



**T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI**

**LORAWAN KABLOSUZ HABERLEŞME PROTOKOLÜNÜN GÜVENLİK
ANALİZİ VE LORAWAN KULLANAN İOT CİHAZLARINA KARŞI
YAPILAN SALDIRILARIN İNCELENMESİ VE ANALİZİ**

YÜKSEK LİSANS TEZİ

AHMET FURKAN AĞRAK

DANIŞMAN: PROF. DR. ABDULKADİR TEPECİK

**YALOVA
ARALIK 2021**



T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

LORAWAN KABLOSUZ HABERLEŞME PROTOKOLÜNÜN GÜVENLİK
ANALİZİ VE LORAWAN KULLANAN İOT CİHAZLARINA KARŞI YAPILAN
SALDIRILARIN İNCELENMESİ VE ANALİZİ

YÜKSEK LİSANS TEZİ

AHMET FURKAN AĞRAK
185105018

DANIŞMAN: PROF. DR. ABDULKADİR TEPECİK

YALOVA
ARALIK 2021

ETİK BEYAN

Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü Tez/Proje Yazım Kuralları'na uygun olarak hazırladığım “LORAWAN KABLOSUZ HABERLEŞME PROTOKOLÜNÜN GÜVENLİK ANALİZİ VE LORAWAN KULLANAN IoT CİHAZLARINA KARŞI YAPILAN SALDIRILARIN İNCELENMESİ VE ANALİZİ” başlıklı bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir, aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi taahhüt ve beyan ederim.

Ahmet Furkan AĞRAK



ÖNSÖZ

Yüksek lisans ve tez çalışmam sırasında tüm bilgi ve deneyimini benimle paylaşarak her aşamada yanımda olan değerli danışman hocam Sayın Prof. Dr. Abdulkadir TEPECİK'e göstermiş olduğu ilgi ve anlayış için sonsuz saygı ve şükranlarımı sunarım.

Çalışmalarım sırasında yardım ve desteklerini esirgemeyen tüm arkadaşlarıma sonsuz teşekkür ederim.

Son olarak, hayatım boyunca yanımda olan ve beni koşulsuz destekleyen aileme sonsuz teşekkürlerimi sunarım.

Aralık 2021

Ahmet Furkan AĞRAK



İÇİNDEKİLER

ETİK BEYAN.....	i
ÖNSÖZ	iii
İÇİNDEKİLER	v
SİMGELER VE KISALTMALAR.....	ix
TABLO LİSTESİ.....	xi
ŞEKİL LİSTESİ.....	xiii
ÖZET.....	xv
ABSTRACT.....	xvii
1. GİRİŞ.....	1
1.1. Tezin Amacı	4
1.2. Tezin Yapısı	5
1.3. Literatür Çalışması	5
2. IoT'DE KULLANILAN KABLOSUZ AĞ TEKNOLOJİLERİ	11
2.1. LPWAN (Düşük Güçlü Alan Ağları).....	11
2.1.1. LoRa, Sigfox ve NB-IOT Teknik Farkları.....	12
2.2. LoRa	13
2.3. LoRaWAN.....	15
2.3.1. LoRaWAN Versiyonları/Standartları	17
2.3.2. LoRaWAN Mimarisi ve Bileşenleri.....	20
2.3.3. LoRaWAN Sınıfları	23
2.3.4. LoRaWAN Ağ Katmanları ve Paket Formatları.....	27
2.3.5. LoRaWAN Güvenliği	31
2.3.6. Neden LoRaWAN?	40
3. LoRaWAN ZAAFIYETLERİ VE RİSK ANALİZİ.....	43
3.1. Analiz Metodu.....	43
3.1.1. LoRaWAN Güvenliği İçin Kullanılan Parametrelerin Zayıf Noktaları ve Saldırganın Hedefini Belirlemek	43
3.1.2. Saldırganın Olası Bir Sızmada Hasar Verme Kapasitesinin Tahmini .	45
3.1.3. LoRaWAN Özelliklerinin Tanımı ve Saldırılarına Karşı Zayıflıklarının Tanımlanması.....	46
3.1.4. Saldırı Çeşitlerini Kategorize Etme	46
3.1.5. Saldırı Senaryoları.....	48
3.2. LoRaWAN'a Karşı Yapılabilecek Saldırıları.....	48
3.2.1. Dinleme (Eavesdropping) Saldırısı	48



3.2.2.	Bit-Flipping Saldırısı.....	54
3.2.3.	Tekrarlama (Replay) Saldırısı	57
3.2.4.	ACK Spoofing Saldırısı	62
3.3.	Risk Analizi	66
3.3.1.	Risk Değerlendirme Metodolojisi	67
4.	SALDIRI ENGELLEME VEYA ETKİSİNİ AZALTMAYA YÖNELİK ÇÖZÜMLER.....	71
4.1.	Dinleme (Eavesdropping) Saldırısı	71
4.1.1.	Saldırı Engelleme veya Etkisinin Azaltılması.....	71
4.1.2.	Öneriler	72
4.2.	Bit Flipping Saldırısı	73
4.2.1.	Saldırı Engelleme veya Etkisinin Azaltılması.....	73
4.2.2.	Öneriler	74
4.3.	Tekrarlama (Replay) Saldırısı	74
4.3.1.	Saldırı Engelleme veya Etkisinin Azaltılması.....	74
4.3.2.	Öneriler	75
4.4.	ACK Saldırısı	75
4.4.1.	Saldırı Engelleme veya Etkisinin Azaltılması.....	75
5.	SONUÇ.....	77
	KAYNAKÇA.....	81



SİMGELER VE KISALTMALAR

Simgeler

ED	Uç Cihaz
Mb	Megabit

Kısaltmalar

ABP	Kişiselleştirme ile Aktivasyon
ADR	Adaptif Veri Hızı
AES	Gelişmiş Şifreleme Standartı
AMQP	Advanced Message Queuing Protocol
CoAP	Constrained Application Protocol
DoS	Denial of Service
DDoS	Dağıtık Hizmet Engelleme
GPS	Global Positioning System
GW	Ağ Geçidi
http	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IoT	Nesnelerin İnterneti
IP	İnternet Protokolü
ISM	Industrial Scientific Medical
LPWAN	Düşük Güçlü Geniş Alan Ağı
MAC	Media Access Control
MHDR	MAC Başlığı
MIC	Mesaj Bütünlük Kodu
MITM	Ortakdaki Adam
MQTT	Message Queuing Telemetry Transport
OTAA	Havadan Aktivasyon
SF	Yayılma Faktörü
SSH	Secure Shell
RFID	Radio-Frequency Identification
TTN	The Things Network
TCP	Transmission Control Protocol
Telnet	Telemetry Network
QoS	Quality of Service
Wi-Fi	Wireless Fidelity
WSN	Kablosuz Sensör Ağı

TABLO LİSTESİ

Tablo 1.1. Ağ Teknolojilerinin Karşılaştırması	3
Tablo 2.1. LoRaWAN, NB-IoT, Sigfox karşılaştırma tablosu	12
Tablo 2.2. Lora, NB-IoT, Sigfox Maliyet Karşılaştırması [46]	13
Tablo 2.3. Farklı Yayılım Faktörleri için Bit ve Sembol Oranı [56]	14
Tablo 2.4. LoRa Hata Algılama ve Düzeltme Oranları [57].....	14
Tablo 2.5. LoRa ISM Frekans Özellikleri [59]	15
Tablo 2.6. SF ve karşılığındaki işaret/Chirp uzunluğu [58].....	15
Tablo 2.7. Anahtar özellik tablosu	34
Tablo 3.1. LoRaWAN ağı güvenliği için kullanılan değerler	43
Tablo 3.2. LoRaWAN ağına karşı olası saldırılar.....	47
Tablo 3.3. ACK Spoofing saldırısı sonucu [88].....	66
Tablo 3.4. Saldırı etki değerlendirme tablosu	67
Tablo 3.5. Saldırı olasılık değerlendirme tablosu	68
Tablo 3.6. Risk değerlendirme tablosu	68
Tablo 3.7. Niteliksel Risk Analizi Tablosu.....	69
Tablo 4.1. Bu çalışmada incelenen saldırıların genel özeti.....	71



ŞEKİL LİSTESİ

Şekil 2.1. Sigfox, LoRa, NB-IoT Genel Karşılaştırması [46]	13
Şekil 2.2. Örnek bir LoRaWAN Yıldız Topolojisi	16
Şekil 2.3. LoRaWAN versiyonları tarihçesi	20
Şekil 2.4. Örnek Bir LoRaWAN Mimarisi	22
Şekil 2.5. LoRa Protokol Yığını [74]	23
Şekil 2.6. A sınıfı uç cihazların alım penceresi diyagramı	24
Şekil 2.7. A Sınıfı Yukarı ve aşağı bağlantı pencereleri	25
Şekil 2.8. B Sınıfı Alım Penceresi Diyagramı [75]	26
Şekil 2.9. LoRaWAN Katmanları	27
Şekil 2.10. Yukarı bağlantı (UL) Fiziksel Katman Mesaj Formatı [68]	28
Şekil 2.11. Aşağı bağlantı (DL) Fiziksel Katman Mesaj Formatı [68]	28
Şekil 2.12. LoRaWAN Çerçeve Yapıları	29
Şekil 2.13. MAC Katmanı Çerçeve Yapısı	29
Şekil 2.14. MAC katmanındaki mesaj tipleri	30
Şekil 2.15. MAC başlığı (MHDR) içeriği [68]	30
Şekil 2.16. MAC yükü içeriği [68]	30
Şekil 2.17. FHDR içeriği [68]	30
Şekil 2.18. OTAA Metodu	33
Şekil 2.19. ABP Metodu	34
Şekil 2.20. Oturum Anahtarlarının Kullanımı	35
Şekil 2.21. OTAA metodunda oturum anahtarları değişimi	36
Şekil 2.22. LoRaWAN Encryption modu ile CTR modu karşılaştırılması	37
Şekil 2.23. ECB cipher blok modu	38
Şekil 3.1. LoRaWAN için Dinleme Saldırısı	50
Şekil 3.2. Dinleme (Eavesdropping) saldırısı örneği	51
Şekil 3.3. Eavesdropping saldırısı için örnek bir kurulum	52
Şekil 3.4. 24 farklı denemede doğru sonuç için olası aday sayısı [87]	54
Şekil 3.5. Bit-Flipping saldırı şeması	56
Şekil 3.6. Örnek bir Bit-Flipping saldırısı sonucu [87]	57
Şekil 3.7. Bir Tekrarlama (Replay) saldırısı örneği	59
Şekil 3.8. Tekrarlama saldırısı için kurulum şeması	60
Şekil 3.9. Kötü niyetli ağ geçidinin kayıtları [39]	62
Şekil 3.10. Hedef sunucunun logları [39]	62



LORAWAN KABLOSUZ HABERLEŞME PROTOKOLÜNÜN GÜVENLİK ANALİZİ VE LORAWAN KULLANAN İoT CİHAZLARINA KARŞI YAPILAN SALDIRILARIN İNCELENMESİ VE ANALİZİ

ÖZET

Bu tez çalışmasında, ağ kapasitesi, ağ güvenliği, pil ömrü, düşük maliyeti ve veri iletim yetenekleri bakımından iyi bir LPWAN adayı olan LoRaWAN protokolü, hakkında yapılan güvenlik ile ilgili çalışmaların sayıca az olmasından dolayı güvenlik zafiyetleri ve riskleri incelenmek ve analiz edilmek üzere seçilmiştir. Nesnelerin İnterneti kavramı incelenip ağ çeşitleri ve yapıları araştırılmış ve LoRaWAN protokolü ile karşılaştırılmıştır. Ardından IoT ağlarına yönelik yapılan saldırılar ve üreticiler tarafından alınan tedbirler ile bu konu üzerine yapılan benzer akademik çalışmalar incelenmiştir. Çalışmanın ana konusu olan LoRaWAN, versiyonları, mimarisi, komponentleri, sınıfları ve ağ katmanları alt başlıklarında detaylıca açıklanmış ve bu protokolün güvenliği başka bir ana başlık altında detaylı olarak incelenmiştir. Zafiyetler, güvenlik riskleri ve saldırı çeşitleri kategorize edilip detaylı olarak açıklanmış ve bu saldırı çeşitlerinin etkileri bakımından risk değerlendirilmesi yapıp risk analizi ortaya çıkarılmıştır. Elde edilen bulgular değerlendirilerek, LoRaWAN protokolünün zafiyetleri ve bu ağa karşı yapılan saldırı çeşitlerinin her biri için ayrı ayrı ve genel olarak saldırıların engellenmesi veya etkisinin azaltılmasına yönelik çözümler önerileri son kullanıcılar için sunulmuştur.

Anahtar Kelimeler: LoRaWAN, IoT, Protokol, Nesnelerin İnterneti, LPWAN.



SECURITY ANALYSIS OF LORAWAN WIRELESS COMMUNICATIONS PROTOCOL AND EXAMINATION AND ANALYSIS OF ATTACKS AGAINST IOT DEVICES USING LORAWAN

ABSTRACT

In this thesis, the LoRaWAN protocol, one of the good LPWAN in terms of network capacity, network security, battery life, low cost and data transmission capabilities, was chosen to examine and analyse its security vulnerabilities and risks because of the few studies on security. The concept of the Internet of Things, network types and structures were examined and compared with the LoRaWAN protocol. Then, attacks on IoT networks, measures taken by manufacturers and similar academic studies on this subject were examined. The main subject of the study, LoRaWAN, is explained in detail in its versions, architecture, components, classes and network layers, and the security of this protocol is examined in detail under another main heading. The vulnerabilities, security risks and types of attacks were categorized and explained in detail. Then, a risk assessment was made in terms of the effects of these attack types and a risk analysis was revealed. By evaluating the findings obtained, solutions for the vulnerabilities of the LoRaWAN protocol and for each of the types of attacks against this network, to prevent or reduce the effects of attacks were presented separately.

Keywords: LoRaWan, Iot, Protocol, Internet of Things, LPWAN.



1. GİRİŞ

Günümüzde teknolojinin hızla gelişmesiyle ve internetin yaygınlaşmasıyla, gündelik hayatta kullandığımız birçok cihaz kendi arasında haberleşebilmekte ve internete bağlanabilmektedir. İnternete bağlanan cihazların sayısının artması ile birlikte ağ kavramının tanımı değişmiştir. Bununla birlikte yeni teknolojilerin ortaya çıkmasına da vesile olmuştur. Bu teknolojilerden biri de IoT'dir. Nesnelerin İnterneti kavramının orijinali olan Internet of Things (IoT) ilk defa 1999 yılında Kevin Ashton tarafından kullanılmıştır [1]. IoT teknolojisi etrafımızdaki cihazların değişimi ve gelişimini sağlamış ve nesnelerin akılcılaşmasına katkıda bulunmuştur [2], [3].

IoT teknolojisi, milyonlarca cihazı farklı platformlarda ve farklı protokollerle birbirine bağlayarak birbiri arasında haberleşmelerini sağlamakta, doğrudan veya dolaylı olarak internete bağlanmalarını sağlamaktadır. Bu sayede hayatımızı kolaylaştırmakta, tarım, sanayi, sağlık, ulaşım ve günlük hayatta kullanılan diğer alanlarda işleri kolaylaştıran ve hızlandıran akıllı ortamlar yaratmayı amaçlamaktadır.

Birçok uygulama alanı olan IoT cihazlar, akıllı şehirler, trafik yoğunluk takibi, yabani hayvanların yaşamlarının takibi, askeri alanlar gibi birçok alanda karşımıza çıkmakta ve bu alanlar sürekli olarak genişleme göstermektedir. Özellikle sağlık alanında yaşam kalitesini arttıracak pek çok uygulama geliştirilmiş ve geliştirilmeye devam etmektedir. Sağlık alanındaki bazı IoT uygulamalarının sunduğu bazı senaryolar ve çözümleri şöyledir: Acil servislerdeki yoğunluğa çözüm aranmış ve geliştirilen bir uygulama ile New York'ta bir hastanenin hastalarının yarısının acil servis bekleme sürelerinin etkili bir şekilde azaldığı gözlemlenmiştir. Diğer bir uygulama da ise hastaların hastaneyi veya acil servisi ziyaret etme zorunluluğunu ortadan kaldırarak uzaktan sağlık ve izleme hizmeti sağlamaktır. Bu uygulama sayesinde maliyet ve ulaşım zorluğu gibi etkenlerin minimuma indirilmesi planlanmıştır. Hastanelerdeki diğer bir sorun ise kritik tıbbi donanımların arıza yapma riskleridir. Bu risklerin önceden anlaşılabilmesi ve çözüm üretilebilmesi için elektronik alet üreten teknoloji firması Philips, "E-Alarm" adı verilen bir sistem geliştirmiştir. Bu sistem cihazlarla etkileşim kurarak arıza riskini ve olası çözüm önerilerini kullanıcıya sunmaktadır. Bir diğer uygulama ise hastanelerde personel, hastalar ve kaynakların takibi gibi günlük aktivitelerin izlenmesi ve bunu asgari maliyetle gerçekleştirmek için gerçek zamanlı konumlandırma sistemleri ile çözümlerdir. IoT uygulamaları çok geniş bir alanda

farklı uygulamalar sunarak geliştirilmiş ilaç ve bağımlılık takibi, kronik hastalık tespit etme gibi fütüristik çözümler sunmakta ve her geçen gün hayatımızda daha çok yer edinmektedir [4].

2021 yılında 25 milyar cihazın internete bağlanacağı [5] ve M2M bağlantı sayısının 2022 yılında 12,3 milyara ulaşp kişi başı 1.5 cihazı düşeceği tahmin edilmekte, 2030 yılına kadar internete bağlı nesnelerin sayısının 500 milyarı geçmesi beklenmektedir [6], [7].

IoT ekosisteminin çalışma prensibi, veri toplamak, bu verileri işlemek, veri göndermek ve alınan komuta göre işlem yapmak üzerinedir. Bunları yapmak için ihtiyaç duyduğu bileşenler ise genel olarak sensörler/cihazlar, ağ geçidi (gateway), bulut ve bir arayüzdür. Veri toplamak için sensörler kullanılırken bu verileri işlemek gömülü işlemcilerin görevidir. Sensörler ısı, ışık, nem, hareket, basınç gibi birçok çevresel olayı ölçebilen ve bu verileri göstermek veya göndermek gibi yeteneklere sahip olan cihazlardır. Bir sensörde ölçülen veri ağ üzerinden gönderilir. Bu noktada ağ geçitlerine ihtiyaç duyulur. Ağ geçitleri, sensörler ile bulut gibi verinin iletileceği ve kaydedileceği yapılar arasında veri iletişimini sağlar. Bir ağ geçidine birçok sensör bağlanabilir. Veri iletimi tek yönlü veya çift yönlü olabilir. Sensörlerden gelen veriler ağ geçitleri üzerinden hedefe varabileceği gibi komutları da ağ geçitleri üzerinden alırlar. Nesnelerden gelen verilerin bir veri tabanında tutulması ve işlenilmesi için Bulut gibi yapılar kullanılır. Arayüz ise cihazları tek bir merkezden takip etmeyi ve kontrol etmeyi sağlamaktadır.

IoT cihazlarının birbirleri ile haberleşmeleri için birçok ağ teknolojisi ve protokol vardır. Burada dikkat edilecek hususlar yüksek güvenilirlik, uygulama yapılandırma yetenekleri, cihaz düzeyinde trafik izleme ve yönetme, minimum gecikme ile gerçek zamanlı veri iletimi, çok sayıda cihaz bağlama kapasitesi, iletişim menzili, parazite karşı dayanıklılık, pil ömrü, ağ kapasitesi ve güvenliği, tek ve çift yönlü iletişim gibi hususlardır.

IoT uygulamalarında LAN (Yerel alan ağları), PAN (Kişisel alan ağları), WAN (Geniş alan ağları), LPWAN (Düşük güçlü geniş alan ağları) gibi ağ yapıları kullanılmaktadır. Bu uygulamalarda yaygın kullanılan kablosuz ağ teknolojileri ise, Bluetooth, Zigbee, WiFi, Hücresel ağlar (2G, 3G, 4G, 5G) ve NB-IoT, Sigfox, LoRaWAN

teknolojileridir. Bu ağ yapıları ve teknolojilerinin kendi aralarında bazı avantaj ve dezavantajları bulunmaktadır. Bundan dolayı bir IoT uygulamasında ağ yapısı ve teknolojisi seçimi önem arz etmektedir. Bir akıllı tarım uygulaması için kısıtlı batarya ve uzun menzil gibi gereksinimleri karşılayacak bir ağ yapısı gerekirken bir akıllı bina uygulamasında en öncelikli faktör hız olabilir. Bu durumdan dolayı IoT uygulamaları için uygun bir ağ yapısı seçimi düşük enerji, uzun menzil, hız ve tek seferde taşınabilen veri paketi büyüklüğü gibi faktörler göz önüne alınarak ihtiyaçlara göre değişebilmektedir. Tablo 1.1’de ağ sistemlerinin karşılaştırılması gösterilmiştir [8], [9], [10].

Tablo 1.1. Ağ Teknolojilerinin Karşılaştırması

	BLE	Wi-Fi	Z-Wave	ZigBee	LTE-M	NB-IoT	Sigfox	LoRaWAN	GPRS	6LoWPAN
Ortalama Menzil	50m	100m+	30m	100m	2.5-5km	20km+	10km+	10km+	35km+	10-100m
Ağ Tipi	PAN	LAN	PAN	PAN	LPWAN	LPWAN	LPWAN	LPWAN	WAN	PAN
Frekans	2.4G Hz	2.4GHZ / 5GHZ	908.42M Hz	2.4GHz	Değişken	Değişken	868/902 MHz	470-510Mhz 865-925MHz	850MHz / 1.9GHz	2.4GHz
Bant genişliği	1MHz	20MHz	-	3MHz	-	180KHz	100KHz	125KHz	-	-
Hız	1Mbps	100-250Mbps	100Kbps	250Kbps	1Mbps	250Kbps	100bps	0,3-50kbps	85kbps	250Kbps
Paket boyutu	47 bytes	2304 Bytes	64 Bytes	127 Bytes	-	-	12 Bytes	256 Bytes	-	-
Standart	IEEE 802.15.1	IEEE 802.11	Z-Wave Alliance	IEEE 802.15.4	3GPP	3GPP	IEEE 802.15.1	IEEE 802.15.g	ETSI	IEEE 802.15.4
Güç Tüketimi	10m W (+yıl)	Yüksek (hafta)	Çok Düşük (+yıl)	Çok Düşük (+yıl)	Orta (ay)	Orta (ay)	Çok Düşük (+yıl)	Çok Düşük (+yıl)	Yüksek (hafta)	Çok Düşük (+yıl)
Kurulum Maliyeti	Bir defaya mahsus	Bir defaya mahsus	Bir defaya mahsus	Bir defaya mahsus	Yinelenen	Yinelenen	Yinelenen	Bir defaya mahsus	-	-
Modül maliyeti	5\$ Altı	10\$ Altı	10\$ Altı	8-15\$	8-20\$	8-20\$	5\$ Altı	8-15\$	-	-
Topoloji	P2P, Star, Mesh	Star, Mesh	Mesh	Mesh	Star	Star	Star	Star	Star	Star
2019 yılındaki dağıtım adedi (milyon)	3,500+	3,200+	120+	420+	7+	16+	10+	45+	-	-
ISM Bandı	Evet	Evet	Evet	Evet	No	Evet	Evet	Evet	Hayır	-

IoT teknolojisinin hızla gelişmesi ve yaygınlaşması sonucunda bazı protokollerin kısıtlı ve yetersiz kaldığı görülmüş ve bu durumdan dolayı bazı çözümler sunulmuştur. Örneğin IPv4 protokolünün yetersiz kalmasından dolayı IPv6 protokolüne geçiş bunlardan biridir [11]. Diğer taraftan bu cihazların yaygınlaşması, kötü niyetli kişilerin ilgisini çekmesiyle ve zararlı yazılımların artması ile sonuçlanabilmektedir.

Klima, Buzdolabı, süpürge ve kapılar gibi akıllı ev sistemlerine müdahil cihazların internete bağlanması, bu aletleri izleyip takip edebilme ve uzaktayken bir merkezden kontrol edebilme her ne kadar hayatımızı kolaylaştırır da bir o kadar da gözetlenme, gizlilik ve güvenlik risklerini arttırmaktadır. Gizlilik ve güvenlik farklı kavramlardır. Gizlilik, kişisel bilgilerin ve geçmiş kayıtların izlenmesin engellenmesini amaçlamaktadır. Güvenlik ise kişisel bilgilere ve verilere istenmeyen kişilerce erişilmesini engellemeyi amaçlar.

IoT cihazlarında amaç hayatı kolaylaştırmaktır. Fakat üretim ve kurulum kaynaklı hatalar ve eksiklikler, cihazların savunmasız kalmasına, kötü amaçlı kişilere fırsat vermesine sebep olabilmektedir. Özellikle son yıllarda yapılan DoS saldırılarının çoğunluğu ve en etkililerinin IoT cihazlarından geldiği tespit edilmiştir. Bu tip saldırılarda ele geçirilmiş IoT cihazlarının tek bir merkezden yönetiliyor olması ve aynı anda saldırı gerçekleştirilmesi sonucunda hedefe önemli ölçüde zarar vermektedir [12]. Bundan dolayı gelecekte siber güvenlik endüstrisinin en büyük sorunlarının başında IoT botnetler olacağı düşünülmektedir [13].

Günümüzde artan siber saldırılara karşı güvenlik çözümleri de gelişmekte ve bu saldırılara karşı tespit etme ve koruma sağlanmaktadır. Bu çözümler, anti virüsler, güvenlik duvarları, içerik filtreleme ve paket analizi gibi kullanımı uzmanlık gerektiren uygulamalardır. Bu tür uygulamalar saldırının tespiti ve önleme konusunda etkili olsalar da küçük ölçekli ağlarda maliyetinden dolayı kullanıcılar tarafından tercih edilmemektedir. Ayrıca IoT cihazlarının kısıtlı işlemci gücü ve enerjilerinden dolayı bu çözümlerin pek uygun olmadığını da unutmamak gerekmektedir.

1.1. Tezin Amacı

Bu çalışmada ağ kapasitesi, ağ güvenliği, pil ömrü, düşük maliyeti ve veri iletim yetenekleri bakımından iyi bir LPWAN adayı olan LoRaWAN, hakkında yapılan güvenlik ile ilgili çalışmaların sayıca az olmasından dolayı güvenlik zafiyetleri ve riskleri incelenmek ve analiz edilmek üzere seçilmiştir. IoT ağlarına yönelik yapılan

saldırılar ve üreticiler tarafından alınan tedbirler ile bu konu üzerine yapılan benzer akademik çalışmalar incelenmiştir.

Elde edilen bulgular değerlendirilerek LoRaWAN teknolojisinin zafiyetleri ve bu ağa yönelik saldırı çeşitleri sınıflandırılarak detaylıca incelenmiş, risk analizi yapılmış ve zafiyetlere yönelik genel önlemler ile saldırıların engellenmesi veya etkisinin azaltılmasına yönelik çözüm önerileri sunulmuştur.

1.2. Tezin Yapısı

I. Bölümde IoT hakkında genel bilgiler verilmiş ve temel gereksinimler ile ağ çeşitleri ve yapılarından bahsedilmiş, ayrıca literatür taraması yapıp benzer çalışmaların özetleri sunulmuştur.

II. Bölümde IoT kablosuz ağ teknolojilerinden LPWAN genel olarak bahsedilmiş ve Lora ve LoRaWAN detaylı bir şekilde açıklanmıştır.

III. Bölümde LoRaWAN yönelik güvenlik tehditleri ve bu protokolün zafiyetlerinden detaylı olarak bahsedilmiş, saldırılar kategorize edilip saldırı çeşitlerinden bahsedilmiş ve detaylı olarak incelenmiştir. Ardından bu saldırıların etkileri bakımından karşılaştırma yapılmış ve detaylı bir risk analizi ortaya çıkarılmıştır.

IV. Bölümde ise LoRaWAN protokolünün güvenlik tehditlerine yönelik genel önlemler ve saldırıların engellenmesi veya etkisinin azaltılmasına yönelik çözümler önerilmiştir.

V. Bölümde bu çalışmanın sonucu ortaya konulmuştur.

1.3. Literatür Çalışması

IoT ortamında kullanılan çeşitli iletişim teknolojilerinden biri olan LPWAN ağları düşük enerji tüketimi ve düşük maliyetlerinin yanı sıra uzun menzilleri sebebiyle, düşük enerji tüketimi olan fakat menzilleri kısa olan Bluetooth, Zigbee ve Z-Wave veya uzun menzilli fakat yüksek maliyetli olan hücresel ağlar gibi iletişim teknolojilerinin arasından sıyrılıp sınırlı kaynağı olan IoT cihazlarında popüler olmuştur [14]. Bu LPWAN ağlarından yakın zamanda ortaya çıkan ve en rekabetçilerinden teknolojilerden biri ise LoRaWAN'dır [15]. Bu bölümde sayıca az olan LoRaWAN ve LoRaWAN güvenliği ile alakalı akademik çalışmalar aşağıda özetlenmiştir.

LoRaWAN için Çift Anahtar Tabanlı Aktivasyon Şeması başlıklı çalışmada [20], LoRaWAN anahtar güncellemesinde ve oturum anahtarı oluşturma sırasındaki bazı güvenlik boşluklarından bahsedilmiştir. LoRaWAN için çift anahtar tabanlı bir aktivasyon şeması önerilmiş ve bu önerinin tam desteklenmeyen anahtar güncellemelerinin yaratacağı güvenlik sorununa iyi bir çözüm olabileceği üzerinde durulmuştur.

LoRaWAN İçin Gelişmiş Bir Anahtar Yönetim Planı adlı makalede [31], 2017 yılının sonlarına doğru yayınlanan LoRaWAN 1.1 versiyonunun genel güvenlik şeması incelenmiş ve anahtar yönetimi açısından daha da geliştirilebilir olduğu üzerinde durulmuştur. LoRaWAN 1.1 güvenliği üzerinde yapılan incelemede kök anahtar güncelleme şemasına sahip gelişmiş bir LoRaWAN güvenliği önerilmiştir.

Elkhodr ve sunduğu karşılaştırmalı bir çalışmada [33], IoT iletişim teknolojileri üzerine genel bir araştırma yapılmış ve LoRaWAN, NB-IoT, Z-Wave, ZigBee, 6lowpan, WiMax, Wi-Fi, Bluetooth gibi teknolojiler hakkında detaylı açıklama yapılmıştır. Bu teknolojilerin kullanım alanları tartışılmış ve genel bir görünüm için bu teknolojilerin enerji ihtiyacı, ağ yapıları, güvenlik, menzil gibi özellikleri karşılaştırılmış ve grafiklerle gösterilmiştir.

Akıllı Şehirlerde Kablosuz Haberleşme Teknolojileri ve Doğru Teknoloji Seçimi adlı makalede [37], akıllı şehirler için hızla gelişen dijital altyapı bileşenlerinden olan güçlü ve hassas ölçümler yapabilen sensörler vb. gibi uç cihazlarının haberleşme gereksinimleri ve gelişmekte olan haberleşme ağları ve verimli altyapılar üzerinde durulmuştur. Sürekli gelişen bu kablolu haberleşme teknolojilerinin yanında, akıllı şehirler için ayrı bir önemi olan Düşük Güçlü Geniş Alan Ağları Teknolojileri (NB-IoT, Sigfox, Lora), Kısa Mesafe Kablosuz Haberleşme Teknolojileri (Z-Wave, Zigbee, Bluetooth) ve Hücreli Haberleşme Teknolojileri (GPRS, 2G, 3G, 4G, LTE) gibi haberleşme teknolojileri incelenmiş ve akıllı şehirlerin gereksinim ve ihtiyaçlarına göre doğru teknoloji seçimi üzerine çalışılmıştır.

Düşük Güçlü Geniş Alan Ağları başlıklı bir analiz çalışmasında [32], LPWAN teknolojileri araştırılmış ve bu teknolojinin zayıf noktalarına değinilmiştir. Uzun menzil, düşük enerji ihtiyacı düşük maliyet ve hizmet kalitesi ile ölçeklenebilirlik özellikleri incelenmiştir. Bu çalışmada LPWAN teknolojilerinden LoRaWAN, Sigfox ve Telensa incelenmek üzere seçilmiş ve bu teknolojilerin veri hızları, MAC

katmanları ve güvenlikleri karşılaştırılmıştır. Ayrıca bu teknolojilerin tedarik, lisanslama, kullanım ömrü gibi çeşitli zorlukları incelenip nasıl çözümler bulunduğu üzerine karşılaştırma yapılmış ve gösterilmiştir.

Güvenli bir LoRa Çözümü Oluşturma başlıklı çalışmada [16], LoRaWAN güvenliğine genel bir bakış atılmış ve bir LoRaWAN ağını yapılandırırken güvenlik özelliklerinin nasıl optimum şekilde yapılandırılabileceğinden bahsedilmiştir. Bir LoRaWAN ağı kurulumunu anlatırken güvenlik anahtarı yönetimini ve buradaki zayıf noktalar belirtilmiştir.

LPWAN için bir değerlendirme çalışmasında [34], LoRaWAN, Sigfox ve Wi-Fi teknolojileri üzerine yoğunlaşmış ve bu teknolojilerin gerçek dünya testleri yapılmıştır. Test kurulumunda açık alanda 25 km mesafede ölçümler yapıp RSSI ve SNR gecikmesi ile güç spektrumları tabloda gösterilmiştir. Bu çalışmada OTAA eksikleri belirtilerek güvenlik gereksinimleri üzerine tartışılmıştır.

LoRaWAN Katılım Prosedürü Analizi konulu çalışmada [35], LoRaWAN teknolojisinin güvenlik değerlendirilmesi yapılmış ve DevNonce özelliği incelenmiştir. DevNonce özelliğinden dolayı ölçeklendirilmiş bir ortamda ortaya çıkabilecek güvenlik açıkları üzerine tartışılmıştır. DoS ve sinyal karıştırma gibi saldırılara karşı alınan bazı öneriler sunulmuştur.

Yang'ın 2017 yılında yaptığı LoRaWAN Güvenlik Açığı Analizi çalışmasında [39], LoRaWAN mimarisi detaylı incelenmiş ve LoRaWAN'ın aktifleştirme (OTAA, ABP), anahtar yönetimi, kriptografi, mesaj kabulü metotları üzerine güvenlik incelemesi yapılmıştır. Ayrıca bu teknolojinin zafiyetleri ve saldırı önleme üzerine incelemede bulunulmuştur.

LoRaWAN Güvenlik Değerlendirmesi konulu makalede [40], Düşük Güçlü Geniş Alan Ağları ve LoRaWAN üzerine çalışılmış, bu teknolojinin kimlik doğrulama gibi gizliliği tehlikeye atacak çeşitli gizlilik ve güvenlik sorunları üzerinde durulmuştur. LoRaWAN mimarisi, uygulamaları ve güvenlik riskleri üzerine tartışılmış ve ele alınan bu sorunlara yönelik öneriler listelenmiştir.

LoRaWAN Güvenlik Risk Analizi konulu makalede [36], LoRaWAN v1.1 versiyonu güvenlik yönünden incelenmiş ve ETSI yönergeleri izlenerek bu protokolün riskleri ve tehditleri tartışılmıştır. Bu çalışma Lora ağı geliştiricilerinin ve LoRaWAN

kullanan organizasyonların özellikle dikkat etmesi gereken, uç cihaza yapılan saldırılar, rogue gateway gibi önemli tehditler üzerinde durulmuştur.

LPWAN Sensörlerin Özellikleri adlı çalışmada [38], Düşük Güçlü Geniş Alan Ağlarının özellikleri ve IoT ağlarında kullanılan diğer ağ teknolojileri ile farkları ile beraber, düşük bant genişliği, veri gönderim sıklığı, hız, enerji tüketimi ve güç optimizasyonu özellikleri incelenmiştir. Ayrıca IoT sistemlerinde kullanılan sensörler, sensörlerin güç optimizasyonu teknikleri ve literatür incelenmiş ve örnek olarak bazı uygulamalar üzerinde tartışılmıştır.

2017 yılında yazılmış LoRa Güvenlik Açıklarının Keşfi isimli çalışmada [17], LoRaWAN ağının replay, wormhole ve jamming saldırılarına karşı duyarlılığını incelenmiştir. J. Kim ise 2017'deki çalışmasında [22] tekrarlama (replay) saldırısının önlenmesi için bir tasarım şeması sunmuştur. W-J. Sung ise RSSI ve handshaking kullanılarak replay saldırısına karşı koruma oluşturulması üzerine 2018 yılında çalışmasını sunmuştur [23]. Yine replay saldırısını tespit edip önlemek için bir STP modeli tasarımı üzerine çalışan S. Gao, çalışmasını 2019 yılında tamamlayıp sunmuştur [27].

2020 yılında hazırlanan LoRaWAN'da MITM Saldırısı önleme adlı çalışmada [28], şifrelenmiş Galois sayaç modu kullanılarak ortadaki adam saldırısını önleme üzerine öneriler sunulmuştur. LoRaWAN Ağ Tasarımı adlı çalışmada [18], LoRaWAN güvenlik yaklaşımları ve sertifika tabanlı güvenlik seçeneklerinin analizi yapılmıştır.

LoRaWAN 1.0 ve 1.1. versiyonlarında güvenlik tehditlerinin özetini konu alan İ. Butun, çalışmasını 2018'de yayınlamıştır [24]. 2017 yılında hazırlanan LoRaWAN güvenliğini artırma konulu çalışmada [19], LoRaWAN 1.0 için ağ sunucusu ile uç cihaz arasındaki anahtarlama yönteminin, güvenliği arttıracak şekilde geliştirilmesine yönelik öneriler sunulmuştur. Güvenli bir Ağ Mimarisi adlı çalışmada [21], LoRaWAN güvenlik analizi ve yeni bir anahtarlama yöntemi önerisinin üzerinde durulmuştur.

LoRaWAN anahtarlama yönetimi için güvenlik risk değerlendirmesi ve yeni bir anahtar yönetim tasarımı adlı çalışma R. Sanchez-Iborra tarafından 2018'de sunulmuştur [25]. K-L. Tsai 2020 yılında hazırladığı çalışmasında [30], sunucular arasındaki iletişim güvenliğinin AES algoritmaları kullanılarak geliştirilmesi üzerine çalışmıştır.

Bu çalışmamız, hızla popülerleşen ve geliştirilmeye devam edilen LoRaWAN teknolojisinin güvenliği ile alakalı çalışmaların sayıca az olması, mevcut çalışmaların yeni versiyonlardan dolayı güncelliğini yitirmeye başlaması ve bu tez çalışmanın hazırlandığı tarih itibarıyla Türkçe dilinde yazılmış akademik bir çalışma bulunmamasından dolayı oluşan ihtiyacı karşılaması için hazırlanmıştır. LoRaWAN güncel versiyonları ve güvenlik önlemleri incelenip olası zafiyetleri ve bu zafiyetleri kullanabilecek 4 farklı saldırı çeşidi analiz edilmiş ve sunulmuştur. Ardından bu saldırıların önlenmesi veya etkisinin azaltılmasına yönelik öneriler sunulmuştur. Çalışmamızın güncel olması ve saldırıların analizi ile beraber bu saldırılara karşı öneriler sunması açısından gelecekteki çalışmalara fayda sağlayacaktır. Ayrıca çalışmanın dili Türkçe olduğundan bu boşluğu da doldurmaya katkı sağlayacaktır.



2. IoT'DE KULLANILAN KABLOSUZ AĞ TEKNOLOJİLERİ

2.1. LPWAN (Düşük Güçlü Alan Ağları)

IoT uygulamalarının kapsamı genişledikçe yeni ihtiyaçlar ortaya çıkmaya devam etmektedir [46]. Bir IoT uygulamasında sensörlerin arasındaki mesafeler arttıkça birtakım zorluklar ortaya çıkmakta ve bununla beraber düşük güç tüketimli uzun mesafe veri iletebilen sensörlere yönelik yeni iletişim teknolojilerine ihtiyaç giderek artmaktadır [45].

Bu boşluğu doldurmak için geliştirilmiş olan LPWAN, bir kablosuz iletişim protokolüdür [47]. Pil ile çalışan ve düşük güç tüketimi odaklı IoT sensörlerinin, küçük boyutlu veri paketlerini uzun menzilli mesafelere gönderebilmelerine olanak sağlayan LPWAN teknolojilerini diğerlerinden ayıran bir diğer faktör ise bu sensörlerin güç optimizasyonu teknikleri ile uzun bir zaman diliminde tek bir pil ile çalışabilir hale getirmesidir [48]. Bundan dolayı geniş IoT ağlarının hücresel bağlantılara ve operatörlere ihtiyaç kalmadan ekonomik maliyetle kurulabilmektedir [38].

LPWAN düşük güç kullanımı düşük maliyeti ve uzun menzili ile özellikle endüstriyel alanda hakimiyetini arttırmaktadır. Kırsal bölgelerde 40 km kentsel bölgelerde ise 5km mesafeye kadar iletişim menzili olması ve bunun yanı sıra 10 yıl kadar pil ömrü sunabilmesi, bu alanlarda popülerleşmesini açıklamaktadır [49]. Günümüzde lisanslı ve lisanssız frekans bantlarında birçok LPWAN teknolojisi ortaya çıkmıştır. Sigfox, LoRa ve NB-IoT teknolojileri bunların önde gelenlerindendir.

Sigfox teknolojisi 2010 yılında Fransa merkezli bir şirket ve ayrıca bir LPWAN ağ operatörü olan Sigfox tarafından geliştirilmiştir. Sigfox günümüzde 31 ülkede kendi IoT çözümlerini kullanıma açmış çeşitli ağ operatörleri ile yaptığı partnerlik anlaşmalarıyla dünya çapında kullanımını arttırmaktadır [50].

Lora teknolojisi ise ilk olarak 2009 yılında Fransa merkezli Cycleo tarafından geliştirilmiştir. Üç yıl sonra ABD merkezli Semtech tarafından satın alındıktan sonra 2015 yılında LoRa, LoRa-Alliance tarafından standartlaştırıldı. Çeşitli mobil operatörlerden de yatırım alarak 42 ülkede halihazırda kullanılmakta ve yaygınlaşmaktadır [51].

NB-IoT dar bant radyo teknolojisine dayalı bir LPWAN teknolojisidir ve 3GPP projesi ile standartlaştırılmıştır. Haziran 2016 tarihinde 3GPP sürüm 13'te yayınlanmıştır. NB-IoT Avrupa'da test aşamasındadır. Vodafone ve Huawei ile ortaklıkları olup ilk NB-IoT standardına uygun mesajı su sayacına takılan bir sensör üzerinden göndermiştir. Halihazırda Huawei, bu teknolojiyi dünya çapında yaygınlaştırmak için ortaklıkları çoğaltmaktadır. Ayrıca Mayıs 2017 tarihinde, Çin Sanayi ve Bilgi Teknolojileri bakanlığı, kamu hizmetleri ve akıllı şehir uygulamaları için NB-IoT'nin ticari kullanımını hızlandırma kararı almıştır.

2.1.1. LoRa, Sigfox ve NB-IOT Teknik Farkları

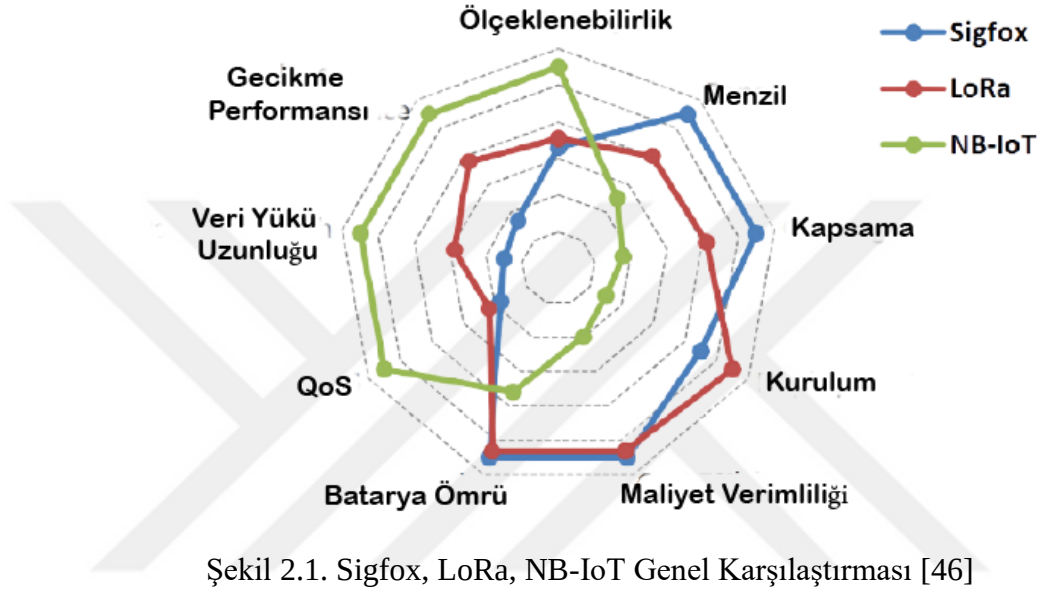
Tablo 2.1'de LoRa, Sigfox ve NB-IoT teknolojilerinin teknik özellikleri karşılaştırılıp gösterilmiştir. Tablo 2.2'de Lora, Sigfox ve NB-IoT teknolojilerinin maliyetleri gösterilmiştir. Şekil 2.1'de bu üç teknolojinin genel özellikleri gösterilmektedir.

Tablo 2.1. LoRaWAN, NB-IoT, Sigfox karşılaştırma tablosu

	LoRaWAN	NB-IoT	SigFox
Modülasyon	CSS	QPSK	BPSK
Frekans	Lisanssız ISM bandı	Lisanslı LTE frekans bantları	Lisanssız ISM bandı
Bant Genişliği	250 kHz ve 125 kHz	200 kHz	100 Hz
Maksimum Veri Hızı	50 kbps	200 kbps	100 bps
Çift yönlülüğü	Evet/ Half-Duplex	Evet / Half-Duplex	Limitli/ Half-duplex
Maksimum Mesaj/Gün	Limitsiz	Limitsiz	140(UL), 4(DL)
Maksimum veri Paketi	243 bytes	1600 bytes	12 bytes(UL), 8 bytes(DL)
Menzil	5km Şehirde, 20km Kırsalda	1km Şehirde, 10km Kırsalda	10km Şehirde, 40km Kırsalda
Parazitten Etkilenme	Yüksek	Düşük	Yüksek
Kimlik Doğrulama ve şifreleme	Evet (AES128)	LTE Encryption	Desteklenmiyor
Uyarlanabilir Veri Hızı (ADR)	Evet	Hayır	Hayır
Lokalizasyon	Evet (TDOA)	Hayır	Evet (RSSI)
Özel Ağa Katılım	Evet	Hayır	Hayır
Standardizasyon	LoRa-Alliance	3GPP	ETSI ile iş birliği içinde

Tablo 2.2. Lora, NB-IoT, Sigfox Maliyet Karşılaştırması [46]

	Spektrum Maliyeti	Kurulum Maliyeti	Uç Cihaz Maliyeti
LoRaWAN	Ücretsiz	>100€/Ağ Geçidi >1000€/Baz İstasyonu	3-5€
NB-IoT	>500M€/MHz	15000€/ Baz İstasyonu	>20€
Sigfox	Ücretsiz	4000€/ Baz İstasyonu	<2€



2.2. LoRa

Semtech firması tarafından geliştirilmeye başlanan LoRa günümüzde LoRa-Alliance tarafından kontrolü sağlanan tescilli bir yayılı spektrum modülasyon teknolojisidir. LoRa'nın diğer LPWAN teknolojileri arasındaki temel farklarından biri de Doppler etkisi ve çok yollu sönmülemeye karşı dirençli olmasıdır. Ayrıca DSSS'in bir alt kategorisi olan ve alıcı hassasiyetini arttıran chirp yayılma spektrumu modülasyonu (CSS) temellidir [52].

Chirp yayılma spektrumu (CSS), radar uygulamaları için 1940'ta geliştirilmiştir. Başta askeri amaçla ve güvenli iletişim için kullanılmaktayken sonrasında birçok haberleşme uygulamasında kullanılmaya başlanmıştır. Bunun sebebi ise Doppler ve bant içi sıkışma, çok yollu sönmüleme gibi kanal bozulmalarına karşı doğal dayanıklılığından dolayıdır. CSS, iletişim aralığını düşük spektral verim maliyetine karşın arttırmayı mümkün kılmakta ve alıcının hassasiyet sorununu aşmayı mümkün kıldığından dolayı IoT ağları için uygun bulunmuştur [53]. LoRa düşük veri oranları ve GHz altındaki

radio bantları sayesinde uzun mesafelerde iletişimi sağlayabilmektedir. Menzile genellikle çevre koşulları ve engellere bağlıdır. Bir ağ geçidi ile tüm şehir veya kilometrelerce alanı kapsama altına alabilir. Uç cihazlar ile ağ geçitleri arasındaki iletişim, farklı veri oranlarında ve farklı frekans kanallarında yayılır. Bu veri oranının yayılım faktörü parametresi belirler. Yayılım faktörü (SF), mesaj süresi ile haberleşme menzili arasında denge kurar ve bu sayede farklı veri oranları ile sinyaller ve mesajların birbirleri ile iletişime girmelerinden kaçınılır. Farklı yayılım faktörleri (SF7, SF8..., SF12) kullanılarak aynı frekans kanalında eşzamanlı haberleşme mümkündür. LoRa lisanssız ISM bantları kullanmaktadır. Bunlar Asya'da 433 MHz, Kuzey Amerika'da 915 MHz ve Avrupa'da 868 MHz'dir. LoRa teknolojisinin veri oranı 0.3 ile 50 kbps arasındadır. Maksimum yük uzunluğu ise 243 bayttır [54], [55].

Tablo 2.3. Farklı Yayılım Faktörleri için Bit ve Sembol Oranı [56]

Yayılma Faktörü (SF)	Sembol Sayısı	Bant Genişliği (Hz)	Sembol Oranı (symbols/sec)	Bit Oranı (Bit Rate) (bits/sec)
7	128	125000	976,56250000	6835,9375000
8	256	125000	488,28125000	3906,2500000
9	512	125000	244,14062500	2197,2656250
10	1024	125000	122,07031250	1220,7031250
11	2048	125000	61,035156250	671,38671875
12	4096	125000	30,517578125	366,21093750

LoRa ve LoRaWAN aynı şeyi ifade etmez. LoRa bir PHY katmanı iken LoRaWAN ise bir MAC katmanıdır. Bu katmanlar birleşerek bir LPWAN ağı ortaya çıkarılırlar.

Tablo 2.4. LoRa Hata Algılama ve Düzeltme Oranları [57]

Kod Oranı	Hata düzeltme (bit)	Hata Algılama (bit)
4/5	0	0
4/6	0	1
4/7	1	2
4/8	1	3

LoRa modülasyonu Yayılma Faktörü (SF), Kod Oranı (CR), Bant Genişliği (BW) gibi çeşitli parametreler ile özelleştirilebilir. İleri Hata Düzeltme (FEC), Kod Oranı (CR) tarafından tanımlanır. LoRa teknolojisinde alıcı hassasiyeti arttırmak için kullanılan tekniklerden biri İleri Hata Düzeltme (FEC)'dir. LoRa ileri hata düzeltme (FEC) için Hamming kodları kullanır. Bu uygulanması kolay bir basit lineer blok kodu algoritmasıdır. LoRa 4/5, 4/6, 4/7, 4/8, kod oranları sunar. Hata düzeltme ve hata algılama oranları Tablo 2.4'te gösterildiği gibidir [57]. Tablo 2.4'te görüldüğü gibi

hata düzeltme sadece 4/7 oranında başlatılır. 4/6 kod oranı sadece hata algılaması ekler ve hata düzeltme yeteneği yoktur. Bundan dolayı hata düzeltme için en az 4/7 kod oranı kullanılmalıdır. LoRa, Yayılım Faktörü (SF) olarak 7 – 12 arasında değerler kullanır. Yayılım Faktörü (SF) bir işarette iletilen bitlerin sayısını tanımlar. Bir işaret tüm frekans bandını kapsayan 2^{SF} Chirp'ten oluşmaktadır. SF ve karşılığındaki işaret/Chirp uzunluğu Tablo 2.6'da gösterilmiştir. Frekans bant genişliği bir Yayılım faktöründeki işaret oranı ve bit hızı ile orantılıdır. Bundan dolayı iletim hızının iki katına çıkması için bant genişliğinin iki katına çıkması gerekmektedir. Bant genişliği (BW) iletilen verinin maksimum ulaşabileceği hız olarak tanımlanabilir. LoRa teknolojisi 125 kHz, 250 kHz ve 500 kHz ile ölçeklenebilir bant genişliğine izin vermektedir [58].

Tablo 2.5. LoRa ISM Frekans Özellikleri [59]

	Avrupa	Kuzey Amerika
Frekans Bandı	867-869 MHz	902-328 MHz
Kanallar	10	64+8+8
Kanal BW Up	125/250 kHz	125/250 kHz
Kanal BW Dn	125 kHz	500 kHz
TX Gücü Up	+14 dBm	+20 dBm typ
TX Gücü DN	+14 dBm	+27 dBm
SF Up	7-12	7-10
Veri Hızı	250 bps- 50 kbps	980 bps- 21.9 kbps
Bağlantı Maliyeti Up	155 dB	154 dB
Bağlantı Maliyeti Dn	155 dB	157 dB

Tablo 2.6. SF ve karşılığındaki işaret/Chirp uzunluğu [58]

Yayılım Faktörü (SF)	İşaret/Chirp 2^{SF}
7	128
8	256
9	512
10	1024
11	2048
12	4096

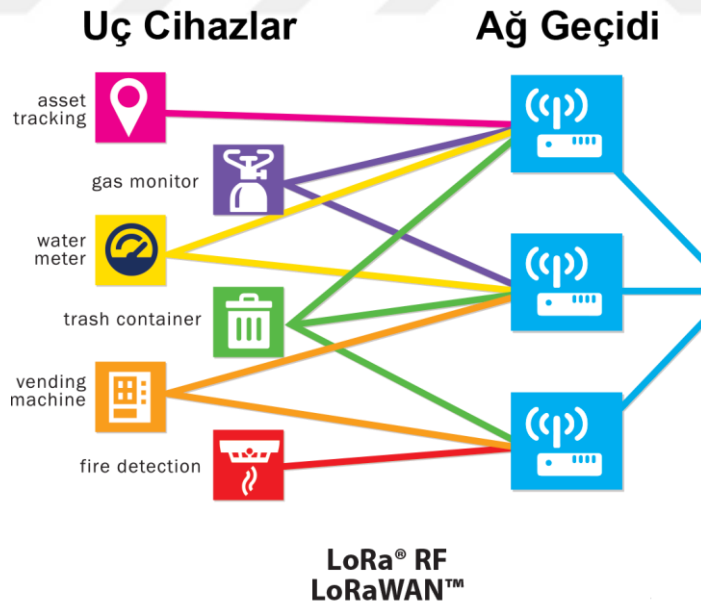
2.3. LoRaWAN

LoRaWAN MAC katmanında çalışan bir LPWAN protokolüdür. LoRaWAN OSI modelinin ağ katmanı ve veri katmanına eşdeğerken LoRa ise OSI modelinin fiziksel katmanına eşdeğerdir. LoRaWAN ağı genellikle yıldız topolojisine göre kurulur. Bu

sayede uç cihaz tek atlamalı olarak LoRa bağlantısı üzerinden bir veya daha fazla ağ geçidine bağlanabilir. Şekil 2.2’de örnek yıldız topolojisi görülmektedir.

Şekil 2.4’te gösterilen LoRaWAN ağ tasarımında ağ geçitleri; uç cihazlar ile ağ sunucusu arasındaki mesajları yönlendirmekle görevlidir. Uç cihazlar birçok ağ geçidi ile tek zıplamalı FSK veya LoRa protokolü ile bağlanabilirken ağ sunucusu ile ağ geçitleri birbirine IP bağlantısı ile bağlanmaktadır. İletişim çift yönlü olarak sağlanmaktadır fakat mesajlaşmada genellikle uç cihazdan ağ geçidine gönderim (Up Link) şeklinde iletişim ağırlıktadır [60].

LoRaWAN iletişimde uç cihazlar ile ağ geçitleri arasında farklı frekans kanalları ve farklı Yayılım Faktörleri (SF) ile iletişim kurulabilir. Yayılım faktörü (SF) seçiminde mesaj süresi ve menzil etkilidir. Ayrıca farklı Yayılım Faktörleri eşzamanlı olarak aynı kanalda sorunsuzca çalışabilmektedir. Veri iletim hızı ve menzil ile Yayılım Faktörü arasında bir korelasyon vardır. LoRa teknolojisi 0.3 kbps ile 50 kbps arasında değişen 6 kanal yayılım faktörü desteklemektedir. Bu sayede LoRaWAN, desteklediği Adaptif Veri Oranı (ADR) yapısını kullanarak her bir cihazın yayılım faktörünü değiştirebilir ve ağ kapasitesi veya batarya verimini arttırmak yönelik ayarlayabilir.



Şekil 2.2. Örnek bir LoRaWAN Yıldız Topolojisi

2.3.1. LoRaWAN Versiyonları/Standartları

LoRa ilk olarak Chirp Spread Spectrum (CSS) teknolojisinden türetilen ve bu modülasyon tekniklerine dayanan bir LPWAN protokolü olarak tanıtılmıştır. LoRa fiziksel katmanda çalışmasından üst ağ katmanları yeteneklerinden yoksun olduğundan dolayı bulut tabanlı bir MAC katmanı protokolü olan LoRaWAN, ağ geçitleri ile uç cihazlar arasındaki iletişimi, güç tüketimini ve veri hızını yöneten bir ağ sistem mimarisi olarak tanıtılmıştır [61], [62].

LoRaWAN, performans ve güvenlik açısından devamlı olarak geliştirilmektedir. Kısıtlı kaynağı olan IoT cihazlarını daha güvenli, daha esnek ve daha gelişmiş uzak mesafe iletişim sağlamak için bugüne kadar yeni sürümler geliştirilerek sunulmuştur.

2.3.1.1. LoRaWAN v1.0.1

LoRaWAN v1.0.1 sürümü 2016 yılının şubat ayında IoT endüstrisine katkı sağlamak amacı ile bir telekomünikasyon teknolojisi olarak sunulmuştur [63]. İlk olarak mobil ağ operatörleri ile IoT cihazları arasında güvenli ve çift yönlü bir iletişim sağlamak amacı ile ortaya çıkmıştır [64]. Bununla beraber LoRaWAN v1.0.1 sınırlamaları ve saldırı almaya müsait yapısının detaylarına güvenlik başlığı altında değinilecektir.

2.3.1.2. LoRaWAN v1.0.2

LoRaWAN v1.0.2 sürümü 2016 yılının temmuz ayında sunulmuştur. Bu sürümde en önemli gelişme, tek bir kök anahtardan türetilen uygulama anahtarı (AppsKey) ve ağ anahtarı (NwkSKey) kullanımınıdır [65]. NwkSKey ağ oturum anahtarıdır ve bütünlüğü kontrol eder. AppsKey ise veri yükü (Payload) uygulama sunucusuna gönderilirken şifrelenmesinden sorumludur [66]. Ancak v1.0.2. sürümünün NONCE değerinin tekrarlı olarak kullanımı ve tekrarlama saldırılarına karşı zayıf koruma mekanizması gibi çeşitli güvenlik zafiyetlerine sahip olduğu ve bir sonraki LoRaWAN sürümü olan v1.1’de önlemleri alınacak olan bazı saldırılara (ACK Spoofing, eavesdropping, DoS vb.) karşı zafiyet gösterebildiği görülmüştür.

2.3.1.3. LoRaWAN v1.1

LoRaWAN v1.1 2017 yılının ekim ayında, önceki versiyonların (v1.0.1, v1.0.2) ana güvenlik açıklarına (zayıf anahtar yönetimi, zayıf şifreleme, zayıf kimlik doğrulama v.b.) ve zafiyetlerine (ACK spoofing, relay, eavesdropping, paket modifikasyonu v.b.)

karşı sunulmuştur [67]. Böylece pil ile çalışan kısıtlı kaynağı olan IoT cihazların güvenliği artırılmıştır [68].

Bu versiyonla gelen yeni spesifikasyonlar şunlardır:

- FCntDown Sayaçları: v1.1 sürümünde, daha önceki versiyonlarda kullanılan (v1.0.1, v1.0.2) tüm portlar için tek bir FCntDown sayacı yerine birçok FCntDown sayacı kullanımını desteklemektedir.
- Sıfırlama Komutları: ResetInd, ResetConf gibi sıfırlama komutları sadece LoRaWAN v1.1 ABP aygıtlarında kullanılabilir. Bu MAC komutları LoRaWAN 1.0.x versiyonlarında mevcut değildir.
- Rekey Komutları: RekeyInd, RekeyConf gibi komutlar sadece LoRaWAN v1.1 OTA cihazlarında kullanılabilir. LoRaWAN 1.0.x sunucularında mevcut değildirler.
- Aygıt Zaman Komutları: DeviceTimeReq, DeviceTimeAns gibi komutlar sadece LoRaWAN v1.1 sürümünde mevcuttur. Bu MAC komutları önceki sürümü kullanan sunucularda kullanılamaz.
- Uygulama Oturum Anahtarı: Bu anahtar sadece LoRaWAN 1.1 ağ sunucularındaki AppKey'den türetilir.
- NWKey Root Anahtarı: LoRaWAN 1.1 aygıtlarının tüm gerekli anahtarlarının türetilmesinden sorumludur.
- Aygıt İstek/Cevap Zaman Komutları: Bu komutlar önceki LoRaWAN versiyonlarında kullanılan BeaconTimingReq ve BeaconTimingAns komutlarının yerine kullanılır.

2.3.1.4. LoRaWAN v1.0.3

LoRaWAN v1.0.3 2018 yılının temmuz ayında, LoRaWAN v1.0.1 ve v1.0.2 sürümlerine göre daha iyi performans gösteren, ayrıca LoRaWAN v1.1 sürümünde bulunan bazı performans kısıtlamalarının üstesinden gelen yeni bir sürüm olarak sunulmuştur [69].

Bu yeni spesifikasyonlar şunlardır:

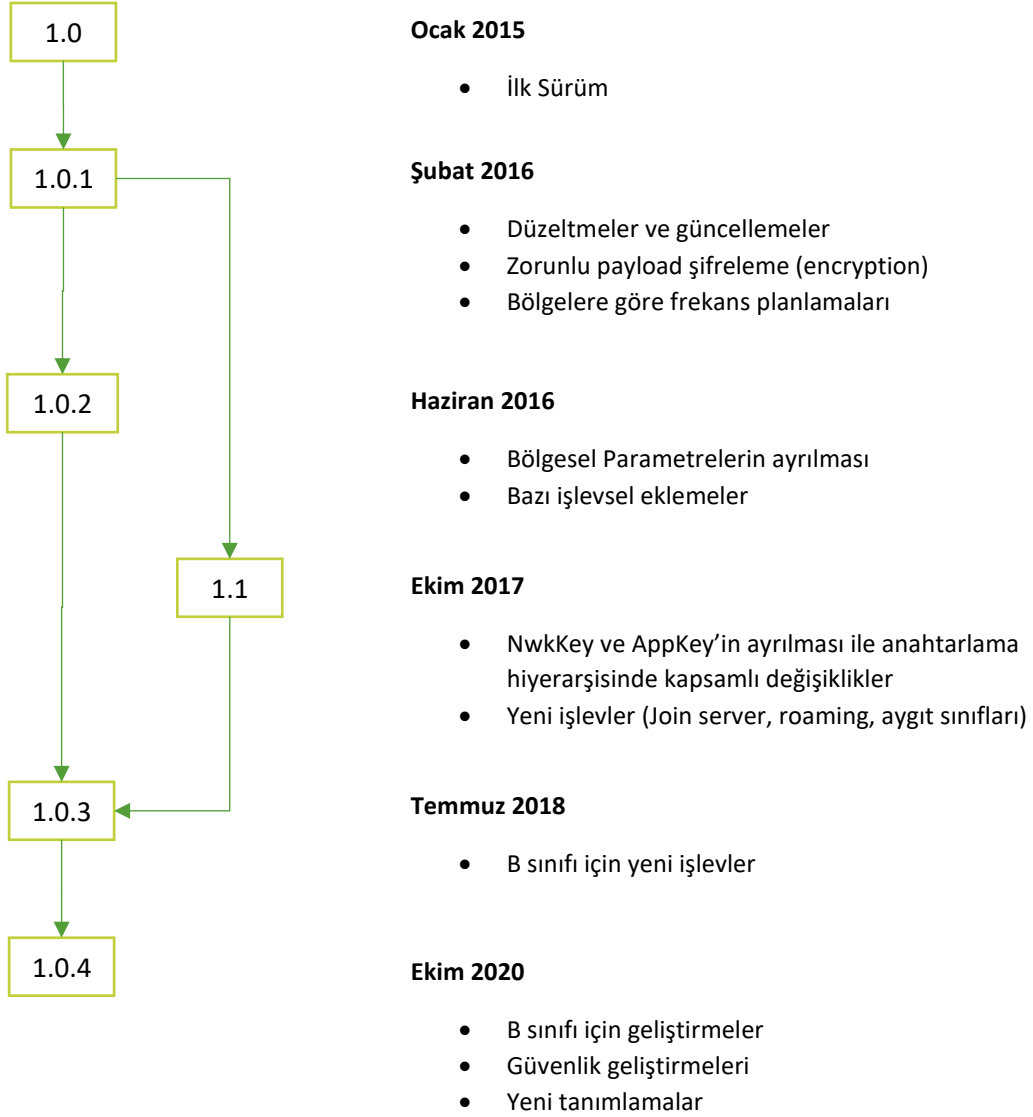
- Aygıt Zaman Komutları: DeviceTimeReq, DeviceTimeAns gibi MAC komutları sadece LoRaWAN v1.0.3 sürümünde mevcut ve aktiftir. Önceki sürümlerde (v1.0.1, v1.0.2) ise mevcut değildirler.

- İşaret (Beacon) Zamanlama İstek/Yanıt Komutları: Bu MAC komutları sadece LoRaWAN v1.0.3 sürümünde ve diğer komutlar (DeviceTimeReq, DeviceTimeAns) ile kullanılabilir.
- Unicast/Multicast Desteği: B sınıfı cihazları desteklemek için LoRaWAN v1.0.3 sürümüne eklenmiştir.
- Aygıt Zaman İsteği Komutu: Bu MAC komutu LoRaWAN v1.0.3'te A ve C sınıfı cihazlar için yeni bir zaman senkronizasyonu özelliği olarak tanıtıldı.
- Uyumluluk: LoRaWAN v1.0.3'teki B sınıfı cihazlar ile LoRaWAN v1.1 sürümündeki B sınıfı cihazlar birbirleri ile uyumludurlar.

2.3.1.5. LoRaWAN v1.0.4

LoRaWAN v1.0.4, 2020 yılının Ekim ayında sunuldu. Bu versiyonla gelen değişiklikler şunlardır [70]:

- Tüm bölgeler için ayrı ayrı olan sertifikasyon spesifikasyonları bire düşürülmüştür.
- DutyCycleReq ve DeviceTimeReq MAC komutları eklenmiştir.
- DeviceStatusReq, NewChannelReq, TXParamSetupReq, LinkADRReq parametrelerinin kullanımında değişiklikler yapılmıştır.
- Çoklu MAC komutu önceliklendirme eklenmiştir.
- Test haritası eklenmiştir.
- B sınıfı için geliştirmeler: Unicast/Multicast için FPending tanımlandı ve işaret (Beacon) çerçeve formatı SF8 ile SF12 için tanımlanmıştır.
- Güvenlik için geliştirmeler: Kalıcı 32bit FCnt parametresi kullanımı ve tekli artan DevNonce gibi değişiklikler yapılmıştır.
- Çeşitli sınıflandırmalar ve tanımlamalar: FPort için 224 üzeri kullanım, ADR yönetimi, MAC komutlarının zorunlu yapısı, DevAddr parametresi içine AddrPrefix, Join prosedürü esnasında kanal seçimi, CFList yönetimi, gibi eklemeler yapılmıştır.



Şekil 2.3. LoRaWAN versiyonları tarihçesi

2.3.2. LoRaWAN Mimarisi ve Bileşenleri

Tüm LoRaWAN ağları temelde aynı yapı taşlarından oluşmaktadır. Şekil 2.4'te de gösterildiği gibi bunlar; LoRa radyo frekansları üzerinden veri gönderen veya alan uç cihaz, uç cihaz ile sunucu arasında verileri yeniden düzenleyen bir veya daha fazla ağ geçidi ve son olarak verileri işleyen sunuculardır.

2.3.2.1. Uç Cihaz

Uç cihazlar, ağ geçitleri ile beraber LoRa Alliance tarafından belirlenen standartlara uygun radyo frekansları üzerinden iletişim kurabilen ağ bileşenleridir. Tüm uç cihazlar bir uygulama katmanına ve bir MAC katmanına sahiptirler. Uygulama katmanı ağ

üzerinden bir uygulama sunucusuna bağlanırken, MAC katmanı ise ağ sunucusunda sonlandırılır. MAC katmanı iletişiminin güvenliği Network Session Key (NwkSKey) ile sağlanırken Uygulama katmanının güvenliği Application Session Key (AppSKey) tarafından sağlanmaktadır.

Uç cihazlar ağda iki farklı şekilde aktifleştirilmektedirler. Bunlardan biri olan Activation by Personalization (ABP), uç cihazı önceden yapılandırılmış olan sunucu bilgilerine göre belirli bir ağda aktifleştirir. Bu metotta uç cihaz tüm zamanlarda aynı oturum anahtarını kullanmaktadır.

Bir diğer aktivasyon metodu olan Over the Air (OTA), uç cihazın ağda aktifleştirilmesi için bir Katılım (Join) Prosedürü ile ilgili sunucuya katılması ve ağda aktive edilmesini sağlamaktadır [71]. OTA aktivasyonu daha esnek ve güvenlik açısından sürekli değişen anahtarlama yöntemi kullandığından genellikle daha çok tercih edilen aktivasyon yaklaşımıdır [36].

LoRaWAN uç cihazları fonksiyonlarına göre üç farklı sınıfa sahiptir. Bunlar A, B ve C sınıflarıdır. Uç cihazlar tüm sınıflarda çift yönlü iletişim yeteneğine sahiptir. Fark ise mesajları alma şekilleridir. Detaylar LoRaWAN sınıfları başlığı altında yazılmıştır.

2.3.2.2. Ağ Geçidi

Ağ geçidinin LoRaWAN ağındaki fonksiyonu uç cihazlar ile ağ sunucusu arasında köprü olmaktır. Ağ geçitleri aralarında farklılıklar gösterebilmekle beraber genel olarak tüm ağ geçitleri aynı temel işlevlere sahiptir.

Ağ geçitleri, üzerinde LoRa kondansatör/yoğunlaştırıcı bulunan yönlendiricilerdir. Kondansatör LoRa demodülatörünü kullanarak farklı frekanslarda LoRa modülasyon kodunu çözebilmektedir. Ağ geçitleri, verileri ağ sunucusuna aktarmak için daha yüksek bant genişliğine sahip ağlar kullanmaktadırlar. Basit ağ geçitleri, bir paket iletici olarak yalnızca gelen verilerin kodunu çözer ve aktarır. Bununla beraber ağ geçitleri kimlik doğrulama ve yetkilendirme gibi üzerlerinde çalışan karmaşık veri işleme yazılımlarına sahip olabilmelerine olanak tanıyan işletim sistemleri üzerinde çalışabilmektedirler. [72], [73].

2.3.2.3. Ağ Sunucusu (NS)

Ağ sunucusu yıldız topolojisinin merkezindedir ve LoRaWAN'ın temel bazı işlevlerinden sorumludur. İşlevselliği ağın mimarisine göre değişkenlik gösterebilmektedir.

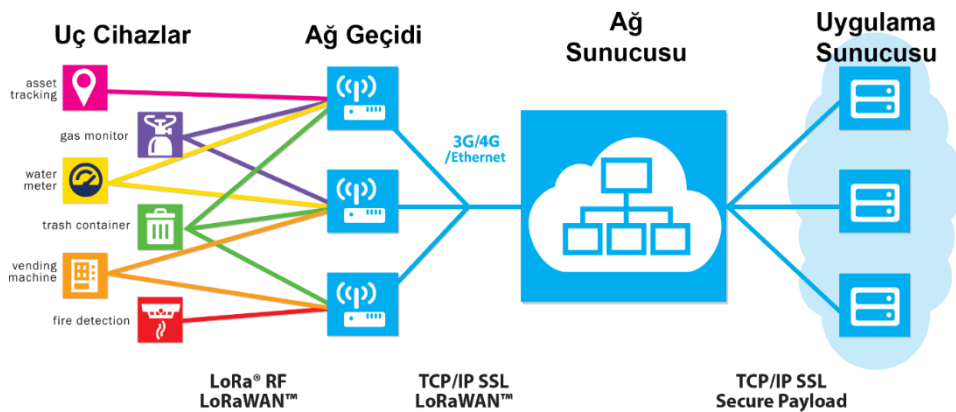
Ağ sunucusu uç cihazın adresini kontrol eder. Uç cihazdan gönderilen tüm Yukarı bağlantı (UL) mesajları kapsamındaki Uygulama Sunucusuna (AS) iletir ve Uygulama Sunucusundan uç cihaza gidecek olan Aşağı Bağlantı (DL) mesajları kuyruğa alır. Ayrıca OTA uç cihazları aktivasyonu için uç cihaz ile Join Server arasında mesaj iletimini sağlamaktadır [71].

2.3.2.4. Uygulama Sunucusu (Application Server)

Uygulama sunucusu, son kullanıcı tarafından erişilen Arayüzden (Interface) sorumludur. Uç cihazlardan gelen Yukarı Bağlantı (UL) mesajlarını yönetir ve Uç cihazlar için Aşağı Bağlantı (DL) yüklerini (payload) oluşturur [71].

2.3.2.5. Join Server

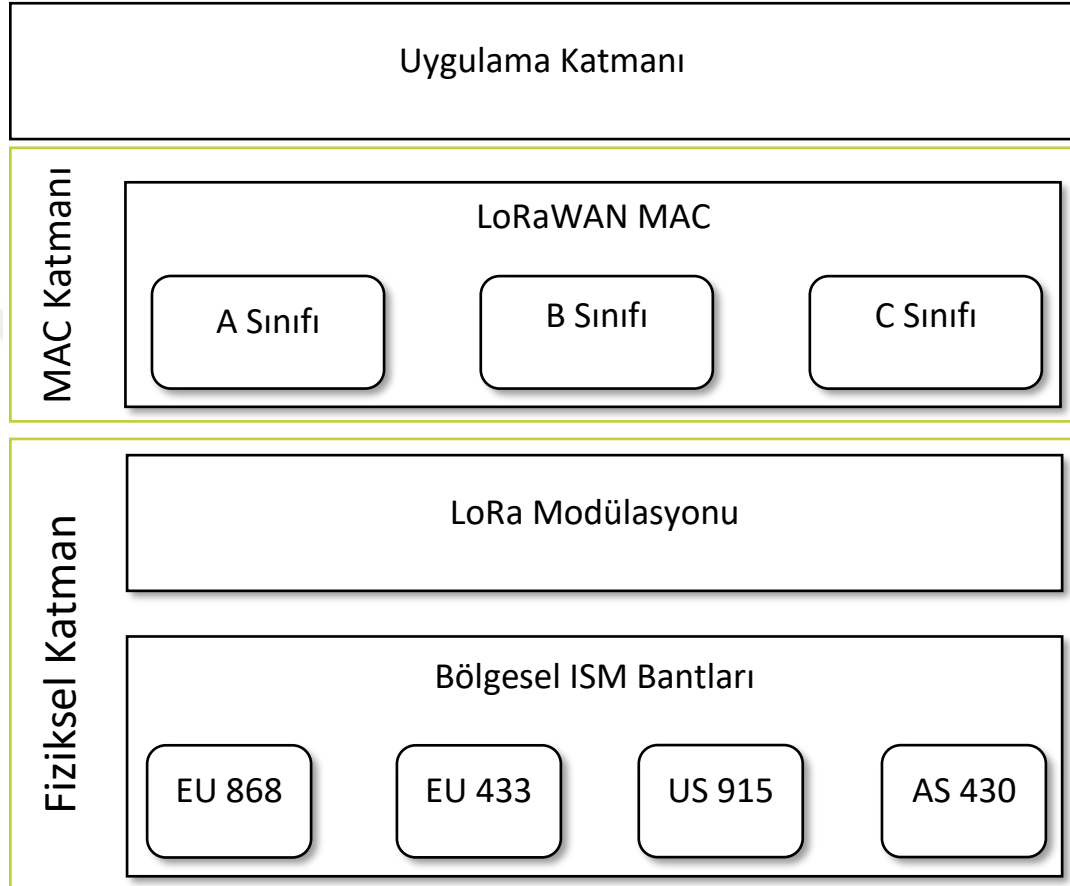
Join Server tüm OTA uç cihazların aktivasyonunu yönetir. Aktivasyon sürecini yönetmek için uç cihaz hakkındaki tüm gerekli bilgiyi tutar. Join Server, NwkSKey'i uç cihazdan Ağ Sunucusuna (NS) yollar ve AppSKey'i Uygulama Sunucusuna gönderir. Bu sayede sunucuların uç cihazı onaylaması ve bağlantı kurulması sağlanmaktadır. AppKey ve NwkKey sadece Join Server'da tutulmaktadır [71].



Şekil 2.4. Örnek Bir LoRaWAN Mimarisi

2.3.3. LoRaWAN Sınıfları

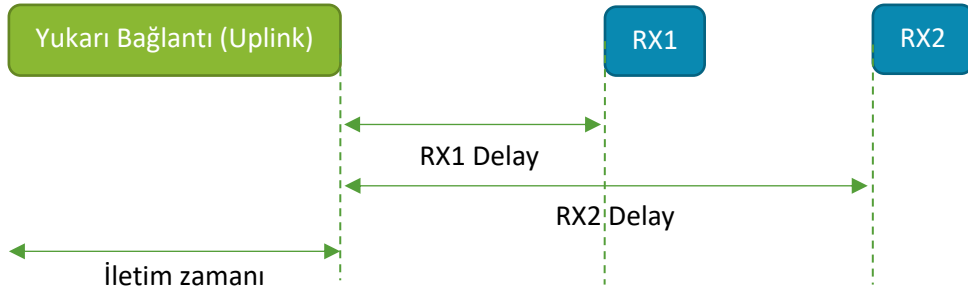
LoRaWAN uç cihazları; A, B ve C sınıfları olmak üzere üç sınıfa ayrılmaktadır. Tüm sınıflar için çift yönlü iletişim mevcut olmakla beraber mesaj alma yöntemlerinde farklılıklar bulunmaktadır.



Şekil 2.5. LoRa Protokol Yığını [74]

2.3.3.1. A Sınıfı

A sınıfı uç cihazlar bu üç sınıf arasında en düşük güç tüketimini sağlamaktadır. Ağ geçidi ile uç cihaz arasında çift yönlü iletişimi desteklemektedir. A sınıfı uç cihazlar yukarı yönlü (UL, uç cihazdan sunucuya) mesajları herhangi bir zamanda gönderebilmektedir. Şekil 2.6’da görüldüğü gibi uç cihaz gönderdiği UL mesajının ardından belirli bir zamana (RX1 delay, RX2 delay) göre iki tane alım penceresi açar. Bu sırada sunucudan yanıt beklenir ve eğer yanıt gelmezse pencereler kapanır ve bir sonraki UL mesajı gönderimine kadar sunucudan mesaj alımı (DL) kapanmaktadır.



Şekil 2.6. A sınıfı uç cihazların alım penceresi diyagramı

Uç cihazdan sunucuya mesaj gittiğinde sunucu, ilk alım penceresi (receive window) veya ikinci alım penceresi ile yanıt gönderebilir fakat her iki pencereyi de kullanamamaktadır. Bunun nedeni, eğer uç cihaz ilk alım penceresi ile bir yanıt aldığı anda ikinci pencereyi açmamaktadır. Bundan dolayı 3 farklı durum ortaya çıkmaktadır [75]. Şekil 2.7’de gösterilen bu durumlardan;

- 1. Durumda, uç cihaz iki alım penceresini de açmış fakat yanıt almadığı görülmektedir.
- 2. Durumda ise ilk alım penceresinde yanıt alınmış ve bundan dolayı ikinci pencere açılmamaktadır.
- 3. Durumda ise UL ardından ilk pencere açılmış fakat herhangi bir yanıt olmadığından dolayı bir süre sonra 2. Alım penceresi açılmış ve yanıt alınmıştır.



A sınıfı Uç cihazların Özellikleri [75]:

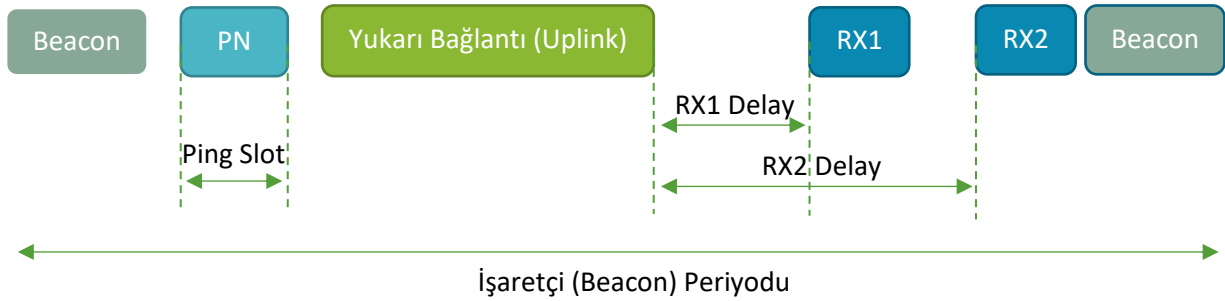
- Genellikle pil ile çalışır
- En düşük enerji tüketimine sahip
- Açık kaldığı sürede çoğu zamanı uyku modunda geçirir
- Genellikle mesaj gönderimleri (uplink) arasında uzun aralıklar olur
- Mesaj alımında (DL) yüksek gecikmeye sahip

Bazı yaygın kullanım alanları [75]:

- Çevre takip sistemleri
- Hayvan takibi
- Yangın Algılama sistemleri
- Erken Deprem Tespiti
- Konum Takibi

2.3.3.2. B Sınıfı

B sınıfı, A sınıfından türetilip sunucudan gelen aşağı bağlantı (DL) mesajları için planlanmış yeni pencereler eklenmiş halidir. B sınıfı Uç Cihazlarda, Ağ Geçidinden iletilen zamana göre senkronize olarak ve belirli zaman aralıklarında Beacons (işaretçiler) kullanarak periyodik olarak alım pencereleri açılmaktadır. İşaretçiler arasındaki zamana göre uç cihaz bir aşağı bağlantı almaya uygun olur. Bu alıma uygun olduğu an Ping Slot'tur Ayrıca bir UL gönderiminin ardından da alım penceresi açılmaktadır. Aşağıdaki Şekil 2.8'de B sınıfı bir uç cihazın bir yukarı bağlantı mesajı gönderdikten sonra açılan alım penceresi görülmektedir [75].

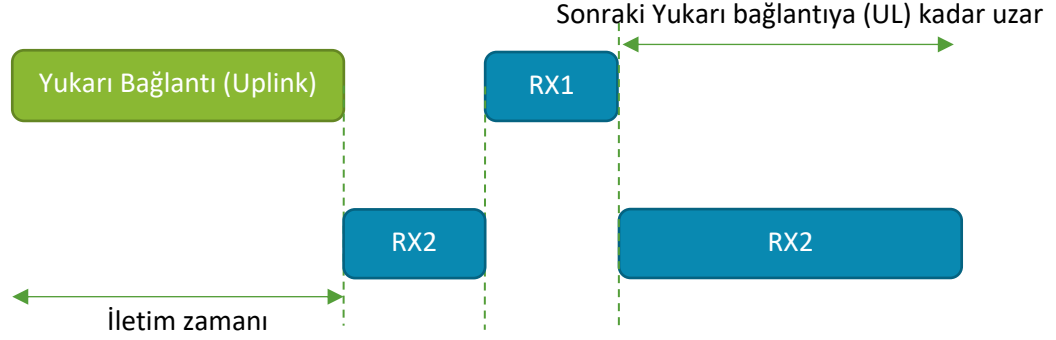


Şekil 2.8. B Sınıfı Alım Penceresi Diyagramı [75]

B Sınıfı uç cihazlar, önceden yapılandırılmış zamanlara göre erişilebilir olduklarından ve bir DL alımı için UL mesajı göndermeleri gerekmediğinden A sınıfına göre daha düşük gecikmeye sahiptir. Fakat A sınıfına göre daha uzun süre aktif kaldıklarından pil ömrü A sınıfına göre daha kısadır.

2.3.3.3. C Sınıfı

C sınıfı uç cihazlar diğerlerinden farklı olarak alım penceresini devamlı açık tutmaktadırlar. Bu sayede en düşük gecikme oranı sağlanırken enerji tüketimi diğer sınıflara göre çok fazla olmaktadır.



C sınıfı uç cihazların özellikleri [75]:

- Genellikle şebekeden güç alırlar
- Aşağı bağlantıda (DL) gecikme yoktur ve alım penceresi her zaman açıktır
- Sokak ışıkları ve sayaçlar gibi birçok uygulamada kullanılmaktadırlar

2.3.4. LoRaWAN Ağ Katmanları ve Paket Formatları

LoRaWAN paketleri/mesajları iki farklı türden oluşmaktadır. Bunlardan birisi aşağı bağlantı (UpLink) ve diğeri yukarı bağlantı (DownLink) mesajıdır. Yukarı bağlantı mesajı (UL) Uç cihazdan ağ geçidine doğru giden mesaj iken aşağı bağlantı (DL), ağ geçidinden uç cihaza doğru gelen mesajlar olmaktadır. UL ve DL mesajlar da iki farklı tipe ayrılmaktadırlar. Bunlar onaylı (confirmed) ve onaysız (unconfirmed) mesajlardır. Bu iki tipin farkı, onaylı mesajda ilgili cihaz mesajın kendisine ulaştığına dair geri bildirim verirken onaysız mesajda geribildirim yoktur [76].

Uygulama Katmanı
MAC Katmanı • A Sınıfı • B Sınıfı • C Sınıfı
Fiziksel Katman
RF Katmanı • 868 ve 433 MHZ (Avrupa) • 915 MHZ (Amerika) • 430 MHZ (AS)

Şekil 2.9. LoRaWAN Katmanları

2.3.4.1. RF Katmanı

Bu katmanda LoRaWAN Modülleri ile ağ geçitleri arasındaki sinyaller iletilmektedir. RF katmanında sinyalin gücü, frekansı, dalga boyu ve desteklenen RF protokolü tanımlanır. Farklı bölgelerde farklı frekanslar kullanılmakla beraber genel olarak Avrupa’da 868 ve 433 MHz, Amerika’da 915 MHz, Asya’da 430 MHz kullanılmaktadır [77]

2.3.4.2. Fiziksel Katman

Bu katmanda iki farklı tür paket formatı kullanılır. Bunlar açık paket ve kapalı pakettir. Açık pakette CRC, CR ve bayt sayısı hakkında bilgi içeren bir başlık vardır [78].

Yukarı bağlantı mesajları (Şekil 2.10) PHY başlığı (PHDR) ve bir başlık CRC’sine (PHDR_CRC) sahip olan açık mesaj paketini kullanır. Burada yükün (payload) bütünlüğünün korunmasını CRC sağlar. Aşağı bağlantı mesaj paketinde (Şekil 11) ise yukarı bağlantıdan fark olarak Yükün (Payload) CRC’si yoktur.

Preamble	PHDR	PHDR_CRC	PHYPayload	CRC*
----------	------	----------	------------	------

Şekil 2.10. Yukarı bağlantı (UL) Fiziksel Katman Mesaj Formatı [68]

Preamble	PHDR	PHDR_CRC	PHYPayload
----------	------	----------	------------

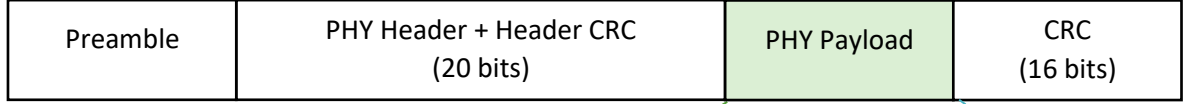
Şekil 2.11. Aşağı bağlantı (DL) Fiziksel Katman Mesaj Formatı [68]

Önsözün (Preamble) görevi alıcıya gelen veri akışını senkronize etmektir. Önsözün senkronize edilmesi için alıcı taraf 5 sembole ihtiyaç duyar. İletilen önsöz ile alım penceresi arasında 5 sembol üst üste gelmesi gerekmektedir. Önsöz (Preamble) değişkeni programlanabilir bir değişken olmakla beraber görev döngüsü azaltılmak istenirse, preamble uzunluğu uzatılabilmektedir [79].

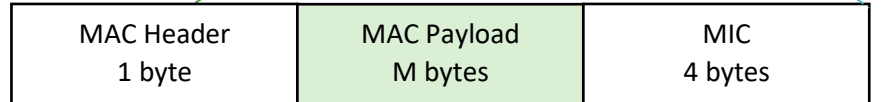
Bu mesaj formatında iki farklı başlık tipi mevcuttur. Bunlarda açık başlık tipinde yük (payload) uzunluğu, ileri hata düzeltme (FEC) ve yük için isteğe bağlı olarak CRC hakkında bilgiler bulunmaktadır. Maksimum hata düzeltme kodu 4/8 ile iletilir. Alıcının geçersiz başlıkları tespit edip yok etmesi için kendi CRC’sine de sahiptir [78].

Bu katman, Şekil 2.12'de gösterildiği gibi çerçeve yapısına sahiptir. LoRaWAN mesaj başlığı; bir Preamble, Payload Header, Veri ve ek olarak CRC'ye sahiptir.

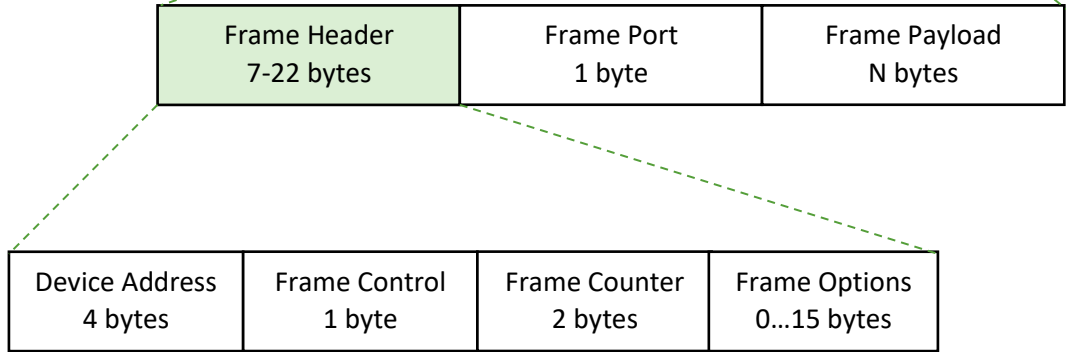
Fiziksel Katman:



MAC Katmanı:



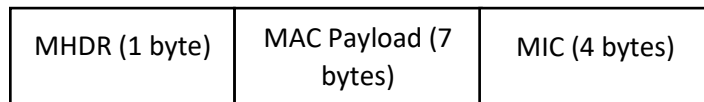
Uygulama Katmanı:



Şekil 2.12. LoRaWAN Çerçeve Yapıları

2.3.4.3. MAC Katmanı

Bu katmandaki mesaj formatı Şekil 2.13'te görüldüğü gibi üç parçadan oluşmaktadır [80]. Bunlar, aşağı bağlantı (downlink) ve yukarı bağlantı (uplink) mesajlarında bulunan bir MAC başlığı (MHDR), Mac yükü (MACPayload), ve mesaj bütünlüğü kodudur (MIC).



Şekil 2.13. MAC Katmanı Çerçeve Yapısı

- MAC Başlığı: Bu alanın içeriğinde Şekil 2.15'te de görüldüğü gibi mesaj tipi (MType), hangi LoRaWAN spesifikasyonunun çerçeve formatı kullanıldığı

bilgisi (Major) ve sonraki güncellemelerde kullanılabilecek bir alan olan RFU alanı bulunur. Özetle bu başlık mesaj tipini ve mesaj formatı versiyonunu belirtmektedir. MType değeri için sekiz farklı seçenek vardır. Bu seçenekler ile MAC mesaj tipleri birbirinden ayrılmaktadır. Bu sekiz farklı değer ve açıklamaları Şekil 2.14’te görülmektedir.

MType Değeri	Anlamı
000	Katılım İsteği
001	Katılım Kabul
010	Onaysız veri yukarı
011	Onaysız veri aşağı
100	Onaylı veri yukarı
101	Onaylı veri aşağı
110	Yeniden katılım isteği
111	Özel

Şekil 2.14. MAC katmanındaki mesaj tipleri

MType	RFU	Major
-------	-----	-------

Şekil 2.15. MAC başlığı (MHDR) içeriği [68]

- MAC Payload: Uygulama başlığı bilgilerine ek olarak kullanıcı verilerini içerir. Ayrıca çerçeve başlığı (FHDR), çerçeve bağlantı noktası (FPort) ve FRMPayload bilgilerini içerir. Çerçeve başlığı (FHDR) ise uç cihazın kısa adresi (DevAddr) ve çerçeve kontrolünü (FCtrl), ve çerçeve sayacı (FCnt) ile MAC komutlarını taşıyan çerçeve seçeneği (FOpts) alanlarını içermektedir.

FHDR (7-22 Bytes)	FPort (1 byte)	FRMPayload (N bytes)
----------------------	-------------------	-------------------------

Şekil 2.16. MAC yükü içeriği [68]

DevAddr (4 bytes)	FCtrl (1 byte)	FCnt (2 byte)	FOpts (0-15 bytes)
----------------------	-------------------	------------------	-----------------------

Şekil 2.17. FHDR içeriği [68]

- MIC: Bu değer MAC başlığını ve payload (yük) bütünlüğünü doğrulamak için ve herhangi bir yetkisiz mesaj değişikliğini önlemeye yönelik kimlik doğrulama için kullanılır. Mesaj kimlik doğrulaması için NwkSKey kullanılırken, MAC payload gizliliği için AES-128 algoritmalı AppSKey anahtarı kullanılmaktadır.

2.3.5. LoRaWAN Güvenliği

Bu bölümde LoRaWAN güvenliği incelenmektedir. İki farklı aktivasyon metodu, anahtar yönetimi, kimlik doğrulama ve kriptografi yöntemleri açıklanmaktadır.

2.3.5.1. Aktivasyon Metotları

LoRaWAN ağında bir uç cihaz 2 farklı aktivasyon metodu ile ağa bağlanabilmektedir. Bunlar Hava Yolu ile Aktivasyon (OTAA) ve Kişiselleştirme ile Aktivasyon (ABP) metotlarıdır. Bu metotlar arasındaki temel fark OTAA metodunda katılım prosedürünün ardından oturum anahtarları türetilirken ABP metodunda bu anahtarlar halihazırda cihazlarda bulunur. Dolayısıyla bu iki aktivasyon metodunda oturum anahtarlarının oluşturulması farklılıklar göstermektedir [16], [31].

2.3.5.1.1. Hava Yolu ile Aktivasyon (OTAA)

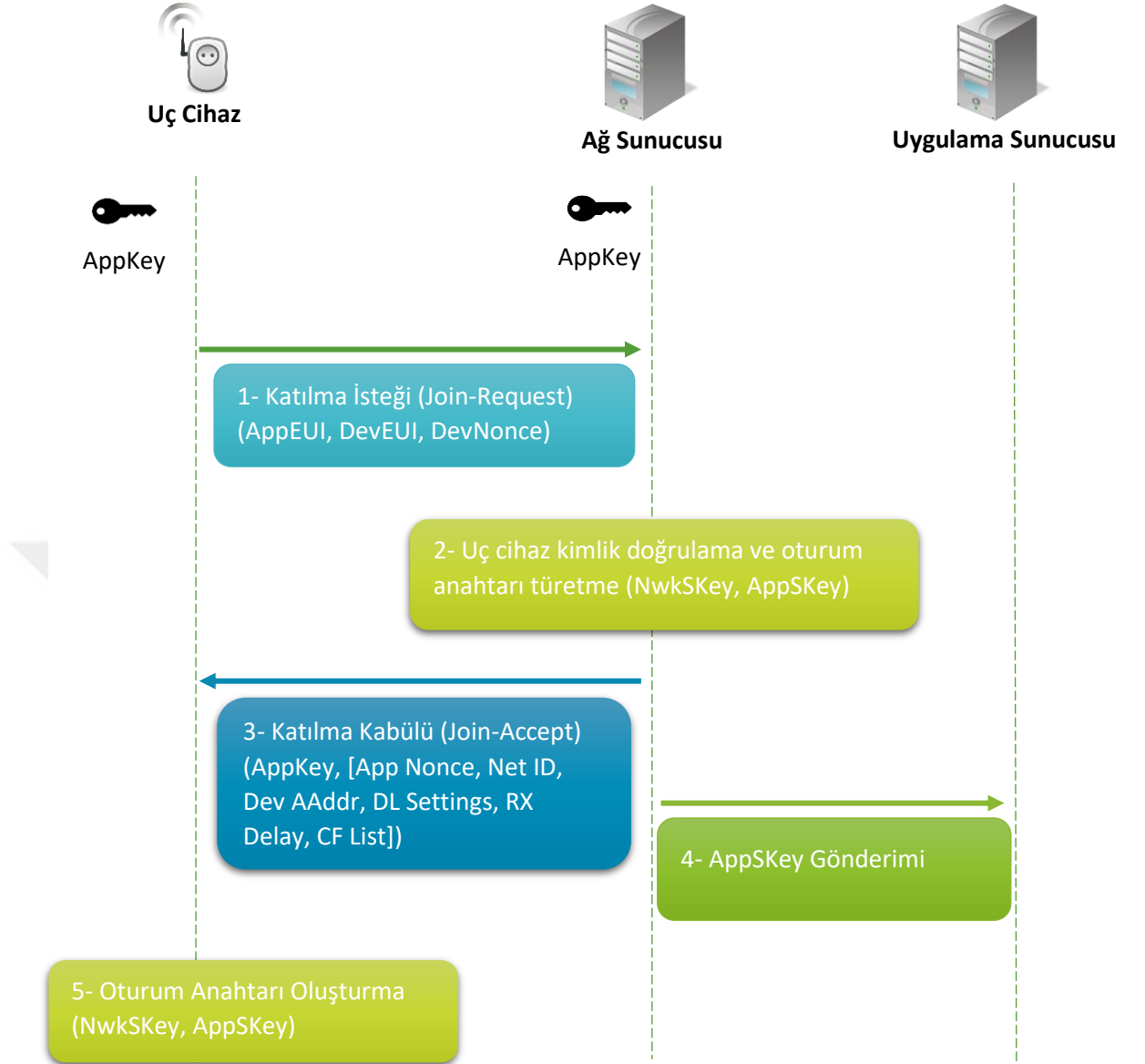
OTAA aktivasyon metodunda uç cihaz ile sunucu kendi aralarında veri alışverişi yapmadan önce katılım prosedürüne uyulması gerekmektedir. Uç cihaz her oturum bilgisini kaybettiğinde yeniden katılım prosedürünü uygulamalıdır. Bu prosedür uç cihaz ile sunucu arasında bir Katılma İsteği (Join-request) ve Katılma kabul mesajından (Join-Accept) oluşmaktadır.

Katılım prosedürüne göre ilk olarak uç cihaz ağ sunucusuna bir katılma talebi mesajını göndererek prosedürü başlatır. Bu mesaj uç cihazda saklı bulunan DevEUI, AppEUI ve DevNonce bilgilerini içermektedir. AES-128 kök anahtarı olan AppKey anahtarı uç cihazda ve ağ sunucusunda saklanmaktadır. Bu anahtar Şekil 2.18’de görüldüğü gibi uç cihaz ile ağ sunucusu arasında kullanılmaktadır [18]. OTAA metodunda aktivasyon prosedürü başlamadan önce uç cihaz DevEUI, AppEUI ve AppKey’i kendi içinde barındırmalıdır. EUI açılımı genişletilmiş benzersiz tanımlayıcıdır ve 64 bit uzunluğunda olup genellikle ağ elemanlarının kimlik tanımlayıcı görevini görür. Uç cihazın kimliği olan DevEUI MAC adres yapısı ile benzerlik gösterirken, Uygulama sunucusunun kimliği olan AppEUI ise port numarası ile benzerlik gösterir. AppKey

ise AES 128 bit bir kök anahtarıdır. MIC değeri bu anahtardan türetilmektedir. Ayrıca uç cihaz ve ağ sunucusu kendi içlerinde sakladıkları AppKey anahtarı aynı olmalıdır.

Katılım mesajı (Join-request) içeriği olan DevEUI ve AppEUI, AppKey tarafından şifrelenmezler. Bu şekilde şifresiz olarak uç cihazdan ağ sunucusuna gönderilen katılım mesajı ağ sunucusuna ulaştığında sunucu öncelikle DevNonce değerinin daha önce kullanılıp kullanılmadığını kontrol eder. Ardından Ağ sunucusu MIC değeri ile uç cihazın kimlik doğrulamasını yapar. MIC değeri AppKey anahtarından türetildiğinden ve uç cihaz ile ağ sunucusu aynı AppKey'e sahip olduğundan, kimlik doğrulaması için ağ sunucusu kendi MIC kodu ile uç cihazdan gelen katılım mesajındaki MIC kodunu karşılaştırarak sonuca ulaşır. Eğer iki MIC değeri aynı ise oturum doğrulaması onaylanır. Ardından katılım kabul mesajı (Join-Accept) MIC değeri ile beraber AppKey tarafından şifrelenerek uç cihaza gönderilir. Aynı zamanda Ağ Sunucusundan Uygulama Sunucusuna AppSKey anahtarı ile DevAddr değeri gönderilir.

Burada kullanılan NwkSKey uç cihaz ile ağ sunucusu arasında yapılan veri alışverişlerinde önemli bir yeri olan MIC değerinin (Mesaj bütünlük kodu) hesaplamasında kullanılır. Ayrıca NwkSKey Yükün (payload) şifrelenmesi veya şifrenin çözülmesinde kullanılır. AppSKey ise uç cihaz ile uygulama sunucusunun uçtan uca iletişimin güvenliğini sağlamakla sorumludur. Uç cihaz ile uygulama sunucusu arasında Yük (Payload) uçtan uca şifrelenmiştir ve şifreleme ile şifre çözme işlemi AppSKey ile yapılmaktadır. Bir diğer nokta ise uç cihaz ile uygulama sunucusu arasındaki veri alışverişinde MIC bulunmaz ve bundan dolayı mesaj bütünlük kontrolü yapılamaz.

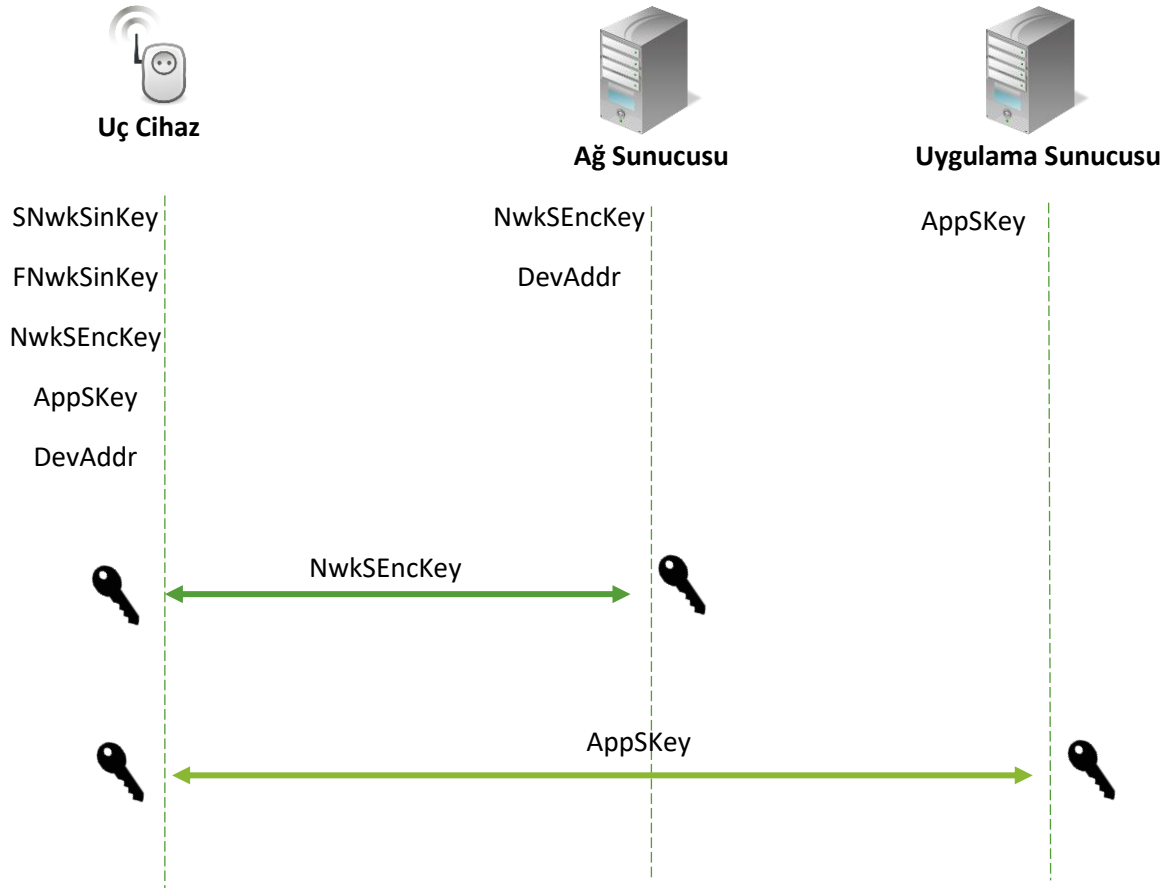


Şekil 2.18. OTAA Metodu

2.3.5.1.2. Kişiselleştirme ile Aktivasyon (ABP)

ABP aktivasyon metodunda bir katılım prosedürü yoktur. Dolayısıyla uç cihaz AppEUI ve AppKey gibi katılım prosedüründe kullanılan değerlere sahip değildir. Bu metotta uç cihaz aktivasyonu katılım prosedürü ile oturum anahtarları türetmek yerine ilk açıldığı andan itibaren kendinde bulunan 4 tane kişiselleştirilmiş NwkSEncKey, AppSKey, SNwkSIntKey, FNwkSIntKey anahtar bulundurmaktadır. Kendi içinde bulundurduğu bu anahtarlar vasıtasıyla doğrudan iletişime hazırdırlar. Her uç cihazın kendine özel 4 oturum anahtarı bulunur ve bu sayede uç cihaz herhangi bir tehlikeye girerse diğer uç cihazlar bu durumdan etkilenmezler [68].

Uç cihaz Ağ sunucusu iletişime geçerken NwkSEncKey oturum anahtarı ile DevAddr kullanılır. Uç cihaz ile ağ sunucusunda halihazırda kimlik doğrulama için uç cihazın DevAddr bilgisi mevcuttur. Aynı şekilde Uygulama sunucusunda DevAddr ve AppSKey bilgileri mevcuttur. Şekil 2.19'da da gösterildiği üzere Uç cihaz Ağ sunucusu veya Uygulama sunucusu ile direk iletişime geçebilir.



Şekil 2.19. ABP Metodu

2.3.5.2. Anahtarlama Yönetimi

LoRaWAN ağlarında güvenlik için AppKey (kök anahtar), NwkSKey ve AppSKey anahtarları kullanılmaktadır. AppKey uygulama sahibi tarafından uç cihazlara konulan 16 byte benzersiz bir anahtardır.

Tablo 2.7. Anahtar özellik tablosu

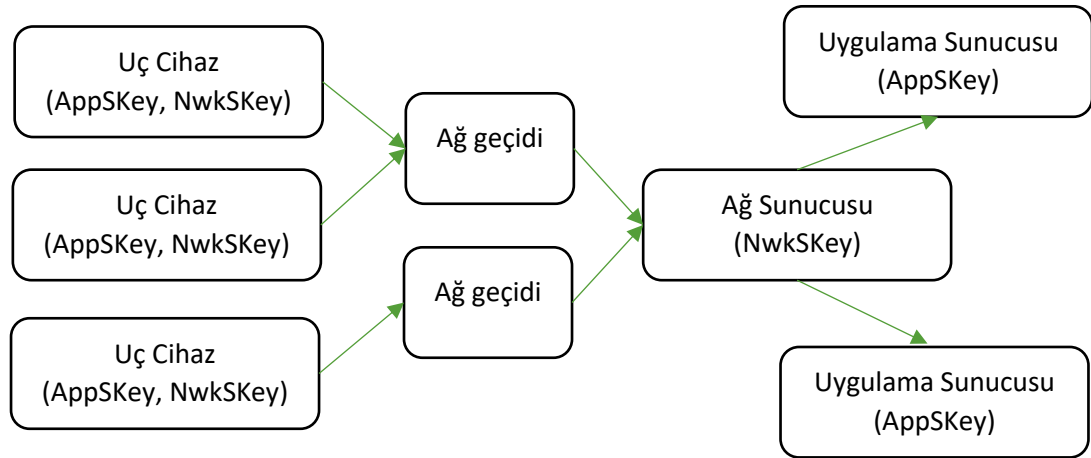
Anahtar Adı	Tipi	Uzunluğu (bit)	Oluşturma	Kullanımı
AppKey	Simetrik	128	Uygulama tarafından	MIC (Katılım/kabul mesajı için)

				Katılım kabul mesajını şifreler Oturum anahtarlarını oluşturur
AppSKey	Simetrik	128	AppKey tarafından	Veri mesajını şifreler
NwkSKey	Simetrik	128	AppKey tarafından	Mesajlar için MIC kullanır Sadece komut içerikli mesajları şifreler

OTAA metodunda Şekil 2.20’de gösterilen diğer iki anahtar, AppKey kullanılarak ve DevNonce ve AppNonce değerleri gözetilerek oluşturulur [81]. Uç cihaz ağa her katıldığında veya sistem sıfırlandığında oturum anahtarları yeniden oluşturulur. Ancak ABP metodunda benzersiz oturum anahtarlar veri alışverişinden önce uç cihazda saklandığından dolayı uç cihaz sıfırlandığında veya ağa yeniden katıldığında yeniden oluşturulmazlar [82], [83].

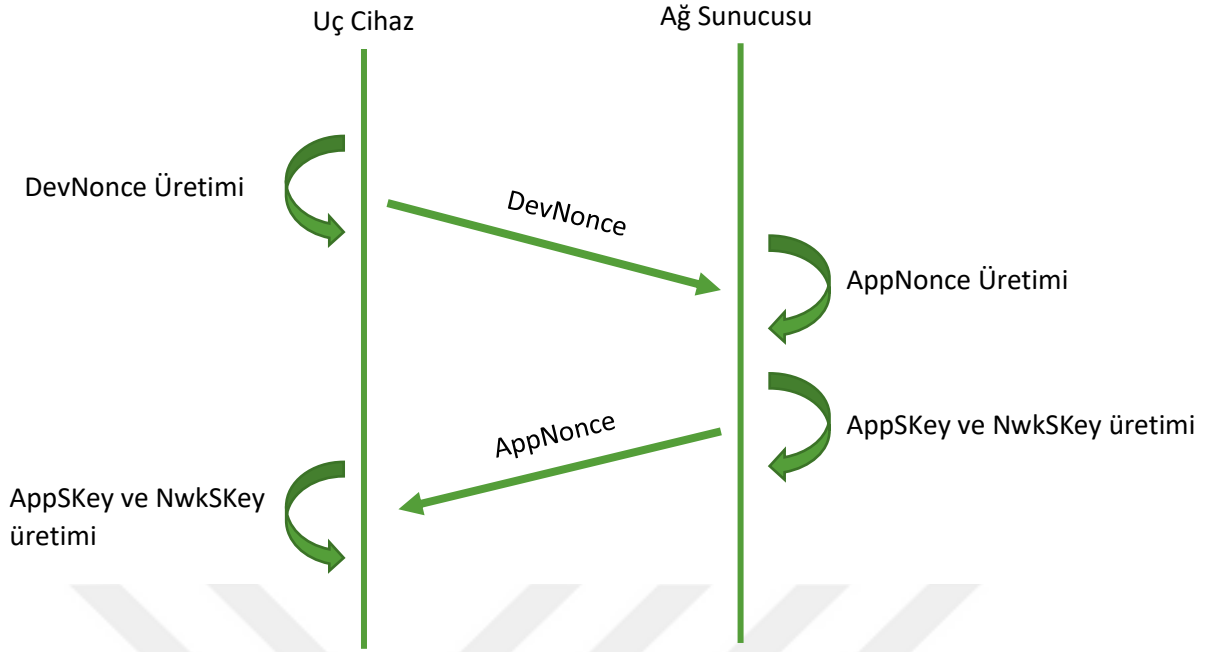
$$NwkSKey = AES128_{Encr}(AppKey, 001 || AppN\ once || NetID || DevN\ once || pad_{16})$$

$$AppSKey = AES128_{Encr}(AppKey, 002 || AppN\ once || NetID || DevN\ once || pad_{16})$$



Şekil 2.20. Oturum Anahtarlarının Kullanımı

OTAA metodunda anahtar değiş tokuşu yapılırken öncelikle uç cihaz ağ sunucusuna DevNonce değeri içeren bir katılım mesajı gönderir. Ağ sunucusu, uç cihazın ağa katılım onayı için kontrol eder ve kabul mesajını gönderirken içerisine AppNonce değerini dahil eder. Uç cihaz ve ağ sunucusu oturum anahtarlarını AppNonce ve DevNonce değerlerine göre oluşturur. Böylece Şekil 2.21’de gözüktüğü gibi anahtarlar yerine sadece iki nonce değeri havadan (OTAA) gönderilir.



Şekil 2.21. OTAA metodunda oturum anahtarları değişimi

2.3.5.3. Kriptografi

2.3.5.3.1. Şifreleme ve Şifre Çözme (Enkript ve Dekript)

Veri Mesajı şifreleme

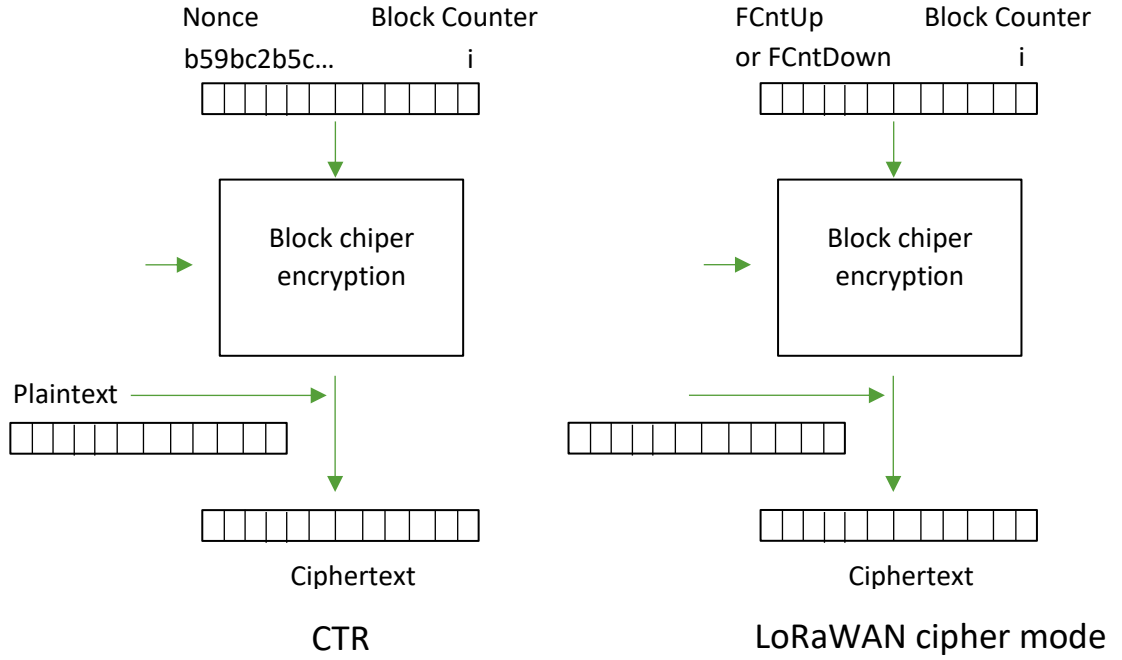
İletişim sırasında önce çerçeve yükü (Frame Payload) şifrelenmektedir. Çerçeve yükü şifrelenirken, içeriğinde sadece MAC komutları barındırıyor ise NwkSKey kullanılır.

Aksi taktirde AppSKey kullanılmaktadır. Şifreleme işlemi aşağıdaki gibidir [39]:

- Define blocks $A_i, i = 1 \dots k, k = \text{ceil}(\text{length}(\text{frame_payload})/16)$
- $S_i = \text{AES128_encrypt}(K, A_i)$ for $i = 1 \dots k, k = \text{NwkSKey or AppSKey}$
- Truncate $(\text{frame_payload} \parallel \text{pad16}) \text{ xor } S$ to the first $\text{length}(\text{frame_payload})$ octets.

Bu şifreleme yöntemi, simetrik bir şifreleme algoritması olan Advanced Encryption Standard (AES)' tir. 128 bitlik blok uzunluğu ve 128, 192, 256 bitlik anahtar uzunluğunu destekler [84]. AES dünya çapında kullanılan ve ABD tarafından kabul edilmiş bir standarttır [85].

Buradaki blok şifreleme modu CTR modu ile benzerlik gösterir. Aşağıdaki şekilde (Şekil 2.22), bir blokta LoRaWAN blok şifreleme modu ile CTR modu karşılaştırılmıştır. CTR modunda, her blokta bir Nonce ve bir blok sayacı olduğu görülebilir [86]. Ancak LoRaWAN için bu nonce değeri, her mesajda sürekli arttırılan FCntUp veya FCntDown değerleri ile değiştirilir [39]:



Şekil 2.22. LoRaWAN Encryption modu ile CTR modu karşılaştırılması

Katılım Mesajı Şifreleme ve Şifre Çözme (Enkript ve Dekript)

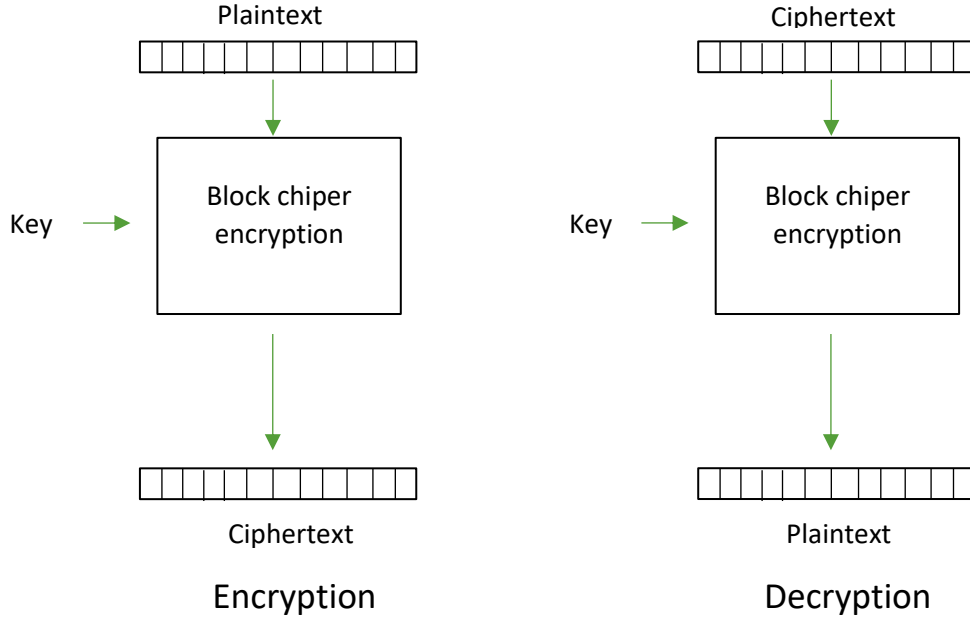
Bu başlık altında katılım isteği mesajlarının şifrelenmediği ve katılım kabul mesajlarının şifrelenmesi gösterilmektedir. İmzalı bir katılım kabul mesajı, aşağıdaki gibi AES128 ECB modu kullanılarak şifrelenir:

AES128_decrypt (AppKey, join_accept | MIC)

Burada şifre çözme işleminin şifreleme için kullanıldığı görülmektedir. Bu gibi durumlarda uç cihaz AES şifreleme işlemini şifre çözme için kullanabilir. Bu durumda işlem karmaşıklığı azalmaktadır.

Bu AES şifrelemesinde ECB modu kullanılmaktadır. Her blok ayrı ayrı şifrelenmektedir. Bu yöntemin dezavantajlarından biri ise düz metin bloklarının aynı şifreli metin bloklarına şifrelenmesidir. Bundan dolayı veriler iyi bir şekilde gizlenemez. Bazı durumlarda ciddi mesaj gizlilik sorunları ortaya çıkabilmekte ve bundan dolayı kriptografiyle ilgili protokollerde kullanılması tavsiye edilmez [87].

Buna rağmen, ECB modu yalnızca katılım isteğinde kullanıldığından ve Nonce nedeniyle bu mesaj hiçbir zaman tekrarlanmayacağından, LoRaWAN'ın ECB modunu kullanması güvenlidir.



Şekil 2.23. ECB cipher blok modu

2.3.5.3.2. Mesaj İmzalama

LoRaWAN’da mesaj bütünlüğünü sağlamak için MIC kodu kullanılır.

Veri Mesajı İmzalama

Mesajları imzalamak için NwkSKey kullanılır. Yukarı bağlantı (UL) mesajları ağ sunucusuna ulaştığında, sunucu önce mesaj bütünlüğünü kontrol eder ardından kontrolden başarıyla geçen mesajı uygulama sunucusuna iletir.

2.3.5.3.3. İmzalama ve Şifreleme Sırası

LoRaWAN ağlarında mesajlar imzalanmalı ve şifrelenmelidir. Fakat bu sıralama veri mesajları ile katılım kabul mesajlarında değişmektedir. Katılım kabul mesajlarında, mesaj önce imzalanıp ardından şifrelenirken veri mesajları önce şifrelenip ardından imzalanmaktadır. Bu iki durumda temel fark şifreli metnin bütünlüğünün sağlanması veya sağlanmamasıdır. İmzala ve şifrele yönteminde şifreli metnin bütünlüğü kontrolü sağlanmamaktadır. Bunun nedeni bütünlük kontrolünün şifre çözme işleminin ardından yapılmakta olmasıdır. Şifreli metnin bütünlüğü olmadan saldırganların şifresini çözebildiği farklı şifreli metinler oluşturması mümkün olmaktadır.

Şifrele ve imzala yöntemi ise şifreli metnin bütünlüğünü sağlamaktadır. Ancak bu durumda ise veri mesajları için şifre çözme ve imza kontrolü iki sunucuda yapıldığından, imza kontrolü ve şifre çözme arasında, veriler değişime ve düzeltmeye açık kalmaktadır.

2.3.5.4. Sayaç Yönetimi

Sayaçlar

Her uç cihazda iki çerçeve sayacı vardır. Bunlar FCntUP ve FCntDown sayaçlarıdır. FCntUp uç cihazdaki yukarı bağlantı mesajlarını sayarken FCntDown sayacı ise ağ sunucusundaki aşağı bağlantı mesajlarını saymaktadır. Yukarı bağlantı ve aşağı bağlantı mesajlarını senkronize tutmak için bir maksimum limit değeri olan MAX_FCNT_GAP değeri vardır. Yukarı bağlantı ve aşağı bağlantı mesajlarının sayıları arasındaki fark MAX_FCNT_GAP değerinden büyük olması durumunda, mesajların dengelenmesi için dengeyi bozanlar çıkarılmaktadır. Bundan dolayı LoRaWAN protokolündeki sayaç mekanizması paket kaybını önlemektedir. Bu sayaç değerleri hem şifreleme hem de imzada kullanılmakta ve aynı değer hiçbir zaman tekrardan kullanılmamaktadır.

Sayaçların Sıfırlanması

LoRaWAN, 16 ve 32 bitlik çerçeve sayaçlarını destekler. Sayaçlarda herhangi bir taşma durumunda sayaç tekrardan 0 değerinden başlatılır. Ayrıca Uç cihaz her sıfırlandığında sayaç değeri de 0 değerinden başlatılır [88].

2.3.5.5. Kimlik Doğrulama

Nesnelerin İnternetinde kimlik doğrulama diğer bir adı Authentication olarak da bilinmektedir. Authentication, bilgileri İnternet gibi güvenli olmayan bir ağ üzerinden seyahat ederken verileri korumak ve erişimi kontrol etmek için IoT makinelerinin ve cihazlarının kimliğine güven oluşturmaya yönelik bir modeldir.

Kimlik doğrulama ayrıca, saldırganların kayıtlı konuşmalar, görüntüler ve diğer potansiyel olarak hassas bilgiler gibi sunuculardaki verilere erişme umuduyla IoT cihazları olduklarını iddia etmelerini önlemeye yardımcı olur.

IoT cihaz iletişimlerini güvenli hale getirmek için güçlü kimlik doğrulaması elde edebileceğimiz birkaç yöntem vardır:

- Tek yönlü kimlik doğrulaması
- İki yönlü kimlik doğrulama
- Üç yönlü kimlik doğrulama
- Dağıtılmış kimlik doğrulama
- Merkezileştirilmiş kimlik

IoT Yetkilendirmesi

Nesnelerin İnterneti (IoT) yalnızca tek bir teknoloji değil, insan etkileşimi olmadan bağımsız olarak birlikte çalışan çeşitli makinelerin (“nesneler”) bağlantılı bir ortamıdır.

Yetkilendirme süreci, IoT sistemindeki her bir uç noktanın kimliğini doğrulamak için kullanılan araçtır. Sertifikasyon süreci, kayıt girişinin ardından yapılandırılır ve kayıt sırasında sistemin kimliği kontrol edilirken kullanılacak yöntemi hizmet sağlayıcıya bildirir [45].

2.3.6. Neden LoRaWAN?

LoRaWAN geniş kapsama alanı, çevik iş modeli ve kolay kurulumu ile Sigfox ve NB-IoT gibi rakip teknolojilere göre daha yaygın kullanılmaktadır. Düşük maliyeti ve yüksek verimi ile tercih sebebi olan LoRaWAN kullanımı için önde gelen nedenler sıralanmıştır.

- **Ultra düşük güç kullanımı.** LoRaWAN uç cihazları düşük güç modunda 10 seneye kadar pil ömrü sağlayabilmektedir
- **Uzun menzil.** LoRaWAN kırsalda 10km’ye kadar yoğun kentsel alanlarda ise 3km’ye kadar menzil sağlayabilmektedir.
- **İç mekân kapsama alanı.** LoRaWAN bina gibi çok katlı yapılarda kolaylıkla kullanılabilir.
- **Lisanssız bantlarda çalışması.** LoRaWAN ağı lisanssız frekanslar kullandığından, lisans ücreti ödenmemektedir.
- **Konum tespiti.** LoRaWAN ağı uç cihazların konumlarını belirlemek için GPS’e ihtiyaç duymamaktadır. 3 farklı ağ geçidinin sinyal alması, uç cihazın konumunun bulunmasında yeterlidir.
- **Yüksek işleme kapasitesi.** Ağ sunucuları binlerce ağ geçidinden gelen milyonlarca mesajı işleme yeteneğine sahiptir.

- **Ağı genişletme.** Aynı donanım ve yazılım kullanılarak bir LoRaWAN ağını genişletmek mümkün ve kolaydır.
- **Uçtan uca güvenlik.** LoRaWAN AES-128 şifreleme protokolünü kullanmaktadır. Bu sayede uç cihaz ile uygulama sunucusu arasında güvenli iletişim sağlanmaktadır.
- **OTA ile güncelleme alması.** Bu sayede uç cihazlar uzaktan güncellenebilmektedir.
- **Düşük maliyet.** LoRaWAN, minimum altyapı maliyeti, düşük maliyetli uç cihazlar ve açık kaynak yazılım sunmaktadır.
- **Roaming.** LoRaWAN uç cihazlara bir ağdan diğerine sorunsuz geçişler sunmaktadır.
- **Sertifika programı.** LoRa Alliance sertifika programı uç cihazları sertifikalandırarak güvenilirliği arttırmaktadır.
- **Ekosistem.** LoRaWAN ağ geçidi, uç cihazlar, antenler, ağ servisleri ve uygulama geliştiricileri ile geniş bir ekosisteme sahiptir.



3. LoRaWAN ZAAFIYETLERİ VE RİSK ANALİZİ

3.1. Analiz Metodu

LoRaWAN ağının güvenlik açıkları ve zayıflıklarını bulmak için bir saldırgan gibi düşünmek durumu kolaylaştırabilmektedir. Bunun avantajı, olası saldırıların önceden değerlendirilmesi ve sorunun kaynağını bulup erken çözüm üretebilmek ve olası bir saldırının ilk hedeflerini tespit edebilmektir.

Bu bölümde LoRaWAN ağının zafiyetleri ve bu ağa karşı yapılabilecek saldırıların analizi için kullanılan yöntemden adım adım bahsedilmiştir.

3.1.1. LoRaWAN Güvenliği İçin Kullanılan Parametrelerin Zayıf Noktaları ve Saldırganın Hedefini Belirlemek

Bir saldırıda, saldırının hedefi iki farklı açıdan ele alınabilir. Bunlar ağın güvenliği ve ağ güvenliği için kullanılan değerleridir. Bir ağın güvenlik özellikleri tanımlanırken 3 özelliğe bakılır. Bunlar gizlilik (confidentiality), bütünlük (integrity) ve erişebilirliktir (availability). Bu özellikler, güvenlik gereklilikleri arasında en popüler olanlardır ve bir güvenlik zafiyeti araştırmak için öncelikle bu üç özelliğe bakılmalıdır. Bir ağda güvenlik parametrelerinin zafiyeti bütün ağı tehlikeye atabilir. Bir güvenlik değerinin etkisi birincil veya ikincil değer olmasına göre değişkenlik göstermektedir. Birincil bir değerde bir zafiyet varsa bu bütün sistemi istismara açık hale getirirken ikincil bir değerdeki zafiyette istismar daha sınırlı olmaktadır. Tablo 3.1’de LoRaWAN ağındaki birincil ve ikincil değerler gösterilmiştir.

Tablo 3.1. LoRaWAN ağı güvenliği için kullanılan değerler

Değerler	Birincil/İkincil
NwkSKey	Birincil
FrmPayload	Birincil
AppSKey	Birincil
DevNonce	İkincil
AppNonce	İkincil
Fcnt	İkincil
AppKey	İkincil
MAC komutları	İkincil

DevAddr	İkincil
ACK	İkincil

NwkSKey: Bu anahtar uç cihaz aktivasyonu sırasında oluşturulur ve mesajı imzalamak için kullanılmaktadır. NwkSKey anahtarının gizlilik ve bütünlüğünün zafiyeti üzerine bir olasılık düşünürsek, gizliliği ihlal edildiğinde dışarıdan bir saldırgan kendi mesajını oluşturup NwkSKey anahtarını kullanabilir ve fark edilmeden imza kontrolünden mesajını geçirebilir. NwkSKey anahtarının bütünlüğünün ihlal edildiği bir olasılıkta ise mevcut oturumdaki tüm mesajlar imza kontrolünden geçemez ve reddedilir.

FrmPayload: Bu değer birincil bir değer olup taşıdığı veriler önemlidir. Sensör verileri bu FrmPayload üzerinden iletilmektedir. FrmPayload değerinin gizlilik ve bütünlüğünün zafiyeti üzerine bir olasılık düşünürsek, gizliliği ihlal edildiği bir durumda sensör verileri üçüncü bir tarafın eline geçebilir. Eğer bütünlüğü ihlal edilirse, bu durumda sensörlerden gelen veriye güvenilemez.

AppSKey: Bu anahtar uygulama sunucusunda kullanılır ve mesajların şifresini çözmek için kullanılmaktadır. AppSKey anahtarının gizlilik ve bütünlüğünün zafiyeti üzerine bir olasılık düşünürsek, gizliliği ihlal edildiği bir durumda tüm mesajların şifresi çözülmeye müsait olacağından tüm ağın gizliliği tehlikeye girebilir. AppSKey anahtarının bütünlüğünün ihlal edildiği bir olasılıkta ise uç cihaz veya uygulama sunucusu, mesajların şifresini çözemeyeceğinden gelen veriler işe yaramayacaktır.

DevNonce: DevNonce değeri uç cihaz tarafından üretilen bir benzersiz bir değerdir. Sadece OTAA metodu ile aktivasyon durumunda kullanılmaktadır. DevNonce değeri, NwkSKey ve AppSKey anahtarlarını oluşturmak için uç cihazdan ağ sunucusuna gönderilerek AppKey tarafından şifrelenir ve oluşturulan anahtarlar uç cihaza gönderilir. DevNonce değerinin bütünlüğü ihlal edildiği bir olasılıkta uç cihazda ve sunucuda üretilen oturum anahtarları farklı olacağından aralarında iletişim kurulamaz.

AppNonce: Bu değer ağ sunucusunda bulunur ve DevNonce ile AppKey vasıtasıyla oturum anahtarlarını oluşturmada kullanılmaktadır. AppNonce değerinin gizlilik ve bütünlüğünün zafiyeti üzerine bir olasılık düşünürsek, AppNonce değerinin gizliliği ihlal edildiği bir durumda, saldırgan oluşturulacak oturum anahtarlarını kolaylıkla tahmin edebilir ve bu durum tüm sistemi istismara açık hale getirir. AppNonce

değerinin bütünlüğü ihlal edilirse, bu durumda uç cihaz ile ağ sunucusunun oluşturduğu oturum anahtarları birbiri ile eşleşmeyeceğinden aralarında iletişim kurulamaz.

FCnt: Bu bir sayaç değeri olup şifresiz bir metin halinde uç cihazda ve sunucuda saklanmaktadır. Uç cihaz ile sunucunun senkronizasyonunda kullanıldığından, bu değer bütünlük ihlali durumunda senkronizasyon sorunu ortaya çıkmakla beraber saldırganın tekrarlama saldırısı (replay attack) yapmasını mümkün kılabilir.

AppKey: Bu anahtar OTAA kullanan uç cihazların aktivasyonu için gereken NwkSKey ve AppSKey anahtarlarının türetilmesinde kullanılmaktadır. Aktivasyondan önce hem uç cihaz hem de sunucuya tanımlanmalıdır. AppSKey anahtarının gizlilik ve bütünlüğünün zafiyeti üzerine bir olasılık düşünürsek, gizliliğin ihlal edildiği bir durumda saldırgan katılım isteği üzerinden tekrarlama saldırısı yapmaya müsait olur. AppKey anahtarının bütünlüğü ihlal edilirse, bu durumda OTAA aktivasyonu sağlanamadığından uç cihaz LoRaWAN ağına bağlanamaz.

MAC Komutları: MAC komutlarının gönderimi FrmPayload veya FOpts değerlerinin içinde gönderilebilir. MAC Komutlarının gizliliği ve bütünlüğünün korunması önemlidir. Aksi takdirde komutların üçüncü bir kişinin eline geçmesine ve ele geçirilen komuta göre sistem ihlaline sebep olabilmektedir.

DevAddr: Bu değer şifresiz olup uç cihazın kimliğini belirtir. DevAddr değerinin bütünlüğünün ihlal edilmesi durumunda uç cihaz ile sunucu haberleşmesi sağlanamamaktadır.

ACK: Bu parametre şifrelenmemiş olup, alınan mesajı onaylamakta kullanılmaktadır. ACK parametresinin bütünlüğünün ihlal edildiği bir durumda, bu değer değiştirilip ACK parametresinin etkisiz kılınması mümkündür.

3.1.2. Saldırganın Olası Bir Sızmada Hasar Verme Kapasitesinin Tahmini

Bu alt başlıkta, Dolev-Yao modeline [89] göre saldırganın etki kapsamı tanımlanmaktadır. Bu modele göre saldırgan tüm ağı kontrol altına alabilmekle beraber ağda mesajları değiştirebilme, iletişimi kesme ve manipüle etme yetkinliğine sahiptir. Bu saldırganın saldırı kapasitesini LoRaWAN ağına uyarlırsak bunlar:

- Fiziksel olarak cihazlara erişme,

- Verileri işleme ve depolama,
- OTAA aktivasyonunda mesajı yakalama ve kendi mesajını gönderme,
- Oturum anahtarlarının ihlali durumunda şifreleme ve şifre çözme,
- LoRa ağı ve cihazlar, sensörler hakkında bilgi sahibi olma

3.1.3. LoRaWAN Özelliklerinin Tanımı ve Saldırılarına Karşı Zayıflıklarının Tanımlanması

Kablosuz Haberleşme: Bir saldırgan için kablosuz haberleşme birçok açıdan saldırgana ihlal fırsatları verebilmektedir. Özellikle sensörlerin kullandığı kablosuz ağlarda ekstra güvenlik önlemi yoksa bu durum saldırganın iştahını arttırabilmektedir.

Limitli Depolama Alanı ve Bellek: Uç cihazların kısıtlı bellek ve depolama kapasitelerinden dolayı güvenlik önlemleri de görece basit olmaktadır. Bu durumun dezavantajı ise saldırganın belleği sömürmesi ve fazla tüketmesine sebep olması gibi saldırılara açık olabilmesidir.

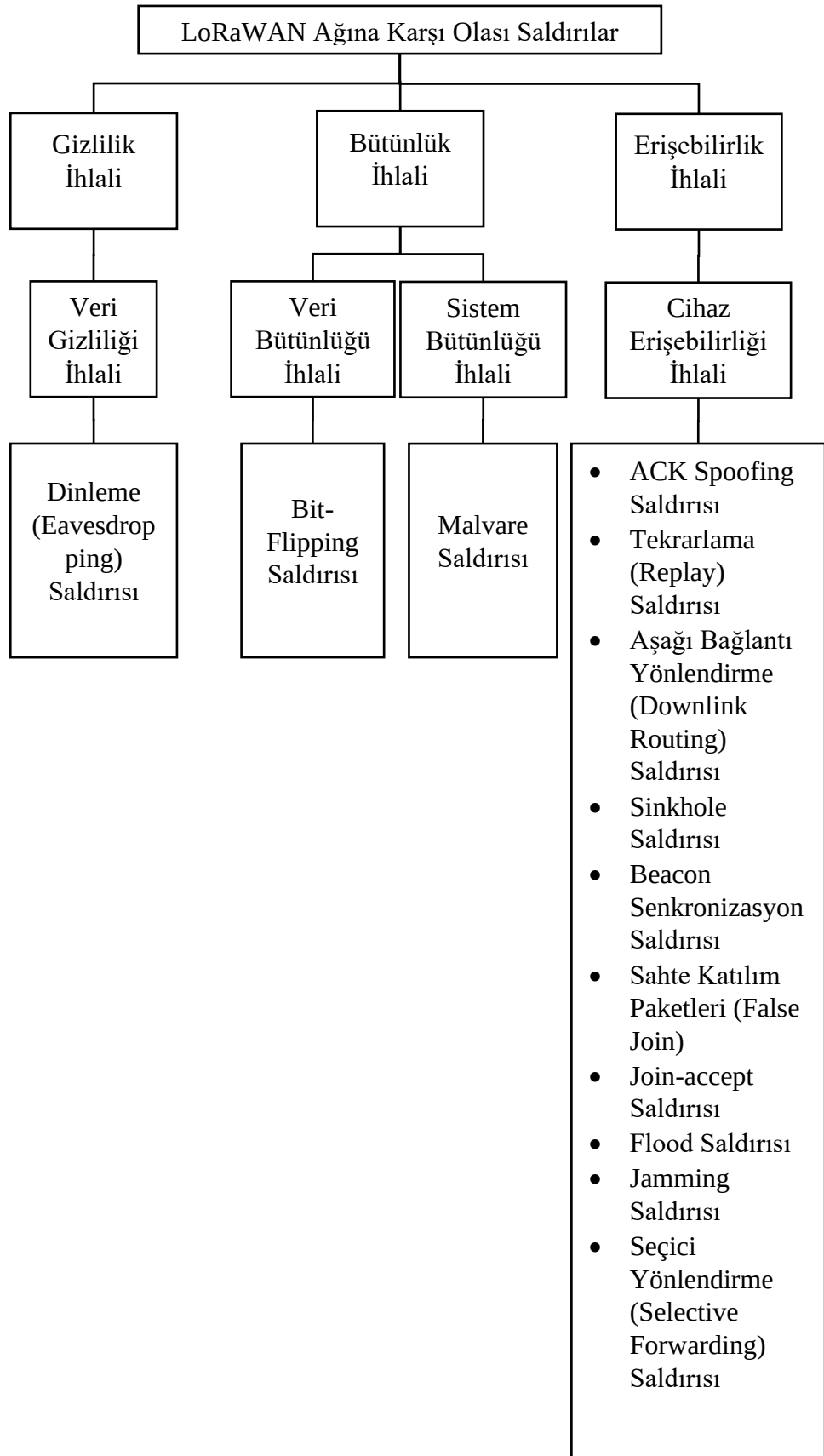
Gecikme: LoRaWAN ağına A ve B sınıflarında aşağı bağlantı gönderimleri kısıtlı enerji kaynağından dolayı gecikmeli gönderilmektedir. Bu durum kritik raporlar veya güvenlik problemlerinde, senkronizasyonun gecikmesinden kaynaklı olarak güvenlik riski oluşturabilmektedir.

3.1.4. Saldırı Çeşitlerini Kategorize Etme

LoRaWAN ağına yönelik olası tehditler bu başlık altında Tablo 3.2’de gösterilmiştir. Bu şekilde tehditler gizlilik, bütünlük, erişebilirlik ve kimlik doğrulama olarak kategorilerine göre ayrılıp gösterilmiştir.

Kablosuz ağlara karşı birçok saldırı çeşidi olsa da bu tezde odaklanılan kısım sadece LoRaWAN protokolünün güvenliğine karşı olan saldırılar olduğundan fiziksel saldırılar gibi LoRaWAN protokolü özelinde olmaya saldırılar odağımızda değildir. LoRaWAN protokolüne karşı yapılabilecek saldırı çeşitlerinin detaylarına “Saldırı Çeşitleri” başlıkta değinilmektedir.

Tablo 3.2. LoRaWAN ağına karşı olası saldırılar



3.1.5. Saldırı Senaryoları

Analiz metodunun 5. kısmı saldırı senaryoları üzerinedir. Ardından bu saldırıların LoRaWAN ağına nasıl etkiler yapabileceği detaylı olarak gösterilmiştir.

3.2. LoRaWAN’a Karşı Yapılabilecek Saldırıları

Çalışmanın bu bölümünde, LoRaWAN ağına yapılabilecek saldırılardan 4 tanesi, analiz metodundaki adımlara göre incelenip gösterilmektedir.

3.2.1. Dinleme (Eavesdropping) Saldırısı

3.2.1.1. Saldırının hedefi

Bu saldırı, LoRaWAN ağında güvenlik için kullanılan şifreleme metodunu aşmayı hedeflemektedir. Saldırgan kablosuz ağ trafiğini dinleyerek ağ sunucusu ile uç cihaz arasında gidip gelen aynı sayaç değeri taşıyan iki mesajdan yola çıkarak şifreli veriyi çözebilmektedir.

Ardından sistemin gizliliği ihlal edildiğinden saldırgan, ağda iletilen sensör verilerine ulaşabilmekte daha önemlisi, iletilen verilerin önem derecesi yüksek ise, bu durumda daha büyük bir gizlilik ihlaline sebep olabilmektedir.

3.2.1.2. Saldırının ihtiyaçları

Dinleme saldırısını gerçekleştirebilmek için saldırganda olması gerekenler:

- Uç cihaz hakkında gerekli temel bilgilere sahip olmak (mesaj formatı, mesaj tipi),
- Kablosuz ağda paketleri dinlemek için bir LoRaWAN dinleme (sniffer) cihazı,
- LoRaWAN ağı trafiğini izlerken aynı zamanda depolamak için bir veritabanı

Ayrıca saldırganın uç cihazı sıfırlama kabiliyeti olduğu bir durumda, saldırının başarılı olma oranı artabilmektedir.

3.2.1.3. Protokolün zafiyeti

Bu saldırının başarıya ulaşmasının sebepleri, protokoldeki iki zafiyettir. Bunlardan biri ABP aktivasyonu metodundan kaynaklı, diğeri ise sayaçların güvenliğinin sağlanamamasından dolayıdır. Bu saldırının kullandığı bir diğeri zafiyet ise blok şifreleme metodunun güvenliğinin yeterli olmamasından kaynaklanmaktadır. Yukarıda

LoRaWAN'ın teknik özelliklerinin anlatıldığı kısımda bahsedilen bu modda, veri mesajlarının blokta bir nonce değeri yerine sayaç kullanmasından kaynaklı bir zayıflık içermektedir.

Her bir sıfırlamada, şifreleme için kullanılan anahtar statik olduğundan aynı sayaç değeri tekrar kullanıldığında aynı anahtar kullanılır. Bundan dolayı aynı sayaç değerini kullanan iki mesaj için aynı anahtar kullanılacaktır. Bu durumu kullanan saldırgan aynı anahtarı kullanan mesajlardan birini ele geçirdiği durumda, şifrelemeyi ihlal edilebilmektedir.

Aynı anahtar tarafından şifrelenen iki mesaj üzerinden gidersek;

$$\text{ŞifresizMesaj1} \oplus \text{Anahtar} = \text{ŞifreliMesaj1}$$

$$\text{ŞifresizMesaj2} \oplus \text{Anahtar} = \text{ŞifreliMesaj2}$$

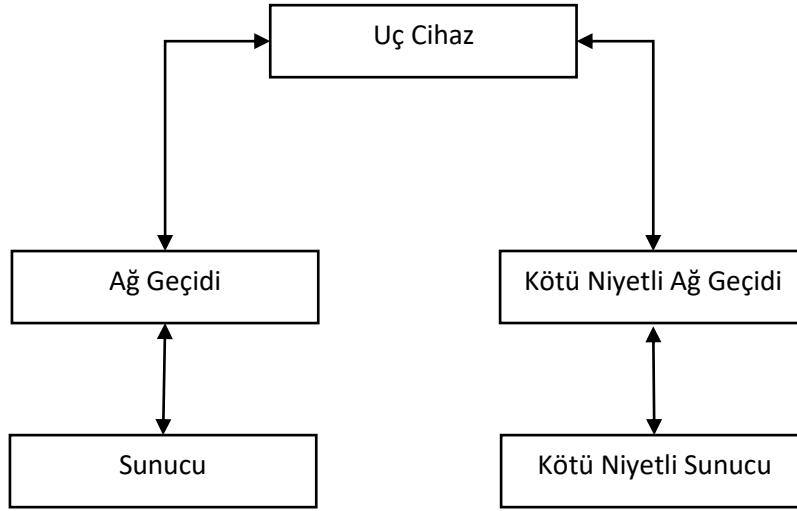
Bu durumda;

$$\text{ŞifresizMesaj1} \oplus \text{ŞifresizMesaj2} = \text{ŞifreliMesaj1} \oplus \text{ŞifreliMesaj2}$$

Mesajın şifrelenmiş hali bilindiğinden, mesajın şifrelenmemiş halinin okunabilir hale getirilmesi işlemi için öncelikle birinci şifresiz mesajın bir kısmı tahmin edilmeye çalışılır ve ikinci şifresiz mesaj ortaya çıkarılmaya çalışılır. Bu tahmin işleminde de ayrıca farklı kalıplar vardır. Şifreli mesajı okunabilir hale getirme olasılığını arttırmak için kullanılan yöntem ise devamlı cihazı sıfırlamaktır. Bu yöntem “crib dragging” yöntemi olarak adlandırılmaktadır [90].

3.2.1.4. Saldırının detaylı açıklaması

Şekil 3.1’de LoRaWAN ağında bir dinleme (eavesdropping) saldırısında saldırganın paketleri yakalaması için gerekli kurulum gösterilmiştir.

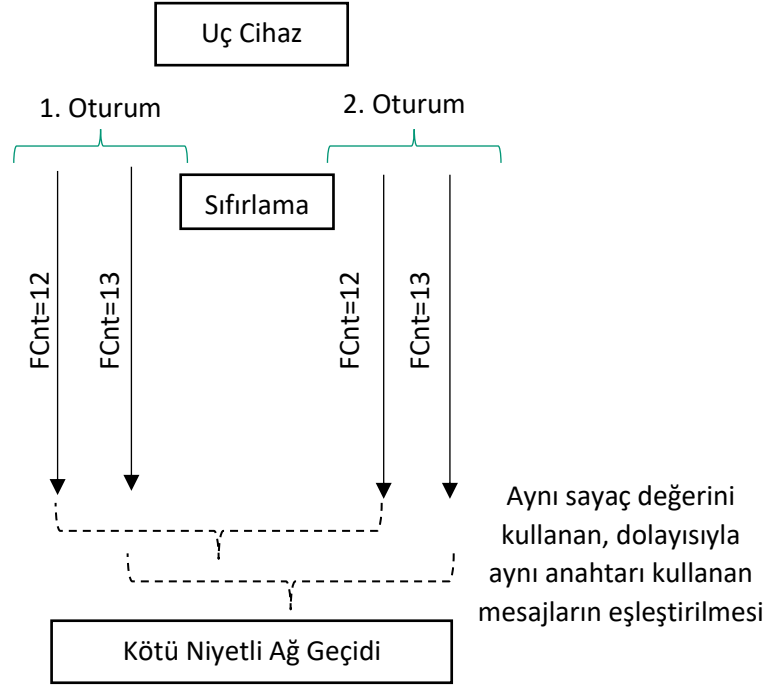


Şekil 3.1. LoRaWAN için Dinleme Saldırısı

Saldırı adımları;

- LoRaWAN paketleri yakalanır ve kaydedilir.
- Sıfırlama yapıp paketler dinlenmeye ve kaydedilmeye devam edilir. Ardından sıfırlamadan önce ve sonra yakalanan paketler karşılaştırılıp aynı sayaç değerine sahip paketler eşleştirilir.
- Crib dragging metodu uygulanıp sonuçlar çıkarılır.

Şekil 3.2’de gösterilen bir dinleme saldırısı örneğinde de gözüktüğü gibi, saldırgan kötü niyetli ağ geçidi ile uç cihazdan gelen mesaj paketlerini dinlemektedir. Aldığı mesaj paketlerini kaydederek, ardından sıfırlayıp aynı işlemi tekrar yapmakta ve sayaç değeri aynı olan mesaj paketlerini eşleştirerek mesajın şifresiz haline ulaşmayı hedeflemektedir.



Şekil 3.2. Dinleme (Eavesdropping) saldırısı örneği

3.2.1.5. Saldırı senaryosu

Aktivasyon metodu olarak ABP metodunu kullanan LoRaWAN aygıtları için Dinleme (Eavesdropping) saldırısının hedefi iletilen verilerin gizliliğini ihlal etmektir. Saldırganın öncelikli olarak bir LoRaWAN alıcısına ihtiyacı vardır. Bu alıcı ile mesajları alıp şifre çözme işlemini gerçekleştirmelidir.

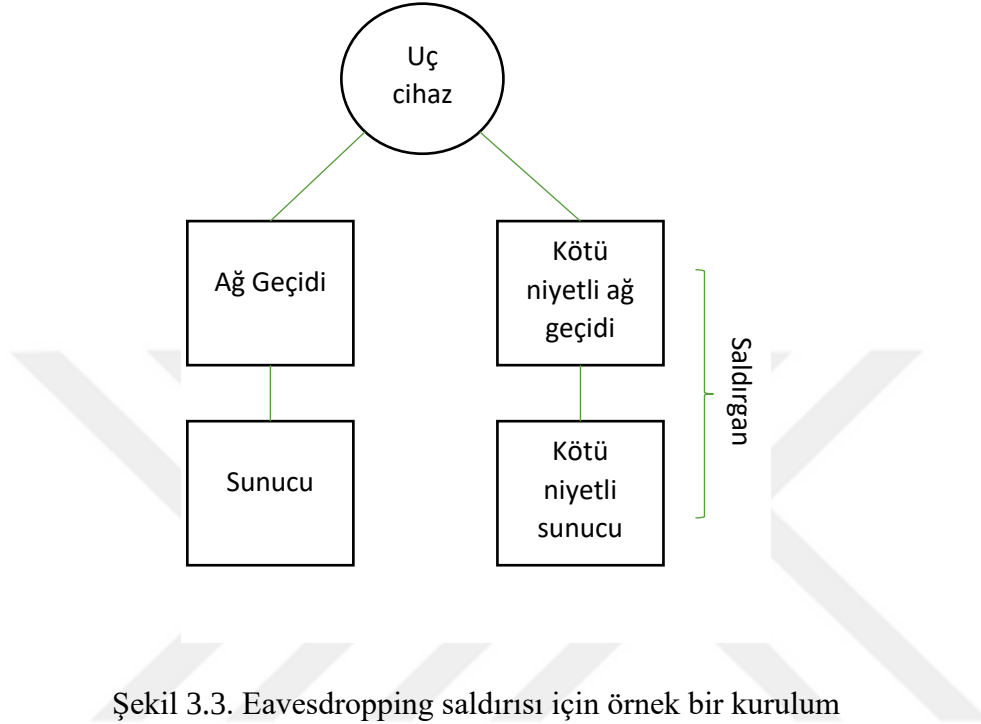
Aynı sayaç değerine sahip mesajları eşleştirmeye dayalı bu yöntem için saldırı uç cihazı sıfırlayarak mesaj yakalama işlemine devam etmeli ve birkaç sıfırlamadan sonra şifreli mesajı çözmek için gereken veriyi elde etmiş olması gerekmektedir. Sıfırlama yapılmazsa yeteri kadar mesaj almak için uzun süre beklenmesi gerekebilir.

Saldırgan alınan şifreli mesajı bir kere çözdükten sonra, alınan diğer şifreli mesajları da çözülebilir hale getirmiş olacaktır. Böylelikle oturum anahtarı değiştirilmediği sürece veri gizliliği ortadan kalkmış olacaktır.

3.2.1.6. Uygulama

Bir Eavesdropping saldırısını gözlemlemek için yapılan uygulamalar araştırılmış ve bu doğrultuda, Yang'ın çalışmasındaki uygulamaya bu çalışmada yer verilmiştir [87]. Yang, yaptığı deneyi bir uç cihazı yapılandırıp periyodik olarak veri mesajı gönderme

varsayımı üzerine kurmuştur. Kurulan bir LoRaWAN ağında kullanılan ağ geçidi, kötü amaçlı bir ağ geçidi rolünde kullanılmış ve uç cihazdan gelen yukarı bağlantı mesajlarını izlemiştir.



Şekil 3.3. Eavesdropping saldırısı için örnek bir kurulum

Prosedür: Bu saldırıda 2 farklı mesaj içeriği olabileceği varsayılmaktadır.

1. Varsayım: Alfanümerik olmayan düz metin ve sayılardan oluşur

- Mesaj formatını tanımlama

LoRaWAN hakkında bilgi sahibi bir saldırgan, ağdaki mesaj formatını çözebilmektedir. Bu durumda, cihaz adres bilgisi ve sayaç değeri gibi parametreler ulaşılabilir olmaktadır.

- Çerçeve tanımlama

Bu uygulamada varsayılan olarak, bir ışık sensörü değeri ve sıcaklık değeri içeren 16 baytlık bir çerçeve yükü içermektedir. Bu cihaz hakkındaki temel bilgilerle, çerçeve yükü için aşağıdaki gibi çerçeve yükleri türetilir:

- Karakterler sadece boşluk ve numaradan oluşabilir. Uzunluğu 8 bit ve her bir karakter için yalnızca 12 ihtimal olabilir.
- Mesaj, sıcaklık ve ışık değeri için aralarında boşluk karakteri olacak şekilde 2 parçaya ayrılabilir.

- Mesajın ilk parçasında ışık değeri bulunur. Bu kısımda en az 2 karakter bulunur.
- Mesajın ikinci parçasında ise sıcaklık değeri bulunur. Burada sıcaklık için 3 karakter vardır.
- Python ile tahmin modelini oluşturma
 - Birinci parça hedef olarak ve ikinci parça ise referans olarak seçilir.
 - Her bir karakter için 12 ihtimali değerlendirip ikinci metnin okunabilir olup olmaması kontrol edilir.
 - Olası seçenekleri azaltmak için belirli kalıplar kullanılır.
 - Hedef seçilen birinci parçanın bulunması için sıfırlama süreleri arttırılır.
- İstatistik için deney sürelerini arttırma

2. Varsayım: Alfanoümerik karakterlerden oluşan düz metin

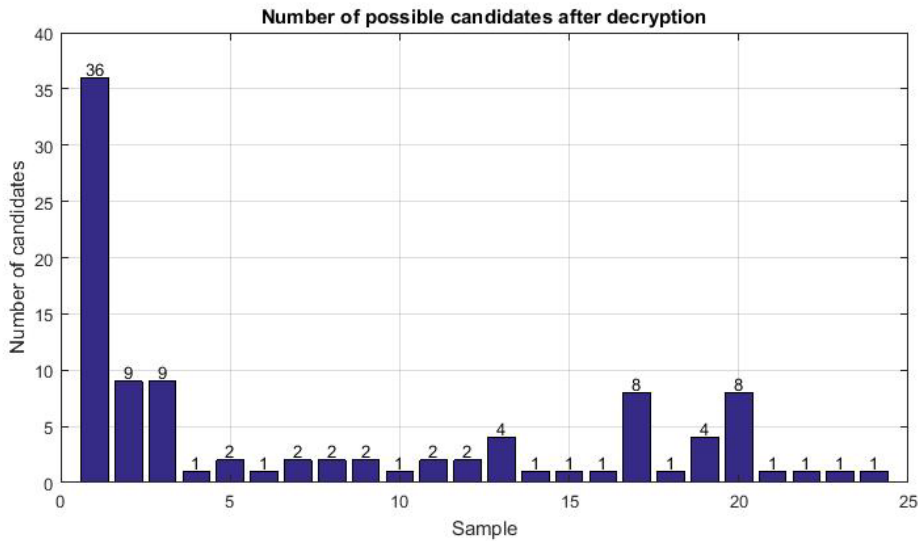
Alfanoümerik karakter içeren mesajların şifrelerini çözmek için Crib dragging metodu kullanılmaktadır. Saldırı başlangıcında, bir kelime tahmin edilir ve karşılık gelen kelime türetilir. Örneğin:

- Alfanoümerik karakterlerden oluşan mesaj, kurban tarafından sunucuya gönderilir ve sayaç sıfırlanır.
- Saldırgan kablosuz ağ trafiğini dinleyerek ele geçirdiği şifreli metinleri depolar. Saldırgan tarafından sayacın sıfırlandığı belirlendiğinde, saldırgan aynı sayaç değerine sahip mesajı eşleştirir. Örneğin sayaç değerleri sayesinde eşleştirilen iki şifreli metin: 8b8049fc25d1246b7d79234e02f0d173 ve bc7d33fd70a123983b7b431a02f0d274.
- Bu iki şifreli metin arasındaki ilişki saldırgan tarafından bilindiğinden dolayı geriye kalan tek şey saldırganın bu ilişkiyi kullanarak rastgele denenen kelimelerden asıl metni bulmasıdır.

Sonuç:

- Yalnızca sayılar kullanıldığında:
 - Bu uygulamanın sonucu Şekil 3.4’de gösterilmiştir. Üç farklı sıfırlamadan sonra olası tahminler hesaplanmıştır.

- Gerçekleştirilen 24 farklı örnekte, %45,8 oran ile doğru sonuçlandığı görülmüştür. Diğer kısım için ise olası aday sayısının oldukça azaldığı görülmüştür (12^8).
- Bu saldırının dayandığı nokta, saldırganın ışık sensöründen gelen değeri manipüle edebileceği varsayımıdır.
- Saldırganın sensör verisini manipüle edememesi durumunda ise daha fazla sıfırlama işlemi yapması gerekecektir.
- Yalnızca alfa nümerik karakterler kullanıldığında ise:
 - Bu deneyin tahminlere dayalı gerçekleştiğinden dolayı, yine aynı sayaç değerine sahip iki şifreli metnin ilişkisi üzerinden yola çıkılacaktır.
 - Bu çalışmanın farklı kısımlarında da belirtildiği gibi, aynı sayaç değeri kullanımından dolayı, LoRaWAN gizliliği tehdit edilebilmekte ve bu zafiyetin suistimal edilebileceği görülebilmektedir.



Şekil 3.4. 24 farklı denemede doğru sonuç için olası aday sayısı [87]

3.2.2. Bit-Flipping Saldırısı

3.2.2.1. Saldırının hedefi

Bu saldırı, ağ sunucusu ile uygulama sunucusu arasında gönderilen mesajın bütünlüğünü hedef alır. Böyle bir saldırıda uygulama sunucusu mesajın kaynağının saldırgan mı yoksa ağ sunucusu mu olduğunu tanımlamaktan yoksundur.

3.2.2.2. Saldırganın ihtiyaçları

Saldırganın bu atağı gerçekleştirebilmesi için gerekenler:

- Ağ sunucusu ile uygulama sunucusu arasında ortadaki adam saldırısını (MITM) gerçekleştirebilmesi
- Paket yükü formatını bilmesi
- Uç cihazdan gelen mesajın tipi ve formatı hakkında temel bilgiye sahip olması

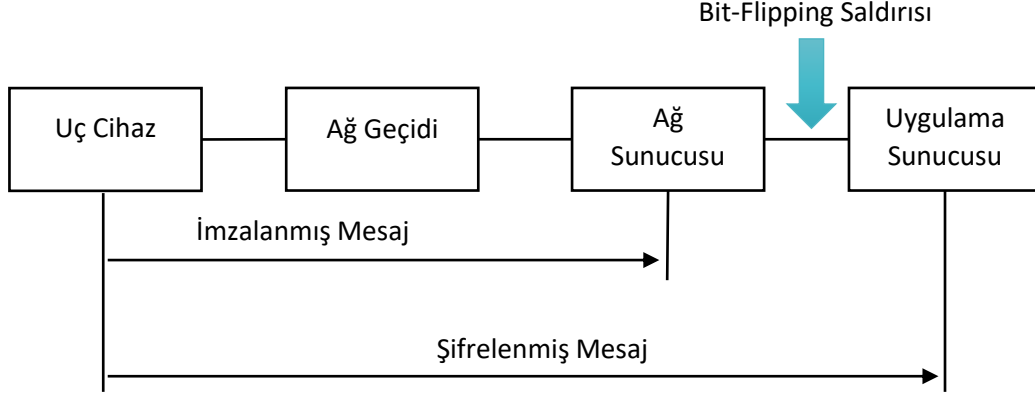
3.2.2.3. Protokolün zafiyeti

LoRaWAN protokolünde ağ sunucusu ile uygulama sunucusu arasındaki iletişimde bir bütünlük kontrol mekanizması bulunmamaktadır. Yukarı bağlantı ile gelen mesajlar önce şifrelenir ardından imzalanır. Ağ sunucusu mesajı aldığı anda NwKSKKey anahtarı ile mesajı kontrol eder ve kabul edilip edilmeyeceğine karar verir. Şifrelenmiş mesaj ağ sunucusu tarafından kabul edildiğinde aynı zamanda uygulama sunucusuna işlenir. Veri paketi ağ sunucusu ile uygulama sunucusu arasındayken ise veri değiştirilmeye açıktır. Buna uygulama sunucusuna ulaşan mesajın bütünlüğü kontrolünün yapılmaması sebep olmaktadır.

3.2.2.4. Saldırının detaylı açıklaması

Bit-Flipping saldırısının kurulumu Şekil 3.4'te gösterilmiştir. Saldırının aşamaları:

- Saldırganın ağ sunucusuna erişebildiği durumda veya ağ sunucusu ile uygulama sunucusu arasında MITM saldırısı gerçekleştirebilmesi durumunda bir Bit-flipping saldırısını gerçekleştirebilmektedir.
- Şifresiz veri ile şifrelenmiş veri arasındaki ilişkiyi kullanan saldırgan şifreli veride değişiklik yaparak verinin şifresiz halini manipüle eder. Saldırganın değiştirebileceği kısımlar içeriği (FrmPayload), uç cihaz adresi (DevAddr) ve sayaç değeri (FCnt) bilgileri olabilir.



Şekil 3.5. Bit-Flipping saldırı şeması

3.2.2.5. Saldırı senaryosu

Bu saldırının tehlikesi, ağ sunucusu ile uygulama sunucusu arasındaki iletişimin ihlalinden kaynaklanmaktadır. Saldırganın ağ sunucusu ile uygulama sunucusu arasındaki iletişimi MITM gibi saldırılarla ihlal ettiği bir senaryoda saldırgan tarafından;

- LoRaWAN paketleri değişikliğe uğratılabilir.
- Sayaç değerinin değiştirildiği bir durumda uygulama sunucusu gelen mesajı reddedebilir.
- FrmPayload değiştirildiğinde, uygulama sunucusunun aldığı veri değiştirilmiş olacaktır. Bu durumda gelen bir sensör verisi yanlış geldiğinden yanlış yorumlanmaya neden olabilir.
- DevAddr değerinin değiştirildiği bir durumda, uygulama sunucusu gelen mesajın kaynağını yanlış tanımlayabilir.

3.2.2.6. Uygulama

Bit-Flipping saldırısı için kurulum şeması Şekil 3.4'te gösterilmiştir. Bunun için bir uygulama sunucusu ile ağ sunucusu kurulur. Bu uygulamayı basit tutmak için sunucuların sadece temel işlevlere sahip olduğu varsayılır. Bu durumda ağ sunucusu imza kontrolü gerçekleştirirken uygulama sunucusu ise şifre çözme görevini yerine getirmektedir.

Prosedür:

- Uç cihaz tarafından gönderilen mesajlar ağ geçidi tarafından alınıp ağ sunucusuna yönlendirilmektedir. Ağ sunucusu NwkSKey anahtarı ile imzayı kontrol edip kabul edilip edilmeyeceğine karar verir.
- Saldırgan tarafından ağ sunucusu ile uygulama sunucusuna Ortadaki adam (MITM) saldırısı yapılır. Saldırı sonrasında saldırgan tarafından sunucular arası veri transferinde veriler değiştirilebilir.
- Bu zafiyete dayanarak saldırgan tarafından orijinal mesajdaki bir bit değiştirilerek mesajın bütünlüğü suistimal edilebilir.
- FrmPayload bitleri değiştirilmesi (Bit-Flipping): Bu durumda sensör verisi değiştirilmiş olacağından verilerin bütünlüğü ihlal edilmiş olacaktır.
- FCnt değerinin bitlerinin değiştirilmesi: Saldırgan tarafından yapılan bu değişiklik ile beraber FCnt değerinden daha büyük bir değer olana kadar sayaç değeri arttırılır. Bunun sonucunda ise mesaj kabul işlemi olumsuz sonuçlanacaktır.
- DevAddr bitlerinin değiştirilmesi: DevAddr verisi değiştirildiğinden mesajın başka bir uç cihazdan geldiği varsayılacaktır.

```

Mon May 22 16:43:01 2017
DevAddr 99999999 , Counter number is 440 , Physical Payload is 409999999900b801295dcbdd2ff168bc7d659d7944
[Network Server]: Signature is correct. Message is pushed to application server
[Network Server]: Message sent to application server is 409999999900b801295dcbdd2ff168bc7d659d7944
[Attack - 316 ]: Bit flipping.....Message 409999999900b801295dcbdd2ff168bc7d is changed to 409999999900b801295dcbdd2ff268bc7d
[Application server]: Message is not the same. Received 612 327 . Mote sent 612 027

```

Şekil 3.6. Örnek bir Bit-Flipping saldırısı sonucu [87]

Bu saldırının odağı direkt olarak veri mesajının bütünlüğüne karşıdır ve Şekil 3.5.’te bu saldırının sonucu görülmektedir. Saldırı sonucu olarak şifrelenmiş mesajda bir bit değiştiğinden dolayı, sıcaklık sensöründen gelen verinin sonucu olan 027’nin 327 olarak değiştirildiği görülmektedir.

3.2.3. Tekrarlama (Replay) Saldırısı

3.2.3.1. Saldırganın hedefi

Tekrarlama saldırısı bir çeşit DoS ve Spoofing saldırısıdır. Saldırganın amacı saldırganın sahip olduğu uç cihazdan gönderilen ve tekrarlanan mesajın sunucu tarafından, ağdaki normal bir uç cihazdan geldiğine inandırmaktır. Bir diğer amaç ise hedef uç cihazın gönderdiği mesajın sunucu tarafından kabul edilmemesidir. Bu

başlıkta ABP aktivasyon metodu kullanan LoRaWAN uç cihazlarına yönelik tekrarlama saldırısı ele alınmıştır.

3.2.3.2. Saldırganın ihtiyaçları

Tekrarlama saldırısını gerçekleştirebilmek için saldırırganın sahip olması gereken bazı nitelikler vardır. Bunlar:

- LoRaWAN mesaj paketlerini uygun frekansta gönderebilmesi için gerekli cihaz
- LoRaWAN mesajlarını yakalamak için gerekli cihaz
- LoRaWAN mesaj formatı hakkında bilgi sahibi olmak
- Hedef uç cihazın frekansının bilinmesi

3.2.3.3. Protokol zafiyeti

Tekrarlama saldırılarının uygulanması için kullanılan zafiyetler bu başlık altında gösterilmiştir.

ABP aktivasyon metodunda kullanılan statik anahtarlardan dolayı kullanılan anahtarlar cihaz sıfırlansa dahi değiştirilmeden kullanılmaktadır. Ayrıca bu aktivasyon metodunda cihazlar etkinleştirildikten sonra herhangi bir katılma isteği-kabulüne gerek duyulmamaktadır. Bu durumda saldırırganın kötü niyetli bir mesajının kabulü için aşağıdaki gereksinimleri karşılanması gerekmektedir;

- Sayaç değerinin kabul edilebilir olması
- DevAddr değerinin kabul edilen uç cihaz ile aynı olması
- Oturum anahtarının kabul edilen uç cihazınki ile aynı olması

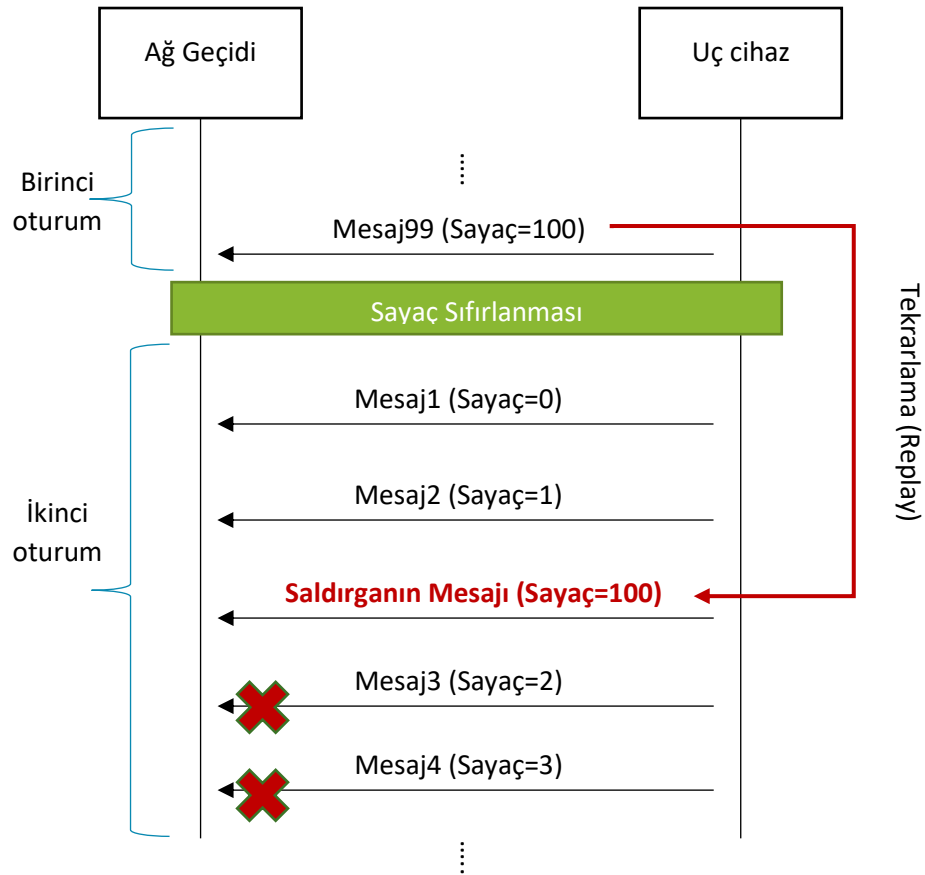
Bu gereksinimlerin karşılandığı bir durumda, saldırırganın tekrar tekrar gönderdiği kötü niyetli mesajın sunucu tarafından hangi oturum sırasında gönderildiği anlaşılamamaktadır.

3.2.3.4. Saldırının detaylı açıklaması

Saldırıyı gerçekleştirmek için gereken adımlar şu şekildedir:

1. Bir dinleme cihazı ile yukarı bağlantı mesajı dinlenir ve mesaj yakalanır. Saldırgan yakaladığı mesajları kaydeder.

2. Sayaç değerleri şifrelenmemiş olduğundan, yukarı bağlantı mesajlarının FCnt değeri alınır.
3. Uç cihaz yeniden başlatılana veya sayaçta taşma olana kadar beklenir.
4. Saldırgan yakaladığı mesajlardan oluşan kendi veritabanından, yakalanmış mesajlar arasında uygun sayaç değerine sahip bir mesajı bulup seçer.
5. Mesaj ağ geçidine tekrar gönderilir ve süreç bu şekilde periyodik olarak tekrarlanır.



Şekil 3.7. Bir Tekrarlama (Replay) saldırısı örneği

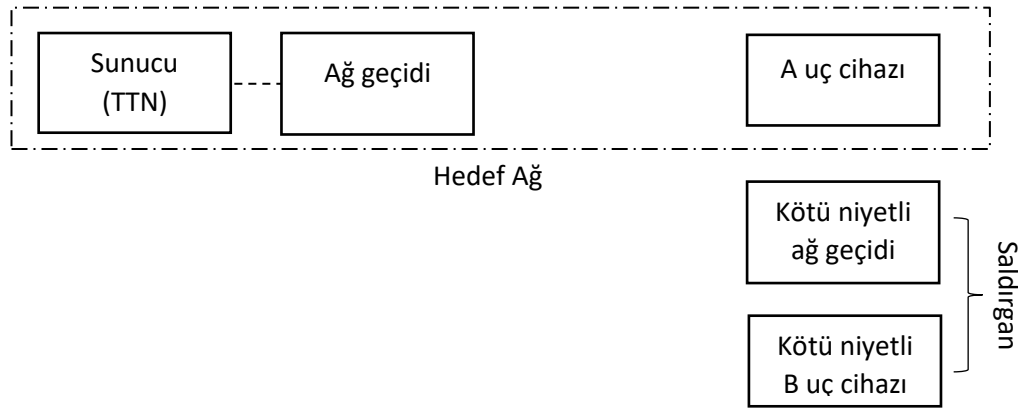
3.2.3.5. Saldırı senaryosu

Saldırgan bu saldırıda öncelikle LoRaWAN kablosuz haberleşme trafiğini dinler ve bir LoRa verici cihazı ile mesajları tekrar ettirebilir. Bu saldırının etkisi büyük olabilir. Eğer LoRaWAN ağı büyük ise saldırıncının uzun bir süreye ihtiyacı olmadan sayaç taşmasını kullanarak ağı büyük zararlar verebilir. Saldırgan kötü niyetli mesajı en

büyük sayaç değeri ile tekrar tekrar gönderebilir ve bu durumda hedef uç cihazdan gelen mesajlar reddedilecektir.

3.2.3.6. Uygulama

Yang'ın gerçekleştirdiği bir uygulamada [39], saldırgan saldırıyı gerçekleştirmek için herhangi bir LoRa alıcısını-vericisini kullanarak kablosuz iletilen mesajları dinleyip, alıp iletmektedir. Bu deneyde alıcı olarak bir LoRaWAN ağ geçidi ve verici olarak ise bir LoRaWAN uç cihazı kullanılmıştır. Şekil 3.7'de saldırı şeması gösterilmiştir. Bu saldırıda saldırganın sahip olduğu, Microchip markasının ölçüm kitine ait bir ağ geçidi ve bir A uç cihazı vardır. Saldırıda bulunulacak sistemde ise A uç cihazı, bir ağ geçidi ve sunucudan (TTN) oluşmaktadır. Hedefteki LoRaWAN ağı etkinleştirme için ABP metodunu kullanmakta ve aktif olarak çalışmaktadır.



Şekil 3.8. Tekrarlama saldırısı için kurulum şeması

Prosedür:

- Hedef uç cihazı ağ geçidi ile iletişim içindedir.
- Saldırgan, mesajları yakalamak için frekansını ayarlar ve kablosuz trafiği dinler.
- Saldırgan, kötü niyetli ağ geçidini, A uç cihazı ile sunucu arasındaki mesajları yakalamak için kullanır. Yakalanan mesajlardaki sayaç değeri, şifresiz veriler ve DevAddr değerleri bir veritabanına kayıt edilir.
- Hedefteki uç cihaz sıfırlanır. Bu durumda anahtarlar değişmez fakat sayaç değeri sıfırlanır.

- Kötü amaçlı ağ geçidi, sıfırlanma durumunu gözlemlediğinde saldırgan, mesajı bulmak için aynı sayaç değeri ve DevAddr değeri ile eşleştirir.
- Saldırgan kötü niyetli B uç cihazı kullanılarak veritabanından uygun bulunduğu sayaç değeri büyük olan bir mesajı yeniden gönderir.
- Sunucu, saldırgan tarafından gönderilen mesajı alırsa, saldırı başarılıdır.

Şekil 3.8’de görülmekte olan kayıtlar, kötü niyetli ağ geçidinden gelen günlük kayıtlardır. İlk satırda kötü niyetli ağ geçidinin yakaladığı kablosuz LoRa paketleri görülmektedir. Burada ağ geçidi, yakaladığı paketlerden mesaj içeriğindeki sayaç değeri, DevAddr değeri ve fiziksel yükü okuyabilmektedir.

İkinci satırda görülenler ise, ağ geçidinin bir sıfırlama işlemini gözlemlediğidir. Bir sıfırlanma işleminin ağ geçidi tarafından fark edilmesi için, geçerli sayaç değerinin önceki sayaç değerinden küçük veya eşit olması gerekmektedir.

Üçüncü satırda ise kötü niyetli mesajların iletimi görülmektedir. Herhangi bir sıfırlanma işlemi fark edildiğinde, saldırganın uç cihazı en sondaki gönderilen mesajı tekrar gönderir.

Dördüncü satırda kötü niyetli ağ geçidinin kötü niyetli mesajı gördüğü görülmektedir. Son satırda ise saldırının bittiği ve kötü niyetli ağ geçidinin mesajları izlemeye devam ettiği ve bir sonraki sıfırlamayı beklediği görülmektedir.

Şekil 3.9’da hedef sunucudaki kayıtlar gösterilmiştir. Burada bir mesajın saat 16:07:59’da alındığı ve 16:08:46’da tekrar gönderildiği, bundan dolayı hedef sunucunun aynı uç cihazdan gelen mesajları 6 dakika boyunca kabul etmediği görülmektedir. Bu reddedilen mesajlar kötü niyetli ağ geçidi tarafından yakalanmaya devam edilmektedir.

Bu uygulamada sayaç yönetimi ve değişken olmayan anahtarlamamanın zafiyetleri ve sonuçları görülmektedir.

Kötü niyetli ağ geçidi 865.5MHz frekansında kablosuz paketleri yakalıyor	<pre> Thu Apr 13 16:04:50 2017 DevAddr 89140126, Counter number is 3, Physical Payload is 4089140126000300530cb6ceal637e08d3c8240257 Thu Apr 13 16:05:49 2017 DevAddr 89140126, Counter number is 5, Physical Payload is 408914012600050086463981fa78962f244c5624f0 DevAddr 24170126, Counter number is 49817, Physical Payload is 40241701260099c20371b1fe383188ac82 DevAddr 89140126, Counter number is 6, Physical Payload is 40891401260006003d226c33a4882c44af7c5bac9b Thu Apr 13 16:06:48 2017 DevAddr 24170126, Counter number is 49819, Physical Payload is 40241701260099c203dd7d7ba55fd710d2 DevAddr 89140126, Counter number is 7, Physical Payload is 40891401260007002972597f1f3eab3c254bcb946 DevAddr 24170126, Counter number is 49820, Physical Payload is 40241701260099c20337e04acfb5a5046fd Thu Apr 13 16:07:47 2017 Thu Apr 13 16:08:46 2017 DevAddr 89140126, Counter number is 10, Physical Payload is 4089140126000a0031d5ef2a97d488b8232c8c9f39 DevAddr 89140126, Counter number is 0, Physical Payload is 4089140126000000473663cblf6a23ec3bf98c4798 </pre>
Ağ geçidi tarafından bir sıfırlama gözleniyor	<pre> Here is a reset! [3, 5, 6, 7, 10, 0] >>RN2483 1.0.1 Dec 15 2015 09:38:09 radio tx 4089140126000a0031d5ef2a97d488b8232c8c9f39 >>ok </pre>
B uç cihazı saldırgan tarafından mesaj iletimi için kullanılıyor	<pre> Attacking..... Thu Apr 13 16:09:48 2017 DevAddr 89140126, Counter number is 10, Physical Payload is 4089140126000a0031d5ef2a97d488b8232c8c9f39 </pre>
Kötü niyetli ağ geçidi mesajı fark ediyor	<pre> Thu Apr 13 16:10:47 2017 DevAddr 89140126, Counter number is 2, Physical Payload is 4089140126000200455e51f71a43d61cba6736abcc DevAddr 89140126, Counter number is 3, Physical Payload is 40891401260003002b0cb4c2a1637e0bd3d68a025f DevAddr 89140126, Counter number is 4, Physical Payload is 40891401260004005477e5b703fea2f3644548aebf Thu Apr 13 16:11:46 2017 DevAddr 24170126, Counter number is 49838, Physical Payload is 402417012600a0c203808788497e5c79a6 DevAddr 89140126, Counter number is 5, Physical Payload is 40891401260005004b46358dfa78962e24a11899da Thu Apr 13 16:12:45 2017 DevAddr 89140126, Counter number is 6, Physical Payload is 408914012600060045206133a4882c42af70467d84 Thu Apr 13 16:13:44 2017 DevAddr 89140126, Counter number is 8, Physical Payload is 408914012600080022c12a31a31c5b626b4c5b62ab DevAddr 89140126, Counter number is 9, Physical Payload is 40891401260009003e507f00b4b0878653e65329af Thu Apr 13 16:14:43 2017 DevAddr 89140126, Counter number is 10, Physical Payload is 4089140126000a0015d4e52297d488bd23a28bfe84 Thu Apr 13 16:15:42 2017 DevAddr 89140126, Counter number is 11, Physical Payload is 4089140126000b00143e307772c1eab47678fb066 DevAddr 89140126, Counter number is 12, Physical Payload is 4089140126000c003d4905e528298ffad1830f2529 </pre>

Şekil 3.9. Kötü niyetli ağ geçidinin kayıtları [39]

	time	counter	port	dev id	
A uç cihazının sayaç değeri, zararlı mesajın sayaç değerinden büyük olduğunda iletişim tekrardan başlıyor	▲ 16:16:00	13	6	22	34 34 37 20 30 32 34 00
	▲ 16:15:25	12	61	22	34 39 36 20 30 32 34 00
	▲ 16:14:51	11	20	22	35 34 33 20 30 32 31 00
Saldırgan B uç cihazını kullanarak son mesajı tekrarlar. Zararlı mesaj kabul edilir	▲ 16:08:49	10	49	22	34 38 30 20 30 32 31 00
A uç cihazı sıfırlanır	▲ 16:08:34	0	71	22	31 39 32 20 30 32 32 00
A uç cihazı sunucu ile iletişime geçiyor	▲ 16:07:59	10	49	22	34 38 30 20 30 32 31 00
	▲ 16:06:16	7	41	22	35 32 37 20 30 32 33 00
	▲ 16:05:42	6	61	22	36 38 37 20 30 32 34 00
	▲ 16:05:07	5	134	22	34 39 34 20 30 32 33 00
	▲ 16:03:59	3	83	22	34 34 38 20 30 32 32 00

Şekil 3.10. Hedef sunucunun logları [39]

3.2.4. ACK Spoofing Saldırısı

3.2.4.1. Saldırganın hedefi

LoRaWAN protokolünde aynı uç cihaza giden mesajlarda aynı ACK kullanılabilir. Bu saldırıda saldırgan, uç cihaza gelen mesajın ACK değerini ele geçirerek kendi gönderdiği mesajda da aynı ACK değerini kullanabilmekte ve bu sayede bu zafiyetten faydalanabilmektedir.

3.2.4.2. Saldırganın ihtiyaçları

Saldırganın bu saldırıyı icra edebilmesi için bazı niteliklere ihtiyacı vardır. Bunlar:

- ACK içeriğini okuyabilmesi, doğru sayaç, uç cihaz adresi (FCnt ve DevAddr) değerlerini kullanabilmek
- ACK mesaj iletimini kesebilmek
- Ağ geçidine erişebilmek
- Seçtiği ACK mesajını uç cihaza gönderebilmek

3.2.4.3. Protokol zafiyeti

LoRaWAN protokolünde bir ACK paketinin, hangi mesaja ait olduğu dolayısıyla hangi mesajı onayladığı belirtilmemektedir. Yalnızca son gelen mesajın onaylanması, kötü niyetli bir saldırıda son gelen mesajın ACK paketinin saklanabilmesi ve gelecekte istenilen mesaj ile beraber gönderilmesi zafiyetini ortaya çıkarmaktadır. ACK kabul işlemi ise uç cihazda ki FCnt değeri, gelen mesajdaki FCnt değerinden küçük olduğu durumlarda kabul olmaktadır.

3.2.4.4. Saldırı senaryosu

ACK saldırısının gerçekleştirilmesi, saldırganın sahte bir ağ geçidi ile sızması veya mevcut ağ geçidini dinlemesi ile mümkün olmaktadır. Bu durumda saldırgan, protokol zafiyeti başlığında belirtilen şekilde bu açığı kullanacak ACK paketlerini kendi isteğine göre ağa zarar vermek üzere kullanabilir.

3.2.4.5. Uygulama

ACK spoofing saldırısı icra edilirken kullanılan zafiyet, bir aşağı bağlantı mesajı ile yukarı bağlantı mesajı arasındaki ilişkideki boşluktur. Hessel'in çalışmasında yaptığı bir uygulamada [88], saldırgan öncelikle ACK içeren bir aşağı bağlantı mesajı toplamaya çalışmaktadır. Burada önemli nokta ise ağ sunucusunun onaylanmış bir yukarı bağlantı mesajı aldığında geçerli bir ACK paketi ilettiğidir. Bundan dolayı saldırgan öncelikle ACK paketi yakalamak için bir yukarı bağlantı mesajı gönderir. Saldırgan bir ACK paketi yakaladıktan sonra ise bir aşağı bağlantı mesajı çerçevesindeki sayaç değerinin mevcut değerden daha yüksek olmasından faydalanarak mesajı geçersiz hale getirir.

Bu durumda Saldırganın bu saldırıyı iki aşamada yaptığı görülmektedir. İlk aşamada ACK içeren bir aşağı bağlantı çerçevesi yakalayıp ardından bu mesajın uç cihaz tarafından geçersiz kılması iken ikinci aşamada ise uç cihaza gelen mesajı onaylatır.

Prosedür:

- Birinci Aşama, Toplama
 - Saldırganın ACK değeri yakalaması gerekir.
 - Bunun için kendi uç cihazının alıcı modunu açar.
 - Bir ACK paketi yakaladıktan sonra uç cihazı aşağı bağlantı çerçevelerini karıştırma moduna geçer.
 - Bu sayede saldırı, eline geçen ACK paketinin işlenmesinin önüne geçer.
 - Bu durumda uç cihazdaki sayaç değeri arttığından ACK geçersiz olacaktır.
 - Saldırgan daha sonra her bir ACK paketi yakalamak için bekler ve ACK alındığında bir sonraki aşamaya geçer.
 - Bu süreçte ACK yakalayamazsa tekrardan bir yukarı bağlantı mesajı beklemeye başlar.
- İkinci Aşama, Spoofing
 - Bu aşamada ilk olarak hedef uç cihazın onaylanmamış mesajları için sinyal karıştırma yapmaktır.
 - Bu sayede saldırı, onaylanan mesajların ağ sunucusu tarafından işlenmediğinden emin olmaktadır.
 - Saldırgan yukarı bağlantı mesajı alma moduna geçer.
 - Saldırgan gelen mesajları kendi yakaladığı ACK ile karşılaştırır.
 - Ağ sunucusu her bir yukarı bağlantı mesajını tek seferlik onayladığından, saldırının yeniden gönderilen mesajları önemsemesi gerekmez.
 - Böylelikle ağ sunucusundan başka mesaj gelmeyeceğinden uç cihaz tarafından mesajlar alınıp işlenirken ağ sunucusunun bu durumdan haberi olmamaktadır.

Bu çalışmada [88] yapılan deneyin sonucu aşağıdaki Tablo 3.3'te gösterilmiştir. Tablodaki sütunların anlamları:

- ID: Deneyi belirtir.
- First Uplink: Onaylanmış yukarı bağlantı mesajını belirtir.
- Server: ACK oluşturmak için yukarı bağlantı mesajının sunucu tarafından alınıp alınmadığını belirtir.
- Node: ACK alınıp alınmadığını belirtir. Saldırının başarılı olması için bu değer olumsuz olmalıdır.
- Sniffer: Uç cihazın, saldırganın karıştırma modunu kullandığı sırada ACK'yı işleyip işlemediğini belirtir.
- Second Uplink: Ağ geçidi tarafından engellenen fakat uç cihaza onaylanarak giden yukarı bağlantı mesajını belirtir.
- Sunucu: Sunucunun yukarı bağlantı mesajını alıp almadığını gösterir. Saldırganın önlemeye çalıştığı durumdur.
- Node: Sunucu tarafından bir yanıt alınıp alınmadığını belirtir.
- Spoof: Ele geçirilen ACK'nın uç cihaz tarafından kabul edilip edilmemesini belirtir. Saldırının başarılı olması için olumlu olması gerekmektedir.

Tablo 3.3. ACK Spoofing saldırısı sonucu [88]

ID	First Uplink			Second Uplink		
	server	node	sniffer	server	node	spoof
D0	rx	lost	rx	–	–	ok
D1	rx	lost	rx	–	–	ok
D2	rx	rx	rx	–	–	DR
D3	rx	lost	rx	–	–	ok
D4	rx	rx	rx	–	–	DR
D5	rx	lost	rx	–	–	ok
D6	rx	lost	rx	–	–	ok
D7	rx	rx	rx	–	–	DR
D8	rx	MIC fail	rx	–	–	ok
D9	rx	lost	rx	–	–	ok
D10	rx	lost	rx	–	–	ok
D11	rx	lost	rx	–	–	ok
D12	rx	MIC fail	rx	–	–	ok
D13	rx	lost	rx	–	–	ok
D14	rx	MIC fail	rx	rx	–	ok
D15	rx	MIC fail	rx	–	–	ok
D16	rx	lost	rx	–	–	ok
D17	rx	lost	rx	–	–	ok
D18	rx	lost	rx	–	–	ok
D19	rx	rx	rx	–	–	DR

Bu deney sırasında 9 mesaj hiç alınamamış ve tabloda gösterilmemiştir.

Tablo 3.3'te gösterilen D2, D4, D7 ve D19 deneylerinde ACK yakalanamamasından dolayı aşağı bağlantı mesajı gönderimi tekrarlanmıştır (DR). D14'te ise spoofing işlemi yapılsa bile ağ sunucusu yukarı bağlantıyı aldığından dolayı başarısız olmuştur.

3.3. Risk Analizi

Bu bölümde LoRaWAN'ın güvenlik tehditlerinin değerlendirmesi yapılmıştır. Farklı risk analiz metotları açıklanmış ve metodoloji gösterilmiştir. Ardından LoRaWAN'a karşı yapılabilecek saldırıların bu çalışmada seçilenlerinin niteliksel bir risk analizi yapılmış ve Tablo 3.7'de gösterilmiştir.

3.3.1. Risk Değerlendirme Metodolojisi

Bu başlıkta 3 farklı değerlendirme metodu açıklanmıştır. Bunlar etki, olasılık ve risk değerlendirme metotlarıdır [24].

3.3.1.1. Etki değerlendirmesi

Etki değerlendirmesinin amacı bir saldırı tehdidinin boyutunu gözlemlemek ve kategorize etmektir. Bir saldırının etki değerlendirmesinde hafif, orta ve ağır etki olarak 3 farklı etki seviyesi kullanılmaktadır. Bunun dışında tespit edilebilirlik ve kurtarılabirlik ile ölçek seviyesi kullanılarak sonucun daha verimli olabilmesi sağlanmaktadır.

Tespit edilebilirlik ve kurtarılabirlik: Yapılan bir saldırının tespit edilebilirliğini, sisteme olan etkisini ve saldırı sonrası oluşan hasarın geri çevrilebilmesini, yüksek, orta ve düşük olarak kategorize eder.

Ölçek seviyesi: Bir saldırı ardından etkilenen alanın ölçeğini uç cihaz, LoRaWAN ve LoRaWAN ağları olarak üç farklı kategori ile gösterir.

Saldırının etkisi: Tespit edilebilirlik ve kurtarılabirlik ile ölçek seviyesini kullanarak göstermektedir. Tablo 3.4’te görülmektedir.

Tablo 3.4. Saldırı etki değerlendirme tablosu

Tespit Edilebilirlik Ölçek Seviyesi	Düşük	Orta	Yüksek
Uç cihaz	Orta	Hafif	Hafif
LoRaWAN	Ağır	Ağır	Orta
LoRaWAN Ağları	Ağır	Ağır	Orta

3.3.1.2. Olasılık değerlendirmesi

Olasılık değerlendirmesinde, bir tehdit 3 farklı seviye ile ölçülebilir. Bunlar; yüksek, orta ve düşük olasılık seviyeleridir. Daha iyi bir çıkarım için teknik zorluklar ve motivasyon gibi faktörlerin de bu değerlendirmeye dahil edilmesi, sonucun doğruluğuna olumlu etki edecektir [24].

Teknik zorluklar: Saldırganın saldırıyı yaparken başına gelebilecek zorlukları kapsar. Bunların çözümünü zorluk olarak, kolay, orta ve zor olarak 3 farklı kategoriye ayırabiliriz.

Motivasyon seviyesi: Saldırganın yapacağı saldırıda karşısına çıkacak zorluklara göre devam edip etmemesini kapsar. Bu motivasyon seviyelerini, yüksek, orta ve düşük olarak ayırabiliriz.

Olasılık: Saldırının teknik zorluklar ve motivasyon seviyesine göre saldırı olasılığını gösterir.

Tablo 3.5. Saldırı olasılık değerlendirme tablosu

Teknik Zorluklar \ Motivasyon	Kolay	Orta	Zor
Düşük	Düşük	Düşük	Düşük
Orta	Yüksek	Orta	Düşük
Yüksek	Yüksek	Yüksek	Düşük

3.3.1.3. Risk değerlendirmesi

Olasılık değerlendirmesi ve Etki değerlendirmesi, Risk değerlendirmesinin doğrudan parçalarıdır. Risk değerlendirmesinde sonuçlar 3 kategoride gösterilmektedir ve Tablo 3.6'da gösterilmektedir. Bunlar;

Düşük risk: Bir saldırının gerçekleşmesi olasılığının düşük ve etkisinin hafif olduğu durumu temsil eder.

Orta risk: Saldırı olasılığının orta olduğu ve etkisinin orta olduğu durumu temsil eder.

Yüksek risk: Saldırı olasılığının yüksek ve etkisinin ağır olduğu durumu temsil eder.

Tablo 3.6. Risk değerlendirme tablosu

Olasılık \ Etki	Düşük	Orta	Yüksek
Hafif	Düşük	Düşük	Düşük
Orta	Düşük	Orta	Orta
Ağır	Düşük	Orta	Yüksek

Tablo 3.7. Niteliksel Risk Analizi Tablosu

Kategori	Gizlilik	Bütünlük	Erişebilirlik	
Saldırı Adı	Eavesdropping	Bit flipping	Replay	ACK Spoofing
Saldırganın ihtiyacı olan Nitelikler	Basit	Basit	Basit	Yüksek
Saldırganın Harcayacağı Zaman	Çok	Az	Çok	Az
Başarı Olasılığı	Orta	Düşük	Yüksek	Düşük
Saldırının Etkisi	Orta	Orta	Yüksek	Orta
Risk	Orta	Düşük	Yüksek	Orta



4. SALDIRI ENGELLEME VEYA ETKİSİNİ AZALTMAYA YÖNELİK ÇÖZÜMLER

Bu bölümde yukarıdaki bölümü destekler nitelikte, LoRaWAN’a karşı yapılan saldırılarının etkilerini minimize etmek için nelerin yapılması gerektiği ele alınmıştır.

Tablo 4.1. Bu çalışmada incelenen saldırıların genel özeti

Saldırılar	Hedef	Zafiyet	Risk
Eavesdropping (Gizlilik)	Şifrelenmiş mesajı çözerek gizlilik ihlali	Sayaç yönetimi	Orta
Bit-Flipping (Bütünlük)	Gönderilen veriyi fark edilmeden bozarak bütünlük ihlali	Uygulama sunucusuna gelen mesaja bütünlük kontrolü yapılmaması	Düşük
Replay (Erişebilirlik)	Zararlı mesajın sunucu tarafından kabul edilmesi ve normal uç cihazdan gelen mesajın sunucu tarafından reddedilmesi	Sayaç yönetimi ve statik anahtarlama	Yüksek
ACK Spoofing (Erişebilirlik)	Uç cihazı etkisizleştirmek ve ağ geçidi ile arasındaki iletişime zarar vermek	Mesaj iletim kontrolü	Orta

4.1. Dinleme (Eavesdropping) Saldırısı

4.1.1. Saldırı Engelleme veya Etkisinin Azaltılması

Saldırı çeşitleri başlığı altında ele alınan bu saldırının aynı sayaç değerinin kullanılmasından dolayı oluşan zafiyeti kullandığı ve şifreli mesajların okunabilir hale getirebildiği görülmektedir. Bunun temel nedeni Block cipher modunun aşılabilmesidir. Aynı uç cihazdan gelen aynı oturum anahtarını kullanan ve aynı sunucuya giden mesaj paketlerinden birinin saldırgan tarafından çözülmesi durumunda, aynı yolu takip eden diğer mesajların gizliliği ortadan kalktığından ihlale açık hale gelmektedir. Bu durumda riski azaltabilmek için yapılabilecekler:

- ABP metodunda saldırganın uç cihazı sıfırlayabilmesi durumunda dinleme saldırısını başarıya ulaştırabilir ve verilerin şifresini kolayca çözebilir. Bu durumda aktivasyon metodu seçilirken yalnızca kritik olmayan durumlarda ABP metodu kullanılabilir. OTAA aktivasyon metodunda ise uç cihazı sıfırlamanın dinleme saldırısı yapan bir saldırgan için etkisi olmayacağından, saldırgan daha uzun süre beklemeli ve daha fazla veri paketi analiz etmesi

gerekir. Bu durumda saldırganın başarı oranı ABP metoduna kıyasla daha düşük olacaktır.

- Bir diğer önlem ise saldırganın uç cihazı sıfırlamasının önüne geçmek olabilir. Dinleme saldırısında saldırganın en önemli kozu uç cihazı defalarca sıfırlayıp aynı sayaç değeri kullanan paketleri yakalamasıdır. Uç cihazın sıfırlanmasının önüne geçildiğinde, saldırganın veri paketlerini yakalayıp kaydetmesi ve aynı sayaç değeri kullanan paketleri eşleştirmesi için birçok oturumu beklemesi gerekir ki bu da uç cihazın bağlantısının kesilip tekrar bağlanması gibi sebepler gerektireceğinden saldırganın bekleme süresi ay veya yıl olabilir. Saldırganın uç cihaza fiziksel olarak erişemediği bir durumda, dinleme saldırısı riski büyük oranda azaltılabilir.
- Bu saldırının hedefi olan aynı sayaç değeri vasıtası ile oturum anahtarına sahip olmayı engellemenin bir diğer yolu da düzenli aralıklarla oturum anahtarının değiştirilmesidir. Dinleme saldırısı yapan bir saldırgan için yakalanan mesaj paketleri ile oturum anahtarını ele geçirmesi zaman alırken, bu anahtarın düzenli olarak değiştirilmesi durumunda, saldırının başarıya ulaşması önemli ölçüde azalabilir. Ayrıca uç cihazda sayaç değeri en sona ulaştığında uç cihazın yeniden başlatılması da saldırganın yeteri kadar paket yakalayamadan başa dönmesi anlamına geleceğinden saldırıyı başarıyla gerçekleştirmesini önemli ölçüde engelleyebilir. OTAA aktivasyonunda Katılım isteği-kabulü prosedürü ile bu işlem yapılabilirken ABP aktivasyonunda manuel yapılması gerekir ki oturum anahtarı değiştirildiğinde uç cihaz ve sunucuda tekrar konfigürasyon yapılması gerektiğinden büyük çaplı ağlar için uygun değildir.

4.1.2. Öneriler

Dinleme saldırısına karşı etkisinin azaltılması birtakım zorlukları beraberinde getirdiğinden bu saldırının önlenmesi için zayıflıkların kapatılması daha etkili olabilir. Dinleme saldırısı için saldırganın kullandığı zafiyetler:

- ABP aktivasyon metodunda kullanılan anahtarların statik olması
- ABP aktivasyon metodunu kullanan cihazların sıfırlanması durumunda sayaç değerinin sıfırdan başlatılması
- LoRaWAN güvenlik özelliklerinden biri olan şifreli blok modunun, aynı sayaç değerinin tekrar kullanılmasına karşı bir kontrolünün olmaması

Bu zafiyetlerin giderilmesi için öneriler:

LoRaWAN güvenlik özelliklerinden olan blok şifreleme modu AES-CTR metoduna benzer olsa da farklı olarak nonce yerine sayaç değeri kullanmaktadır. Nonce değeri tekrarlanmadığından bu zafiyete bir çözüm olabilir fakat bilinmelidir ki nonce kullanımı sayaç değeri kullanımına göre paket yük uzunluğunu arttırmakla beraber alıcı ve vericide saklı kalması gerektiğinden verimlilik noktasında dezavantajlıdır.

Oturum anahtarlarının statik olması yerine uç cihaz sıfırlandığında veya sayaç son değerine ulaştığında değiştirilebilir. Bu durumda sayaç değeri bir nonce gibi güvenliği artırılmış olabilir.

4.2. Bit Flipping Saldırısı

4.2.1. Saldırı Engelleme veya Etkisinin Azaltılması

Bit flipping saldırısı ağ sunucusu ile uygulama sunucusu arasındaki bütünlüğün korunamamasına sebebiyet veren zafiyeti kullanır. Bundan dolayı bu saldırının başarılı olabilmesi için iki sunucu arasındaki iletişime saldırılması gerekir. Saldırının başarı oranını azaltmak için saldırının etkisini azaltan yöntemler kullanılabilir.

Ağ sunucusu ile uygulama sunucusu arasında güvenli bir iletişim yöntemi kullanılmalıdır. Bu iletişim için hücresel ağlar, Ethernet ve WiFi gibi seçenekler mevcuttur ve güvenlik direkt seçilen iletişim yöntemine göre değişir. Söz konusu durumdan dolayı yetkili kişinin iletişim için seçilecek yöntem hakkında güvenlik konusuna ve olası tehditlere hâkim olması, saldırıyı önleme veya etkisini azaltmak için bir avantajdır.

Ağ sunucusundan gelen mesajların uygulama sunucusuna geçeriz olarak iletilmesi Bit flipping saldırısının bir işareti olabilir. Saldırgan şifrelenmiş veri paketi bitlerini değiştiriyor olabilir. Böyle bir saldırıda saldırgan, bit değişimini yaptıktan sonra mesajın şifresini çözmesi ve okunabilir hale getirmesi olası değildir.

Saldırgan çeşitli yöntemler ile çeşitli sonuçlar alabilir. Örneğin FrmPayload değeri ihlal edildiği ve değiştirildiği bir durumda, sonuçları okunabilirken, FCnt veya DevAddr değerinin ihlal edildiği durumda sonuç okunamaz. Bunun sebebi bu parametrelerin hem uç cihazda hem de sunucuda saklanmasıdır.

Genellikle gelen fakat okunamayan mesajlar bit çevirme saldırısını hatırlatmalı ve ağın güvenliğinin ihlal edilmesi durumunu göz önüne alarak sunucular arası bağlantı kontrol edilmelidir.

4.2.2. Öneriler

Bütünlüğün korunması açısından ağ sunucusu ile uygulama sunucusu arasındaki iletişimin güvenliği için uçtan uca şifreleme yöntemi kullanılabilir.

Bütünlüğü korumanın diğer bir yolu ise ağ sunucusundan gelen mesajın uygulama sunucusunda MIC değerinin tekrar kontrol edilmelidir. Böylelikle mesajın yolda değişip değişmediği anlaşılabilir.

4.3. Tekrarlama (Replay) Saldırısı

4.3.1. Saldırı Engelleme veya Etkisinin Azaltılması

Tekrarlama saldırıları ABP aktivasyon metodunu kullanan uç cihazların aktivasyon ve sayaç değerlerini hedef alınmaktadır. Bu saldırı sayaç değerinin yeniden kullanılması sağlanarak icra edilmektedir. Aşağıdaki gösterilen önlemler, tekrarlama saldırısı risklerini azaltmada etkili olacaktır.

- Uç cihazların fiziksel olarak korunması, tekrarlama saldırısının riskini azaltmak için önemli önlemlerden biridir. Kötü niyetli bir saldırganın uç cihaza fiziksel olarak erişebilmesi durumunda, uç cihazın gücünü kesip sıfırlaması ve aynı sayaç değerine sahip mesajları bulana kadar bu işleme devam etmesi, saldırganı zaman kazandırabilmekte ve saldırının icra edilme süresini azaltmaktadır. Uç cihazın fiziksel olarak korunduğu durumda ise saldırganın tekrarlama saldırısını icra etmek için sayaç değeri taşmasını (overflow) beklemesi gerekmektedir.
- ABP aktivasyon metodunu sadece belirli durumlarda kullanmak saldırı önlemede etkilidir. Bunun nedeni ABP metodunun statik anahtarlama kullanması ve bu durum kötü niyetli bir saldırgan tarafından kullanılıp tekrarlama saldırısı icra edilmesinin önünün açık olmasıdır. Dinamik anahtarlama kullanan OTAA metodunda da tekrarlama saldırısı riski bulunmakla beraber, saldırganın daha çok çaba ve zaman sarf etmesi gerektiğinden risk daha azdır.

- Bir diğ er  nlem ise, saya   değ eri her maksimum değ ere ulařtıđında u  cihazın oturma anahtarının değ iřtirilmesidir. Bu saya   değ erinin yeniden kullanılması durumunda, oturma anahtarının farklı olması sebebiyle tekrarlama saldırısı bařarıya ulařmayacaktır.

Yukarıda maddeler halinde belirtilen  nlemler, saldırı etkisinin hafifletilmesi ve riskin azaltılmasında etkili olmakla beraber, u  cihazların oturma anahtarı değ iřimi veya b y k  aplı sistemlerde her u  cihazın fiziksel olarak korunması ekstra bir maliyet getirmektedir.

4.3.2.  neriler

Yukarıdaki bařlıkta tekrarlama saldırısına karřı riski azaltmak i in yapılabilirler yazılmıştır. Fakat bu y ntemler tekrarlama saldırısının tamamen engellenmesi i in yetersizdir. Tekrarlama saldırılarına karřı daha g   l  bir  nlem i in zafiyete sebep olan LoRaWAN g venlik mekanizmalarının geliřtirilmesi i in bu bařlık altında  neriler yazılmıştır:

- Saldırmanın g ndereceđi y ksek saya   değ erli zararlı mesajın sunucu tarafından alındıktan sonra normal u  cihazdan gelen mesajları, son mesajın saya   değ erinden k   k olduđu i in reddetmesi saldırıyı bařarıya ulařtırmaktadır. Bu durumun engellenmesi i in sunucu tarafında oluřturulacak bir fonksiyon ile belli bir sayının  zerinde reddedilme olursa, u  cihazı saya   değ erinin sıfırlanması ve saya   değ erinin sıfır yerine son kabul aldıđı değ erden itibaren bařlatması  zerine bir tetikleme fonksiyonu oluřturulabilir. Bu durumda saldırının bařarıya ulařması engellenecek ve saldırı her ger ekleřtiđinde u  cihaz sunucu tarafından tetiklenip saya   değ erini g ncelleyerek saldırıyı etkisiz hale getirecektir.

4.4. ACK Saldırısı

4.4.1. Saldırı Engelleme veya Etkisinin Azaltılması

Bu saldırının kullandıđı zafiyet, LoRaWAN protokol n n herhangi bir ACK paketinin hangi mesajı onayladıđının belirtilmemesidir. Bu saldırının riskinin azaltılması i in:

- Bir mesaj alınıp onaylandıđı durumda bu onayı ve mesajı kontrol etmek, olası bir saldırının erken tespitini m mk n kılabilir.

- ACK saldırısında ağ geçidi kilit derecede bir öneme sahip olduğundan ağ geçidinin korunması bu saldırının önlenmesinde etkili bir yöntem olabilmektedir.



5. SONUÇ

Bu çalışmada, son yıllarda popülerlik kazanmaya başlayan uzun menzili ve düşük güç ile çalışabilmesinden ötürü, nesnelerin internetinde kullanılan ağlardan biri olan ve bu bağlamda güvenliği ele alınan LoRaWAN protokolü incelenmiştir. Bu araştırmada güvenliği anlamak için sorulan sorular;

- LoRaWAN protokolü nedir? Nasıl çalışır? Rakiplerinden farkı nelerdir?
- LoRaWAN protokolünün güvenlik önlemleri nelerdir?
- LoRaWAN ne kadar güvenli?
- LoRaWAN güvenliğinin zayıf noktaları nelerdir?
- LoRaWAN'a karşı yapılabilecek saldırılar nelerdir?
- Bu zayıflıklar ve saldırılara karşı nasıl önlemler alınabilir?

Bu sorulardan yola çıkarak detaylı incelemenin ardından, LoRaWAN protokolünün düşük güç tüketimli diğer geniş alan ağ teknolojilerinden olan SigFox ve NB-IOT gibi rakiplerine, kurulum maliyeti, menzil, ulaşılabilirlik ve topluluk bakımından daha öne çıktığı görülmüştür.

LoRaWAN protokolü güvenliği incelendiğinde, uç cihaz ile sunucular arasındaki iletişimi güvenli bir şekilde kurmak için OTAA ve ABP aktivasyon metotları kullanıldığı görülmüştür. Aktivasyon metotları ağda bağlantı kurulurken kullanılan oturum anahtarlarının türetilmesinden sorumludur. Bu iki metodun avantaj ve dezavantajına odaklanırsak, OTAA metodunda anahtarlama işlemi güvenli bir şekilde uç cihaz ve sunucu arasında havadan iletilme ve uç cihaz ve sunucu tarafında kullanılmaktadır ve iki tarafta da mesaj şifrelenmesinde ve imzalanmasında kullanılmaktadır. Mesaj kabul prosedüründe kullanılan sayaç vasıtasıyla mesaj onaylarken, mesaj güvenliğini sağlamak için gereken anahtar AES-128 ile türetmekte, mesajı imzalama ve şifreleme için ise şifreli blok modunu (cipher block mode) kullanmaktadır.

LoRaWAN ağına karşı yapılabilecek saldırıları tespit için bir risk analiz yöntemi verilmiş ve bu yöntemle göre öncelikle saldırı hedefi detaylandırılıp saldırganın kabiliyeti, protokolün zafiyeti, saldırı senaryosu, bu çalışmada işlenen her bir saldırı için sunulmuştur.

LoRaWAN protokolünün güvenlik zafiyetleri, bu zafiyetler üzerinden gizliliği, bütünlüğü ve erişebilirliği ihlal eden saldırılar üzerinden gösterilmiştir. Bu tez çalışmasında incelenen saldırılar; Dinleme (eavesdropping) saldırısı, Bit flipping saldırısı, Tekrarlama (Replay) saldırısı ve ACK spoofing saldırısıdır

Dinleme (eavesdropping) saldırısının, LoRaWAN güvenlik özelliklerinden biri olan sayaç mekanizmasının zafiyetinden faydalanmakta olduğu ve mesajların şifresini çözebildiği görülmüştür. Bit flipping saldırısında ise, temel olarak LoRaWAN protokolünün sunucular arası iletişimde bütünlüğü koruyamadığından kaynaklı olduğu görülmüştür. Tekrarlama (Replay) saldırısının ABP aktivasyon metodunu hedef aldığı ve yine sayaç yönetiminden kaynaklanan bir zafiyeti kullanarak sunucuya gelen mesajların sunucu tarafından reddedilmesine sebep olduğu görülmüştür. ACK spoofing saldırısında, gönderilen mesaj formatındaki bir zafiyet sebebiyle saldırgan rasgele paketler göndererek sistemi manipüle edip mesaj onayı sağlayabildiği görülmüştür.

LoRaWAN'a karşı yapılabilecek saldırıların engellenmesi ve etkisinin azaltılması için, saldırılar detaylıca incelenmiş ve saldırıları engellemek için yöntemler ile zafiyetlere yönelik güvenlik önerileri sunulmuştur.

Bu çalışmada genel olarak LoRaWAN protokolünün güvenlik analizi yapılmış, zafiyetleri tespit edilip bu zafiyetleri hangi saldırı çeşitlerinin kullanabileceği gösterilmiştir. Sonuç olarak LoRaWAN protokolünün henüz tam anlamıyla güvenli olmadığı, kritik bilgilerin gönderiminde ve kritik sistemlerde kullanımda riskli olabileceği, fakat bu zafiyetlerin ve saldırıların riskinin bu çalışmada sunulan önlem ve öneriler ile azaltılabileceği gösterilmiştir.

LoRaWAN protokolünün güvenlik açısından geliştirilmeye ihtiyacı olsa da yaygınlaşmasının devam edeceğini ve hayatımızda ki yerinin giderek artacağını öngörüyoruz.





KAYNAKÇA

- [1] K. ASHTON, «That ‘Internet of Things’ Thing,» [Çevrimiçi]. Available: <https://www.rfidjournal.com/articles/view?4986>. [Erişildi: 25 05 2021].
- [2] A. Nordrum, «İnternet: Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated,» [Çevrimiçi]. Available: <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>. [Erişildi: 25 05 2021].
- [3] D. Evans, «The Internet of Things How the Next Evolution of the Internet Is Changing Everything,» [Çevrimiçi]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Erişildi: 25 05 2021].
- [4] «SAĞLIK SEKTÖRÜNDE NESNELERİN İNTERNETİ KULLANIMI VE AVANTAJLARI,» [Çevrimiçi]. Available: <https://www.dermedya.com/tr/post/saglik-sektorunde-nesnelerin-interneti-kullanimi-ve-avantajlari>. [Erişildi: 25 05 2021].
- [5] Gartner, «Gartner Identifies Top 10 Strategic IoT Technologies and Trends,» [Çevrimiçi]. Available: <https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends>. [Erişildi: 25 05 2021].
- [6] Cisco, «Internet of Things,» [Çevrimiçi]. Available: <https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf?dtid=ossdc000283..> [Erişildi: 25 05 2021].
- [7] Cisco, «Cisco Visual Networking Index: Forecast and Trends, 2017–2022,» [Çevrimiçi]. Available: <https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf>. [Erişildi: 25 05 2021].
- [8] J. Marcel, «Wireless Connectivity Options for IoT Applications,» [Çevrimiçi]. Available: <https://www.bluetooth.com/blog/wireless-connectivity-options-for-iot-applications>. [Erişildi: 25 05 2021].
- [9] R. Harada ve E. Sotter, «Automated Monitoring for Inspections and Condition-based Maintenance- Part III: Industrial IoT Networks,» [Çevrimiçi]. Available: <https://electricenergyonline.com/energy/magazine/1166/article/Automated-Monitoring-for-Inspections-and-Condition-based-Maintenance-Part-III-Industrial-IoT-Networks.htm>. [Erişildi: 25 05 2021].
- [10] R. Kumar, T. W. Au, W. Susanty ve H. Suhaili, «Exploring Data Security and Privacy Issues in Internet of Things Based on Five-Layer Architecture,»

- [11] F. A. Ghumman, «Effects of IPV4/IPv6 Transition Methods in IoT (Internet of Things):A survey,» 17 05 2019. [Çevrimiçi]. Available: <https://ssrn.com/abstract=3402664>.
- [12] T. Say, EV, OFİS VE IoT AĞLARININ AĞ GEÇİDİNDE BÜTÜNLEŞİK TEHDİT YÖNETİMİ İLE GÜVENLİĞİN SAĞLANMASI, 2019.
- [13] B. Dickson, «IoT botnets might be the cybersecurity industry's next big worry,» [Çevrimiçi]. Available: <https://www.iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/>. [Erişildi: 25 05 2021].
- [14] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari ve M. Ayyash, «Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,» *EEE Communications Surveys Tutorials*, cilt 17, no. 4, pp. 2347-2376, 2015.
- [15] O. Georgiou ve U. Raza, «Low Power Wide Area Network Analysis: Can LoRa Scale?,» *IEEE Wireless Communications Letters*, cilt 6, no. 2, pp. 162-165, 2017.
- [16] J. Kim ve J. Song, «A Dual Key-Based Activation Scheme for Secure LoRaWAN,» *Wireless Communications and Mobile Computing*, pp. 1-12, 2017.
- [17] J. Han ve J. Wang, «An Enhanced Key Management Scheme for LoRaWAN,» *Cryptography*, cilt 2, p. 34, 2018.
- [18] M. Elkhodr, S. Shahrestani ve H. S. Cheung, «Emerging Wireless Technologies in the Internet of Things : A Comparative Study,» *International Journal of Wireless & Mobile Networks*, cilt 8, 2016.
- [19] A. Baloğlu ve O. Karademiroğlu, «Akıllı Şehirlerde Kablosuz Haberleşme Teknolojileri Ve Doğru Teknoloji Seçimi,» *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, cilt 1, no. 1, pp. 22-29, 2019.
- [20] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist ve Z. Zhang, «Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs,» *IEEE Access*, cilt 6, pp. 77454-77473, 2018.
- [21] R. Miller, «LoRa Security Building a Secure LoRa Solution,» 2016. [Çevrimiçi]. Available: <https://labs.f-secure.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf>. [Erişildi: 25 05 2021].

- [22] K. E. Nolan, W. Guibene ve M. Y. Kelly, «An evaluation of low power wide area network technologies for the Internet of Things,» %1 içinde 2016 *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016, pp. 439-444.
- [23] S. Tomasin, S. Zulian ve L. Vangelista, «Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks,» pp. 1-6, 2017.
- [24] X. Yang, *LoRaWAN: Vulnerability Analysis and Practical Exploitation*, 2017.
- [25] H. Noura, T. Hatoum, O. Salman ve J.-P. A. Yaacoub, «LoRaWAN Security Survey: Issues, Threats and Possible Mitigation Techniques,» *Internet of Things*, 2020.
- [26] I. Butun, N. Pereira ve M. Gidlund, «Security Risk Analysis of LoRaWAN and Future Directions,» *Future Internet*, cilt 11, 2018.
- [27] L. APİLİOĞULLARI, «LPWAN SENSÖRLERİN ÖZELLİKLERİ VE IOT UYGULAMALARINA ETKİLERİ,» *International Journal of 3D Printing Technologies and Digital Industry*, cilt 4, no. 2, pp. 152-160, 2020.
- [28] G. S. R. P. L. D. H. E. Aras, «Exploring the security vulnerabilities of LoRa,» %1 içinde *In Proceedings of the 3rd International Conference on Cybernetics (CYBCONF)*, NJ, USA, 2017.
- [29] J. S. Jaehyu Kim, «Simple and Efficient Replay Attack Prevention Scheme for LoRaWAN,» 2017.
- [30] H. -G. A. J. -B. K. a. S. -G. C. W. -J. Sung, «Protecting end-device from replay attack on LoRaWAN,» %1 içinde *20th International Conference on Advanced Communication Technology (ICACT)*, 2018.
- [31] S.-Y. Gao, X.-H. Li ve M.-D. Ma, « A Malicious Behavior Awareness and Defense Countermeasure Based on LoRaWAN Protocol,» %1 içinde *Sensors* , 2019.
- [32] S. C. S. C. a. V. P. J. Thomas, «Man in the Middle Attack Mitigation in LoRaWAN,» %1 içinde *International Conference on Inventive Computation Technologies (ICICT)*, 2020.
- [33] B. Oniga, V. Dadarlat, E. D. Poorter ve A. Munteanu, «Analysis, design and implementation of secure LoRaWAN sensor networks,» %1 içinde *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, 2017, pp. 421-428.
- [34] N. P. ., M. G. I. Butun, «Security risk analysis of LoRaWAN and future directions,» *Future Internet* , cilt 3, no. 11, (2019) .

- [35] M. E. E. L. A. S. S. Naoui, «Enhancing the security of the IoT LoRaWAN architecture,» %1 içinde *International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, 2016 .
- [36] V. D. E. D. P. A. M. B. Oniga, «A secure LoRaWAN sensor network architecture,» %1 içinde *IEEE SENSORS*, 2017.
- [37] S.-G. J. P. S. F. P. S. J. H.-R. J. S. A. Sanchez-Iborra R, « Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach,» *Sensors*, 2018.
- [38] F. -Y. L. L. -L. H. a. C. -Y. K. K. -L. Tsai, «Secure Session Key Generation Method for LoRaWAN Servers,» *IEEE Access*, no. 8, pp. 54631-54640, 2020.
- [39] A. Rymaszewska, P. Helo ve A. Gunasekaran, «IoT powered servitization of manufacturing – an exploratory case study,» *International Journal of Production Economics*, cilt 192, 2017.
- [40] L. Apilioğulları, *Dijital Dönüşüm-Akıllı Fabrikalar*, İstanbul: Aura, 2019.
- [41] O. Vermesan, «Internet of Things Cognitive Transformation Technology Research Trends and Applications,» *River Publisher Series in Communications*, 2015.
- [42] Lora Alliance , «Lora Alliance Introduction,» [Çevrimiçi]. Available: <https://lora-alliance.org>. [Erişildi: 25 05 2021].
- [43] M. Centenaro, L. Vangelista, A. Zanella ve M. Zorzi, «Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios,» *IEEE Wireless Communications*, cilt 23, no. 5, pp. 60-67, 2016.
- [44] Sigfox, «Sigfox world coverage,» [Çevrimiçi]. Available: <https://www.sigfox.com/en/coverage>.
- [45] LoRa Alliance, «LoRaWAN® Coverage,» [Çevrimiçi]. Available: <https://lora-alliance.org/lorawan-coverage/>. [Erişildi: 25 05 2021].
- [46] E. B. F. C. F. M. Kais Mekki, «A comparative study of LPWAN technologies for large-scale IoT deployment,» 2019. [Çevrimiçi]. Available: https://www.researchgate.net/figure/Respective-advantages-of-Sigfox-LoRa-and-NB-IoT-in-terms-of-IoT-factors_fig3_322018958. [Erişildi: 25 Temmuz 2021].
- [47] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen ve M. Pettissalo, «On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology,» %1 içinde *2015 14th International Conference on ITS Telecommunications (ITST)*, 2015, pp. 55-59.

- [48] G. Ferré ve E. Simon, «An introduction to Sigfox and LoRa PHY and MAC layers,» 2018. [Çevrimiçi]. Available: <https://hal.archives-ouvertes.fr/hal-01774080/document>. [Erişildi: 25 05 2021].
- [49] K. Mekki, E. Bajic, F. Chaxel ve F. Meyer, «A comparative study of LPWAN technologies for large-scale IoT deployment,» *ICT Express*, cilt 5, pp. 1-7, 2019.
- [50] A. Sanfratello, «Enabling relay-based communication in LoRa networks for the Internet of Things: design, implementation and experimental evaluation,» 2016.
- [51] G. DOĞAN, %1 içinde *Study of LoRaWAN wireless communication protocol and an IoT application*, 2019, p. 23.
- [52] «Lora and Lorawan,» [Çevrimiçi]. Available: <https://loradevelopers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/>. [Erişildi: 25 05 2021].
- [53] U. Noreen, A. Bounceur ve L. Clavier, «A study of LoRa low power and wide area network technology,» %1 içinde *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, 2017, pp. 1-6.
- [54] Semtech Corporation, «LoRa® and LoRaWAN®: A Technical Overview,» 2019. [Çevrimiçi]. Available: https://loradevelopers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf. [Erişildi: 25 05 2021].
- [55] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas ve M.-D. Cano, «Performance Evaluation of LoRa Considering Scenario Conditions,» *Sensors*, cilt 18, p. 772, 2018.
- [56] L. Ntseane ve B. Isong, «Analysis of LoRa/LoRaWAN Challenges,» %1 içinde *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 2019, pp. 1-7.
- [57] G. Avoine ve L. Ferreira, «Rescuing LoRaWAN 1.0,» 2018, pp. 253-271.
- [58] LoRa Alliance, «LoRaWAN R1.0 Open Standard Released for the IoT,» 2015. [Çevrimiçi]. Available: <https://www.businesswire.com/news/home/20150616006550/en/LoRaWAN-R1.0-Open-Standard-Released-for-the-IoT>. [Erişildi: 25 05 2021].
- [59] N. Sornin, M. Luis, T. Eirich, T. Kramp ve O. Hersent, «LoRaWAN™ Specification,» 2016. [Çevrimiçi]. Available: https://loralliance.org/wp-content/uploads/2020/11/lorawan1.0.1final_05apr2016_1099_1.pdf. [Erişildi: 25 05 2021].

- [60] LoRa Alliance Technical committee, «LoRaWAN™ 1.0.2 Regional Parameters,» 2017. [Çevrimiçi]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_regional_parameters_v1.0.2_final_1944_1.pdf. [Erişildi: 25 05 2021].
- [61] O. G. Aliu ve M. Kretschmer, «LoRaWAN Evaluation for IoT Communication,» %1 içinde *nternational Conference on Advances in Computing, Communications and Informatics (ICACCI 2018)*, Bangalore, India, 2018.
- [62] LoRa Alliance Technical Committee, «LoRaWAN™ 1.1 Regional Parameters,» 2017. [Çevrimiçi]. Available: <https://lora-alliance.org/wp-content/uploads/2020/11/lorawan-regional-parameters-v1.1ra.pdf>. [Erişildi: 25 05 2021].
- [63] LoRa Alliance Technical Committee, «LoRaWAN™ 1.1 Specification,» 2017. [Çevrimiçi]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_-v1.1.pdf. [Erişildi: 25 05 2021].
- [64] LoRa Alliance Technical Committee, «LoRaWAN™ 1.0.3 Specification,» 2018. [Çevrimiçi]. Available: <https://lora-alliance.org/wp-content/uploads/2020/11/lorawan1.0.3.pdf>. [Erişildi: 25 05 2021].
- [65] L. A. T. Committee, «LoRaWAN® 1.0.4 Specification,» 2020. [Çevrimiçi]. Available: https://lora-alliance.org/resource_hub/lorawan-104-specification-package/. [Erişildi: 25 05 2021].
- [66] N.SORNIN ve A.YEGIN, «LoRaWAN™ Backend Interfaces 1.0 Specification,» 2017. [Çevrimiçi]. Available: <https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm-backend-interfaces-v1.0.pdf>. [Erişildi: 25 05 2021].
- [67] «Gateways,» [Çevrimiçi]. Available: <https://www.thethingsnetwork.org/docs/gateways/>. [Erişildi: 25 05 2021].
- [68] «Connecting the Internet of Things,» [Çevrimiçi]. Available: <https://www.loriot.io/lorawan.html>. [Erişildi: 25 05 2021].
- [69] M. A. Ertürk, «Lorawan indoor performance analysis,» *International Research Journal of Computer Science*, 2017.
- [70] thethingsnetwork.org, «Device Classes,» [Çevrimiçi]. Available: <https://www.thethingsnetwork.org/docs/lorawan/classes/>. [Erişildi: 25 05 2021].
- [71] J. Petajajarvi, K. Mikhaylov, M. Pettissalo ve J. Janhunen, «Performance of a low-power wide-area network based on LoRa technology: Doppler robustness,

scalability, and coverage,» *International Journal of Distributed Sensor Networks*, cilt 13, pp. 1-16, 2017.

- [72] A. Lavric ve V. Popa, «Internet of Things and LoRa™ low-power wide-area networks challenges,» %1 içinde *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1-4.
- [73] Semtech, «Semtech SX1276-7-8-9 Datasheet,» 2016. [Çevrimiçi]. Available: https://semtech.my.salesforce.com/sfc/p/E0000000JelG/a/2R0000001Rbr/6EfVZUorrpoKFfvaF_Fkpgp5kzjiNyiAbqcpqh9qSjE. [Erişildi: 25 05 2021].
- [74] Semtech, «Recommended SX1276 Settings for LoRaWAN Network Operation,» 2015. [Çevrimiçi]. Available: https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/440000001NAw/7YN8ZamV70_xR.vPDAAAshm.0Wt4jmRX0nOKkOzQqiI. [Erişildi: 25 05 2021].
- [75] I. Butun, N. Pereira ve M. Gidlund, «Analysis of LoRaWAN v1.1 Security,» %1 içinde *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects (SMARTOBJECTS '18)*, 2018.
- [76] S. Z. ., L. V. S. Tomasin, «Security analysis of LoRaWAN join procedure for internet of things networks,» %1 içinde *Wireless Communications and Networking Conference Workshops (WCNCW)*, 2017.
- [77] J. Zhang, A. Marshall ve L. Hanzo, «Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks,» *IEEE Transactions on Vehicular Technology*, cilt 67, no. 12, pp. 12462-12466, 2018.
- [78] W. Xu, S. Jha ve W. Hu, «Exploring the Feasibility of Physical Layer Key Generation for LoRaWAN,» *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, no. 231-236, 2018.
- [79] V. R. Joan Daemen, «Aes Proposal: Rijndael,» 1999.
- [80] J. Schwartz, «Us selects a new encryption technique,» *New York Times*, cilt 3, 2000.
- [81] D. P. R. Helger Lipmaa, «Comments to nist concerning aes modes of operation: Ctr-mode encryption,» 2000.
- [82] N. C. S. D. (. S. T. G. (STG)., «Block cipher modes,» April 12, 2013.

- [83] C. Ç. Y. E. E. Faruk AKTAŞ, «Nesnelerin İnterneti Teknolojisinin Biyomedikal Alanındaki Uygulamaları,» *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, pp. 4-7, 2016.
- [84] I. Cervesato, « The dolev-yao intruder is the most powerful attacker,» *In 16th Annual Symposium on Logic in Computer Science—LICS*, no. volume 1, 2001.
- [85] [<http://travisdazell.blogspot.nl/2012/11/many-time-pad-attack-cribdrag.html>]. [Çevrimiçi]. [Erişildi: 2021].
- [86] E. K. C. D. F. K. Xueying Yang, «Security Vulnerabilities in LoRaWAN,» 2018.
- [87] F. P. Hessel, *LoRaWAN Security Analysis: An Experimental Evaluation of Attacks*, 2019.
- [88] H. ALTINPULLUK, «Nesnelerin interneti teknolojisinin eğitim ortamlarında kullanımı,» *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, pp. 4-8, 2018.
- [89] Anonim, «Nesnelerin İnterneti Nedir? IoT Ne işe yarar?,» [Çevrimiçi]. Available: <https://proente.com/nesnelerin-interneti-nedir/>.
- [90] Z. R. Sumit KUMAR, «Using Supply Chain Management Approach for Message Forwarding for Internet of Things (IoT),» *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, pp. 1-6, 2018.
- [91] M. TAŞTAN, «Akıllı Ev Uygulamaları için Yeni Nesil IoT Denetleyici ile Gerçek Zamanlı Uzaktan İzleme ve Kontrol Uygulaması,» *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 2019.
- [92] E. B. Tolga Kılıç, «An Investigation on Internet of Things Technology (IoT) In Smart Houses,» *Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi*, pp. 2-6, 2017.
- [93] M. K. Tuncay ERCAN, «Endüstride Nesnelerin İnterneti (IoT) Uygulamaları Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi,» *Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi*, pp. 3-6, 2016.
- [94] M. N. N. N. İ. N. Abdulkadir ÖZDEMİR, «2014-2018 Yılları Arasında Nesnelerin İnterneti Üzerine Bir Literatür Taraması,» *Bandırma Onyedli Eylül Üniversitesi Sosyal Bilimler Araştırmaları Dergisi*, pp. 11-13, 2018.
- [95] Anonim, «Nesnelerin İnternetinin Uygulamaları ve Örnekleri,» 28 Nisan 2020. [Çevrimiçi]. Available: <https://ioturkiye.com/2020/04/nesnelerin-interneti-uygulamaları-ve-ornekleri/>.
- [96] S. N. BIÇAKÇI, «Nesnelerin İnterneti,» *Takvim-i Vekayi*, pp. 5-7, 2019.

- [97] B. A. Can AYDIN, «Talaşlı İmalat Sektöründe Nesnelerin İnterneti ve Anlık Veri Analizi Yöntemleri Kullanarak Üretim Etkinliğinin Artırılması,» *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, pp. 5-8, 2018.
- [98] M. CINGI, «Nesnelerin İnterneti ve İşbirliği Çağı,» *TRT Akademi*, pp. 3-5, 2016.
- [99] A. A. F. T. Fatma SÖNMEZ ÇAKIR, «Nesnelerin İnterneti Ve Giyilebilir Teknolojiler,» *Sosyal Araştırmalar ve Davranış Bilimleri Dergisi*, pp. 7-9, 2018.
- [100] V. GÖÇÖĞLU, «Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme,» *MANAS Sosyal Araştırmalar Dergisi*, pp. 3-6, 2020.
- [101] S. B. İbrahim KARATAŞ, «Contiki İşletim Sisteminde Cooja Simulatörü Kullanılarak Örnek Bir Nesnelerin İnterneti Uygulaması,» *Avrupa Bilim ve Teknoloji Dergisi*, pp. 1-6, 2020.
- [102] E. E. İlkey Ejder Erturan, «Muhasebe Denetiminde Nesnelerin İnterneti: Stok Döngüsü,» *Muhasebe ve Finansman Dergisi*, pp. 9-11, 2017.
- [103] M. B. Levent GÖKREM, «Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum,» *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, pp. 6-8, 2016.
- [104] E. T. G. M. Murat TOPALOĞLU, «Akıllı Cihaz ve İnsan Etkileşimi: Nesnelerin İnterneti,» *Ege Eğitim Teknolojileri Dergisi*, pp. 2-5, 2019.
- [105] F. ASLAY, «Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi,» *International Journal of Multidisciplinary Studies and Innovative Technologies*, pp. 1-5, 2017.
- [106] H. YEŞİLYURT, «Finansal Hizmet Sektöründe Siber Güvenlik Riskleri ve Çözüm Yolları: Ödeme Sistemleri ve Tedarik Zinciri Bütünlüğü,» *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, p. 4, 2015.
- [107] O. YILMAZ, «Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik,» *Cyberpolitik Journal*, pp. 8-9, 2017.
- [108] N. C.-R. J. J. R.-M. a. P. M.-L. J. Navarro-Ortiz, «Improving Hardware Security for LoRaWAN,» %1 içinde *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2019.
- [109] V. Ribeiro, R. Holanda, A. Ramos ve J. Rodrigues, «Enhancing Key Management in LoRaWAN with Permissioned Blockchain,» 2020.

ÖZGEÇMİŞ

İlk ve orta öğrenimimi Bursa’da tamamladım. 2013 yılında girdiğim Namık Kemal Üniversitesi Bilgisayar Mühendisliği Bölümünden 2017 yılında mezun oldum. 2019 yılından beri Yalova Üniversitesi Lisansüstü Eğitim Enstitüsünde Bilgisayar Mühendisliği Yüksek Lisansı yapmaktayım.

