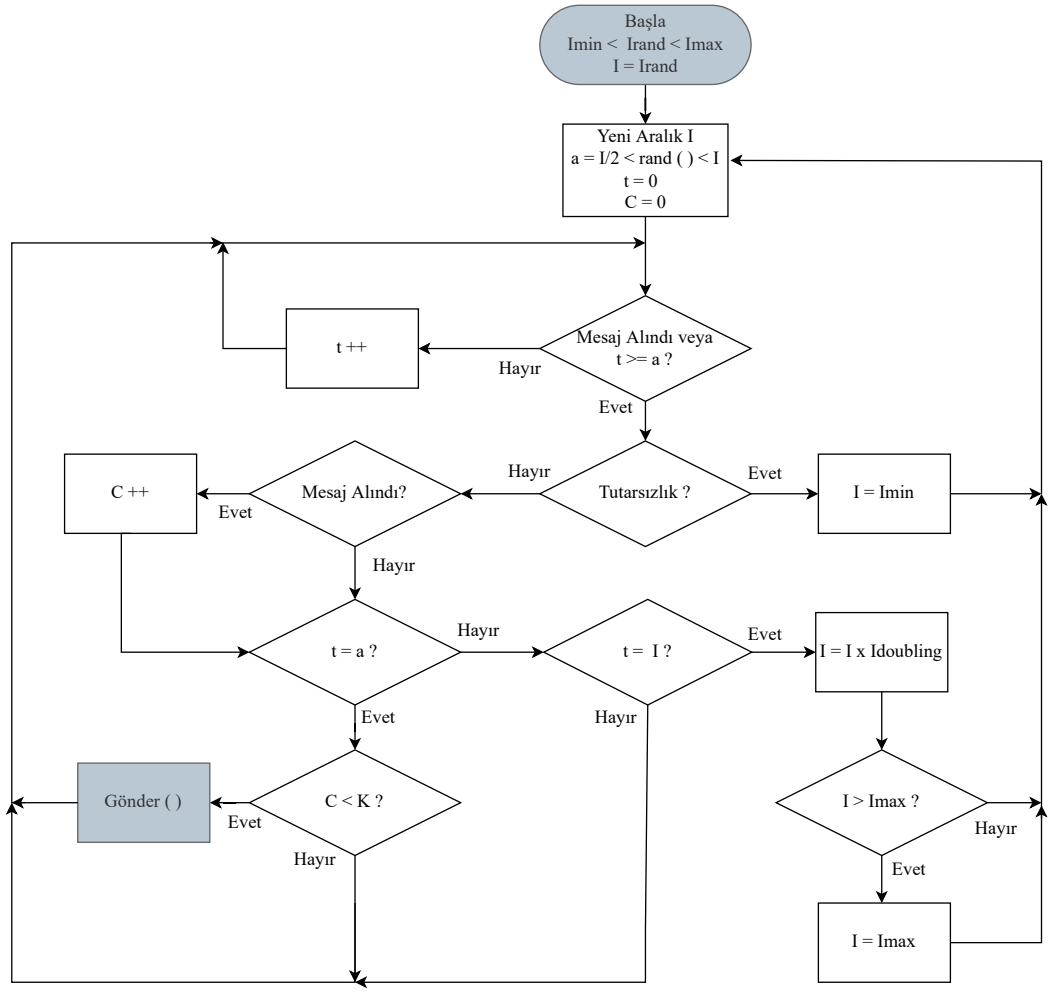
Tip değeri 0x63 olan RPL opsiyonu içindeki bayraklar alanının ilk iki bayrak değeri döngü algılanmasında kullanılır. Bu bayraklardan birincisi, 'O' (Down) bayrağıdır. Bu bayrak ilgili veri paketinin aşağı yönlü mü yoksa yukarı yönlü mü gönderildiğini belirtir. Eğer bu bayrağın değeri 1 ise paket aşağı yönlü gönderilmek istenmiş demektir. Bu bayraklardan ikincisi 'R' (Rank Error) bayrağıdır. Paketin 'O' bayrağından anlaşılan yön, paket içerisindeki gönderici rank değeri ve ilgili paketi alan düğümün rankı arasında bir çelişki döngü var anlamına gelir ve 'R' bayrağı 1 değerine kurularak paket gönderici düğüme geri yollanır. Bu durum tekrarlanır ise lokal onarım işlemi başlatılabilir. Üçüncü bayrak ise yönlendirme hatası (Forwarding Error, F) bayrağıdır. Eğer bir veri paketi için paketin yönlendirileceği hedef düğüm mevcut değil ise bu bayrak 1 değerine kurulur ve paket gönderici düğüme geri yollanır. Gönderici düğüm depolama modunda çalışıyor ise F bayrağı 1'e kurulmuş paketi aldığında ilgili yönlendirme kaydını yönlendirme tablosundan düşürür.

2.3.5 Lokal ve global onarım

Ağ topolojisinin onarılabilmesi bir yönlendirme protokolü için önemli özelliklerden biridir [28]. RPL de bağlantı ve düğüm problemleri oluştuğunda ağ çizelge yapısını onarma mekanizmalarına sahiptir. Bu mekanizmalar iki isim ile anılırlar. Birinci lokal diğeri ise global onarımdır. Lokal onarım, döngü algılandığında ve yönlendirelecek paket için hedef düğüm mevcut olmadığı durumlarda başlatılır. Daha önceki bölümlerde bahsedildiği gibi lokal onarımı başlatan düğüm rank değerini `INFINITE_RANK` (rank alanı tüm bit'lerin 1'e kurulması) değerine çekip DODAG'a ve dolayısıyla çocuk düğümlere olan bağlantısını kopartır. Daha sonra yeniden DODAG'a yeni hesapladığı rank değeri ile yeni ebeveyn seçimi yapar. Lokal onarım ağın sadece bir bölümünü etkiler. Öte yandan evresel onarım ise sadece kök düğüm tarafından başlatırılır ve ağın tüm düğümlerini etkiler. Global onarım kararının hangi durumlarda verileceği standart tarafından net bir şekilde belirtilmemiş gerçekleme özeline bırakılmıştır. Global onarım kararı veren kök düğüm DODAG Versiyon Numarası'nı arttırır, bu durumda kök düğümün komşularından başlayarak DODAG yeni kurulduğunda olduğu gibi yeni DODAG'a katılım prosedürü uygulanır ve ağın uçlarına doğru ilerler.

2.3.6 Zamanlayıcı yönetimi

RPL'in, daha az kısıtlı ortamlar için kullanılan yönlendirme protokollerinin özelliklerinden farklı özelliğe sahip olduğu bir başka mekanizma ise zaman yönetimidir. Özellikle enerji tasarrufu yapması gereken kısıtlı cihazlardan oluşan düşük güçlü ve kayıplı ağlarda (LLNs) kontrol düzlemi mesajlaşmalarının sıklığının sınırlayıcı bir mekanizmasının olması istenen bir özelliktir. Fakat, sıklığın azalması ağ bilgilerinin tezeliğinin de kaybolmasına neden olmamalıdır. RPL protokolünde bu ihtiyacı karşılamak amacı ile kontrol düzlemi mesajlaşmalarının sıklığını adaptif şekilde kontrol eden Trickle Zamanlayıcısı [23] adında bir zamanlayıcı algoritması kullanılmaktadır. Trickle zamanlayıcısı RPL protokolünde en çok kullanılan kontrol mesajı olan DIO'nun sıklığını kontrol etmektedir. Döngü algılanması, bir düğümün ağa yeni katılması ve rank değerindeki değişiklikler Trickle tarafından tutarsızlık olarak yorumlanır ve zamanlayıcı sıfırlanarak DIO mesajı gönderimi yapılır. Eğer Trickle'ın bir periyodu boyunca ağ kararlı ve herhangi bir tutarsızlık yok ise Trickle zamanlayıcısı değerini katlama katsayısı ile çarpılarak arttırılır ta ki periyot maksimum değerine ulaşana kadar. Trickle zamanlayıcısının kullandığı Minimum DIO Aralığı (DIOIntervalMin), DIO Aralık Katlanma Sayısı (DIOIntervalDoublings) ve DIO Yedeklilik Sabiti (DIORedundancyConstant) gibi parametreler daha önce bahsedilen ve DIO ile beraber kullanılan DODAG Konfigürasyon opsiyonu ile taşınmaktadır. Şekil-4.2 [23] Trickle algortimasının akış diyagramını göstermektedir. Son olarak, RPL standardı [20], DAO gecikme zamanlayıcısı (DelayDAO timer), yönlendirme kaydı silme zamanlayıcısı (RemoveTimer) gibi zamanlayıcılardan da çok detay vermeden de olsa bahsetmiştir, ancak bu tez kapsamında bu zamanlayıcıların anlatımına yer verilmeyecektir.



Şekil 2.17 : Trickle zamanlayıcısı algoritmasının akış diyagramı

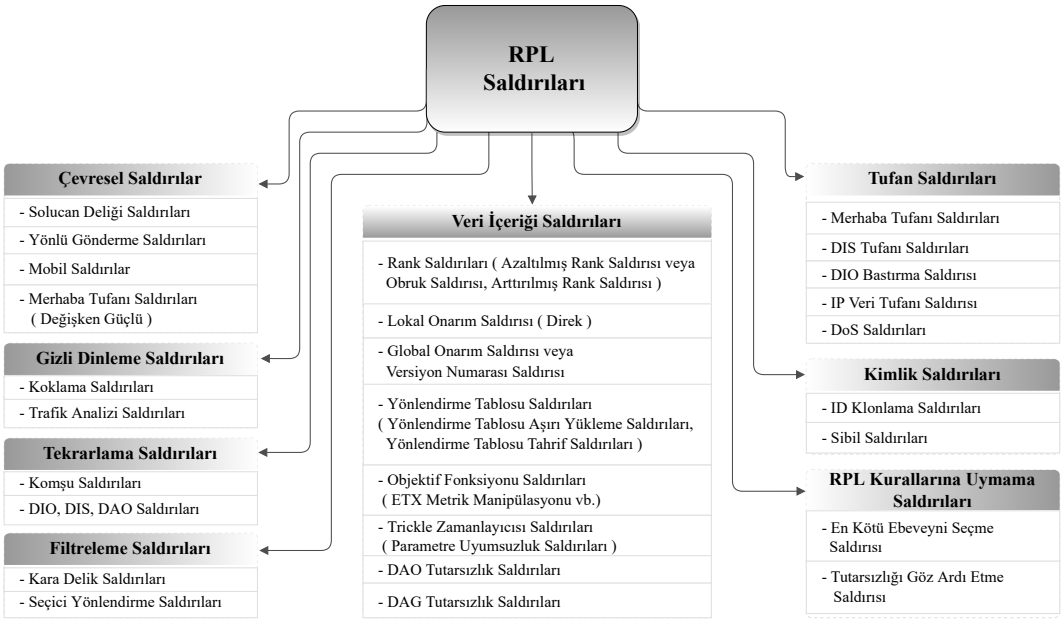
3. RPL GÜVENLİK SALDIRILARI VE ÖNLEMLERİ

3.1 RPL Güvenlik Saldırıları

RPL, Düşük Güçlü ve Kayıplı Ağ'lar (LLNs) için optimize edilmiş, binlerce ağ düğümünü organize edebilen, kendini tamir edebilen ve enerji verimliliği göz önünde bulunduran adaptif bir yönlendirme protokolüdür [20] Ancak, RPL protokolünün hassas mesaj içerikleri ve mekanizmaları , diğer yandan da RPL protokolünü kullanan hafıza, enerji ve işlem gücü bakımından kısıtlı kaynaklara sahip 6LoWPAN ağ cihazları kablosuz paylaşımlı medyaları ile birçok güvenlik tehdidi ve saldırıya karşı kolay etkilenir durumdadır. Yönlendirme protokolünü hedef alıp işleyişini bozan, kısıtlı düğümün kaynağını aşırı tüketen, veri iletim oranını düşüren ve hizmet reddine neden olan tüm saldırılar Düşük Güçlü ve Kayıplı Ağ yönlendirme saldıraları veya RPL saldırıları olarak adlandırılabilir.

Bugüne kadar araştırmacılar birçok RPL saldırısını inceledi ve bunları birkaç farklı şekilde sınıflandırdı. Raoof vd. [31] RPL saldırılarını iki kategoriye ayırdı. Bunlardan birincisi, geleneksel İnternet Ağlarından ve Kablosuz Sensör Ağlarından miras kalan saldırılar, diğeri ise, RPL'e özel saldırılar. Verma vd. [32]'de saldırıların hedeflediği ağ elemanlarına göre bir sınıflandırma önermiştir; kaynaklar, topoloji ve trafik. IETF, yönlendirme saldırılarına ilişkin değerlendirmesini [36]'da sunmuş ve bunları CIA güvenlik ihtiyaçları üzerindeki etkileri açısından kategorize etmiştir; gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability).

Bu tez çalışması, iyi bilinen RPL saldırılarını kapsayacak şekilde birkaç yeni olası saldırı yöntemi de önerecektir. Var olan ve önerilen saldırıların tümü Şekil-3.1 ve Şekil-3.2 ile listelenmiştir. Bu sınıflandırmalar saldırganların yöntemlerine göre yapılmış, kötüye kullanılan hassas RPL mesaj içeriklerine ve mekanizmalarına dikkat çekilmiştir.



Şekil 3.1 : RPL saldırıları

3.1.1 Veri içeriği saldırıları

RPL kullanan ağlarda, ağ topolojisinin oluşturulması ve sonrasında ağın sürdürülmesi RPL kontrol mesajları ve veri paketleri başlıklarına eklenen RPL opsiyonu alanı [27] ile dinamik şekilde yönetilir. Ancak bu değişken mesaj içerikleri ile RPL'in kendi kendini organize etmesi, kendi kendini iyileştirmesi, bu mesaj içeriklerinde kötü niyetli bir değişiklik yapıldığında RPL'in mekanizmalarını kolayca etkileyebilmesine açık hale getirmiştir. Bu içeriklerdeki herhangi bir kötü niyetli değişiklik, fazlalık veya eksiklik, düğümlerin beklenen davranışlarından uzaklaşmasına neden olur. Şekil-3.2 ile Veri İçeriği Saldırıları, kullandıkları hassas veriler ve etkiledikleri mekanizmalar ile sunulmuştur.

Rank saldırıları

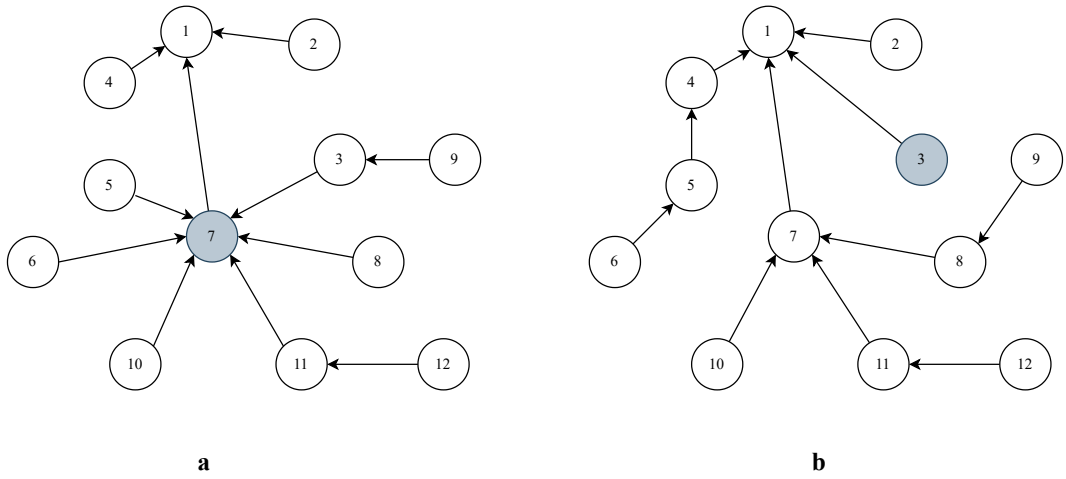
Rank değeri, RPL'in ağ topolojisini oluşturma mekanizması için kilit bir değerdir ve DIO mesaj içeriğinde bulunur. Objektif Fonksiyonu (OF)'nuda belirtilen kurallar ile Rank değeri hesaplanır ve hesaplanan bu rank değerine göre ebeveyn düğümü seçimi yapılır. Yüksek rank değerine sahip düğümler komşusu olduğu düğümler arasında en düşük rank değerine sahip komşusunu ebeveyn olarak seçer. Bir DODAG

Veri İçeriği Saldırıları (Fabrikasyon veya Modifikasyon)			
Saldırı İsmi	**Tetikleyici Mesaj**	**Hassas Veri**	**Etkilenen Mekanizma**
Rank	DIO Baz Objesi	Rank	DODAG Topolojisi Oluşturma
Lokal Onarım	DIO Baz Objesi	Rank	Lokal Onarım
Global Onarım	DIO Baz Objesi	Versiyon Numarası	Global Onarım
Objektif Fonsiyonu	DIO: DAG Metrik Konteynır Opsiyonu	Metrik Verisi (ETX, Atlama Sayısı vb.)	DODAG Topolojisi Oluşturma (OF ile Rank Hesaplanması ve Ebeveyn Seçimi)
Trickle Zamanlayıcısı	DIO: DODAG Kofigürasyon Opsiyonu	DIO Katlanma Çarpanı DIO Yedeklilik Sabiti Minimum DIO Aralığı	Trickle Zamanlayıcısı
Yönlendirme Tablosu	DAO: Transit Bilgisi Opsiyonu veya DAO: RPL Hedef Opsiyonu	Ömür Süresi veya Hedef Ön-eki	Yönlendirme (Yönlendirme Tablosu)
DAO Tutarsızlık	IPv6 Veri Paketi Hop-by-Hop başlığı: RPL Opsiyon Alanı	'F' Bayrağı	DAO Tutarsızlık İyileştirmesi ve Yönlendirme (Yönlendirme Hatası Tespiti ve Yönlendirme Tablosu)
DAG Tutarsızlık	IPv6 Veri Paketi Hop-by-Hop başlığı: RPL Opsiyon Alanı	'O' Bayrağı ve Gönderici Rank'ı Alanı	DAG Tutarsızlık Döngü İyileştirmesi ve Lokal Onarım (Döngü Tespiti)

Şekil 3.2 : Veri İçeriği saldırıları

ağında DODAG kökü en düşük rank değerine sahip olup, DODAG'ın derinlerine gittikçe düğümlerin rank değeri artmaktadır. Eğer bir düğüm rank değerini kötü niyetli bir şekilde düşük yayınlar ise etrafındaki düğümler onu ebeveyn düğümü olarak seçebilir. Bu şekilde topolojiyi bozar ve trafiği aldatıcı bir şekilde kendi üzerine çeker. Bu tür saldırılara Azaltılmış Rank Saldırıları (Decreased Rank) veya Obruk Saldırıları (Sinkhole Attack) denir [31]. Aksine, kötü niyetli bir düğüm rank değerini arttırarak komşularının başka bir yönlendirme yolu bulmasına veya başka bir ebeveyn seçmesine sebep olursa, bu tür saldırılara da Arttırılmış Rank Saldırıları (Increased Rank) denir [31]. Şekil-3.3a ve Şekil-3.3b [31] ile sırasıyla azaltılmış rank değeri saldırısı ve arttırılmış rank saldırı örneği sunulmuştur. Şekil-3.3a'da 7 numaralı düğüm olması gerekenden daha düşük rank değeri yayınladığı için komşu düğümleri tarafından ebeveyn olarak tercih edilmiştir. Bu sayede kötü niyetli düğüm veri trafiğini üstüne alıp verilerin DODAG köküne, DODAG kök düğümünden de diğer düğümlerine ulaşmasına mâni olabilir. Veri filtrelemesi yapmasa bile daha kaliteli bir yol seçecekken düğüm 7'üzerinden yolu seçen düğümlerin kayıplı ortamlarda paketlerinin daha büyük olasılıkla kayba uğrayacağı aşikardır. Şekil-3.3b'de de 3 numaralı düğüm sahip olduğundan daha büyük değerde rank değeri yayınlamasaydı 8 ve 9 numaralı düğümler tarafından ebeveyn olarak seçilecekti. Ancak, 7 numaralı

düğüme bağlanarak belki de daha kayıplı bir yol üzerinden DODAG kök düğümüne ulaşabilecekler.



Şekil 3.3 : a) Azaltılmış Rank saldırısı b) Arttırılmış Rank saldırısı

Objektif fonksiyonu saldırıları

Bir DODAG instance için Objektif Fonksiyonu (OF), Tahmini Gönderim Sayısı (ETX) ve Atlama Sayısı (Hop Count) gibi metrikler kullanarak Rank değerini hesaplamaktadırlar. Bu metrikler ile alakalı parametreler, DAO ve DIO mesajına ek olarak kullanılabilen DODAG Konfigürasyon Opsiyonu mesajı ile taşınırlar. Bu mesaj içeriklerinde yapılacak herhangi değişiklik Objektif Fonksiyonunu yanıltarak Rank değerini yanlış hesaplamasına sebep olacak, bu durum da düğümlerin ağdaki hiyerarşisinin değişmesine yanlış ebeveyn seçimi yapmasına sebep olacaktır. Sonuç olarak Rank saldırıları ile benzer etkileri olacaktır. Verma vd. [32]'de, saldırganların ETX metriklerini manipüle edip düğümlerin komşu düğümlerini yanıltmasını incelemiştir. Bu tür saldırılar diğer OF metriklerini için de yapılabileceği için ismini genelleyerek Objektif Fonksiyonu Saldırıları veya Objektif Fonksiyonu Metrik Saldırıları diyebiliriz.

Versiyon numarası saldırıları

Bu saldırı, sadece DODAG kök düğümü tarafından değiştirilebilen ve DIO mesajları içerisinde taşınan DODAG versiyon numarası değiştirilerek Global Onarım (Global Repair) mekanizmasının gereksiz yere tetiklenmesi ile yapılmaktadır. Normal bir

işleyişte, DODAG kökü sabit bir versiyon numarası ile ağı kurar ve ağ hakkında çok büyük bir problem olmadığı sürece numarasını arttırmaz. Ancak ağda çok büyük bir problem olduğunda versiyon numarasını arttırır ve bu durumda ağın tüm elamanları mevcut ağ ile bağlantısını koparır ve yeni ağa girerken uyguladıkları işlemleri uygularlar. Bu da zaten kısıtlı enerji kaynağına sahip düğümler için yüksek enerji maliyeti demektir. Eğer DODAG versiyon numarası kötü niyetli bir şekilde değiştirilirse ağdaki düğümler mevcut ağı bırakıp Global Onarım mekanizmasına başlarlar [31]. Bu tür saldırılar Versiyon Numarası Saldırıları veya Global Onarım Saldırıları olarak adlandırılar. Versiyon Numarası Saldırıları oluşturdukları etki bakımından en zarar verici Veri İçerik Saldırısı olarak değerlendirilebilir.

Yönlendirme tablosu saldırıları

RPL depolama modunda aşağı yönlü yönlendirme altyapısı oluşturulması için ebeveyn düğümler altındaki düğümlerinin yönlendirme bilgilerini yönlendirme tablolarında tutarlar. Bu tablolar çocuk düğümlerin ebeveyn düğümlerine yolladıkları DAO ve ona eklenmiş DAO opsiyonları; RPL Hedef Opsiyonu mesajı ve Taşıma Opsiyonu mesajları ile oluşturulur [20] Bu mesajların suistimal edilerek kullanılması, bu mesajlara maruz kalan düğümde yanlış veya fazla yönlendirme bilgisi kayıtlarına neden olabilir [31]. Bu yanlış veya eksik kayıtlar aşağı yönlendirilecek veri paketlerinin iletilememesi, döngülerin oluşması gibi etkiler doğuracaktır. Sonrasında RPL iyileştirme mekanizmaları tetikleyecek ve düğümlerin enerjisini harcamasına sebep olacaktır. Bu tür saldırılar Yönlendirme Tablosu Saldırı'ları olarak isimlendirilebilir.

Lokal onarım saldırıları

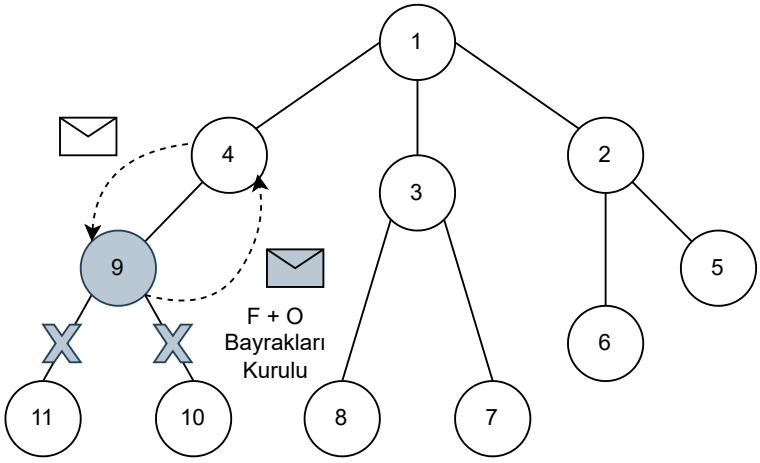
Lokal onarım, RPL'in normal işleyişinde döngü algılanması, ebeveyn düğüme ulaşılamaması, ağ topolojisinde bozulmalar gibi sebepler ile başlatılır. Ancak kötü niyetli bir düğüm DIO mesajının içerisindeki rank değerini `INFINITE_RANK` yapıp yayın yaparak bir lokal onarım süreci başlatabilir. Bu durumda ilgili düğümün alt düğümleri etkilenir ve kontrol sinyalleşmesi sıklığını artırarak başka bir ebeveyn arayışına geçerler. Bu şekilde lüzumsuz yere lokal onarım prosedürü başlatan saldırıları Lokal Onarım Saldırısı olarak adlandırabilir [20,35].

Trickle zamanlayıcısı saldırıları

Trickle zamanlayıcısı, adaptif yapısı ile enerji tüketilmesine sebep olan kontrol düzlemi mesajlaşmalarının sıklığını kontrol eden ve RPL'i diğer yönlendirme protokollerinden ayıran en önemli mekanizmalardan biridir [28]. Trickle zamanlayıcısının kullandığı bazı parametreler DODAG kökü tarafından belirlenir ve DIO mesajı ile birlikte kullanılan DODAG Konfigürasyon opsiyonu mesajı içinde taşınarak diğer düğümlere aktarılır. Yaptığımız araştırmalara göre literatürde bu konuda bir saldırı incelemesi yapılmamıştır. Ancak, [23]'da da belirtildiği gibi; Trickle zamanlayıcısının Yedeklilik Sabiti (Redundancy Constants), Imin, Imax parametrelerinde oluşacak uyuşmazlık düğümler arası dengesiz kontrol mesajı sinyalleşme sıklığına sebep olacaktır. Bu durum da düğümlerin gereksiz yere enerji harcamasına sebep olacaktır. DIO mesaj içeriğinde Trickle zamanlayıcısı parametrelerinde yapılan kötü niyetli saldırıları Trickle zamanlayıcısı saldırıları olarak isimlendirebilir.

DAO tutarsızlık saldırıları

RPL'in normal işleyişinde DAO Tutarsızlığı, düğümlere ulaşan veri paketi başlığında RPL Opsiyonu alanında bulunan F (Forwarding Error) bayrağı ile anlaşılır [20]. Bir düğüme gelen bir pakette F biti 1'e kurulmuş ise, bu veriyi yollayan düğüm paketin yollanacağı yönlendirme yolunu bulamamış anlamına gelmektedir. Bu durumda yönlendirme hatalı kabul edilerek ilgili yönlendirme kaydı yönlendirme tablosundan silinir. Bu tür tutarsızlıklar devam ederse de RPL onarımlarından biri devreye girebilir. Kötü niyetli şekilde bu bayrağın değerinin lüzumsuz yere 1'e kurulması, düğümlerde RPL DAO Tutarsızlığı var izlemini yaratarak düğümlerin yönlendirme tablolarını yanıltır ve belki lokal onarım başlatmasına sebep olur. Bu tür saldırılar DAO Tutarsızlık Saldırıları olarak adlandırılabilir. Şekil-3.4 [31] ile DAO tutarsızlık saldırısına bir örnek sunulmuştur. 9 numaralı düğüm onun aracılığı ile düğüm 10 ve düğüm 11'e yollanan paketleri 'F ' bitini 1'e kurarak 4 numaralı düğüme geri yolladığında. 4 numaralı düğüm 10 ve 11 numaralı düğümleri yönlendirme tablosundan silecektir. Bu şekilde 10 ve 11 numaralı düğümler ulaşılamaz hale gelecektir ancak düğümlerin bu durumdan haberi olmayacaktır.



Şekil 3.4 : DAO Tutarsızlık saldırısı senaryosu

DAG Tutarsızlık saldırıları

DAG tutarsızlığı, DAO tutarsızlığı algılama yönteminde olduğu gibi veri paketleri başlığında bulunan RPL opsiyonu alanında yer alan yön bayrağı ve gönderici Rank bilgileri ile takip edilirek fark edilir [20]. Bu bayrak ve yön bilgisindeki herhangi bir uyuşmazlık, örneğin; yukarı yönlü bir paket düşük rank'a sahip bir düğümden geliyor ise, bu durum DAG tutarsızlığı olarak algılanır. Döngü oluştuğu varsayılarak lokal onarım başlatılabilir. Bu sebeple veri paketi başlığında RPL opsiyonun alanındaki ilgili alanların kötü niyetli şekilde değiştirilmesi gereksiz yere DAG tutarsızlığı algılanmasına sebep olur. Bu tür saldırılar DAG Tutarsızlık Saldırıları olarak adlandırılır [31].

3.1.2 Tufan saldırıları

Mesaj gönderme sıklığını arttırarak yapılan saldırılar ağa zarar vermek için yapılan saldırılardan biridir. RPL ağları özelinde, sıklığı arttırılan bu mesajlar hem RPL kontrol mesajı hem de standart IP veri paketi olabilir. Standard IP veri paketlerinin yollanması düğümlerin diğer paketleri işleyememesine ve hatta servis dışı kalmasına sebep olabilir. Ayrıca fazla ağ trafiği doğurarak gönderme yapan düğümlerin güçlerini tüketebilirler. Kontrol mesajları ile yapılan Tufan saldırıları ise, RPL kontrol mesajlarına maruz kalan düğümde iki farklı şekilde sonuç doğurabilir. Birincisi, sabit bilgi içeren DIO mesajları göndererek Trickle zamanlayıcısı tutarlılık sayacının artmasına ve tutarlılık katsayısından fazla bir değere ulaşmasına sebep

olarak düğümün gönderecek olduğu DIO mesajı bastırılabilir, ikincisi DIS mesajı ile Trickle zamanlayıcısını tetikleyerek maruz kalan düğümün gereksiz sıklıkta DIO kontrol mesajı göndermesine sebep olarak fazla enerji kaybetmesine sebep olabilir. Her iki saldırıda da ağ normal işleyişinden sapmış olacaktır. Bu saldırılar sırası ile DIO Bastırma (DIO Supression) [37] ve DIS Tufanı (DIS Flooding) [32] olarak adlandırılır.

3.1.3 Tekrarlama saldırıları

Kötü niyetli bir saldırgan legal düğümler arasında gelip giden DIO, DAO ve DIS gibi RPL kontrol mesajlarındaki bilgileri direk değiştirmeden kullanabilir. Bu tür saldırılar literatürde Komşu Saldırısı (Neighbor Saldırısı) veya Tekrarlama Saldırısı (Replay Attack) [31] olarak adlandırılmıştır. Tekrarlama saldırının etkileri tekrarlanan mesaj ve mesaj içeriğine bağlı olarak Veri İçerik Saldırıları ile aynı kötü sonuçları doğurur.

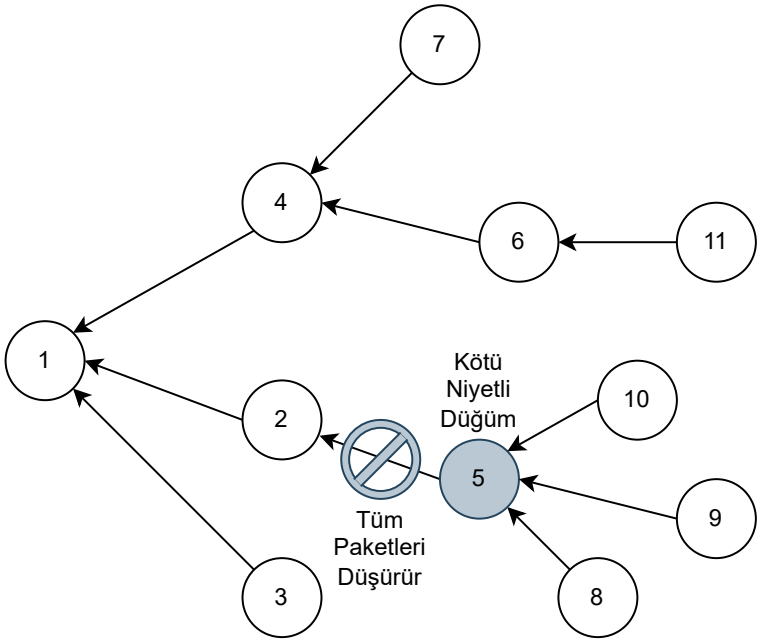
3.1.4 Kimlik saldırıları

Kötü niyetli bir düğüm legal düğümlerin kimliklerini (Global IPv6 adresleri veya Link-Local adreslerini) [36] kullanıp ağ içinde kontrol haberleşmesi yaparak legal düğümleri kandırabilir. Dahası, kötü niyetli düğüm birden fazla legal düğümün kimliğini kullanabilir. Literatürde, tek bir kimlik kullanarak yapılan saldırılar Kimlik Kopyalama (Clone ID) saldırısı olarak adlandırılırken, birden fazla kimliğin kopyalanması yapılan saldırılar Sibil Saldırısı (Sybil Attack) olarak adlandırılmıştır [35]. Kimlik saldırılarının etkisi, saldırı sırasında kullanılan Kontrol mesajı ve içeriğine bağlı olarak Veri İçerik Saldırıları ile aynıdır.

3.1.5 Filtreleme saldırıları

Kötü niyetli bir düğüm üzerinden geçmesi beklenen paketlerin hepsini veya bir kısmını iletmesi gereken düğüme iletmeyebilir. Bu tür saldırılar sırasıyla Kara Delik (Black Hole) ve Seçmeli Yönlendirme (Selective Forwarding) saldırıları [31] olarak adlandırılır. Şekil-3.5 ile Kara Delik saldırısına bir örnek sunulmuştur. 5 Numaralı düğüm kendisi üzerinden 8,9 ve 10 numaralı düğümlere gönderilen ve bu düğümlerin kendisine gönderdiği paketleri düşürerek bu düğümleri ulaşılmaz kılmıştır. 5 numaralı

düğümün RPL kontrol mesajlaşmalarını doğru bir şekilde yerine getirmiş olması onun saldırgan olmadığını ispatlamaya yetmeyecektir.

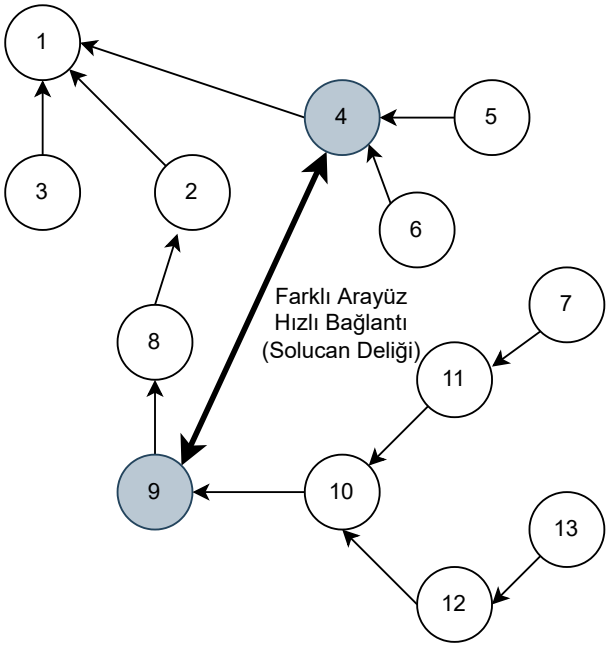


Şekil 3.5 : Kara Delik saldırısı senaryosu

3.1.6 Çevresel saldırılar

Düğümler rank hesaplarını her ne kadar metriklere ve Objektif Fonksiyon'a göre yapsalar da genel beklenti Radyo Frekansı (RF) kalitesi ve DODAG köküne yakınlığı ile orantılı bir rank dağılımı olması [20]. Kayıplı ve düşük güçlü ağlarda sağlıklı bir RF ortam olmaması (asimetrik bağlantılar ve RF girişimler) Objektif Fonksiyonu seçimi ile sağlıklı bir hiyerarşi yaratılmak istenmiştir. Kötü niyetli bir düğüm gönderme gücünü olması gerektiğinden daha az değere veya yüksek bir değere ayarlayarak, komşu düğümlerinin yaptığı metrik hesaplamalarını yanıltabilir. Yine kötü niyetli bir düğüm yönlü bir anten kullanarak gönderdiği paketlerin sadece belirli düğümler tarafından duyulmasını sağlayabilir. Son olarak; sadece kablosuz haberleşme yapması beklenen bir düğüm farklı ara yüzler aracılığı ile iş birliği yaptığı yine kötü niyetli bir düğüme kendi çevresinde edindiği RPL kontrol mesajı trafiği hakkında bilgileri göndererek legal düğümleri kandırma amacıyla kullanmasına yardımcı olabilir. Literatür incelemelerinden yola çıkarak bu tür fiziksel çevrenin ve konumun

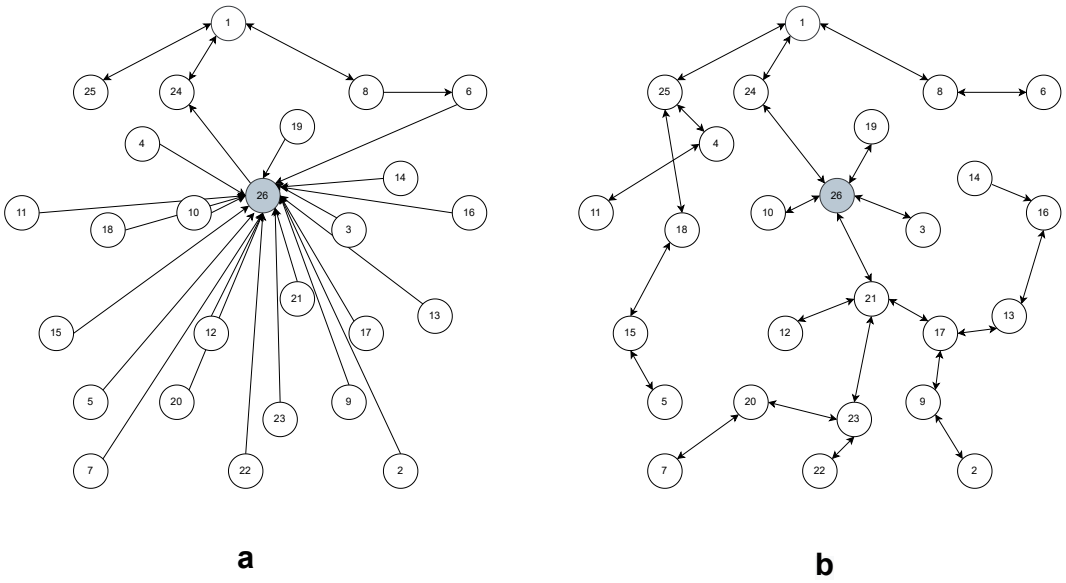
yanıltıcı etkisini kullanan saldırılara, Solucan Deliği Saldırıları (Wormhole Attacks) [31], Hareketli Saldırganlar (Mobile Attackers), ve güç değişimi ile gerçekleştirilen Merhaba Tufanı Saldırıları (Hello Flood) [31] örnek verilebilir. Bu tür saldırılar, bu tez kapsamında Çevresel Saldırılar olarak isimlendirilmiştir. Şekil-3.6 ile [31] Solucan deliği saldırısı için bir örnek sunulmuştur. 9 numaralı ve 4 numaralı kötü niyetli düğümler kendilerine farklı bir ara yüz ile farklı bir veri yolu kurup birbiri ile bilgi casusluğu saldırısı yapmaktadırlar. Şekil-3.7'te [34] ise 26 numaralı düğüm ilk önce güçlü RF yayınım yaparak etrafındaki düğümlerin kendisini ebeveyn düğüm olarak seçmesini sağlamış, sonrasında ise gönderme gücünü kısarak kendine bağlanan çocuk düğüm sayısını azaltmıştır. Bu topoloji değişimleri fazladan RPL kontrol mesajlaşması doğurarak maruz kalan düğümlerin fazla enerji harcamasına sebep olacaktır.



Şekil 3.6 : Solucan Deliği saldırısı senaryosu

3.1.7 Gizli dinleme saldırıları

RPL kontrol mesajları ve standart IP veri paketleri başlığında bulunan RPL Opsiyonu alanı, RPL protokolünün ağ topolojisini oluşturması ve ağın devamlılığını sağlaması için çok değerli bilgiler taşımaktadır [20,33]. Bu bilgilerin elde edilmesi tek başına diğer RPL saldırıları gibi etkili bir saldırı olmasa da bu bilgilerin kötü niyetli



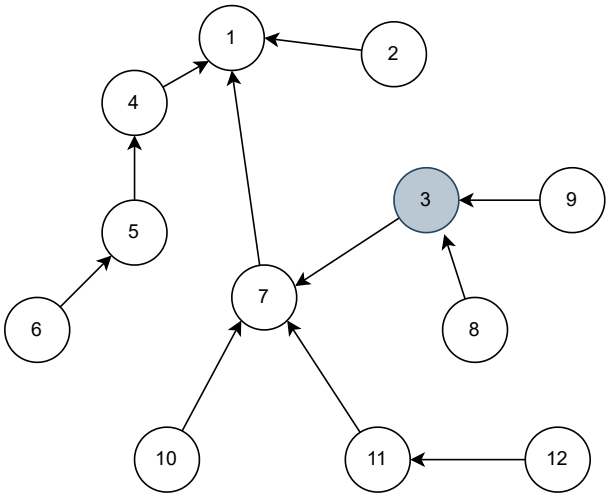
Şekil 3.7 : Gönderme gücü değiştirmesi ile gerçekleştirilen bir Merhaba Tufanı saldırısı senaryosunun gösterimi a) Düğüm yüksek güçte yayınım yapıyor b) Düğüm düşük güçte yayınım yapıyor

şekilde kullanılması RPL'de tanımlanan diğer saldırıların gerçekleştirilmesine sebep olabilir. Aslında bu bilgilerin gizliliği sağlanmış olsaydı, hiçbir RPL saldırısı gerçekleştirilemezdi. Literatürde bu tür saldırılara Trafik Analizi Saldırıları veya Gizli Dinleme Saldırıları olarak ele alınmıştır [33].

3.1.8 RPL kurallarına uymama saldırıları

Kötü niyetli bir node tüm RPL kontrol mesajı sinyalleşmelerini doğru yapabilir ancak, onun kendi içinde yaptığı hesaplamaları, tuttuğu yönlendirme bilgilerini kararları, hangi sinyalleri alıp almadığını kimse bilemez. Bu sebeple, kötü niyetli düğüm tüm sinyalleşmeleri usülüne uygun şekilde yapıp, RPL'in sunduğu ancak diğer düğümler tarafından bilinemeyecek mekanizmalarda uygun olamayan davranışlar sergileyebilir. Örneğin; Raoof vd. [31] ve Verman vd. [32] bu tür bir saldırı olan Kötüyü Ebevey Seçme Saldırısından (Worst Parent Atack) bahsetmiştir. Bu saldırıda saldırgan düğüm, tüm RPL sinyalleşmeleri doğru şekilde yerine getirip ebeveyn adayı komşularından en kötü şartlara sahip olanı kendisine ebeveyn olarak seçmiştir. Bu tür bir seçim paket kayıplarına belki de ileride lokal veya global onarıma sebep olabilir. Bu tez kapsamında, saldırıyı yapan dışındaki düğümlerin bilmesine imkân olmayan saldırı örnekleri çoğaltılabilir örneğin, rank değerini yanlış hesaplayıp yayınlama,

bir tutarsızlık durumunda görmezden gelme gibi... Yine bu tez çalışmasında bu tür saldırılar genelleştirilerek RPL Mekanizmalarına Uymama veya RPL Kurallarına Uymama saldırıları olarak adlandırılmıştır. Şekil-3.8 ile bir Kötü Ebeveyn Seçme saldırısı örneği sunulmuştur. 3 numaralı kötü niyetli düğüm belki 1 veya 2 numaralı düğümü ebeveyn olarak seçebilecekken 7 numaralı düğümü seçerek yukarı ve aşağı yönlü veri yolunu uzatmıştı.Belki bu şekilde paket gecikmelerine veya kayıplarına sebep olacaktır.



Şekil 3.8 : Kötü Ebeveyn Seçme saldırısı senaryosu

3.2 RPL Güvenlik Önlemleri

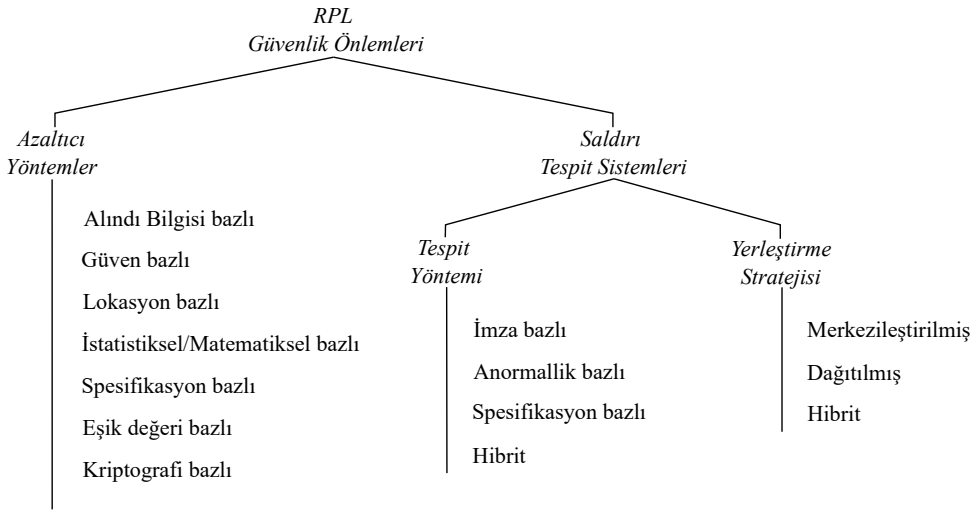
RPL saldırılarını önlemeye veya tespit etmeye yönelik eklenen herhangi bir karşı önlem, büyük olasılıkla, kısıtlı ağ cihazlarının bellek, işlem gücü, enerji ve bant genişliği gibi kaynaklarının RPL'in normal akışında olduğundan daha fazla tüketilmesine sebep olacaktır. Bu nedenle sistem üzerinde konuşlandırılacak yöntemlerin çok dikkatli ve detaylı bir şekilde yönetilmesi gerekmektedir.

RPL saldırılarına karşı önerilen bir güvenlik önlemi;

- Yeterince hafif ve ağın kaynak kısıtlı düğümleri ile uygulanabilir olmalıdır.
- Karşı önlem uygulanmamış haliyle kıyasla uygulama özelinde kabul edilebilir enerji tüketmelidir.

- RPL'in ağ kurulum ve kendi kendini iyileştirme mekanizmalarının sürelerini arttırmamalı veya uygulama özelinde kabul edilebilir bir süre arttırmalıdır.
- Aldığı aksiyonlar ile RPL'in normal işleyişine engel olmamalıdır.
- Saldırıyı tam olarak önlemese de saldırının etkilerinin tüm ağa yayılmasını önleyerek belli bir bölgede sınırlı kalmasını sağlamalıdır [38].

RPL Güvenlik Saldırılarına karşı IETF (Internet Engineering Task Force) RFC dokümanlarında [20] kendi güvenlik modlarını önermesinin yanı sıra araştırmacılar da bu konuya odaklanmış ve birçok yöntem önermiştir [31]–[35]. Önerilen bu yöntemler genel olarak iki kategoriye ayrılabilir. Bunlardan birincisi, RPL'in kendi mekanizması ile iş birliği yaparak onu daha güvenli hale getiren Hafifletici Yönlemler (Mitigation Methods); diğeri ise, ağda saldırı sebebiyle doğan anormallikleri fark ederek saldırıların tespit edilmesini sağlayan ve ikinci bir sistem olarak RPL güvenliğine yardımcı olan Saldırı Tespit Sistemleri (Intrusion Detection System, IDS)'dir. Sınıflandırılmış hafifletici yöntemler ve IDS'ler Şekil-3.9 ile sunulmuştur. Bu sınıflandırmaların metodolojik sınıflandırmalar olduğu ve önerilen bir RPL güvenlik çözümünde bu sınıflandırmadan aynı anda bir veya daha fazla farklı yöntem kullanabileceğini unutulmamalıdır. Öreğin, RPL'in standartlarında önerilen güvenlik çözümleri hem eşik bazlı yöntemler hem de kriptolojik yöntemler içermektedir.



Şekil 3.9 : RPL güvenlik önlemlerinin sınıflandırılması

Bu sınıflandırmalar metodolojik sınıflandırmalar olup, önerilen bir RPL güvenlik çözümünde bu sınıflandırmada yer alan bir veya daha birden fazla azaltıcı yöntem veya hata tespit sistemlerinde kullanılan tespit ve yerleştirme yöntemi aynı anda kullanılmış olabilir. Örneğin, RPL'in standartlarında önerilen güvenlik çözümleri hem eşik bazlı yöntemler hem de kriptoloji bazlı yöntemler içermektedir. Bu bölümde, literatürde yer alan RPL saldırıları için önerilen güvenlik sistemleri, azaltıcı yöntemler sınıflandırması baz alınmış başlıklar altında anlatılacaktır. Sunulan yöntemlerin incelenmesi ile hedeflenen, RPL'e karşı yapılan güvenlik saldırılarına alınan önlemlere daha yöntemsel bakış açısı ile yaklaşıp, yöntemlerin avantaj ve dezavantajlarını analiz ederek RPL saldırıları için daha uygun ve etkin bir güvenlik sistemi önerebilir hale gelmektir.

3.2.1 Alındı bilgisi bazlı yöntemler

Bu yöntemlerin temel mantığı, ağ elemanına bir mesaj atıp buna karşılık alındı bilgisi almaya dayanmaktadır [31]. Alındı bilgisi bazlı yöntemlere çok temel bir örnek olarak [34]'de önerilen Kalp Atışı (Heartbeat) yöntemi verilebilir. Kalp atışı yönteminde kök düğüm her bir düğümü ICMPv6 eko mesajı yollamakta ve alındı bilgisi beklemektedir. Eğer alındı bilgisini yollamayan bir düğüm var ise bu düğüm ya ele geçirilmiş ya da kötü niyetli bir düğüm olarak değerlendirilir. Bu bağlamda, Kalp atışı yöntemi merkezileştirilmiş ve anormallik bazlı hata tespiti yapan bir yöntem de denebilir. Araştırmacılar önerdiği sistemlerini Cooja [56] ile simule ediyor ve yöntemin düğümler üstünde RPL mekanizmasından sadece %10 daha fazla enerji harcamasına sebep olduğunu gösteriyorlar. Bu enerji tüketimi uygulama özelinde belki kabul edilebilir ancak, ICMPv6 mesajlarının kriptosuz şekilde yollanması onları kötü niyetli düğümlerin ayırt edebilmesini sağlıyor. Buna çözüm olalarak yazarlar, önerdikleri yöntemin kriptolu ICMPv6 paketleri ile amacına daha iyi hizmet ederek RPL Filtreleme Saldırıları karşı etkili olabileceğini belirtiyorlar.

3.2.2 Güven bazlı yöntemler

Bu yöntemlerde, düğümler komşu düğümlerini izler, bazı algoritmalar kullanarak onları derecelendirir ve bu derecelendirmelere bağlı olarak onlar ile güven ilişkisi

oluştururlar. Her ne kadar kaplayacağı hafıza alanı büyük ve yoğun ağlarda problem olasa datta bazı uygulamalarda güvendikleri düğümlerden (beyaz liste) [45] veya güvenmedileri düğümlerden (kara liste) [44] oluşan listeler kullanılmaktadır. Ariehrour vd. [46] ile, karadelik ve seçici yönlendirme saldırılarına karşı Güvene-Dayalı RPL ("Trust-Aware RPL") yönlendirme protokolünü geliştirmişlerdir. Sunulan çalışmadaki temel mantık ilk olalarak, kara delik ve seçici yönlendirme yapan saldırganların paket düşürme oranının daha yüksek olduğu bilgisini kullanmaktır. Bu davranış ile düğümlerin davranışları değerlendirilerek bir güven değerine sahip olmaları sağlanmıştır. Sahip olunan bu güvenilirlik dereceleri optimal yönlendirme seçimlerinde kullanılmaktadır. Bu seçimler RPL'in kendi mekanizmasında (OF0 [21], MRHOF [22] gibi) Objektif Fonksiyon'lar ile sağlanmaktadır. Yazarlar önerdiği yöntem ile MRHOF-RPL'in performanslarını karşılaştırarak özellikle saldırı altında kendi yöntemlerinin daha iyi sonuç aldığını göstermişlerdir. Ancak bu yöntemin de bir kaç dezavantajı bulunmaktadır [32]. Bu dezavantajlara örnek olarak; birincisi uygulanan bu yöntemin getirdiği yük ile düğümler daha fazla enerji harcamaktadır. İkinci olarak bazı legal düğümlerin kayıplı ortam sebebi iletemediği paketler o düğümlerin saldırgan olduğu kanısına varılmasına sebep olmasıdır. Aynı yazarlar [47] ile zamana ve güvene dayalı, SecTrust-RPL olarak isimlendirdikleri bir RPL protokolü önermişlerdir. Önerilen bu RPL varyantı ile güvenli bir sistem ile haberleşerek saldırgan düğümlerin tespit edilip izole edilmesini sağlayarak Rank ve sibil saldırılarına karşı azaltıcı bir sonuç elde etmektedir. Önerilen güven mekanizması ile ağda bulunan düğümlerin bir şekilde komşu düğümlerinin güven değerlerini hesaplanması sağlanmıştır. SecTrust-RPL sisteminde 5 adet modül yer almaktadır. Bunlardan birincisi; güven değerlerini hesaplamaktan sorumlu güven değeri hesaplama modülüdür. İkincisi, güven izleme modülüdür. Bu modül düğümlerin güven değerlerini periyodik ve raktif şekilde güncellenmesinden sorumludur. Üçüncüsü, güven değerlerinin sıralanmasından sorumlu güven derecelendirme modülüdür. Dördüncü ise, güven değerlerini yüksek kalitede yönlendirme yollarını seçme ve saldırgan düğümleri tespit etmek için kullanılan modüldür. Beşinci sonuncusu ise, yedekleme ve iyileştirme süreci olarak adlandırılan modüldür. Bu modül fazla korumacı davranan legal düğümleri

enerjisini korumak için veya saldırgan zannedildikleri için RPL üzerindeki etkisinin gereksiz yere azalttığı durumdan çıkarmak için kullanılan bir geribesleme modülüdür. SecTrust-RPL, standart RPL ile kıyaslandığında saldırılara karşı daha etkili olmasına karşılık, fazla enerji tükettikleri için sadece gerek duyulduğu taktirde kullanılması onu daha verimli bir yöntem haline getirecektir [32].

3.2.3 Lokasyon bazlı yöntemler

Lokasyon bazlı yöntemler, düğümleri veya paketleri ağ içindeki konumlarıyla ilişkilendirir. Bu konum ilişkilendirmesi GPS gibi gerçek konum bilgisini kullarak da olabilir, bağlantı katmanından alınacak sinyal gücü değerinden mesafeyi kestirmek de olabilir, veya gönderilen bir paketin geri dönüş süresinden de kestirilebilir [31]. Bu yönteme güzel bir örnek olarak 2003 yılında Kablosuz Sensör Ağlar'ı için önerilen [39] Paket Tasmaları (Packet Leashes) yöntemi gösterilebilir. Bu yöntemde, paketlere eklenen güvenli konum eklentileri ile coğrafi olarak gidebileceği yerler sınırlandırılmaktadır. Ancak bu yöntem için düğümlerde ya donanımsal olarak entegre edilmiş GPS alıcıları ya da çok hassas zamanlayıcılar gerekmektedir.

3.2.4 İstatistiksel ve matematiksel bazlı yöntemler

İstatistiksel ve matematiksel modeller kullanarak saldırılarının tespitinin veya etkisinin azaltılmasının sağlandığı yöntemlerdir. Örneğin; Surendar ve Umamakeswari [40] istatistiksel/matematiksel ve anormallik tespiti bazlı hibrit yerleştirilme içeren Saldırı Tespit ve Müdahale Sistemi (Intrusion Detection and Response System) InDReS'i önermişlerdir. Önerilen sistemde ağ kümelere bölünüyor, her bir kümede olasılıksal bir yöntem ile bir düğüm lider seçiliyor. Bir kümedeki tüm düğümler rank değerlerini o kümedeki lider düğüme yolluyor, lider düğüm de Dempster-Shaffer kanıt teorisini kullanarak saldırganları tespit ve izolasyonunu gerçekleştiriyor. Bu tespitten sonra DODAG kökü saldırganı hariç tutarak yeni bir ağ kuruyor. Bu sistem ilk önce Obruk Saldırı'larını önlemek için geliştiriliyor ancak yazarlar yöntemin geliştirilerek diğer RPL saldırılarına karşı da kullanılabileceğini öne sürüyorlar.

3.2.5 Spesifikasyon bazlı yöntemler

Bu yöntemler, saldırıları tespit etmek için RPL'nin kendi özelliklerini (Rank ve DODAG versiyonu gibi) kullanır. Glissa vd. [41] RPL'in mekanizmalarına birçok eklenti yaparak güvenli RPL (Secure-RPL: SRPL) olarak isimlendirdikleri sistemleri sunmuşlardır. Bu yöntemde değiştirdikleri ilk mekanizma, RPL ağ topolojisinin en temek bileşeni olan Rank değeri güncelleme mekanizması olmuştır. SRPL'de rank arttırımı işlemi için çocuk düğüm sayısını ve düğümün kendi rank değerini göz önünde bulunduran, rank azaltma işlemi için de ebeveyn düğüm sayısını ve düğümün kendi rank değerini göz önünde bulunduran formül uygulanıyor. Böylece rank güncelleme işlemi adaptif bir fonksiyon ile kontrol altında tutulup saldırının ağda bir tutarsızlık yaratmasının önüne geçiliyor. Yazarlar sundukları mekanizmanın Obruk Saldırıları ve Rank Saldırılarına karşı başarılı olduğunu gösteriyorlar ancak yöntemlerini Kara Delik ve Seçici Yönlendirme Saldırıları ile birlikte denerken bir çok düğümün aynı anda ağdan kopması uygulanan yöntemin bazı saldırılar karşısında büyük zarar görebileceğini göstermektedir.

3.2.6 Eşik değeri bazlı yöntemler

Eşik seviyesi mekanizmaları haberleşme sistemlerinde aynı mesaja karşılık verebilecek tepki sayısını kontrol altında tutmak için kullanılan yöntemlerdir. RPL'in çalışma mekanizmasının mesaj ve mesajlara verilen tepki sıklığını Trickle algoritması sağlamaktadır. Standartlar , Trickle zamanlayıcısı algoritmasında [23] zaten var olan yedeklilik katsayısını ('C') bir eşik değeri olarak kullanmakta, hem de yine Trickle zamanlayıcısının kullandığı "Tutarsızlık" terimini değerlendirmede benzer bir mekanizmanın eklenmesini önermekte ve sunmaktadır [20]. Bu mekanizmalar, istenen ağ performansını korurken savunma davranışı açısından daha sağlam hale getirirler [32]. Örneğin; [42]'te RPL DODAG tutarsızlık saldırıları için Adaptif Eşik Değeri (Adaptive Threshold AT) adında bir mekanizma geliştirmişlerdir. Bu çözümde değerini her IPv6 veri başlığındaki 'O' (yön bayrağı) ve 'R' (Rank hatası) bayrağı kurulu olduğunda 1 arttıran ve limit değeri 20'ye sabit olarak kurulan bir eşik seviyesi değeri bulunmaktadır. Bu değer 20'yi geçtikten sonra gelen tüm paketler

ihmal edilmektedir. Sonra, bu değer her saatte bir yenilenmektedir. Ancak bu mekanizmayı bilen saldırganlar bunu fırsata çevirip 20 kez tutarsız mesaj attıktan sonra, düğümün diğer gerekli RPL kontrol mesajlarını da almasına engel olabilir veya farklı paket sıklıkları ile yine enerji tüketici bir saldırıda bulunabilirler. Mayzaud vd. ise [43] ile adaptif eşik değeri mekanizmasında geliştirmeler yaparak Dinamik Eşik Değeri mekanizmasını önermişlerdir. Sunulan eşik seviyesi mekanizması tamamen otomatik olup RPL ağının dinamik karakterini hesaba katıp DODAG tutarsızlık saldırılarına karşı etkili olmayı hedeflemiştir. Dinamik eşik seviyesi yönteminde ek olarak bir ön hesaplamaya ihtiyaç doğmadan tüm gerekli bilgileri ağın karakteristiğinden elde etmektedir. Örneğin, ağ kurulum süresini ölçüp kullanmaktadır. Yazarlar kurdukları güvenlik sisteminde trickle zamanlayıcısının gereksiz gördükleri resetlenme koşullarını azaltıp fazla DIO gönderiminin önüne geçmişlerdir. Son olarak yazarlar araştırmasında, önerdikleri yöntemin adaptif eşik seviyesi yöntemine kıyasla, enerji tüketimi, paket teslim oranı ve uçtan-uca gecikme metrikleri açısından daha etkin bir yöntemlerinin olduğunu göstermişlerdir.

3.2.7 Kriptografi bazlı yöntemler

Özet fonksiyon, Mesaj Doğrulama Kodu (MAC), sayısal imza, mesaj kriptolama gibi simetrik veya asimetrik kriptolojik fonksiyon veya yöntemlerin en az birini bulunduran, RPL saldırılarını engelleyen veya tespit eden sistemler Kriptografi bazlı yöntemler olarak sınıflandırılabilir. Geleneksel kriptografi algoritmaları ve yöntemleri yüksek seviye koruma sağlasa da kapladıkları kod hafıza büyüklüğü, harcadıkları CPU döngü sayısı ve enerji ile birçok araştırmacı için kısıtlı cihazlara uygulanılmasından uzak durulan yöntemler olmuştur [32,33]. Aksine, bu bölümde, RPL'i saldırılara karşı korumak için kriptoloji bazlı yöntemler kullanan bir çok çalışmadan bahsedilecektir.

Versiyon Numarası ve Rank Doğrulması (Version Number and Rank Authentication) [48] kısaca VeRA, RPL protokolünde ağın en önemli iki parametresi sayılabilecek Versiyon Numarası ve Rank değerinde olabilecek gayri meşru değişimleri engellemek amacı ile geliştirilmiştir. Önerilen yöntemdeki ana mantık, rank ve versiyon numarası değişimlerini özet fonksiyon zinciri mekanizması ile korunmasıdır. VeRA, küçük zaman birimlerinin karmaşıklığını içeren özet fonksiyonu işlemlerine dayanan bir

kimlik doğrulama mekanizmasıdır. VeRA'nın en büyük dezavantajı, rank sahteciliği ve tekrarlama saldırıları ile baypas edilebilmesidir. [49]'de ise yazarlar ilk olarak VeRA'nın güvenlik birkaç açığını bulup geliştirmişlerdir. Ayrıca TRAIL (Trust Anchor Interconnection Loop) isminde bir ağ topolojisi doğrulama yöntemi önermişlerdir. TRAIL'de, her bir düğüm yukarı yönlü kök düğüme doğru yönlendirme yolunu doğrulayarak rank sahteciliği olup olmadığını tespit eder ve kötü niyetli düğümlerin ağ topolojisinden izole edilmesini sağlar. Hem VeRA hem de TRAIL kaynak kısıtlı düğümlerde gerçeklenmesi için fazla hafıza alanı harcayan yöntemler olarak görülmektedir [32].

[37]'de yazarlar, RPL standardında [20] yer alan RPL ön yüklemeli anahtar güvenlik modunu yine standartta yer alan tekrarlama koruma mekanizmasını da içerecek şekilde implemente etmişlerdir. Bu çalışmada, güvenlik modu uygulanmamış hali ile RPL(1) , sadece güvenlik modu eklenmiş RPL (2) ve hem güvenlik modu hem de tekrarlama korumasını içeren RPL (3) olmak üzere üç tip RPL gerçeklemesi, düğümlerin güç harcaması, RPL kontrol sinyalleşmesi yükü, ağ kurulum süresi metirkleri açısından Cooja [56] simülatörü kullanılarak analiz edilmiştir. Analiz sonuçları incelendiğinde sadece ön yüklemeli anahtar güvenliği eklenen RPL, güvenli mod gerçeklenmemiş RPL ile arasında bahsi geçen metrikler açısından çok da fazla yük yaratmadığını göstermiştir. Ancak, tekrarlama koruma mekanizmasının sahip olduğu sinyalleşme mesajları RPL üzerine oldukça fazlaca yük bindirmiştir. Bu çalışmada [37] güvenli mod RPL saldırı altında incelenmemiş olup, [54]'de güvenli mod RPL'i yaygın dört tip saldırı altında incelemişleridir. Ek olarak, düğümlerin anahtarları bir şekilde ele geçirildiğinde ön yüklemeli RPL güvenlik modu etkisiz olacağı aşikardır. Bu dezavantajı yenmek için ön yüklemeli RPL güvenlik moduna bir anahtar dağıtım yöntemi uygulamak RPL'in güvenlik mekanizmasını daha etkili hale getirecektir.

[52]'de yazarlar, düğümler arasında güven oluşturmak ve güvenli bir anahtar değişimi sağlamak için Güvenilir Platform Modülü (Trusted Platform Module) kullanan bir Güvenli Hesaplama Mimarisi (TCA: Trusted Computing Architecture) önermiştir. Çalışmada, bu amaçla, düğümler ile işbirliği yapabilecek düşük maliyetli bir TPM geliştirmesi üzerinde durulmuştur. Önerilen mimari düğümleri, kurcalama, hizmet reddi ve yönlendirme saldırılarına karşı koruma sağlamaktadır. TPM'ler sunulan

mimaride, kimliği doğrulanmış düğümler için anahtar sağladığı için önemli bir rol oynamaktadır. Ancak TPM bu mimaride tek hata noktası olduğundan, TPM'in kurcalanması veya bozulması ağ performansının düşmesine ve güvenlik açıklarına sebep olacaktır [32]. [53]'da ise araştırmacılar, Eliptik Eğri Kriptolojisi (ECC), özet fonksiyon ve önden paylaşımlı kripto anahtarları içeren bir grup anahtarı dağıtım şeması önermişlerdir. Bu yöntem grup anahtarının sahip olması gereken ileriye dönük ve geriye dönük gizlilik [55] özelliğini sağlayan, çoğa gönderim ile anahtar dağıtımı yapan, anahtar yenileme mekanizması bulunan bir anahtar dağıtım şemasını içermektedir. Önerilen şema Contiki işletim sisteminde [56] gerçeklenmiş ve Cooja [56] simülatörü kullanılarak analiz edilmiştir. Bu yöntemde, düğüm başına düşen enerji tüketimi kabul edilir bir seviyede olsa da çoğa gönderim olarak anahtar dağıtımı mesajının ağdaki düğüm sayısı ile artması hafıza kısıtı bulunan düğümler için sorun teşkil etmektedir. Anahtar dağıtımını konu almış bir çalışma da [51] ile sunulmuştur. Bu yöntemde ağa katılmak isteyen yeni düğüm komşu düğümüne kriptosuz mesaj atarak ağa katılma isteğini kök düğüme ulaştırmaktadır. İstekte bulunan düğüm legal bir düğüm ise kök düğüm bu düğüm için kriptolu anahtar mesajını aşağı yönlü komşu düğüm üzerinden istekte bulunan düğüme ulaştırır. Eğer düğüm bu anahtar dağıtım mesajını açabilir ise ağ anahtarına sahip olmuş olur ve üzerinden anahtar istediği komşu düğüme bu anahtarla kapatılmış bir mesaj atarak komşusuna kimliğini doğruladığını ilan eder. [50] ile iki aşamalı kimlik doğrulamaya sahip bir protocol ile düğümlere kimlik doğrulamalı bir anahtar dağıtım şeması önerilmiştir. Ancak bu yöntemde düğümlerin hafızasında birbirlerinin genel anahtarlarını ve kimliklerinin özet fonksiyon çıktılarını tutmaları ve iki aşamalı kimlik doğrulamanın sahip olduğu sinyalleşme yükünün büyük ağlarda enerji ve hafıza kısıtı bakımından problem yaratması muhtemel gözükmektedir.

3.3 RPL Standardı Güvenlik Özellikleri

RPL güvenliği sadece ağ katmanında uygulanan güvenlik yöntemleri ile kısıtlı değildir. 6LoWPAN standartlaşmış protokol yığını ağ katmanından daha alt katman olan veri bağlantı katmanında bir güvenlik önlemi alınmasına da imkân tanımaktadır. Veri bağlantı katmanı (IEEE 802.15.4 MAC) simetrik anahtar kriptoloji teknikleri ile 8

farklı güvenlik moduna sahiptir [2B]. Bu katmanda güvenlik koruması etkin ise RPL katmanına özel bir güvenlik önlemi alınmasına gerek kalmayabilir [20,34]. Çünkü veri bağlantı katmanında güvenli mod etkinleştirilmiş ise RPL (ağ) katman başlıkları ve mesaj yükünü de kapsayacak şekilde daha üst katmanlar da kriptolu olacaktır [34]. 6LoWPAN standartlaşmş protokol yığını için IEEE 802.15.4 MAC veri bağlantı katmanının güvenlik modu iplementasyonu ve değerlendirilmesi [57]'deki araştırmacılar tarafından yapılmıştır.

Veri bağlantı katmanının yanında, RPL'in (ağ katmanında) kendine ait üç farklı güvenlik modu vardır [20].

1. **Güvenli olmayan mod (unsecured):** RPL'in varsayılan güvenlik modudur. Bu modda güvenlik için herhangi bir mekanizma uygulanmamakla birlikte, RPL'in güvenliği veri bağlantı katmanında alınan güvenlik önlemine bağlıdır.

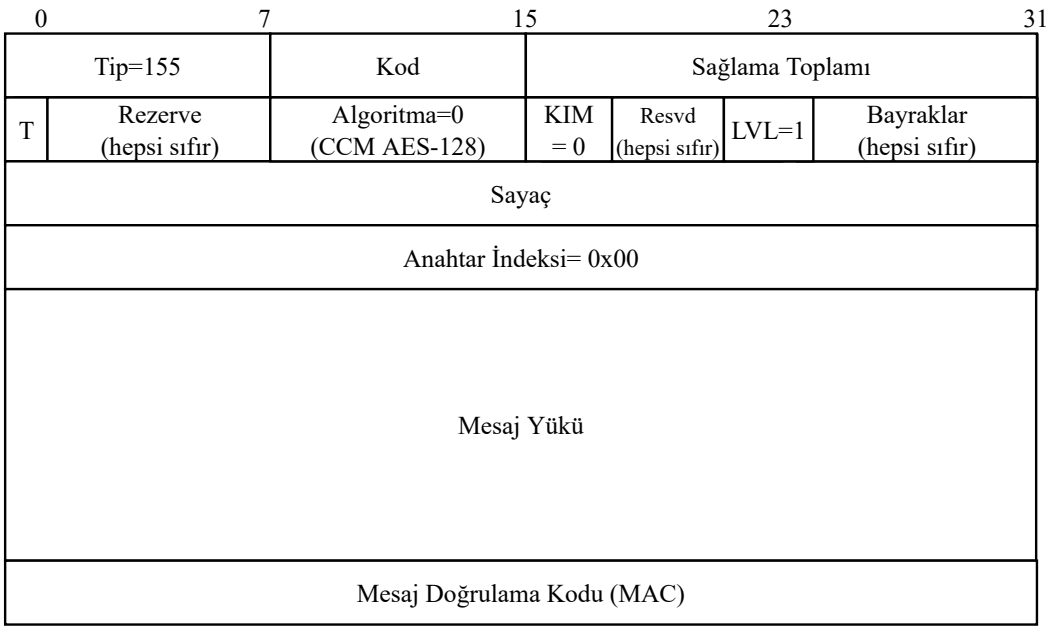
2. **Önceden yüklenmiş mod (pre-installed mode):** Ağ devreye alınmadan önce düğümlere yüklenmiş simetrik kripto anahtarı ile RPL kontrol mesajlarının kriptolandığı ve sadece bu kriptolu mesajlar ile RPL protokolünün sürdürüldüğü moddur.

3. **Kimliği doğrulanmış mod (authenticated mode):** Ağa sadece katılmak isteyen düğümlerin ön yüklenmiş moddaki gibi sadece bir simetrik anahtara sahip olduğu ancak RPL protokolünün koşturulması ve ağ topolojisinde söz sahibi olmak isteyen düğümlerin ek olarak ikinci bir anahtara sahip olması gereken moddur.

RPL standardının [20] önceden yüklenmiş ve kimliği doğrulanmış modun kısıtlı cihazlarda gerçeklenebilirliği konusunda çekinceleri olsa da dokümanlarında bu modların tanımlamarına yer vermiştir. Bu tanımlamaların bazılarına oldukça detaylı yer verilmişken bazı mekanizmalar ise gelecek zaman çalışması olarak bırakılmıştır. Ancak, [37]'da araştırmacılar ön yükleme modunun gerçeklemesini yapıp analiz ederek, RPL güvenlik modlarının kısıtlı cihazlarda da uygulanabilir olduğunu göstermiştir.

3.3.1 Önceden yüklenmiş mod

Önden yüklenmiş modda, RPL kontrol mesajları düğümler devreye alınmadan önce yüklenmiş olan simetrik kripto anahtarı ile korunmaktadır. RPL standardı bu mod ile veri gizliliği, veri doğruluğu (data authenticity) ve tekrarlama koruması özelliklerini sağlamaktadır. Bu özellik seçeneklerinden veri gizliliği ve tekrarlama koruması opsiyonel iken veri doğruluğu zorunlu kılınmıştır. RPL kontrol mesajları Tip:155 olan ve Kod alanı ile birbirinden ayrılan ICMPv6 mesajlardır. Güvenli olmayan modda kullanılan (Kod: 0x00 DIS, Kod: 0x01 DIO, Kod: 0x02 DAO, Kod: 0x03 DAO-ACK) RPL kontrol mesajları, farklı kod değerleri ile (Code: 0x80 Güvenli DIS, Kod: 0x81 Güvenli DIO, Kod: 0x82 Güvenli DAO, Kod: 0x83 Güvenli DAO-ACK) önden yüklenmiş modda kullanılmaktadır. Güvenli bir RPL kontrol mesajının mesaj yapısı Şekil-3.10'te verilmiştir.



Şekil 3.10 : Güvenli RPL kontrol mesajı yapısı

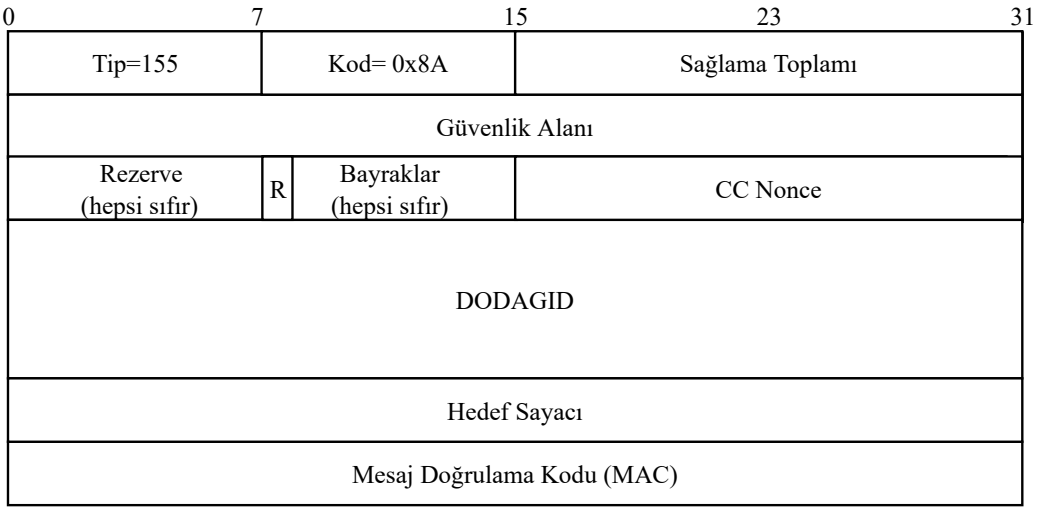
ICMPv6 başlığında, Tip ve "Code"alanından sonraki ve üçüncü alan "Checksum" olup, bu alan mesajın içeriğinde bozulma olup olmadığının tespit edilmesinde kullanılır. RPL güvenli modlarında ICMPv6 başlığı ile kontrol mesajı yükü arasında bir Güvenlik Alanı (Security Field) bulunmaktadır. Bu alanda RPL güvenli

modunun konfigürasyon parametreleri yer almaktadır. Bu alanlardan anlamlı ilk alanı Algoritma alanıdır. RPL standardı güvenli modda farklı algoritmaların kullanılmasının altyapısını oluşturmuştur ancak ön yüklemeli modda bu alan '1' değerini almalıdır. Bu değer kullanılan algoritmanın AES-128/CCM (CBC-MAC/CTR) [58] olduğunu belirtir. CCM, 128-bit blok şifreleyiciler için bir çalışma şekli olup, CTR (Counter) ve CBC-MAC (Cipher Block Chaining Message Authentication Code) çalışma modlarının birleşiminden oluşur. Bu nedenle CCM hem mesaj doğruluğu hem de veri gizliliği sağlayacak mekanizmaya sahiptir [58]. Sıradaki alan "LVL" (Güvenlik Seviyesi) alanıdır. Bu alan, uygulanan güvenlik yönteminde sadece mesaj doğruluğu servisinin sağlandığını ya da hem mesaj doğruluğu hem de veri gizliliği servisinin sağlandığını gösterir. Örneğin bu alanın değeri '1' ise hem mesaj doğruluğu hem de veri gizliliği servileri sağlanmaktadır. Sıradaki alan Anahtar Tanımlayıcı Modu (KIM) alanıdır. Standart bu alanın önden yüklenmiş modda '0' değerini alması gerektiğini belirtmiştir. Sıradaki alan Sayaç alanıdır ve gönderilen her güvenli RPL mesajı ile arttırılır. Bu değer, tekrarlama koruması özelliğini sağlayacak olan CTR kripto modu için bir girdi olarak kullanılır. Ağa yeni katılan bir düğümün bu sayaç değerine sahip olması için Kod alanı 0x84 olan Tutarlılık Kontrolü (CC: Consistency Check) mesajı kullanılmaktadır. CC mesajının yapısı Şekil-3.11'de verilmiştir.

CC mesajı hedefi son geçerli sayaç değerini bildirmek için kullanılır ve jenerik meydan okuma – yanıt (challenge-response) el sıkışması mantığı ile kullanılmaktadır. "CC Nonce" değeri mesajın tazeliği için kullanılırken Hedef Sayacı alanı ise mevcut sayaç değerini bildirmek için kullanılır. Mesajın içindeki 'R' bayrağı ise CC mesajının istek mi yoksa cevap mı olduğunu gösterir.

Tekrarlama koruması olmayan mod:

Bu modda, ICMPv6 başlık sonrası kripto konfigürasyonu hakkında bilgiler içeren güvenlik alanı hemen sonrasında kriptolu mesaj yükü, sonrasında da veri bütünlüğü koruması sağlayan Mesaj Doğrulama Kodu (MAC) bulunur. Bu modda ağa katılmak isteyen düğüm güvenli olmayan modda uyguladığı ebeveyn seçme prosedürünü



Şekil 3.11 : Tutarlılık Kontrolü mesajı yapısı

uygular. Ek olarak bu modda düğüm, gelen DIO mesajlarının MAC alanını kontrol edip mesajın kriptosunu çözmek durumundadır.

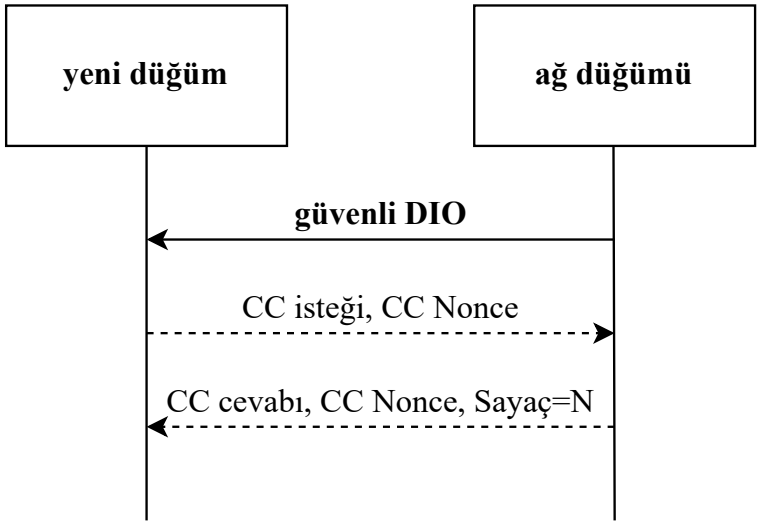
Güvenli mod için ayrıca şu kuralları belirtilebilir:

- Ağa atılmak isteyen düğüm eğer bir süre DIO duymayıp DIS mesajı gönderecek olursa, bu DIS mesajının güvenlik alanı önden yüklenmiş anahtar konfigürasyonunda (KIM:0 LVL:1) olmalıdır.
- Ağa katılmak isteyen düğümün DIS mesajını duyan ağdaki bir düğüm, trickle zamanlayıcısını ancak DIS mesajı önden yüklenmiş anahtar ile kriptoluysa resetleyecektir. DIS'e karşılık attığı DIO ise, alınan DIS ile birebir aynı kripto konfigürasyonunda olmalıdır. Bu düğüm DIS mesajına karşılık DIO mesajını henüz atmamış iken ikinci bir DIS mesajı geldi ise, cevaben atılan DIO mesajı son gelen DIS'in kripto konfigürasyonunda olmalıdır.
- Önden yüklemeli kripto konfigürasyonunda olmayan ve MAC alanı yanlış olan tüm RPL kontrol mesajları ihmal edilmelidir.

Tekrarlama koruması olan mod:

Tekrarlama koruması olan modda, tekrarlama koruması olan moda ek olarak kontrol mesajları güvenlik alanında bulunan sayaçların takip edilmesi gerekmektedir. Her

düğüm komşu düğümlerden aldığı güvenli kontrol mesajlarının sayaç değerlerini takip etmek durumundadır. Gelen her geçerli bir güvenli kontrol mesajında bu değer kaydedilir. Aynı düğümden alınan bir sonraki mesajda bu sayaç değeri artmalıdır. Bir komşudan gelen mesajda bu alan bir önceki ile aynı veya küçük değerde ise bu mesaj ihmal edilir. Ağa yeni katılan bir düğüm bir komşusunun güncel sayaç değerini öğrenmek istiyorsa CC mesajlarını kullanarak [37] Şekil-3.12'deki protokolü uygulamak zorundadır. Ağa yeni katılan bu düğüm komşusunun sayaç değerini öğrendikten sonra komşusunun bundan sonraki güvenli kontrol mesajlarını bu alanı takip ederek dikkate alacaktır.



Şekil 3.12 : Tekrarlama koruması olan önden yüklenmiş güvenlik modunda komşu düğümün sayacını öğrenme prosedürü

3.3.2 Kimliği doğrulanmış mod

Ağ ömrü boyunca sabit simetrik grup anahtarına sahip olan önden yüklenmiş güvenlik modunda, ağ düğümlerinden herhangi birinin ele geçirilmesi ve anahtarlarına ulaşılması durumunda tüm ağın güvenliği tehlikeye girecektir. RPL standardı bu durumun önüne geçmek için kimliği doğrulanmış güvenlik modunu önermiş ve RPL'in bir kimlik doğrulamalı bir anahtar değişim mekanizmasına ihtiyacı olduğunu açıkça belirtmiştir [20] Standart, böyle bir güvenlik mekanizmasının ancak asimetrik anahtarlı

kriptoloji yöntemleri ile sağlanabileneceğini belirtip standartta kimliği doğrulanmış mod için birçok detaydan bahsetmemiş ve gelecek zaman çalışması olarak bırakmıştır.

Standartta [20] kimliği doğrulanmış mod için koyulmuş kurallar ve tanımlamalar şu şekildedir:

- Ağa katılma prosedürü ön yükleme modu ile aynıdır. Ancak kimlik doğrulanmış modda önden yüklenmiş anahtar ile ağa katılan düğümler sadece ana bilgisayar düğümü (Host Düğüm veya Yaprak Düğüm) olabilirler. RPL protokolü ile ağ kurulumu ve bakımından sorumlu olan yönlendirici olmak için bir anahtar değişim mekanizma ile ikinci bir anahtara sahip olmaları gerekir.
- RPL kontrol mesajları önden yüklemeli moddaki gibi güvenli kontrol mesajı yapısına uymalı, ek olarak DIO ve DAO mesajları ile kullanılabilen DODAG Konfigürasyon Opsiyonunda bulunan 'A' kimlik doğrulama modu aktif bayrağı '1' e kurulmalıdır.
- Ana bilgisayar düğümleri, önden yüklemeli anahtar kripto konfigürasyonu ile yaydığını DIO'larda rank değeri olarak sadece `INFINITE_RANK` değeri yayabilirler. Bu durumun dışındaki DIO mesajları kimliği doğrulanmış yönlendirici düğümler tarafından ihmal edilir.
- Ana bilgisayar düğümleri, önden yüklemeli anahtar kripto konfigürasyonu ile yaydığını DAO Hedef Opsiyon mesajında ön ek değeri olarak sadece kendi adresini yayınlayabilir. Bu durumun dışındaki DAO mesajları kimliği doğrulanmış yönlendirici düğümler tarafından ihmal edilir.

Bu tez kapsamında, kimliği doğrulanmış mod daha detaylı analiz edilecek, standartta açık bırakılmış bazı senaryolarını da içerecek kapsamlı bir sistem çözümü tasarlanacaktır.

4. PROBLEM TANIMI VE ÇÖZÜM

RPL saldırıları incelendiğinde, saldırıların çoğunun veri içeriği saldırısı (Rank, Lokal Onarım, Yönlendirme, Objektif Fonksiyonu, DAO Tutarsızlık ve DAG Tutarsızlık saldırıları) olduğu görülmektedir. Bu saldırıları gerçekleştirmek için saldırgan modelleri, RPL kontrol mesajı içeriklerini ("hassas veri"leri) kullanarak RPL'in dinamik mekanizmalarını hedef almışlardır. Literatürde bu tür saldırılar için bir çok yöntem önerilmiş, ancak önerilen metodlar ya bu sadırıların sadece bir veya bir kaçına çözüm olmuş ya da birçoğu zaten kısıtlı kaynağa sahip ağ düğümlerinin hafıza, enerji ve işlem gücü bakımından fazla kaynak harcamasına sebep olmuştur. Araştırmacılar gün geçtikçe RPL veri içerikleri ile ilgili saldırgan modelleri öne sürmeye ve bu saldırgan modellerine karşı önlem geliştirmeye devam etmektedir. Ancak RPL'in kontrol mesajlarının ve dinamik mekanizmalarının yeni bir saldırı modeli önerilmesi beklenmeksizin koruma altına alınmalı ve bu saldırıları koruyabilecek daha bütüncül bir çözüm önerisi sunmak gerekmektedir.

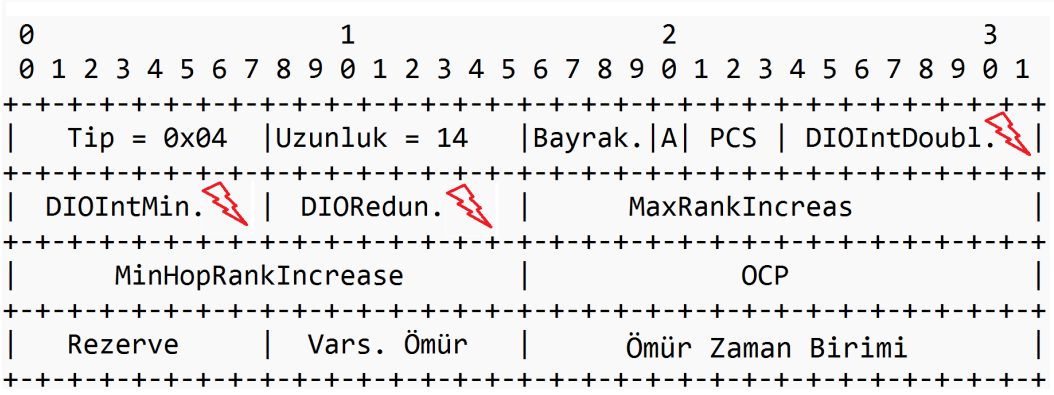
Bu bölümde ilk olarak, literatürde daha önce (bildiğimiz kadarıyla) konu alınmamış bir RPL içerik saldırısı olan Trickle zamanlayıcısı saldırısını tanımlayıp, bu saldırının RPL ağları üzerindeki etkisini inceleyeceğiz. Daha sonra, RPL içerik saldırılarının önüne geçeceğini düşündüğümüz RFC standartları ile uyumlu kapsamlı bir kimliği doğrulanmış RPL güvenlik modu önereceğiz. Bu kapsamda, RPL kimliği doğrulanmış modu için gerekli kimlik doğrulama ve anahtar yönetim protokolü tasarlayacağız. Tasarlanan bu şemanın resmi güvenlik doğrulamasını yapıp RPL ağlarına adapte edeceğiz.

4.1 Yeni bir RPL içerik saldırısı: Trickle Zamanlayıcısı Saldırısı

Trickle zamanlayıcısı, RPL ağlarının kurulması ve idamesinde kullanılan DIO kontrol mesajların gönderim sıklığını kontrol eden ve RPL'in adaptif ve enerji etkin bir yönlendirme protokolü olmasını sağlayan en temel mekanizmasıdır. DIO, içeriğinde

ve beraberinde taşıdığı opsiyon mesajları ile ağı tanımlayan bilgilerin yanında ağın durumuna göre dinamik değiştirilebilen parametreler de içermektedir. Bu parametrelerden üç tanesi Trickle zamanlayıcı algoritmasını birebir etkileyen ve DODAG Konfigürasyon opsiyonu mesajı içinde bulunan, DIO Aralık Katlanma Sayısı (DIOIntDoubl. ya da 'Idoubling'), Minimum DIO Aralığı (DIOIntMin ya da 'Imim') ve Yedeklilik Katsayısı (DIORedun. ya da 'K') alanlarıdır. (Şekil-4.1).

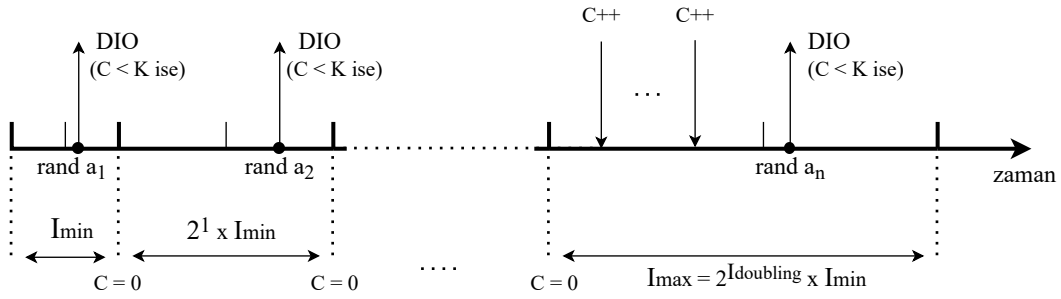
Tutarlılık kavramı Trickle zamanlayıcı için kullanılan bir terminolji olup ağın ve kontrol mesajlarının istikrarını belirtir. Standart, tutarlı ve tutarısız kavramlarının gerçekleme özelinde değişebileceğini belirtirken, bazı durumları açıkça tutarlılık veya tutarsızlık olarak açıkça belirtilmiştir.Bir tutarsızlık örneği olarak DIO mesajının içindeki Versiyon Numarası artışı verilebilirken, tutarlılık örneği olarak da hiç bir bilgisi güncellenmemiş bir DIO mesajı alınması verilebilir.



Şekil 4.1 : DODAG konfigürasyon opsiyon mesajı Trickle zamanlaycısı parametreleri

Ağ düğümü çalışmaya başladığı zaman Trickle zamanlayıcısı DIO aralığını rasgele bir zaman aralığına kurar ve herhangi bir tutarsızlık durumunda değerini minimum değerine (Imin) çeker. Bir aralık boyunca bir tutarsızlık olmaz ise değerini ikiye katlar. Bu değerin kaç kez katlanacağını DIO katlanma sayısı (Idoubling) belirler. Her aralıkta rasgele bir 'a' zaman değeri seçilir ve bu zamana erişildiğinde DIO gönderilip gönderilmemesi için bir koşula bakılır. Bu koşul Tutarlılık Sayacı'nın (C) yedeklilik katsayısı (K)'dan küçük olma koşuludur. Eğer koşul sağlanıyor ise DIO mesajı gönderilir. C sayacı ise; her yeni Trickle aralığında 0 değerine resetlenmekte,

her tutarlı mesaj ile arttırılmaktadır. Trickle zaman aralığının katlanma durumu ve DIO gönderme koşulu Şekil-4.2 ile sunulmuştur.



Şekil 4.2 : Trickle zamanlayıcısı mekanizması

Trickle zamanlayıcısı parametrelerinin DODAG kök (veya sistem kullanıcısı) tarafından ağın yoğunluğuna veya kararlılığına göre belirlenmesi beklenir. Mevcut parametreler ile çalışan bir RPL ağında bu parametrelerde yapılacak herhangi bir içerik saldırısı ağın gerekenden daha fazla kontrol mesajı (DIO) yollamasına sebep olacağı Trickle zamanlayıcısı mekanizması incelendiğinde açıkça görülmektedir. Kontrol mesajı sıklığı artması da, kısıtlı kaynaklı düğümlerin daha fazla güç harcamasına sebep olacaktır.

4.1.1 Saldırgan modeli ve simülasyon ortamı

Contiki, kablosuz sensör ağları için özel geliştirilmiş düşük güçlü ve az hafıza alanı kaplayan bir işletim sistemidir [59]. Kullandığı uygulamaların ve kendisinin C programlama dilinde yazılmış olması, 6LoWPAN standartlaşmış protokol yığınının ve RPL protokolünün gerçeklemesini içermesi, Texas Insturement MSP430 gibi düşük güçlü işlemciler ile uyumlu olması ve bir çok simülasyon aracına sahip olması ile, Contiki işletim sisteminin ve onun geliştirme ortamının literatürdeki bir çok araştırmada tercih edilmesini sağlamıştır [29].

Cooja ise, Contiki sensör ağı işletim sistemini çalıştıran ve sensör ağlarını simüle etmek için tasarlanmış Java tabanlı bir simülasyon aracıdır [60]. Simülatör Java'da gerçeklenmiş olsa da C programlama dilinde yazılmış düğüm yazılımların kullanılmasına imkân tanır. Sağladığı kullanıcı arayüzü, simülasyon esnekliği ve bir

çok eklenti aracı ile Cooja da en çok tercih edilen simülasyon ortamlarından biri olmuştur [29].

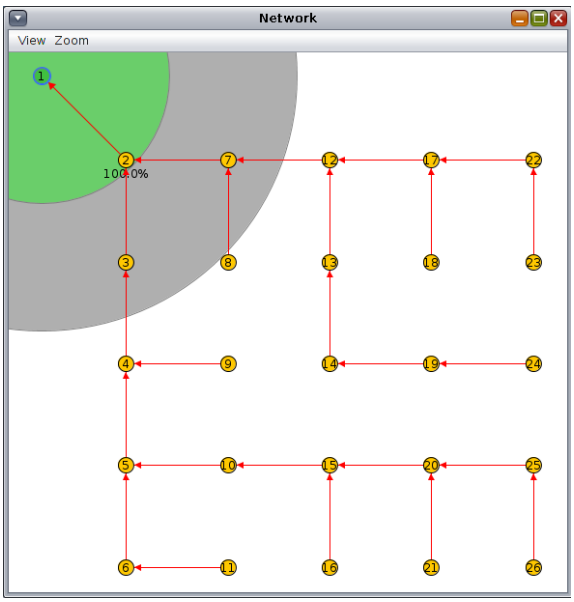
Önerdiğimiz Trickle zamanlayıcısı saldırısını modellemek için Contiki İşletim sisteminde yer alan RPL gerçeklemesinde öncelikle kod ve parametre değişikliğini yapacağız. Sonra, Cooja simulator ile bu saldırgan düğümün RPL protokolünü işleten bir ağ üzerindeki etkilerini gözlemleyeceğiz. Önemli simülasyon ve ağ parametreleri, Trickle zamanlayıcısı meşru ağ ve saldırgan düğüm parametrelerini de içerecek şekilde Çizelge-4.1 ile sunulmuştur. Meşru ağ parametreleri Contiki gerçeklemesinde yer alan varsayılan parametreler olmakla beraber, saldırgan için belirlenen parametreler içerisinde sadece Imin ve Idoubling değerleri saldırı altında kalan meşru düğümlerin DIO gönderme sıklığını arttıracak şekilde değiştirilmiştir. K değerinin yani yedeklilik katsayısının azaltılması da ağ senaryosuna göre dolaylı yoldan DIO sıklığını arttırabilirdi ancak bu tez kapsamında Trickle zamanlayıcı içeriklerinin değiştirilmesinin yıkıcı etkileri sunulmak istendiği için Trickle zamanlayıcısına direk etki eden parametrelerin değiştirilmesi tercih edilmiştir. Örneğin; Idoubling parametresi Trickle zamanlayıcısına katsayı çarpanı olarak etki ederken, Imin için RPL parametresi 2'nin kuvveti olarak Trickle zamanlayıcı süresine etki etmektedir. Ek olarak, simülasyon süresi Trickle zamanlayıcısının Imin değerini Idoubling kere katlanmasını yani maksimum süresine ulaşması için gereken süreyi içerecek şekilde belirlenmiştir.

Meşru RPL ağı saldırı altında olmayan ve saldırıya maruz kalacak ağ anlamına gelmektedir. Meşru ağın şebeke yerleşimi Şekil-4.3'te sunulmuştur. Kare şebeke ağı, sol üst köşesinde konumlanmış 1 numaralı DODAG kökü ve 25 ağ yönlendirici düğüm olmak üzere toplam 26 meşru düğümden oluşmaktadır. Yeşil alan düğümün gönderme mesafesini, gri alan ise enterferans mesafesini gösterirken 2 numaralı düğümün üzerinde yer alan "%100" değeri gönderilen paketi hedef düğümün alma olasılığını belirtmektedir. Kırmızı oklar ise DODAG topolojisini yani düğümlerin ebeveyn düğüm seçimini göstermektedir.

Saldırgan düğümler meşru düğümlerden birinin sonradan bozulma veya ele geçirilmesi sonucu farklı içerik (Trickle zamanlayıcısı parametresi) yayınlayacak şekilde planlanmıştır. Saldırgan düğümlerin yerleşimleri DODAG kökünden uzaklıkları (düğüm

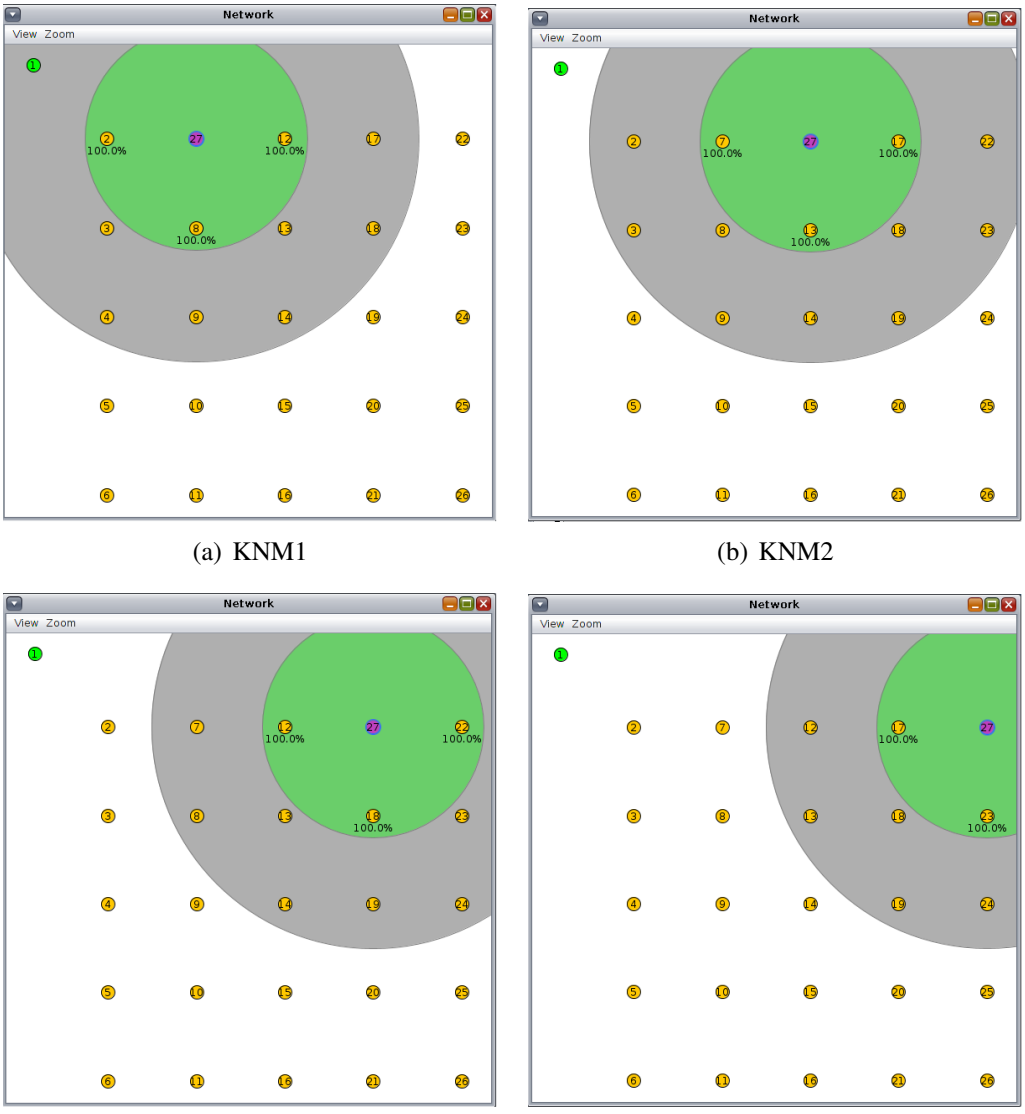
Çizelge 4.1 : Simülasyon Parametreleri

Parametre	Değeri
Objektif Fonksiyonu	MRHOF
Alma/Gönderme Oranı	%100
Gönderme Mesafesi	50m
Enterferans Mesafesi	100m
Alma Oranı	%100
Radyo Ortamı	Birim Disk Grafik Ortamı (UDGM: Mesafe Kayıplı)
Topoloji	200mx200m Şebeke
Simülasyon Zamanı	1800 saniye
Düğüm Sayısı	26
Meşru Ağ Trickle Parametreleri	$I_{min} = 2^{RPLparam}$ ms, RPLparam=12 $I_{doubling} = 8$ K=10
Saldırgan Düğüm Trickle Parametreleri	$I_{min} = 2^{RPLparam}$ ms, RPLparam=9 $I_{doubling} = 6$ K=10



Şekil 4.3 : Saldırgan olmayan meşru ağ

atlama sayısı olarak) artacak şekilde sırasıyla "KNM1","KNM2","KNM3" ve "KNM4" etiketleri ile Şekil-4.4 ile sunulmuştur. Saldırgan düğümlerin sadece dikey eksendeki komşularına ulaşabildiği görülmektedir ancak, DIO mesajlarının yayılım deseni (DODAG kökünden ağın dışına doğru) göz önünde bulundurulduğunda yapılacak saldırının etkisinin etkisinin DODAG köküne yakınlaştıkça artması beklenmektedir.



(a) KNM1 (b) KNM2

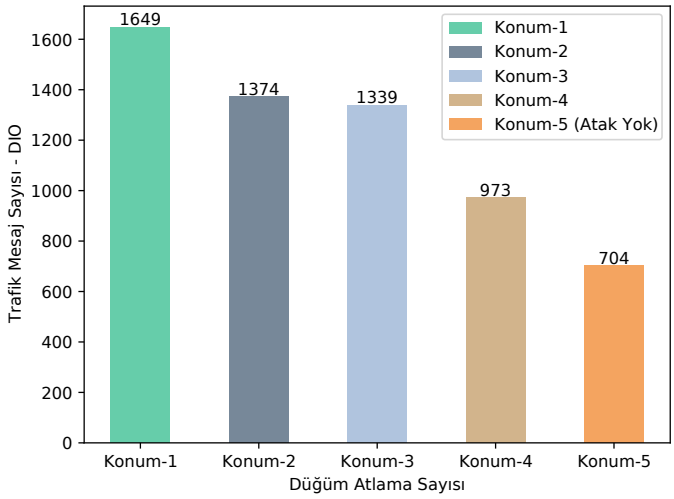
(c) KNM3 (d) KNM4

Şekil 4.4 : Saldırgan konumları

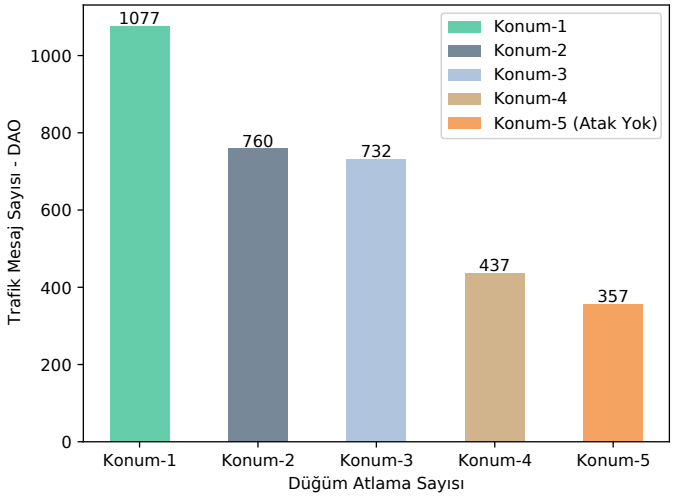
4.1.2 Saldırının etkilerinin değerlendirilmesi

Bir RPL ağında DIO mesajları DODAG kökünden başlayarak ağın derinliklerine (DODAG kökünden uzağa) doğru yayılmaktadır. Trickle parametreleri de DODAG kökü tarafından belirlenen ağ konfigürasyonlarının bulunduğu DODAG konfigürasyon

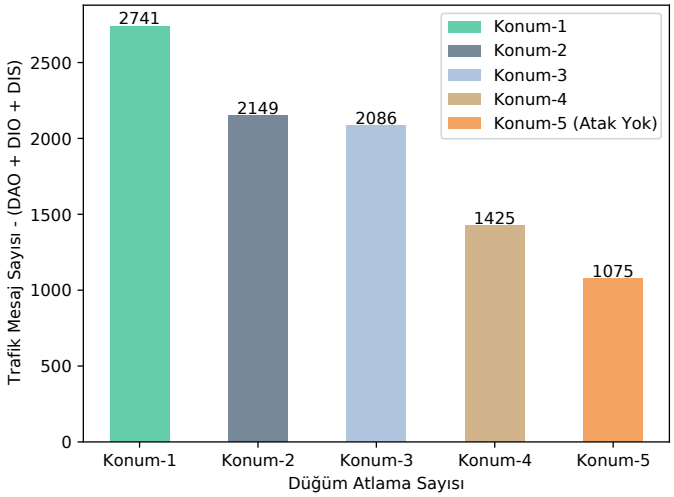
opsiyonu mesajı içinde DIO mesajına eklenmiş şekilde düğümlere yayılmaktadır. Saldırı simülasyonunda saldırgan düğümün yaydığı yanlış Trickle parametreleri komşu düğümleri tarafından alınmış, aldıkları bu yanlış parametreleri de kendi çocuk düğüm ve komşularına çoğayayım mesajı olarak yaymışlardır. Beklendiği gibi saldıraya maruz kalan ağdaki trafik yoğunluğundaki artış saldırının lokasyonu DODAG köküne yakınlaştıkça daha da çok artmıştır. Şekil-4.5, Şekil-4.6 ve Şekil-4.7 ile ağ düğümlerinin saldırı olmayan duruma göre RPL kontrol mesajlarındaki artış açıkça görülmektedir. Saldırının sonuçları incelendiğinde bir detay dikkat çekmektedir. DODAG köküne en yakın yapılan saldırı ile saldırı olmayan durum karşılaştırıldığında gönderilen toplam DIO sayısı yaklaşık 2.2 katına çıkarken toplam DAO sayısı 3 katına çıkmıştır. Mevcut RPL gerçeklemesinde Trickle zamanlayıcısı parametrelerinde olan bir değişikliği köklü bir değişiklik olarak nitelendirilmiş ve bu parametrelerde değişiklik yapıldığında DODAG güncellemesi olarak da yorumlanmıştır. DODAG yenilenmesi ile yeni bir düğümü ebeveyn olarak seçen düğümler yeni DAO mesajlarının sayısında artışa sebep olmuştur. Yine ikinci bir detay olarak, düğümlerin gönderdiği DIS sayısında bir değişiklik olmamıştır. Çünkü, DIS mesajları düğümlerin belli bir süre DIO mesajı almadığında komşu düğümlerini DIO atması için tetikleyen bir mesajdır. Yapılan saldırı zaten DIO trafiğini yoğunlaştırdığı için düğümlerin DIS gönderme sayısında bir artışa sebep olmamıştır.



Şekil 4.5 : Saldırı süresince düğümlerin gönderdiği toplam DIO mesajı sayısı



Şekil 4.6 : Saldırı süresince düğümlerin gönderdiği toplam DAO mesajı sayısı



Şekil 4.7 : Saldırı süresince düğümlerin gönderdiği toplam DAO mesajı sayısı

RPL ağlarında kullanılan kısıtlı kaynağa sahip düğümler için, gönderme sayısının artması harcadıkları gücün artmasına ve zaten kısıtlı olan güç kaynaklarının daha hızlı bitmesine sebep olacaktır. Simülasyon sonuçlarından açıkça görülüyor ki Trickle parametreleri saldırıları ağdaki trafik yoğunluğunun oldukça artmasına ve düğümlerin olması gerekenden çok daha fazla güç tüketmesine sebep olmaktadır. Trickle zamanlayıcısı saldırısının ve etkilerinin sunulmasının bir amacı da şudur ki;

RPL kontrol mesajlarıyla taşınan tüm bilgiler değerlidir ve korunmaya ihtiyacı vardır. Bunun için ayrı ayrı parametreleri koruyacak kısmi saldırı önlemleri önermek yerine daha bütüncül bir yöntem önermek gerekmektedir.

4.2 RPL Kimliği Doğrulanmış Mod Tasarımı

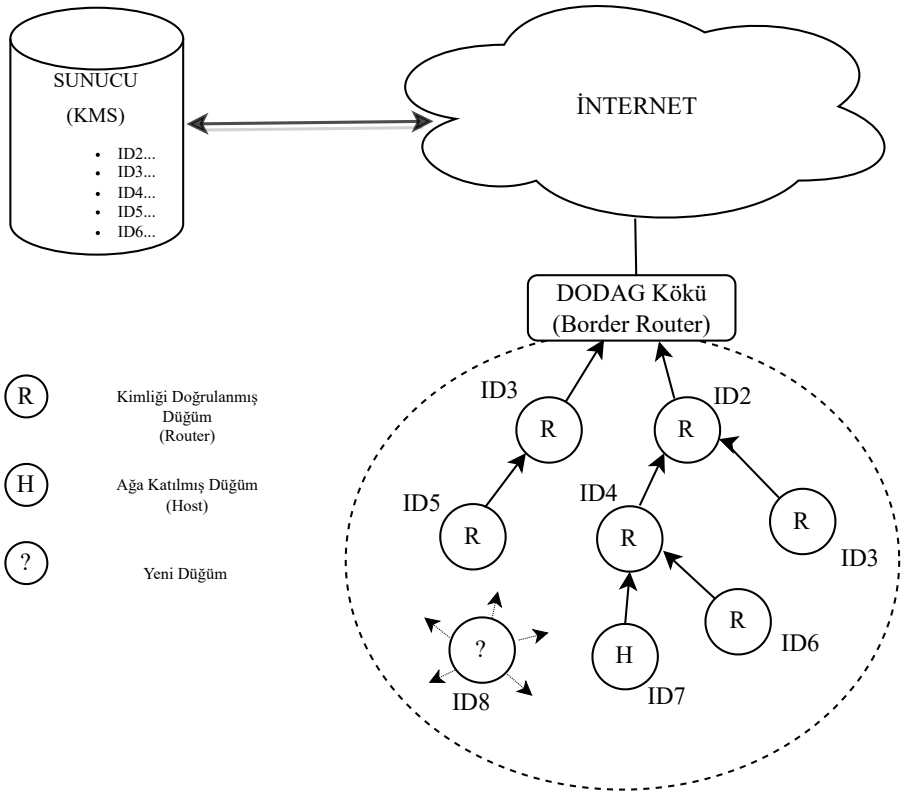
RPL önden yüklenmiş güvenlik modu hali hazırda mesaj gizliliği, mesaj bütünlüğü ve mesaj doğruluğu (özgünlük) korumasını desteklemektedir. Ancak, bu mekanizmadaki "özgünlük" Mesaj Doğrulama Kodu (MAC) ile sağlanmakta olup mesajı gönderenin kimliğini doğrulamayı sağlamamaktadır. RPL saldırıları incelendiğinde, eğer bir düğüm gelen bir kontrol mesajının gerçekten legal bir düğümden gelip gelmediğini bilseydi birçok RPL saldırısının önüne geçilirdi. Bu da literatürde kaynak veya kullanıcı kimlik doğrulaması olarak geçmektedir ve sadece asimetrik kriptoloji yöntemleri ile sağlanabilmektedir.

RPL standardı kripto konfigürasyon opsiyonları ile kontrol mesajlarında dijital imza vb. asimetrik anahtarlı kriptoloji yöntemlerinin kullanılması için bir altyapı imkânı sunsa da, gönderilen her kontrol mesajına açık anahtar tabanlı kriptolojik hesaplamaların uygulanması kısıtlı düğümlerde harcayacağı fazla enerji ve zaman gecikmesi göz önünde bulundurulduğuna düşük güçlü ve kayıplı ağlarda uygulanması pek mümkün görünmemektedir. Bu doğrultuda asimetrik anahtarlı kriptoloji daha nadir ve özel koşullarda uygulanmalı. Örneğin, lokal ve global onarım sırasında, sadece rank güncellemesi olduğunda veya ebeveyn düğüme yönlendirme bilgisi aktarılırken gibi. Bunların yanında RPL standardı, çok açık kapı ve eksiklikler ile kimliği doğrulanmış güvenlik modu tanımlamıştır.

Bu bölümde standardın gereksinimlerine, katı yasaklarına ve önerilerine bağlı kalarak, standartta eksik ve gelecek çalışması olarak bırakılmış noktaları tamamlayıp kapsamlı bir kimliği doğrulanmış RPL güvenlik modu tasarlayacağız.

4.2.1 Sistem yaklaşımı

Sistem modeli Şekil-4.8'te görüldüğü üzere dört temel birimden oluşmaktadır. Birincisi yetki ve anahtar yönetiminden sorumlu ve önerilecek güvenlik sisteminde gerekli



Şekil 4.8 : Kimliği doğrulanmış RPL için sistem modeli

tüm bilgileri veritabanında içeren Anahtar Yönetim Sunucusu (Key Management Server ya da KMS)'dur. İkincisi, DODAG'ın kurulumundan sorumlu ve 6LoWPAN ağını dış IP (Örneğin, internet.) ağlar ile bağlantısını sağlayan DODAG kökü (Root, DODAG root ya da Border Router)'dür. Ek olarak, DODAG kökü önerilen kimlik doğrulama şemasını da yönetilmesinde görev alır. Sıradaki birim ise kimlikleri sistem yöneticisi tarafından sisteme kayıtlı ve RPL protokolünü kullanmakta yetkili ağ düğümleri olan yönlendiricilerdir (Router ya da 'R')'dır. Ancak, bir ağ düğümünün bu yetkilere sahip olması için ilk önce DODAG kökü üzerinden kimliğini doğrulamalı ve RPL protokolünü koşturmak için ikinci bir simetrik kripto anahtarına sahip olmalıdır. Sistem modelinin dördüncü ve son birimi ana bilgisayarlardır (Host, 'H', Leaf ya da Yaprak düğüm). Bu düğümler sadece ağa katılır ve ağı uygulama amacına yönelik kullanabilirler, RPL protokolünün işletmesinde ve ağ topolojisi üzerinde bir etkileri olamaz.

Çalışmamız aşağıdaki aşamaları içerecek şekilde sunulacaktır:

- Kimlik doğrulamalı anahtar değişim protokolü tasarımı ve doğrulanması
- Sistem modelinin bütününü kapsayacak varsayımlar ve ön hazırlıklar
- Kimliği doğrulanmış RPL güvenlik modunda kullanacak kontrol mesajlarının formatları
- Ana Bilgisayar (Host) olarak ağa katılma
- Önerdiğimiz kimlik doğrulama ve anahtar yönetim şeması ile yönlendirici olarak ağa katılma
- Ana bilgisayar ve yönlendiricilerin ağ davranışları
- Anahtar güncelleme senaryosu

4.2.2 Kimlik doğrulamalı anahtar değişim protokolü tasarımı ve doğrulanması

Kimliği doğrulanmış RPL güvenlik modunda kullanılan ve yenilenmesine ihtiyaç duyulan kripto anahtarı RPL kontrol mesajları üzerinde uygulanan bir simetrik grup anahtarıdır. Bu nedenle tasarlanacak kimlik doğrulamalı anahtar dağıtım protokolünde hem kimliği doğrulanmış RPL güvenlik modunun hem de bir grup anahtarının güvenlik ve performans gereksinimleri dikkate alınacaktır.

Tasarlanacak protokol için belirlenen güvenlik ve performans kriterleri aşağıdaki gibidir:

- **Hafiflik (lightweightness):** Kısıtlı hafıza,enerji ve işlem gücüne sahip ağ düğümlerinde gerçeklenebilir olmalı ve bu kaynaklarını aşırı ömür süresine kıyasla büyük oranda tüketmemelidir.
- **Ölçeklenebilirlik (scalability):** Grup anahtarının güncellenmesi ve dağıtılması ağ düğüm sayısı (n) arttıkça beraberinde, iletişim , işlem ve zaman yükü doğuracaktır. [61] Grup üyesi (ağ düğümü) sayısının artması ile artan bu metrikler protokolü koşturan temsilciler (Şekil-4.9) ve ağ altyapısı (bant genişliği, trafik yoğunluğu vb.) tarafından üstesinden gelinebilir olmalıdır.

- **İleriye dönük gizlilik (forward secrecy):** Gruptan ayrılan bir grup elemanının gelecekteki anahtara ve korunacak veriye ulaşamaması gerekmektedir. [61] Bunun için bir anahtar güncelleme mekanizması olmalı ve gruptan ayrılan ağ elemanı bu anahtar mekanizmasına şahit olsa dahi yeni anahtara sahip olamamalıdır.
- **Karşılıklı kimlik doğrulama (mutual authentication):** Protokolü gerçekleştiren temsilcilerin ikisinin de birbiri ile kimlik doğrulaması yapması gerekmektedir. [62] DODAG istekte bulunan düğümün gerçekten o düğüm mü olduğundan emin olmalı, istekte bulunan düğümün ise cevap verenin gerçekten DODAG kökünün olduğundan emin olmalıdır.

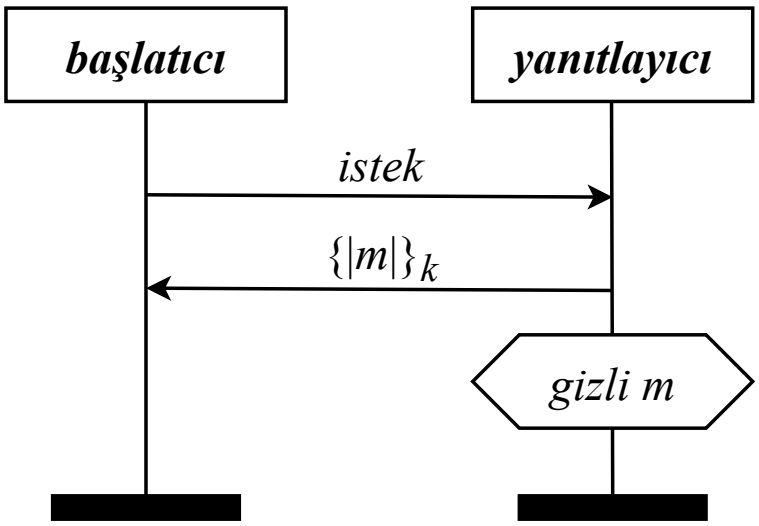
Gereksinimlere uygun mükemmel bir kriptolojik şema tasarlamak maalesef tüm iletişim güvenliğini garanti altına almamaktadır. Kriptolojik yöntemler tek başına iletişim güvenliğini garanti için yeterli değildir. [62]'de yazarlar bu durumu şu şekilde açıklamışlardır; "Güçlü bir bisiklet kilidi ile yanlış şekilde bağlanmış bir bisikletin çalınmayacağının garantisi yoktur." Bu sebeple bu tez kapsamında kriptolojik yöntemlerden ("bisiklet kilidi") çok güvenlik protokolünün güvenliği ("kilidin nasıl bağlandığı") ile ilgilenilecektir.

Güvenlik protokollerinin doğrulanması konusunda Burrows, Abadi ve Needham [63] 1989'da protokol davranışlarını ve saldırıları matematiksel modellemesini yaparak protokol doğrulama konusunda çığır açan BAN mantığını geliştirmişlerdir. Bu metodoloji araştırmacılar tarafından yıllar içinde güncellenerek güvenlik protokolü doğrulama amacı için kullanmıştır. [62] Günümüzde ise, temeli yine BAN mantığına dayanan bir çok güvenli protokolü doğrulama aracı mevcuttur (Scyther, ProVerif, Athena, Avispa ve Casper/FDR gibi. [64]) . Bu tez kapsamında önerilen protokolün doğrulanması için; Güvenlik Protokolü Tanımlama Dili (SPDL) ile kullanılan ve güvenlik açıklarını kullanıcı ara yüzü ile açıklayıcı bir şekilde gösteren Scyter [65] güvenlik protokolü doğrulama aracı kullanılacaktır.

Önerilen protokolün son haline (Genişletilmiş BKE) ulaşmak için üç aşamada geliştirme yapılmıştır. Her aşamada [62] ve [65]'da belirtilen ve Scyter aracının da desteklediği dört tip kimlik doğrulama derecesi (Niagree, Nisync, Alive ve Weakagree) ve gizlilik kriterlerinin sağlanıp sağlanmadığı incelenmiştir. Birinci

aşamada ağ düğümün kimlik doğrulama ile ilk simetrik grup anahtarını alma gereksinimi karşılaması amacı ile üç mesaj içeren bir şema tasarlanmıştır. Ancak şema Scyther aracı ile doğrulanmak istendiğinde güvenlik zafiyeti olduğu ortaya çıkmıştır. İkinci aşamada bu zafiyet giderilerek güncellenmiş ve Scyter aracı ile tamamen doğrulanmıştır. Güncellenen bu protokolün BKE (Bilateral Key Exchange) [66] protokolüne benzerliği dikkat çekmiştir. Üçüncü ve son aşamada ise protokol anahtar güncelleme ihtiyacını karşılamak amacı ile güven zincirine dayalı bir mekanizma ile genişletilmiş ve doğrulanmıştır. Anahtar güncellemeyi de içeren bu kapsamlı güvenlik protokolü ise "Genişletilmiş BKE" protokolü olarak adlandırılmıştır.

Üç aşamada sunulacak protokol şemaları Uluslararası Haberleşme Birliği (ITU) tarafından tanımlanan terminolojiye [67] göre yapılmıştır. Şekil-4.9'te bu terminolojiye uygun bir şema modeli sunulmuştur. Bir güvenlik protokolünde gerçekleştirilen davranışlar "rol" (role) olarak adlandırılırken, bu rolleri gerçekleştiren birimlere de "temsilci" (agent) denilmektedir. Çizelgede yer alan en üstteki dikdörtgenler içinde belirtilen birimler temsilciler, dikey çizgiler ise rollerdir.



Şekil 4.9 : ITU standartlaşmış güvenlik protokolü modelleme notasyonu

Aşama-1: Kimlik doğrulama ve ilk simetrik anahtarın alındığı şema ve güvenlik zafiyetinin bulunması

Birinci aşamada tasarlanan 3 mesajlı kimlik doğrulama ve anahtar değişim protokolü Şekil-4.10 ile gösterilmiştir. Bu şema başlatıcı ve yanıtlayıcı olarak iki temsilciden oluşmaktadır. Temsilcilerin üzerinde yazan anahtarlar şema öncesi bildikleri anahtarları göstermektedir. Şema, anahtar isteme, anahtar cevabı ve anahtar cevabı alındı bilgisin mesajlarından oluşmakta olup bu mesajların işleme alınması ve işlevleri aşağıda detaylı şekilde sunulmuştur.

- **Anahtar isteme (Gönderme):** Başlatıcı taze bir kerelik sayı (n_i) üretir. Bu sayı anahtar isteğinin eşsiz olduğunu belirtir. Anahtar isteme düz metni sadece bu sayıdan oluşur. Düz metin yanıtlayıcının açık anahtarı ($Kpub_r$) ile kriptolanır ve yanıtlayıcıya gönderilir. Başlatıcı bilir ki bu şifreli metin ancak gerçek yanıtlayıcı tarafından açılabilir.

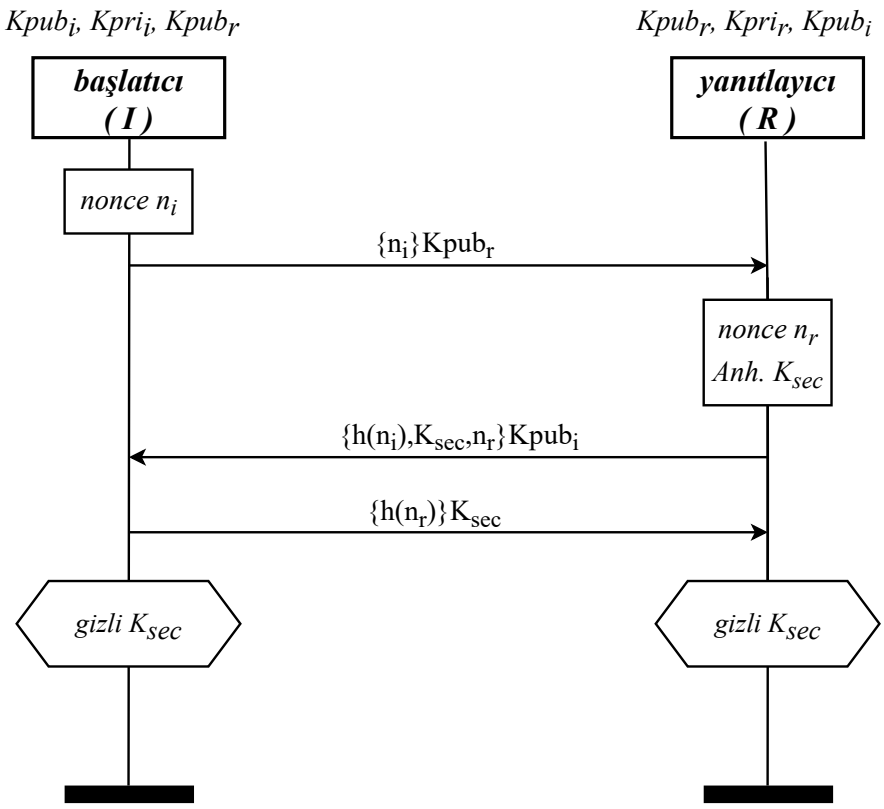
- **Anahtar isteme (Alma):** Yanıtlayıcı anahtar isteme mesajını alır ve şifreli mesajı gizli anahtarı $Kpri_r$'yi kullanarak çözer. (n_i) değerini kontrol ederek mesajın eşsizliğinden emin olur ve bu sayıyı daha sonra kullanmak üzere özet fonksiyonundan geçirir ve $h(n_i)$ değerini oluşturur.

- **Anahtar cevabı(Gönderme):** Yanıtlayıcı meydan okuma değeri olarak kullanacağı n_r taze bir kerelik sayıyı ve $Ksec$ simetrik grup anahtarını hazırlar. Sonra, $h(n_i)$, $Ksec$ ve n_r değerlerinden oluşan düz metnini başlatıcının açık anahtarı $Kpub_i$ ile kriptolar ve başlatıcıya gönderilir. Yanıtlayıcı bilir ki bu şifreli metin ancak gerçek başlatıcı tarafından açılabilir.

- **Anahtar cevabı(Alma):** Başlatıcı anahtar cevabını mesajını alır ve şifreli mesajı gizli anahtarı $Kpri_i$'yi kullanarak çözer. Elde ettiği düz metinde ilk olarak, anahtar isteme mesajında gönderdiği n_i değerinin özet fonksiyon çıktısı $h(n_i)$ değerini kontrol eder. Eğer bu değer doğru ise, başlatıcı emin olur ki bu sayı sadece kendisi ve yanıtlayıcı tarafından bilinmektedir dolayısıyla gelen anahtar cevabı yanıtlayıcdan geldiğine inanır. Düz metinde yer alan K_sec simetrik grup anahtarını kullanıma alır.

- **Anahtar cevabı alındı bilgisi (Gönderme):** Başlatıcı anahtar cevabı içerisinde gelen n_r değerini özet fonksiyonda geçirerek $h(n_r)$ değerini oluşturur. Sadece bu değerden oluşan düz metni K_sec simetrik grup anahtarını kullanarak kriptolar ve şifreli metni yanıtlayıcıya gönderir.

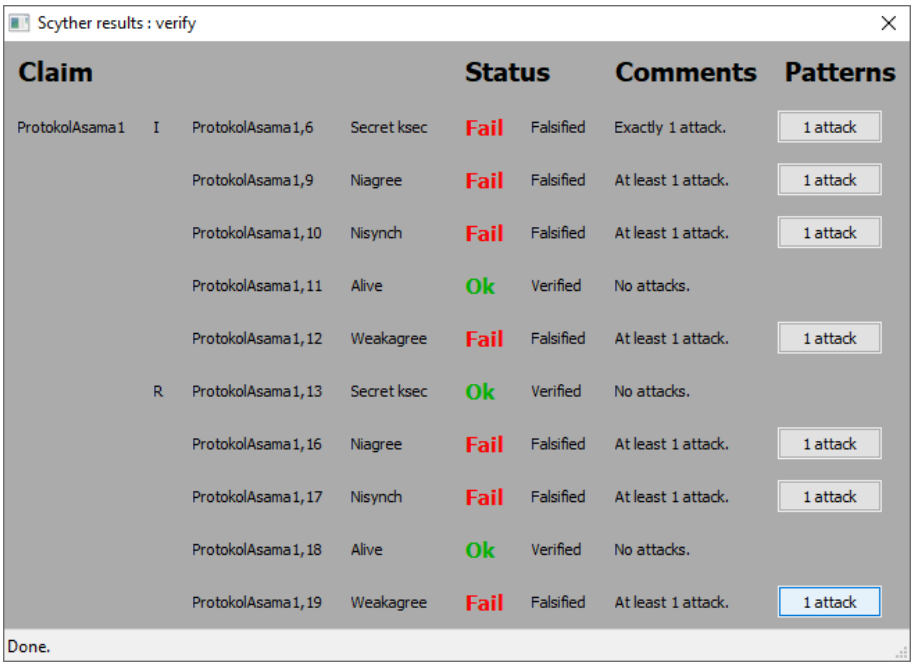
- **Anahtar cevabı alındı bilgisi (Alma):** Yanıtlayıcı anahtar cevabı alındı bilgisi mesajını alır ve K_sec simetrik grup anahtarı ile şifresini çözer. Düz metin içindeki meydan okuma cevabı $h(n_r)$ değerini meydan okuma değeri n_r değeri ile karşılaştırır ve bu şekilde şemanın başından itibaren gerçek başlatıcı ile protokolü işettiğinden emin olur.



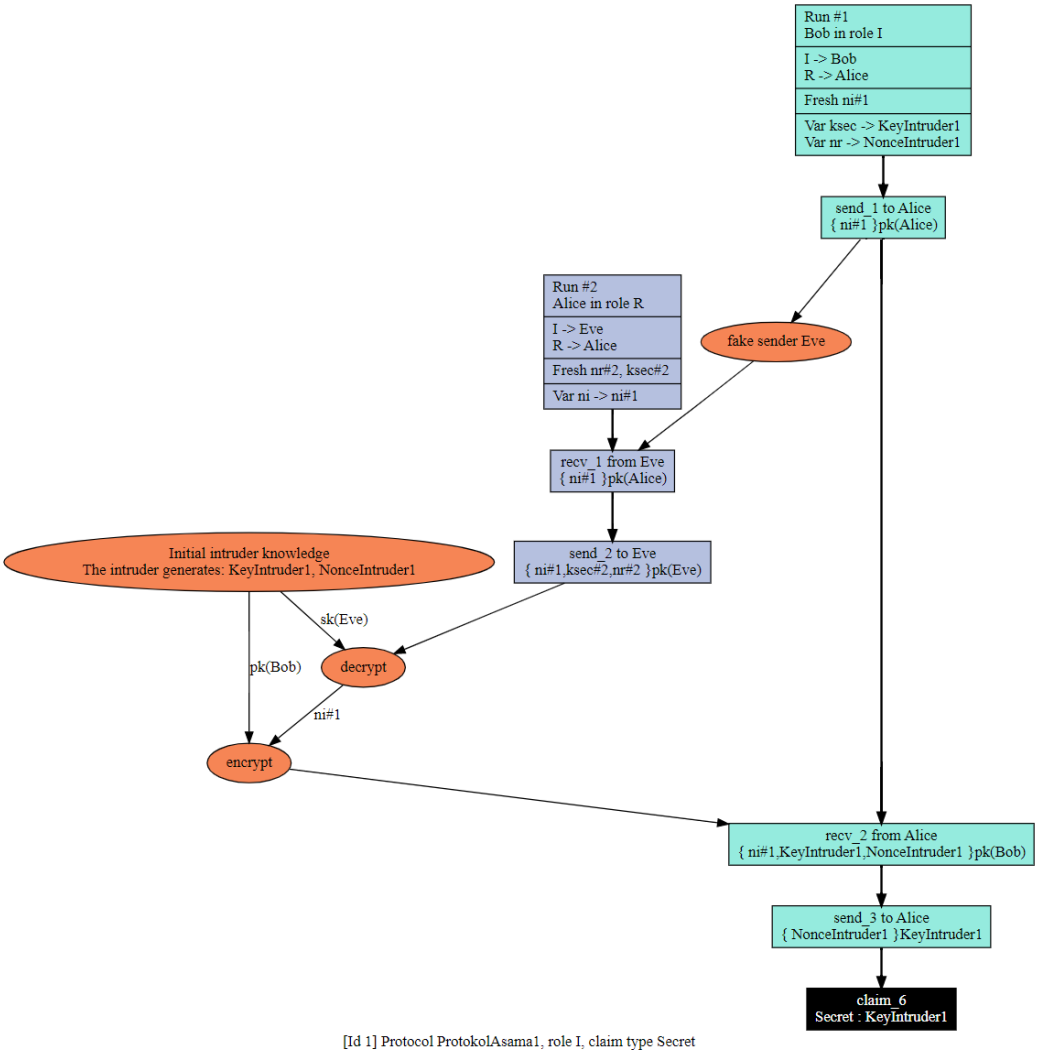
Şekil 4.10 : Birinci aşamada tasarlanan kimlik doğrulama ve anahtar değişim protokolü (aşama-1)

Birinci aşamada tasarlanan şema SPDL diline çevrilerek Scyther güvenlik protokolünde incelemeye alınmıştır. Sychter çıktıları Şekil-4.11'de sunulmuştur. Çıktılardan görüldüğü üzere gizlilik ve kimlik doğrulama açısından bir çok kriter

sağlanamamıştır. Bu sebeple ilk hata olan grup simetrik anahtarı K_sec'in gizliliğinin neden güvenliğinin sağlanamadığı Şekil-4.12'de sunulan Scyther aracı saldırgan modelinde incelenmiştir. Yanıtlayıcının $Kpub_r$ anahtarının açık olması anahtar isteğini herhangi üçüncü şahıs bir başlatıcı ile yapıldığında yanıtlayıcının anahtar cevabı olarak olarak üçüncü şahsa onun açık anahtarı ile yollanması K_sec anahtarının başlatıcı ve yanıtlayıcı arasındaki gizliliğini bozacağını ve başlatıcının alması gerekenden farklı bir simetrik alacağı açıklayıcı şekilde göstermiştir. İlgili güncelleme aşama-2 ile yapılacaktır.



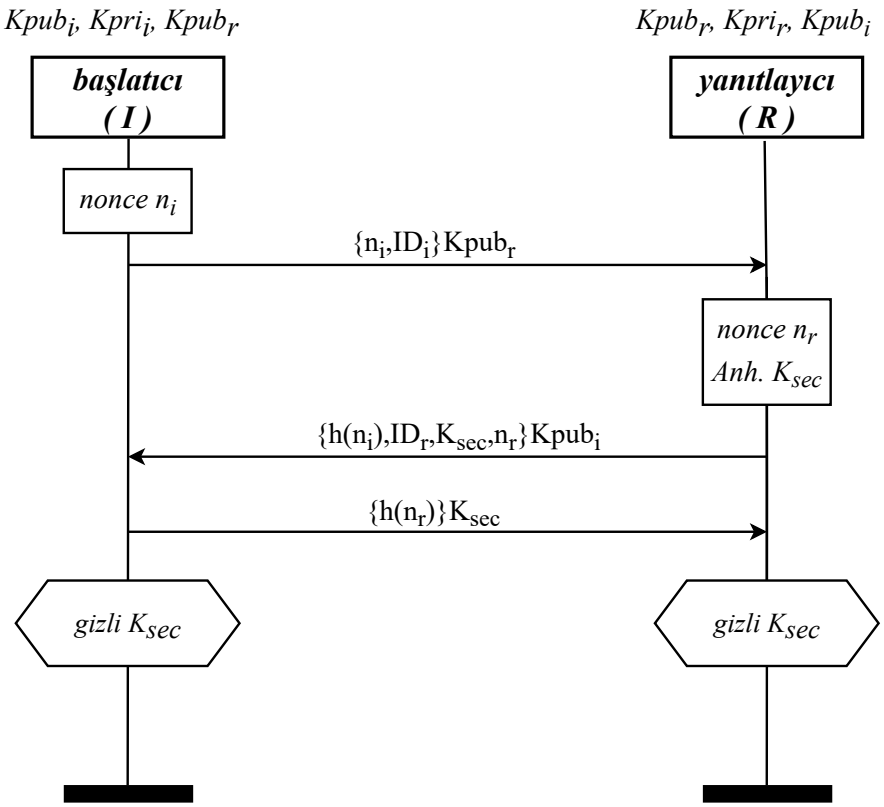
Şekil 4.11 : Birinci aşamada tasarlanan şemanın Scyther aracı doğrulama çıktısı (aşama-1)



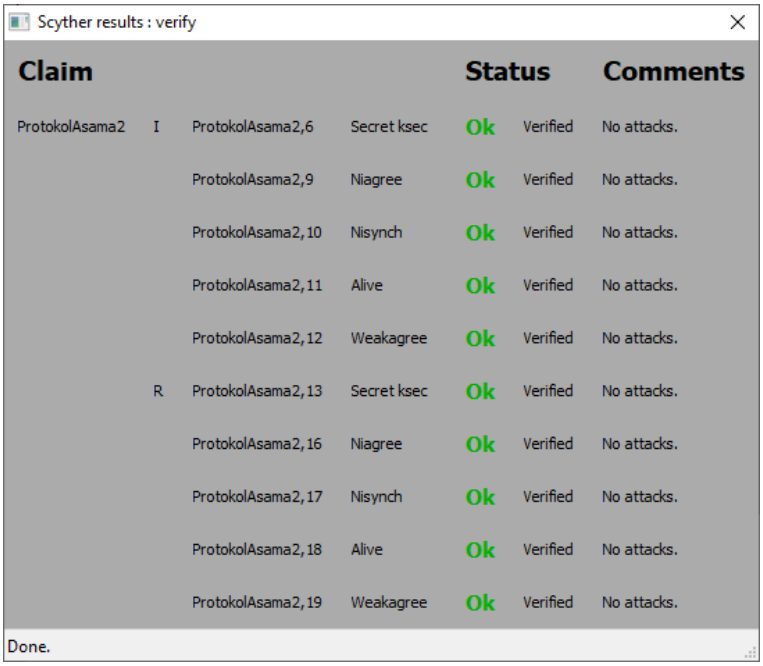
Şekil 4.12 : Birinci aşamada tasarlanan şemanın Scyther aracı saldırı modeli (aşama-1)

Aşama-2: Güvenlik zafiyeti giderilerek güncellenen şema ve doğrulanması

Bu aşamada, Anahtar isteme mesajına ve Anahtar cevabı mesajına sırasıyla başlatıcı kimliği (ID_i) ve yanıtlayıcı (ID_r) kimlikleri eklenerek protokol şeması Şekil-4.13'deki gibi güncellenmiştir. Aşama-1'de anahtar isteme, anahtar cevabı ve anahtar cevabı alındı bilgisin mesajlarının işlevi detaylı şekilde anlatıldığı için bu aşamada detaylı anlatım yapılmayacaktır. Güncellenen protokol SPDL diline çevrilerek Scyther aracı ile incelenmiş beklenen tüm gizlilik ve kimlik doğrulama gereksinimlerinin karşılandığı görülmüştür. Scyther aracı çıktıları Şekil-4.14'de sunulmuştur.



Şekil 4.13 : İkinci aşamada güncellenen kimlik doğrulama ve anahtar değişim protokolü (aşama-2)



Şekil 4.14 : İkinci aşamada güncellenen protokolün Scyther aracı doğrulama çıktısı (aşama-2)

Aşama-3: Anahtar güncelleme gereksinimi için şemanın genişletilmesi ve doğrulanması

İkinci aşama sonrasında ilk anahtarın alınması ve karşılıklı kimlik doğrulama gereksinimleri karşılanmıştır. Ancak güvenlik protokolünün bir de anahtar güncelleme şemasına ihtiyacı bulunmaktadır. Bu kapsamda aşama-2'de kurulan kimlik doğrulama mekanizmasından yararlanarak yanıtlayıcının anahtar cevabı mesajı içerisine ek olarak ürettiği taze bir kerelik sayısı n_i' değeri bir sonraki ilk anahtar güncelleme mesajında kullanılmak üzere eklenmiştir. Bunun dışında şemaya, biri yeni simetrik grup anahtarı K_sec''i içeren anahtar güncelleme ve diğeri anahtar güncelleme alındı bilgisi olmak üzere iki mesaj eklenmiştir. Tasarlanan yeni şema Şekil-4.15'te sunulmuştur.

Üçüncü şema ile eklenen iki ek mesajın işleme alınması ve işlevleri aşağıda detaylı şekilde sunulmuştur.

- **Anahtar güncelleme (Gönderme):** Yanıtlayıcı biri meydan okuma değeri (n_r') olarak bu güncelleme şemasında diğeri bir sonraki güncelleme şemasında kullanılmak üzere (ni'') iki adet taze bir kerelik sayı üretir. Bir önceki anahtar cevabında başlatıcıya gönderdiği n_i' değerini ise özet fonksiyonundan geçirerek $h(n_i')$ değerini oluşturur. Sonra, $h(n_i')$, ID_r,K_sec',n_r' ve n_i'' değerlerinden oluşan düz metni başlatıcının açık anahtarı $Kpub_i$ ile kriptolar ve başlatıcıya gönderir. Yanıtlayıcı bilir ki bu şifreli metin ancak gerçek başlatıcı tarafından açılabilir.

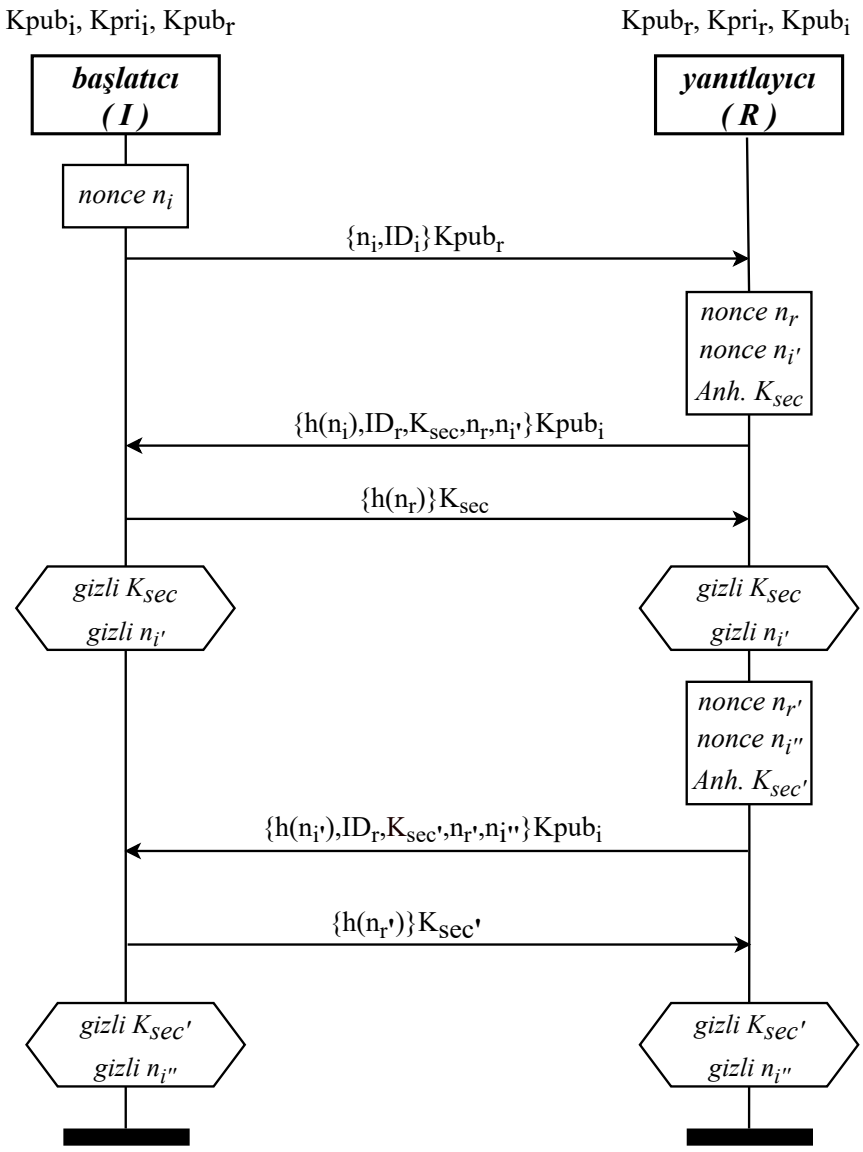
- **Anahtar güncelleme (Alma):** Başlatıcı aldığı şifreli metni gizli anahtarı $Kpri_i$'yi kullanarak düz metine ulaşır ve $h(n_i')$ değerini kontrol eder. Daha önce anahtar cevabı ile gerçek yanıtlıyıcıdan geldiğine emin olduğu n_i' değerinin $h(n_i')$ değeri ile örtüşmesi ile başlatıcı anahtar güncelleme mesajının yanıtlayıcıdan geldiğine emin olur. Bu şekilde yeni simetrik grup anahtarı K_sec''i kullanıma alır. Ayrıca başlatıcı, n_i'' değerini bir sonraki anahtar güncelleme mesajı içerisinde gelecek olan h_ni'' değeri ile karşılaştırmak için güven değeri olarak saklar.

- **Anahtar güncelleme alındı bilgisi (Gönderme):** Başlatıcı anahtar güncelleme mesajı içerisinde gelen n_r' meydan okuma değerini özet fonksiyondan geçirerek

$h(n'_r)$ değerini oluşturur. Sadece bu değerden oluşan düz metni yeni simetrik grup anahtarı K_sec' ile kriptolayarak şifreli mesajı yanıtlayıcıya yollar.

- **Anahtar güncelleme alındı bilgisi (Alma):** Yanıtlayıcı anahtar güncelleme alındı bilgisi mesajını alır ve K_sec' yeni simetrik grup anahtarı ile şifresini çözer. Düz metin içindeki meydan okuma cevabı $h(n'_r)$ değerini meydan okuma değeri n'_r değeri ile karşılaştırır ve bu şekilde güncelleme mesajının başlatıcıya ulaştığından ve anahtar güncelleme şemasının tamamlandığından emin olur.

Üçüncü aşamada tasarlanan şema (Genişletilmiş BKE) SPDL diline çevrilerek Scyther güvenlik protokolünde incelemeye alınmıştır. Sychter çıktıları Şekil-4.16'de sunulmuştur. Çıktılardan görüldüğü üzere gizlilik ve kimlik doğrulama açısından belirlenen kriterlerin sağlandığı görülmüştür.



Şekil 4.15 : Üçüncü aşamada genişletilerek anahtar güncelleme prosedürü eklenen protokol: Genişletilmiş BKE protokolü (aşama-3)

Şekil 4.16 : Genişletilmiş BKE protokolü Scyther aracı doğrulama çıktısı (aşama-3)

4.2.3 Notasyonlar ve açıklama

Önerilen sistem çözümde kullanılan notasyonlar ve açıklamaları Çizelge-4.2 ile verilmiştir.

Çizelge 4.2 : Sistem Çözümünde Kullanılan Notasyonlar

Notasyon	Açıklama
K_{pik}	Önden yüklenmiş simetrik anahtar
$Kpri_r, Kpri_i$	Kök ve düğüm *i* gizli anahtarı
$Kpub_r, Kpub_i$	Kök ve düğüm *i* açık anahtarı
K_{sec}	İkinci simetrik anahtar
${}^*K_{sec}$	*Anahtar Kaynağı*, *Anahtar İndeksi* ve K_{sec}
$K_{sec'}$	Güncellenmiş ikinci simetrik anahtar
${}^*K_{sec'}$	Güncellenmiş ${}^*K_{sec}$
ID_r, ID_i	Kök ve düğüm *i* kimlikleri
n_i	Düğüm *i* tarafından üretilen taze bir kerelik sayı
$n_r, n_{r'}$	Kök tarafından üretilen *meydan okuma* taze bir kerelik sayıları
$n_{i'}, n_{i''}$	Kök tarafından üretilen *güven zinciri* taze bir kerelik sayıları
$h(.)$	Özet fonksiyonu
$\{dzmetin\}_K$	Anahtar K ile şifrelenmiş $dzmetin$

4.2.4 Varsayımlar ve ön hazırlık aşaması

- RPL doğrulanmış modunun birincil varsayımı şudur; *Ksec* ikinci anahtarına sahip yönlendiricilerin meşru ve doğrulanmış olduğu varsayılır. RPL protokolü ikinci anahtara sahip yönlendiriciler arasında çalıştırılır.
- DODAG kökü her zaman güvenilirdir ve kablolu ağ bağlantılarının güvenliği bu çalışmanın kapsamı dışındadır. Kök ile KMS arasındaki herhangi bir iletişimin doğrulanmış ve güvenli olduğu varsayılır. Bu nedenle DODAG kökü, önerilen şema kapsamında hem sunucuyu hem de kendisini temsil eder.

- DODAG kökü, diğer ağ düğümlerine kıyasla daha fazla kaynağa (enerji, hafıza alanı, işlem gücü gibi) sahiptir.

- DODAG kökü, veritabanı bilgilerini bilir veya kablolu kanal aracılığıyla ulaşabilir. Bu bilgiler, kimlik verileri ID_i, diğer düğümlerin açık anahtarları $Kpub_i$ ve kimlikler ile meşru düğümlerin Genişletilmiş Benzersiz Tanımlayıcı (EUI-64) [10] adresleri arasındaki ilişki gibi bilgilerdir.

- Her düğümün özgün bir EUI-64 adresi vardır.

- DODAG root kendi gizli anahtarı $Kpri_r$ 'i ve önden yüklenmiş simetrik anahtarı $Kpik$'i bilir. DODAG kökünün anahtarlarının kötü niyetliler tarafından ele geçirilmeyeceği varsayılır.

- DODAG kökü, ağ oluşumunu tetiklemeden önce mevcut ikinci simetrik anahtar $Ksec$'i bilir ve anahtar güncelleme gerektiğinde güvenli kablolu kanal aracılığıyla yeni ikinci simetrik anahtarlara (yani, $Ksec'$) ulaşabilir.

- Düğümler, ağ devreye alınmadan önce ön yükleme aşamasında üzerlerine yüklenmiş olan kendi açık anahtarları $Kpri_i$'yi ve önden yüklenmiş simetrik anahtarı $Kpik$'i bilirler.

- Düğümümler, DODAG kökünün açık anahtarı $Kpub_r$'yi bilirler. Bu ağ anahtara ağ devreye alınmadan önce ön yükleme yolu ile veya ağ devreye alındıktan sonra kontrol mesajı sinyalleşmesi ile (örneğin DIO'lara ek bir opsiyon alanı olarak eklenmiş şekilde) ulaşmış olabilirler.

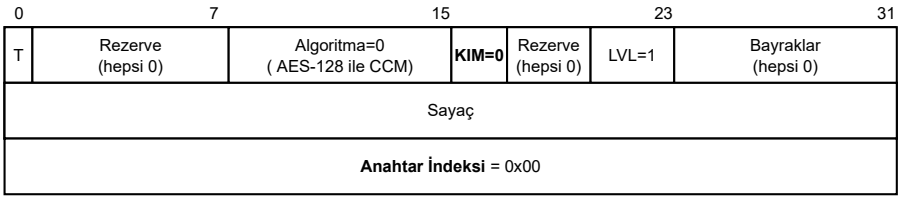
- DODAG kökü ve düğümler tüm güvenlik şeması boyunca üretilen ve kullanılan bir kerelik numaraların (n_i, $n_{i'}$, $n_{i''}$, n_r, $n_{r'}$) taze ve ilk kez kullanışmış değerler olduğuna inanır.

- İkinci simetrik anahtarlar ($Ksec$ and $Ksec'$) güvenli, rastgele ve güçlü simetrik şifreleme anahtarları olarak üretilmiştir.

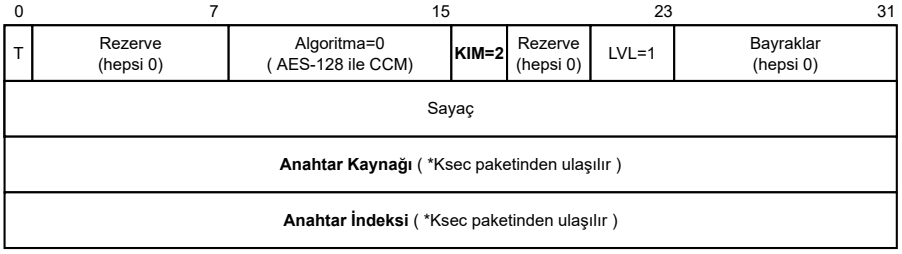
4.2.5 Mesaj yapıları

Kimliği doğrulanmış RPL modunda da önden yüklenmiş RPL moddaki gibi güvenli RPL kontrol mesajları kullanılmaktadır. Ancak, kimliği doğrulanmış mod, kontrol mesajlarını güvenceye almak için iki farklı anahtar kullanır. İlki, ağa katılmak için önceden yüklenmiş olan $Kpik$ anahtarı, diğeri ise bir Yönlendirici olabilmek için gerekli olan ikinci anahtar $Ksec$. Bu iki anahtarın ayrı ayrı kullanıldığı kontrol mesajları, Şekil-4.17 ile gösterdiği gibi iki farklı konfigürasyona sahip güvenlik alanı doğrmaktadır. İki konfigürasyonda da standartta tanımlı olan algoritma yani AES-128 bit CCM çalışma şekli kullanılır. Farklılık gösteren alanlar Anahtar Tanımlama Modu (KIM) ve Anahtar Tanımlıyıcı (Anahtar Kaynağı ve Anahtar İndeksi) alanlarıdır. Önden yüklenmiş modda KIM alanı 0 olarak kullanılır. Bu da anahtar tanımlayıcı olarak sadece Anahatar İndeksini belirtmenin yeterli olacağını ifade etmektedir. Anahtar İndeks'i de önden yüklenmiş anahtar modunda 0x00 olarak tanımlıdır. Kimliği doğrulanmış modda ise, KIM alanı 2 olarak kullanılır. Bu da anahtar tanımlayıcısı olarak hem Anahtar Kaynağı alanının hem de Anahtar İndeksi alanının kullanılması gerektiğini belirtir. Kimliği doğrulanmış modda bu alanlar için anahtar değiişim protokolünde Anahtar sunucusundan alınan $^{*}Ksec$ ikinci anahtar paketi içerisinden ulaşılır.

Kimliği doğrulanmış modda konf,gürasyondan bağımsız tüm RPL kontrol mesajları kritpolu olmalıdır. Kriptosuz ve MAC'i tutmayan mesajlar tüm ağ elemanları tarafından göz ardı edilmelidir. Bunların yanında kimliği doğrulanmış modda RPL kontrol mesajları için bir değişiklik daha mevcuttur. Bu değişiklik genelde DIO mesajı ile birlikte kullanılan DODAG konfigürasyon opsiyonu mesajındadır. Kimliği doğrulanmış modda kullanılan tüm DODAG konfigürasyon opsiyonu mesajlarında Kimlik Doğrulama Aktif bayrağı Şekil-4.18'te görüldüğü şekilde 1'e kurulu olmalıdır.

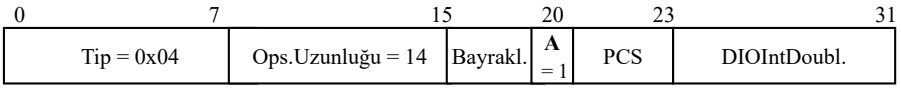


(a)



(b)

Şekil 4.17 : a) Önden yüklemiş mod ve b) kimliği doğrulanmış mod için güvenlik alanları



Şekil 4.18 : DODAG konfigürasyon opsiyonu içindeki 'A' bayrağı

4.2.6 Ana bilgisayar olarak ağa katılma ve ağ davranışları

Güvenli bir ağa katılmak isteyen yeni bir düğüm, önceden yüklenmiş anahtarla kriptolanmış bir DIO mesajı duymak için önce kısa bir süre bekler. Eğer önceden yüklenmiş anahtarla kriptolanmış bir DIO mesajı duymaz ise, komuşu sayısına bağlı olarak, çoğagönderim veya teke gönderim olarak DIS mesajı yollar. Bu DIS mesajını alan ağ düğümleri Trickle zamanlayıcısı aralığını resetleyerek bu mesaja karşılık aynı konfigürasyonda bir DIO mesajı gönderir. Bu DIO mesajında bulunan DODAG konfigürasyon opsiyonu içindeki A bayrağı 1'e kuruludur. DIO mesaj(lar)ını alan düğüm diğer ağ parametrelerini de öğrenerek kendine bir ebeveyn seçer ve ek bir mesaj yollamasına gerek olmaksızın ağa katılır. Eğer DIO mesajının içinde belirtilen DODAG çalışma modu çift yönlü yönlendirme aktif olarak belirtilmiş ise (örneğin; depolama olan mod) ve ağa katılan düğüm sadece ana bilgisayar olarak çalışacaksa

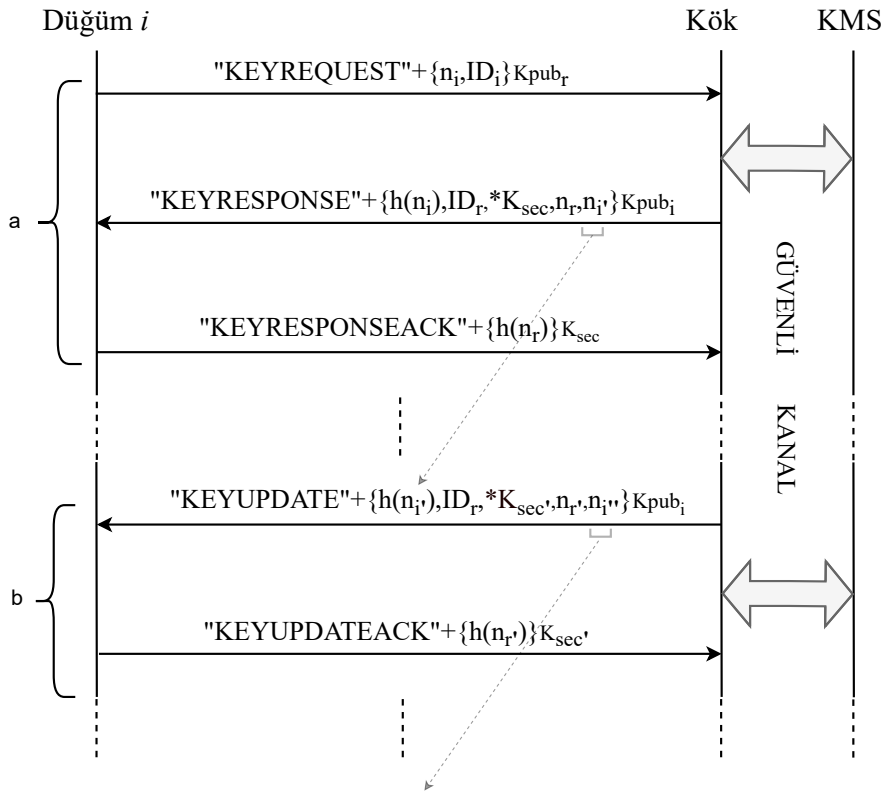
ebeveyn düğümüne kendisini yönlendirme tablosuna eklemesi için Hedef Opsiyonu mesajı içinde sadece kendi IPv6 adresi olan bir DAO mesajı atar. Bu mesajı alan ebeveyn düğüm ana bilgisayarı yönlendirme taablosuna ekler. Bu ana bilgisayara atılan paketler ebeveyn düğümü üzerinden ana bilgisayara düğümüne iletilir. Eğer ana bilgisayar herhangi bir sebepten dolayı Trickle zamanlayıcısını resetlerse attığı DIO mesajlar içerisindeki rank değeri `INFINITE_RANK` olmalıdır. Ana bilgisayar düğümü RPL topolojisinde sadece bir yönlendiriciye bağlı olabilir ve altına herhangi bir çocuk düğüm bağlanamaz. Eğer ana bilgisayar Hedef Opsiyonu adres alanı ve Rank alanında belirtilen değerlenden başka bir değer gönderir ise bu mesajlar diğer ağ düğümleri tarafından ihmal edilir.

4.2.7 Yönlendirici olarak ağa katılma ve ağ davranışları

Kimliği doğrulanmış bir RPL ağında yönlendirici olabilmek için, önden yüklenmiş anahtar ile ağa katılmış olan düğüm bir otorite tarafından doğrulanmalı ve ikinci simetrik anahtara sahip olmalıdır. Bunun için, yönlendirici olmak isteyen düğüm DODAG kökü üzerinden anahtar ve yönetici sunucusu (KMS)'ye ulaşıp kendini doğrulatmalı ve ikinci anahtara sahip olmalıdır. Bu şekilde, ikinci anahtara sahip düğümler, kimliği doğrulanmış yönlendiriciler haline gelir ve bu anahtarla kriptolanmış RPL kontrol mesajlarını kullanılan yönlendiriciler birbirlerine güvenirler.

Yönlendirici adayı düğümler ağa katılmak için ana bilgisayar düğümleri ile birebir aynı prosedürü uygularlar. Bir düğüm ağa katılıp kendine ebeveyn düğüm seçtikten sonra yukarı yönlü yönlendirme yolu kurulmuş olup düğüm DODAG köküne ulaşabilir ve yukarı yönlü standart IP veri paketi yollayabilir duruma gelir. Bu sayede düğüm, Şekil-4.19 ile gösterilen kimlik doğrulama ve anahtar değişim mekanizmasını başlatabilir.

Bu doğrultuda; ilk olarak bir taze rasgele sayı n_i'yi üretir. Sonra bu taze sayı n_i ve kimlik değeri ID_i'den oluşan bir düz metin oluşturur. Bu düz metin DODAG kökünün açık anahtarı $Kpub_r$ ile kriptolanır ve oluşan kriptolu mesaja mesaj tipini belirleyen "KEYREQUEST" sözcüğünü ekler. Oluşturulan bu mesaj anahtar istek mesajıdır.



Şekil 4.19 : Önerilen a) kimlik doğrulama ve anahtar değişim b) anahtar güncelleme şeması

Düğüm oluşturduğu anahtar istek mesajını adresi DODAGID olan DODAG köküne yollar.

Anahtar istek mesajını alan DODAG kökü kriptolu mesajı kendi gizli anahtarı $Kpri_r$'yi kullanarak gelen mesaj içerisindeki ID_i alanına ulaşır. Daha sonra, gelen mesajın kaynak IPv6 adresinden kolayca hesaplanabilen (gönderici düğümün) EUI-64 adresini hesaplar. DODAG kök hesapladığı EUI-64 adresi, IPv6 ve mesaj içindeki ID_i ilişkisinden istekte bulunan düğümün yönlendirici olmaya yetkisinin olup olmadığını kontrol eder. Eğer istekte bulunan düğüm yönlendirici düğüm olmaya yetkili ise DODAG kökü ona göndermek üzere bir anahtar istek cevabı mesajı hazırlar.

Bu amaçla DODAG kökü iki adet taze rasgele sayı üretir, n_r ve $n_{i'}$. Bunlardan ilki olan n_r *meyadan okuma* içindir ve bu mesaja cevaben atılacak olan anahtar cevabı alındı bilgisi mesajında özet fonksiyondan geçmiş hali ile *meydan okuma cevabı* amacı ile eklenecektir. İkinci taze sayı $n_{i'}$ ise DODAG kökü ile düğüm arasında kurulacak *güven zinciri* için başlangıç değeridir ve bir sonraki ilk anahtar güncelleme

mesajında zincirin bir parçası olarak kullanılacaktır. Daha sonra, DODAG kökü $h(n_i)$, DODAG kökünün kimliği ID_r, ikinci anahtar paketi $^*Ksec$, n_r ve $n_{i'}$'den oluşan bir düz metin hazırlanır. $^*Ksec$ paketi içerisinde Anahtar Kaynağı ve Anahtar İndeksi bilgileri ile ikinci anahtarın yer aldığı mesaj paketidir. Hazırlanan bu düz metin anahtar isteğini yapan düğümün $Kpub_i$ ile kriptolanır. Oluşan kriptolu mesajın başına mesaj tipini belirleyen "KEYRESPONSE" sözcüğü eklenir. Hazırlanan anahtar cevap mesajı istekte bulunan düğüme gönderilir.

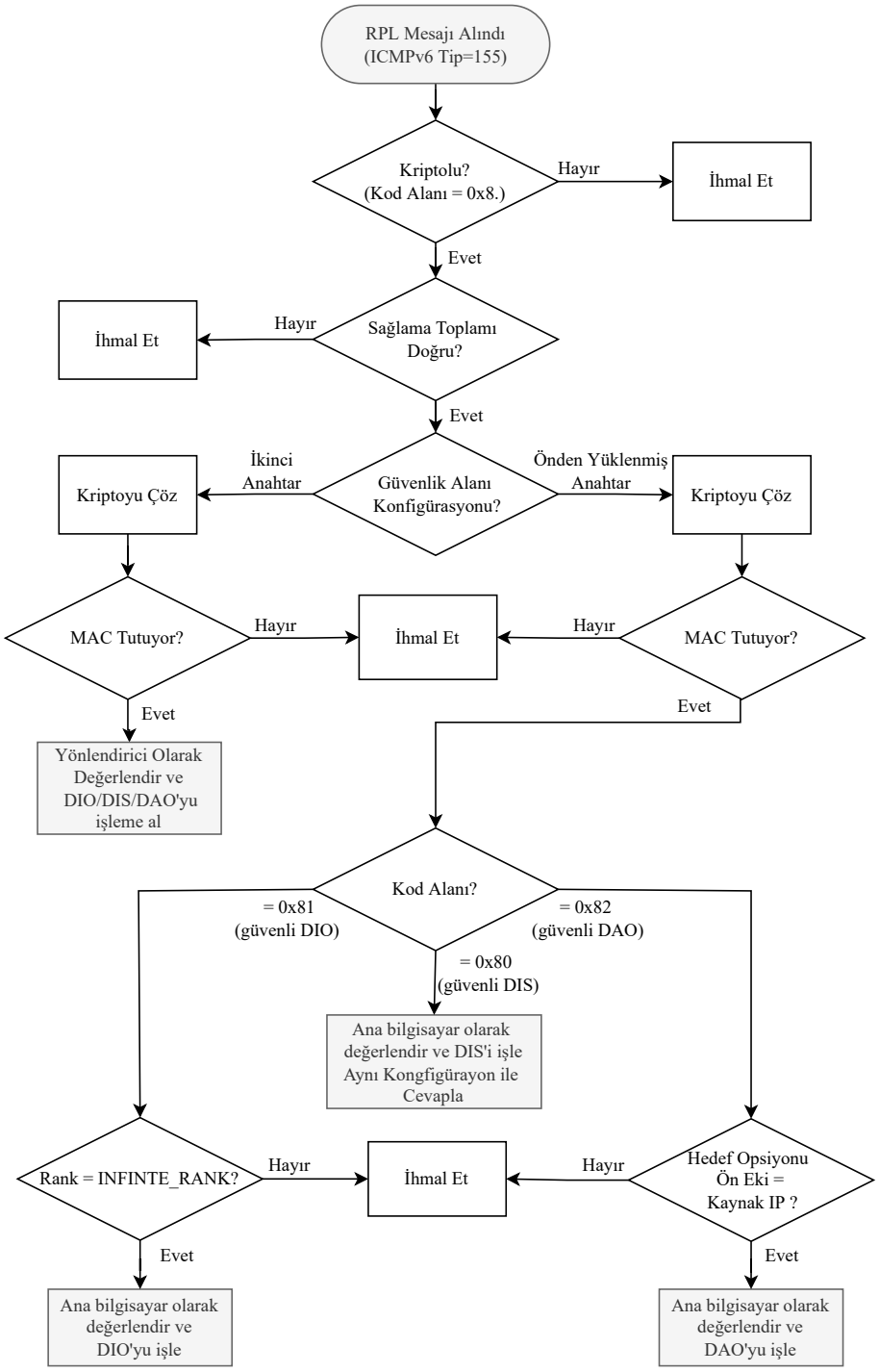
Kriptolu anahtar cevabı mesajını alan düğüm mesajı kendi gizli anahtarı $Kpri_i$ ile çözer ve mesajın gerçek DODAG kökünden gelip gelmediğini anlamak için $h(n_i)$ ve ID_r alanlarını kontrol eder. Çünkü sadece DODAG kökü n_i bilebilir. Eğer düğüm gelen mesajı doğrular ise ikinci anahtar $Ksec$'i devreye alır ve kimliği doğrulanmış yönlendirici düğüm olur. Ancak karşılıklı kimlik doğrulama için DODAG kökü halen *meydan okuma cevabı* beklemektedir.

Bunun için, düğüm (artık kimliği doğrulanmış yönlendirici) $h(n_r)$ değerini $Ksec$ ile kriptolayarak bir kriptolu metin oluşturur. Oluşturulan mu kriptolu metinin önüne mesaj tipini belirtmesi için "KEYRESPONSEACK" sözcüğü eklenir. Sonra oluşturulan anahtar cevabı alındı bilgisi DODAG köküne gönderilir.

DODAG kökü anahtar cevabı alındı bilgisi mesajını alır ve *meydan okuma cevabı*bilgisi $h(n_r)$ değerini kontrol eder ve mesajın kimliği doğrulanmış yönlendirici düğümden geldiğine ve kimlik doğrulama ve anahtar değişim prosedürünün başarıyla tamamlandığına emin olur.

Kimliği doğrulanmış düğüm yani yönlendirici düğüm artık ağ topolojisinin bir parçası olabilir ve bu amaç için ikinci anahtar konfigürasyonuyla RPL kontrol düzlem sinyalleşmesi yapabilir. Eğer DIO mesajınları içinde belirtilen DODAG çalışma modu çift yönlü yönlendirme aktif olarak belirtilmiş ise (örneğin; depolama olan mod) yönlendirici düğüm Hedef opsiyon mesajı içerisinde kendisi ve çocuk düğümleri olacak şekilde bir DAO mesajı ebeveyn düğüme atarak ebeveyn düğümünün yönlendirme tablosunu güncellemesini sağlayacaktır. Bu DAO mesajını alan ebeveyn düğüm bu mesaj ikinci anahtar ile kriptolanmış ise kimliği doğrulamış bir yönlendiriciden geldiğini düşünerek mesajı kabul edecektir ve cevaben DAO mesajıyla

aynı konfigürasyonda DAO-ACK mesajı atacaktır. Kimliği doğrulanmış mod için kontrol düzlemi sinyalleşmeleri ve filtreleme mekanizması Şekil-4.20 ile sunulan akış diyagramı ile daha detaylı incelenebilir.



Şekil 4.20 : Kimliği doğrulanmış yönlendiricinin kontrol mesajlarını alma akışı

4.2.8 Anahtar güncelleme prosedürü

Kimliği doğrulanmış RPL güvenlik modunda kullanılan ikinci anahtar bir simetrik grup anahtarıdır ve ağın güvenlik gereksimine göre kasıtlı veya periyodik olarak güncellenmesi gerekir. Çalışmamız hali hazırda BKE (Bilateral Key Exchange) protokolünü RPL'e adaptasyonunu sağlayarak kimlik doğrulama ve anahtar değişim prosedürüne uygulandı. Daha sonra bu protokol anahtar güncelleme gereksinimi de göz önünde bulundurularak başta kurulan ikili kimlik doğrulamadan yararlanarak ve *güven zinciri* mekanizması içerecek şekilde genişletilmiştir. Kapsamlı kimlik doğrulama ve anahtar değişim mekanizması ve devamındaki anahtar güncelleme prosedürü mesajları Şekil-4.19'te yeniden incelenebilir.

Anahtar güncelleme prosedürünü başlatan ve yöneten ağ birimi KMS sunucusu ile iş birliği içinde DODAG köküdür. Anahtar güncelleme mesajları teke gönderim olduğu için protokol her düğüm için ayrı ayrı koşturulacaktır. DODAG kökü ağın güvenlik ihtiyacı veya konfigürasyonuna göre anahtar güncelleme için düğüm sırasını belirleyebilir. Örneğin, DODAG köküne yakın olan düğümlerden başlayarak ağın daha dışındaki düğümlere doğru ilerleyebilir ya da başka bir ağ konfigürasyonunda kimlik doğrulama yapılma sırasına göre ilerleyebilir.

DODAG kökü anahtar güncelleme başlatmaya karar verdiği zaman güncellemenin başlatılacağı düğüm için anahtar güncelleme mesajı hazırlar. Bu amaç için iki adet teze rasgele sayı üretir, $n_{r'}$ ve $n_{i''}$. Bunlardan birincisi olan $n_{r'}$ bir *meydan okuma*değeridir ve anahtar güncelleme mesajını alan yönlendirici düğümün atacağı anahar güncelleme alındı bilgisi mesajı içerisinde *meydan okuma cevabı* amacı ile kullanılacaktır. İkinci taze sayı olan $n_{i''}$ ise anahtar güncelleme mesajları için *güven zinciri* durumunun takibi için bir sonraki anahtar güncelleme mesajında hedef düğüme güven vermek amacı ile özet fonksiyonu çıktısı ile yeniden kullanılacak olan değerdir. Daha sonra, DODAG kökü $h(n_{i'})$, DODAG kökü kimliği ID_r, güncellenmiş ikinci anahtar paketi ${}^{*}Ksec'$, iki yeni taze sayı n'_r ve $n_{i''}$'den oluşan bir düz metin hazırlar. Hazırlanan bu düz metin hedef yönlendiricinin açık anahtarı $Kpub_i$ ile kriptolanır. Oluşturulan kriptolu mesajın

başına mesaj tipini belirten “KEYUPDATE” sözcüğü eklenir ve anahtar güncelleme mesajı olarak hedef yönlendiriciye gönderilir.

Anahtar güncelleme mesajını alan yönlendirici düğüm ilk olarak kriptolu kendi gizli anahtarı $Kpri_i$ ile çözer ve $h(n_{i'})$ alanını kontrol eder. DODAG kökü $n_{i'}$ değerini kimlik doğrulama ve anahtar değişim aşamasındaki anahtar cevabı mesajında *güven zinciri* değeri olarak göndermişti. Bu kontrol ile anahtar güncelleme mesajının DODAG kökünden geldiğine emin olur. Eğer kontrol sonucunda bir problem yok ise yönlendirici yeni ikinci anahtarı $Ksec'$ devreye alır. Diğer yandan DODAG kökü halen *meydan okuma cevabı* beklemektedir.

Bunu sağlamak için yönlendirici düğüm $h(n_{r'})$ değerini yeni anahtar $Ksec'$ ile kriptolar. Oluşan kriptolu mesaja mesaj tipini belirten “KEYUPDATEACK” sözcüğünü ekler. Daha sonra oluşturulan anahtar güncelleme alındı bilgisi mmesajını DODAG köküne yollar.

Anahtar güncelleme mesajını alan DODAG kökü *meydan okuma cevabı* değeri $n_{r'}$'yü kontrol ederek hem anahtar güncelleme prosedürün tamamlandığını hem de cevabın gerçek yönlendiriciden geldiğini öğrenmiş olur. Çünkü sadece gerçek yönlendirici düğüm $n_{r'}$ değerini bilebilir.

Başarılı bir anahtar güncelleme aşamasından sonra DODAG kökü $n_{i''}$ değerini bir sonraki anahtar güncelleme prosedüründe *güven zinciri* değeri olarak kullanmak üzere saklar. DODAG kökü bir sonraki güncelleme mesajında $h(n_{i''})$ değerini hedef yönlendirici düğüme güven vermek için kullanacaktır.

5. SONUÇ VE ÖNERİLER

Bu tez kapsamında öncelikle RPL mekanizmaları ve literatürdeki mevcut saldırılar detaylı bir şekilde incelenerek RPL'in zayıf noktaları kavranmış ve RPL içerik saldırı özelinde gelecekte daha da çeşitlenebileceği keşfedilmiştir. Daha sonra, literatürdeki RPL güvenlik saldırılarına karşı önerilen güvenlik önlemleri incelenmiş ve bu yöntemlerin birçoğunun RPL içerik saldırılarını önlemekte yetersiz kaldığı fark edilmiştir. Bu doğrultuda ilk olarak, bu tez ile birlikte yeni önerilen ve bir RPL içerik saldırısı olan Trickle zamanlayıcı saldırısı modellenerek RPL içerik saldırılarının RPL ağları üzerindeki yıkıcı etkisi gösterilmiştir. Daha sonra kimlik doğrulama ve anahtar değişim protokolü yine bu tez kapsamında tasarlanıp doğrulması yapılarak standart uyumlu ve iyi kurgulanmış kapsamlı bir RPL kimliği doğrulanmış güvenlik modu tasarlanmıştır. Önerilen tasarım, simetrik ve asimetrik kriptolojik yöntemler ve güven zincirine dayalı karşılıklı kimlik doğrulamalı anahtar kurulumunun yanı sıra ağ elamanlarının davranışlarını da içermektedir.

IoT cihazlarına, yazılımlarını güncellemek, gerekli ağ parametrelerini ve kripto anahtarlarını yüklemek için operasyon alanına (kullanım alanına) göndermeden önce zaten bir ön yapılandırma işlemi uygulanır. Bu aşamada düğümlere yüklenen birkaç fazla küçük veri sayesinde 6LoWPAN kablosuz ağ ortamında doğabilecek haberleşme ve hesaplama yükünü önemli ölçüde azaltmak gayet mantıklı ve uygulanabilirdir. Örneğin, açık ve gizli anahtar üretiminin bu aşamada yapılıp IoT cihazlarına yüklenmesi 6LoWPAN tarafında doğacak haberleşme ve işlem yükünü önemli ölçüde azaltacaktır. Bu nedenle, önerilen çözümde yer alan açık anahtar kriptoloji süreçlerinin bir kısmı radyo tabanlı IoT sistemlerinde ve uygulamalarında zaten önemli bir rol oynayan dağıtım öncesi aşamaya aktarılmıştır.

Sağlam ve güvenli bir ağa sahip olmak için, kriptolojik yöntemden doğacak makul seviyede bir ek yük kabul edilebilir. Ancak, bu sistem RPL'nin adaptif doğasına uygun olarak dikkatle uygulanmalıdır. Örneğin; anahtar güncelleme işlemi periyodik

döngüler ile gerçekleştirilebilir, ağda herhangi bir anormallik tespiti yoksa bu süresi kademeli olarak arttırılabilir. Hatta söz konusu sadece RPL'in güvenliği ise bariz bir saldırı, anahtar çalınması veya ağ deformasyonu yoksa anahtar güncelleme işleminin çok sık bir şekilde yapılmasına gerek yoktur. Öte yandan, kullanım süresi yıllara varacak şekilde uzun olan düşük güçlü kablosuz ağlarda, ilk ağ kurulumu sırasında kimlik doğrulama ve anahtar dağıtım mekanizmasından dolayı doğacak ek zaman yükü, ağ ömrünün yanında ihmal edilecek kadar küçüktür. Aynı doğrultuda, ağda büyük bir problem olduğunda DODAG kökü tarafından başlatılan global onarım gibi kapsamlı bir iyileştirme mekanizmasında tüm ağ yeniden kurulacağı için eklenen kimlik doğrulama ve anahtar dağıtım şemasının doğuracağı yük yine kabul edilebilir seviyede kalacaktır.

RPL'de kimliği doğrulanmış güvenlik modunun kullanılması, asimetrik anahtarlar kullanan veya kullanmayan başka bir hafif IDS ve azaltıcı yönteminin uygulanmasını engel değildir. Aksine, bu tür bir birleştirme RPL'in güvenlik seviyesini arttıracağı gibi fazla enerji harcayacağı durumların önüne geçirebilir. Örneğin, DODAG versiyon artırımında dijital imzanın kullanılması veya anahtar güncelleme zamanını belirlemek amacı ile IDS sistemlerinin kullanılması gibi. Dahası, RPL kimliği doğrulanmış güvenlik modu için bu tez kapsamında önerilen yöntem ile elde edilen kriptolojik anahtarlar 6LoWPAN standartlaşmış protokol yığınının anahtara ihtiyaç duyan diğer katman güvenlik mekanizmalarında da kullanılabilir.

Özetle, 6LoWPAN ağlarında dikkatli şekilde uygulanacak bir kriptolojik yöntem kaçınıldığı kadar fazla ek yük yaratmayacağı gibi RPL içerik saldırılarının önlemesine büyük katkı sağlayacaktır.

KAYNAKLAR

[1] **Sheng, Z.**, **Yang, S.**, **Yu, Y.**, **Vasilakos, A.V.**, **McCann, J.A. ve Leung, K.K.** (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities, *IEEE wireless communications*, *20*(6), 91–98.

[2] **Abbasi, K.M.**, **Khan, T.A. ve Haq, I.U.** (2019). Hierarchical modeling of complex internet of things systems using conceptual modeling approaches, *IEEE Access*, *7*, 102772–102791.

[3] **Li, S.**, **Oikonomou, G.**, **Tryfonas, T.**, **Chen, T.M. ve Da Xu, L.** (2014). A distributed consensus algorithm for decision making in service-oriented internet of things, *IEEE Transactions on Industrial Informatics*, *10*(2), 1461–1468.

[4] **Cisco, U.** (2021). Cisco annual internet report (2018–2023) white paper. 2020, *Acessado em*, *10*(01).

[5] **Group, I.S.** (2016). ITU-TS Recommendation Y.4451 Framework of constrained device networking in the IoT environments.

[6] **Raoof, A.**, **Matrawy, A. ve Lung, C.H.** (2019). Routing Attacks and Mitigation Methods for RPL-Based Internet of Things, *IEEE Communications Surveys Tutorials*, *21*(2), 1582–1606.

[7] **Landsmann, M.**, **Wahlisch, M. ve Schmidt, T.C.** (2013). Topology Authentication in RPL, *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, s.73–74.

[8] **Burrows, M.**, **Abadi, M. ve Needham, R.** (1990). A Logic of Authentication, *ACM Trans. Comput. Syst.*, *8*(1), 18–36, `https://doi.org/10.1145/77648.77649`.

[9] **Crawford, D.M.** (1998). *Transmission of IPv6 Packets over Ethernet Networks*, RFC 2464, `https://www.rfc-editor.org/info/rfc2464`.

[10] **Deering, D.S.E. ve Hinden, B.** (2006). *IP Version 6 Addressing Architecture*, RFC 4291, `https://www.rfc-editor.org/info/rfc4291`.

[11] **Montenegro, G.**, **Hui, J.**, **Culler, D. ve Kushalnagar, N.** (2007). *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, RFC 4944, `https://www.rfc-editor.org/info/rfc4944`.

[12] **Thubert, P. ve Hui, J.** (2011). *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*, RFC 6282, https://www.rfc-editor.org/info/rfc6282.

[13] **Tsiftes, N.**, **Eriksson, J. ve Dunkels, A.** (2010). Low-power wireless IPv6 routing with ContikiRPL, *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, s.406–407.

[14] **Madakam, S.**, **Lake, V.**, **Lake, V.**, **Lake, V.** *ve diğerleri* (2015). Internet of Things (IoT): A literature review, *Journal of Computer and Communications*, *3*(05), 164.

[15] **Alshohoumi, F.**, **Sarrab, M.**, **AlHamadani, A. ve Al-Abri, D.** (2019). Systematic review of existing IoT architectures security and privacy issues and concerns, *Int. J. Adv. Comput. Sci. Appl*, *10*(7), 232–251.

[16] **Al-Sarawi, S.**, **Anbar, M.**, **Alieyan, K. ve Alzubaidi, M.** (2017). Internet of Things (IoT) communication protocols, *2017 8th International conference on information technology (ICIT)*, IEEE, s.685–690.

[17] **Annamalai, P.**, **Bapat, J. ve Das, D.** (2018). Emerging access technologies and open challenges in 5G IoT: From physical layer perspective, *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, IEEE, s.1–6.

[18] **Palattella, M.R.**, **Accettura, N.**, **Vilajosana, X.**, **Watteyne, T.**, **Grieco, L.A.**, **Boggia, G. ve Dohler, M.** (2012). Standardized protocol stack for the internet of (important) things, *IEEE communications surveys & tutorials*, *15*(3), 1389–1406.

[19] **Olsson, J.** (2014). 6LoWPAN demystified, *Texas Instruments*, *13*.

[20] **Alexander, R.**, **Brandt, A.**, **Vasseur, J.**, **Hui, J.**, **Pister, K.**, **Thubert, P.**, **Levis, P.**, **Struik, R.**, **Kelsey, R. ve Winter, T.** (2012). *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, RFC 6550, https://www.rfc-editor.org/info/rfc6550.

[21] **Thubert, P.** (2012). *Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)*, RFC 6552, https://www.rfc-editor.org/info/rfc6552.

[22] **Gnawali, O. ve Levis, P.** (2012). *The Minimum Rank with Hysteresis Objective Function*, RFC 6719, https://www.rfc-editor.org/info/rfc6719.

[23] **Levis, P.**, **Clausen, T.H.**, **Gnawali, O.**, **Hui, J. ve Ko, J.** (2011). *The Trickle Algorithm*, RFC 6206, https://www.rfc-editor.org/info/rfc6206.

[24] **Culler, D.**, **Hui, J.**, **Vasseur, J. ve Manral, V.** (2012). *An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)*, RFC 6554, https://www.rfc-editor.org/info/rfc6554.

[25] **Barthel, D.**, **Vasseur, J.**, **Pister, K.**, **Kim, M. ve Dejean, N.** (2012). *Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks*, RFC 6551, https://www.rfc-editor.org/info/rfc6551.

[26] **Tsvetkov, T.**, **Klein, A.** *ve diğerleri* (2011). RPL: IPv6 routing protocol for low power and lossy networks, *Network*, *59*, 59–66.

[27] **Hui, J. ve Vasseur, J.** (2012). *The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams*, RFC 6553, https://www.rfc-editor.org/info/rfc6553.

[28] **Vasseur, J.**, **Agarwal, N.**, **Hui, J.**, **Shelby, Z.**, **Bertrand, P. ve Chauvenet, C.** (2011). RPL: The IP routing protocol designed for low power and lossy networks, *Internet Protocol for Smart Objects (IPSO) Alliance*, *36*.

[29] **Ali, H.** (2012). *A performance evaluation of rpl in contiki*.

[30] **Gaddour, O.**, **Koubaa, A.**, **Chaudhry, S.**, **Tezeghdanti, M.**, **Chaari, R. ve Abid, M.** (2012). Simulation and performance evaluation of DAG construction with RPL, *Third international conference on communications and networking*, IEEE, s.1–8.

[31] **Raoof, A.**, **Matrawy, A. ve Lung, C.H.** (2018). Routing attacks and mitigation methods for RPL-based Internet of Things, *IEEE Communications Surveys & Tutorials*, *21*(2), 1582–1606.

[32] **Verma, A. ve Ranga, V.** (2020). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review, *IEEE Sensors Journal*, *20*(11), 5666–5690.

[33] **Mayzaud, A.**, **Badonnel, R. ve Chrisment, I.** (2016). A Taxonomy of Attacks in RPL-based Internet of Things, *International Journal of Network Security*, *18*(3), 459–473.

[34] **Wallgren, L.**, **Raza, S. ve Voigt, T.** (2013). Routing attacks and countermeasures in the RPL-based internet of things, *International Journal of Distributed Sensor Networks*, *9*(8), 794326.

[35] **Pongle, P. ve Chavan, G.** (2015). A survey: Attacks on RPL and 6LoWPAN in IoT, *2015 International conference on pervasive computing (ICPC)*, IEEE, s.1–6.

[36] **Tsao, T.**, **Alexander, R.**, **Dohler, M.**, **Daza, V. ve Lozano, A.** (2012). A Security Framework for Routing over Low Power and Lossy Networks, **Internet-Draft draft-ietf-roll-security-framework-07**, Internet Engineering Task Force, https://datatracker.ietf.org/doc/

html/draft-ietf-roll-security-framework-07, work in Progress.

[37] **Perazzo, P.**, **Vallati, C.**, **Anastasi, G. ve Dini, G.** (2017). DIO suppression attack against routing in the Internet of Things, *IEEE Communications Letters*, *21*(11), 2524–2527.

[38] **Watteyne, T.**, **Winter, T.**, **Barthel, D. ve Dohler, M.** (2009). *Routing Requirements for Urban Low-Power and Lossy Networks*, RFC 5548, https://www.rfc-editor.org/info/rfc5548.

[39] **Hu, Y.C.**, **Perrig, A. ve Johnson, D.B.** (2003). Packet leashes: a defense against wormhole attacks in wireless networks, *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, cilt 3, IEEE, s.1976–1986.

[40] **Surendar, M. ve Umamakeswari, A.** (2016). Indres: An intrusion detection and response system for internet of things with 6lowpan, *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, s.1903–1908.

[41] **Glissa, G.**, **Rachedi, A. ve Meddeb, A.** (2016). A secure routing protocol based on RPL for Internet of Things, *2016 IEEE Global Communications Conference (GLOBECOM)*, IEEE, s.1–7.

[42] **Sehgal, A.**, **Mayzaud, A.**, **Badonnel, R.**, **Chrisment, I. ve Schönwälder, J.** (2014). Addressing DODAG inconsistency attacks in RPL networks, *2014 Global Information Infrastructure and Networking Symposium (GIIS)*, IEEE, s.1–8.

[43] **Mayzaud, A.**, **Sehgal, A.**, **Badonnel, R.**, **Chrisment, I. ve Schönwälder, J.** (2015). Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks, *International Journal of Network Management*, *25*(5), 320–339.

[44] **Weekly, K. ve Pister, K.** (2012). Evaluating sinkhole defense techniques in RPL networks, *2012 20th IEEE International Conference on Network Protocols (ICNP)*, IEEE, s.1–6.

[45] **Zhang, K.**, **Liang, X.**, **Lu, R. ve Shen, X.** (2014). Sybil attacks and their defenses in the internet of things, *IEEE Internet of Things Journal*, *1*(5), 372–383.

[46] **Airehrour, D.**, **Gutierrez, J. ve Ray, S.K.** (2017). *Journal of Telecommunications and the Digital Economy*, *5*(1), 50–69, https://search.informit.org/doi/10.3316/informit.752286025338502.

[47] **Airehrour, D.**, **Gutierrez, J.A. ve Ray, S.K.** (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things, *Future Generation Computer Systems*, *93*, 860–876.

[48] **Dvir, A.**, **Buttyan, L.** *ve diğerleri* (2011). VeRA-version number and rank authentication in RPL, *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, IEEE, s.709–714.

[49] **Perrey, H.**, **Landsmann, M.**, **Ugus, O.**, **Schmidt, T.C. ve Wählisch, M.** (2013). TRAIL: Topology authentication in RPL, *arXiv preprint arXiv:1312.0984*.

[50] **Razali, M.**, **Rusli, M.**, **Jamil, N. ve Yussof, S.** (2018). Two phases authentication level (tpal) protocol for nodes authentication in internet of things, *Journal of Fundamental and Applied Sciences*, *10*(2S), 190–200.

[51] **Taylor, C. ve Johnson, T.** (2015). Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks, *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, s.1835–1840.

[52] **Seeber, S.**, **Sehgal, A.**, **Stelte, B.**, **Rodosek, G.D. ve Schönwälder, J.** (2013). Towards a trust computing architecture for RPL in cyber physical systems, *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, IEEE, s.134–137.

[53] **Ferrari, N.**, **Gebremichael, T.**, **Jennehag, U. ve Gidlund, M.** (2018). Lightweight group-key establishment protocol for IoT devices: Implementation and performance Analyses, *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, IEEE, s.31–37.

[54] **Raoof, A.**, **Matrawy, A. ve Lung, C.H.** (2020). Enhancing routing security in iot: Performance evaluation of rpl's secure mode under attacks, *IEEE Internet of Things Journal*, *7*(12), 11536–11546.

[55] **Mridula, R. ve Rajesh, S.** (2013). Group Key Management Techniques, *Global Journal of Computer Science and Technology*.

[56] **Abdelzaher, T.**, **Voigt, T. ve Wolisz, A.** (2010). Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN'10: Foreword, *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN'10*.

[57] **Raza, S.**, **Duquennoy, S.**, **Höglund, J.**, **Roedig, U. ve Voigt, T.** (2014). Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN, *Security and Communication Networks*, *7*(12), 2654–2668.

[58] **Whiting, D.**, **Housley, R. ve Ferguson, N.** (2003). *RFC3610: Counter with CBC-MAC (CCM)*.

[59] **Dunkels, A.**, **Gronvall, B. ve Voigt, T.** (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors, *29th annual IEEE international conference on local computer networks*, IEEE, s.455–462.

[60] **Osterlind, F.**, **Dunkels, A.**, **Eriksson, J.**, **Finne, N. ve Voigt, T.** (2006). Cross-level sensor network simulation with cooja, *Proceedings. 2006 31st IEEE conference on local computer networks*, IEEE, s.641–648.

[61] **Seetha, R. ve Saravanan, R.** (2015). A survey on group key management schemes, *Cybern. Inf. Technol*, *15*(3), 3–25.

[62] **Cremers, C. ve Mauw, S.**, (2012). Operational semantics, Operational semantics and verification of security protocols, Springer, s.13–35.

[63] **Burrows, M.**, **Abadi, M. ve Needham, R.M.** (1989). A logic of authentication, *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *426*(1871), 233–271.

[64] **Dalal, N.**, **Shah, J.**, **Hisaria, K.**, **Jinwala, D.** *ve diğerleri* (2010). A comparative analysis of tools for verification of security protocols, *Int'l J. of Communications, Network and System Sciences*, *3*(10), 779.

[65] **Cremers, C.J.** (2008). The Scyther Tool: Verification, falsification, and analysis of security protocols, *International conference on computer aided verification*, Springer, s.414–418.

[66] **Clark, J.A. ve Jacob, J.L.** (1997). A survey of authentication protocol literature: Version 1.0.

[67] **Mauw, S.** (1997). ITU-TS Recommendation Z. 120: Message Sequence Chart (MSC).

ÖZGEÇMİŞ

Adı Soyadı: Arif Burak ORDU

Doğum Yeri ve Tarihi: Balıkesir/TÜRKİYE, 02.12.1990

E-Posta: ordua@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans:** 2013, İstanbul Teknik Üniversitesi, Elektrik ve Elektronik Fakültesi, Elektronik Mühendisliği
- **Y. Lisans:** 2022, İstanbul Teknik Üniversitesi, Elektronik Mühendisliği

MESLEKİ DENEYİMLER VE ÖDÜLLER:

- Sistem Tasarım Kıdemli Uzman Mühendisi - Haberleşme ve Bilgi Teknolojileri Sektörü ASELSAN A.Ş. *(2014 - günümüz)*

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Ordu, A.B.,** Bayar, M., Ors, B. (2022). "RPL Authenticated Mode Evaluation: Authenticated Key Exchange and Network Behavioral". The 13th International Conference on Ubiquitous and Future Networks (ICUFN'22). *Accepted-Presented*