

PAMUKKALE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

**KABLOSUZ SENSÖR AĞLARININ İP TABANLI AĞLARLA
BİRLEŞTİRİLMESİ**

**YÜKSEK LİSANS TEZİ
Ahmet Çağdaş SEÇKİN**

Anabilim Dalı : Elektrik-Elektronik Müh. A.B.D.

Bölümü : Elektrik-Elektronik Müh.

Tez Danışmanı: Yrd. Doç. Dr. Ahmet ÖZEK

OCAK 2011

YÜKSEK LİSANS TEZİ ONAY FORMU

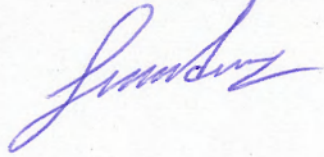
Ahmet Çağdaş SEÇKİN tarafından Yrd. Doç. Dr. Ahmet ÖZEK yönetiminde hazırlanan "Kablosuz Sensör Ağlarının IP Tabanlı Ağlarla Birleştirilmesi" başlıklı tez tarafımızdan okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Başkanı

Yrd. Doç. Dr. Ahmet ÖZEK

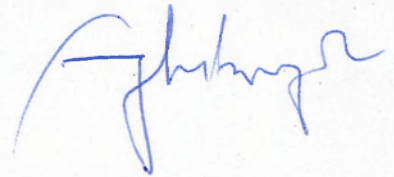
Jüri Üyesi

Yrd. Doç. Dr. Gürhan GÜNDÜZ



Jüri Üyesi

Doç. Dr. Ceyhun KARPUZ



Pamukkale Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

20.../...01.../2011 tarih ve 03-14... sayılı kararıyla onaylanmıştır.

Enstitü Müdürü

Prof. Dr. Halil KARAHAAN

TEŐEKKÜR

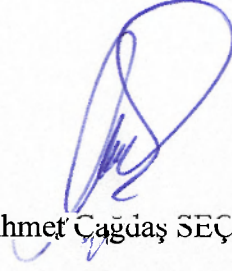
Tez alıőmam boyunca bilimsel katkıları ile bana destek olup, eđitimim süresince yardımlarını esirgemeyen, tez danışmanım ve deđerli hocam Yrd. Do. Dr. Ahmet ÖZEK'e ve her őart altında manevi desteklerini benden esirgemeyen aileme ok teőekkür ederim.

BİLİMSEL ETİK SAYFASI

Bu tezin tasarımı, hazırlanması, yürütülmesi, arařtırmaların yapılması ve bulguların analizinde bilimsel etięe ve akademik kurallara özenle riayet edildiđini; bu çalışmanın doğrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etięe uygun olarak kaynak gösterildiđini ve alıntı yapılan çalışmalara atfedildiđini beyan ederim.

İmza

:



Öğrenci Adı Soyadı : Ahmet Çağdaş SEÇKİN

ÖZET

KABLOSUZ SENSÖR AĞLARININ IP TABANLI AĞLARLA BİRLEŞTİRİLMESİ

Seçkin, Ahmet Çağdaş

Yüksek Lisans Tezi, Elektrik - Elektronik Mühendisliği A.B.D.

Tez Yöneticisi: Yrd. Doç. Dr. Ahmet ÖZEK

Aralık 2010, 71 Sayfa

Kablosuz sensör ağları, çevreden veri toplamaya yarayan birçok sensör düğümünden oluşan kablosuz kişisel alan ağlarıdır. Kablosuz sensör ağı düğümleri arasındaki haberleşmede IEEE 802.15.4 ve ZigBee standartları kullanılmaktadır. Bu standartlar ile düşük güç tüketen, az maliyetli, güvenilir ve genişletilebilir ağlar oluşturulabilmektedir. Tezde kablosuz sensör ağı düğümleriyle IP-tabanlı ağlar arasında haberleşme yapıp internete girilebilen her noktadan sensör ağı düğümlerine ulaşmak hedeflenmektedir. Bu hedef doğrultusunda kablosuz sensör ağı ve IP tabanlı ağlarda kullanılan standartlar hakkında literatür araştırması yapılmıştır. Literatür araştırması sonucunda iki ağ arasında haberleşme yapılabilmesi için veri paketleme, adresleme, servis keşfi ve güvenlik problemlerinin aşılması gerektiği sonucuna varılmıştır. Problemlerin tespitinden sonra bunları aşmak için hali hazırda kullanılan yöntemler incelenmiştir. Ağlar arası haberleşme tekniklerinin incelemesiyle mevcut standartları koruyan en verimli yöntemin sunucu tabanlı yöntem olduğu sonucuna varılmıştır.

Literatür araştırması sonuçlarına dayanılarak çalışmada ağlar arası haberleşme için sunucu tabanlı yöntem tercih edilmiştir. Çalışmada oluşturulan sunucu tabanlı ağlar arası haberleşme sistemi sunucu, ağ geçidi ve kablosuz sensör ağından oluşmaktadır.

Sistemde kullanılan sunucu internet tarafındaki kullanıcılara kablosuz sensör ağı kaynaklarını sunan birimdir. Çalışmada sunucu sistemi olarak bir mesajlaşma protokolü olan XMPP teknolojisi tercih edilmiştir. XMPP teknolojisinin tercih edilmesinin sebebi sunucu olarak klasik web sunucusu yerine, farklı teknolojilerin sunucu olarak kullanılabilirliğini bir uygulamayla örneklemektir. Sistemde ağlar arası tercüme işleminin gerçekleştirildiği birim ağ geçididir. Ağ geçidi hem internet hem de kablosuz sensör ağıyla haberleşebilen tek cihazdır. Ağ geçitleri, sistemde veri depolama, servis sağlama, paketleme, adresleme, servis keşfi ve güvenlik işlemlerini üstlenmektedir. Kablosuz sensör ağı ise sensör düğümlerinden oluşmaktadır ve bulunduğu ortam ile çeşitli şekillerde etkileşime girmektedir.

Sonuçta kablosuz sensör ağı ile IP tabanlı ağların bütünleştirilmesi sunucu tabanlı bir sistem tasarlanarak gerçekleştirilmiştir. Tasarlanan sistem ile sunucu tabanlı yöntem kullanılarak ağlar arası haberleşmede ZigBee standardının avantajlarının korunması sağlanmıştır. Ayrıca sunucu tabanlı sistemlerde klasik web sunucusu yerine XMPP sunucusunun kullanılabilirliği tez kapsamında yapılan uygulamayla sınıanmıştır.

Anahtar Kelimeler: Kablosuz Sensör Ağları, LR-WPAN, Ağlar Arası Haberleşme, İnternet, ZigBee, IEEE 802.15.4, Ağ geçidi, XMPP

ABSTRACT

COMBINING WIRELESS SENSOR NETWORKS AND IP BASED NETWORKS

Seçkin, Ahmet Çağdaş

M.Sc. Thesis in Electrics – Electronics Engineering

Supervisor: Asst. Prof. Dr. Ahmet ÖZEK

December 2010, 71 Pages

Wireless sensor networks are a kind of personal area network that consists of sensor nodes which collect data from environment. IEEE 802.15.4 and ZigBee standards are used in communication among the wireless sensor network nodes. Low power consuming, low cost, reliable and expandable networks can be created with these standards. The aim of this thesis is enlarging accessibility of wireless sensor networks by internetworking with IP-based networks. The mean of enlarging accessibility is to provide access to wireless sensor networks from where we can access internet connection. A literature study was made about standards which are used in IP based networks and wireless sensor networks to find out problems in internetworking. The literature study concluded that packaging, addressing, service discovery and security are major problems in internetworking. After the identification of problems an examination was made about to find best internetworking method which conserves standards and provides effective communication. Examination of existing internetworking techniques concluded that server based method is the most appropriate method about protecting existing standards and efficiency.

Basing on literature studies, server based systems was preferred for the internetworking system which is used in thesis. System which is created in the application is consisted from server, gateway and wireless sensor network. The server which is an internet unit of the server based system serves wireless sensor networks resources to users who located in internet. XMPP which is an instant messaging protocol is used as server system in this thesis. The reason of preferring XMPP technology is sampling usage of different technology instead of classical web server. XMPP server which is located on internet side of the system provides instant messaging service. Gateway is translator unit of server-based system which is between sensor network and XMPP server. Gateway is only device can communicate both wireless sensor networks and IP-based networks. Data storage, service delivery, packing, addressing, service discovery and security operations are handled by gateways. Wireless sensor networks are consisted from sensor nodes which measuring environmental magnitudes and interact with the environment in various ways.

As a result of the application in this thesis, integration of wireless sensor network with IP-based networks was realized by designing a server based system. ZigBee standard benefits were protected with server based internetworking application. In addition, the availability of using XMPP server instead of conventional web server in the server based systems has been tested.

Keywords: Wireless Sensor Networks, LR-WPAN, Internetworking, Internet, ZigBee, IEEE 802.15.4, Gateway, XMPP

İÇİNDEKİLER

Sayfa

YÜKSEK LİSANS TEZİ ONAY FORMU	I
TEŞEKKÜR	II
BİLİMSEL ETİK SAYFASI	III
ÖZET	IV
ABSTRACT	VI
İÇİNDEKİLER	VIII
ŞEKİLLER DİZİNİ	X
TABLolar DİZİNİ	XII
SİMGELER VE KISALTMALAR DİZİNİ	XIII
1. GİRİŞ	1
2. GENEL BİLGİLER	3
2.1. TCP/IP ve Özellikleri	3
2.2. IEEE 802.15.4 Standardı ve Özellikleri	5
2.2.1. IEEE 802.15.4 fiziksel katmanı	6
2.2.2. IEEE 802.15.4 MAC katmanı	8
2.2.2.1. Süper çerçeve yapısı	8
2.2.2.2. Kanal erişimi	9
2.2.2.3. Veri aktarım modeli	11
2.2.2.4. GTS ve GTS dağıtma	12
2.2.2.5. MAC çerçeve yapısı.....	13
2.3. ZigBee Standardı ve Özellikleri	13
2.3.1. Ağ topolojileri ve bileşenleri	14
2.3.2. Ağ katmanı.....	17
2.3.3. Uygulama katmanı	18
2.4. XMPP ve Özellikleri	19
3. AĞLAR ARASI HABERLEŞME	21
3.1. IEEE 802.15.4/ZigBee ile TCP/IP Ağları Arasındaki Farklar ve Ağlar Arası Haberleşmede Karşılaşılan Sorunlar	21
3.2. Ağlar Arası Haberleşme Yöntemleri	22
3.2.1. IEEE 802.15.4 standart yığını üzerinden ağlar arası haberleşme	23
3.2.2. ZigBee standart yığını üzerinden ağlar arası haberleşme	25
4. AĞLAR ARASI HABERLEŞME SİSTEMİ	28
4.1. ZigBee Modülü	30
4.1.1. XBee modül özellikleri	31
4.1.1.1. Şeffaf (Transparent) mod	31
4.1.1.2. API modu	32
4.1.1.3. Giriş-çıkış birimi ve analog sayısal çevirici.....	34
4.1.1.4. XBee ağı.....	34
4.1.1.5. Çalışma modları	37
4.1.2. XBee modül yapılandırması	38
4.2. Ağ Geçidi Donanımı ve Gereksinimleri	39

4.3.	Sistem Yazılımı ve Yönetimi	40
4.3.1.	Ağ geçidi yazılımı.....	40
4.3.1.1.	ZigBee arayüzü ve dinleyicisi.....	48
4.3.1.2.	XMPP arayüzü ve dinleyicisi.....	49
4.3.2.	Kullanıcı yazılımı.....	51
5.	SCADA UYGULAMASI	53
5.1.	Kablosuz Sensör Ağı Düğüm Donanımı	53
5.1.1.	Mikrodenetleyici özellikleri ve yazılımı	54
5.1.2.	XBee modül yapılandırması	57
5.2.	XMPP Kullanıcı Yazılım Uygulaması.....	58
6.	SONUÇ VE ÖNERİLER.....	60
	KAYNAKLAR	63
	EKLER.....	65
	ÖZGEÇMİŞ.....	71

ŞEKİLLER DİZİNİ

	Sayfa
Şekil- 2.1: OSI modeli ve TCP/IP modeli.....	3
Şekil- 2.2: TCP/IP kapsülleme işlemi	5
Şekil- 2.3: OSI modeli ve IEEE 802.15.4-ZigBee modeli.....	6
Şekil- 2.4: Fiziksel katman veri paketi.....	8
Şekil- 2.5: Süper çerçeve yapısı	9
Şekil- 2.6: Uyarının hedef şaşırabileceği düğüm yerleşmi	10
Şekil- 2.7: IFS süreleri	11
Şekil- 2.8:MAC katmanı çerçeveleri	14
Şekil- 2.9: Kablosuz sensör ağlarında çocuk-ebeveyn ilişkisi.....	15
Şekil- 2.10: Yıldız ağ topolojisi	16
Şekil- 2.11: Mesh ağ topoloji	16
Şekil- 2.12: Ağaç ağ topolojisi.....	17
Şekil- 2.13: XMPP ağ mimarisi	20
Şekil- 3.1: IEEE 802.15.4 yığını üzerine TCP/IP yığını yerleştirilmesi	23
Şekil- 3.2: 6LoWPAN ağ geçidi	24
Şekil- 3.3: IPv6 ve EUI-64.....	24
Şekil- 3.4: ZigBee yığınının genişletilerek TCP/IP yığına erişim	26
Şekil- 3.5: ZigBee yığını üzerine TCP/IP yığını yerleştirilmesi	27
Şekil- 3.6: Sunucu tabanlı sistem.....	27
Şekil- 4.1: ZigBee ve İnternet ağları arası haberleşme sistemi.....	30
Şekil- 4.2: API çerçeve yapısı.....	33
Şekil- 4.3: XBee giriş-çıkış pin başlık yapısı.....	34

Şekil- 4.4: XBee giriş çıkış pin veri formatı	34
Şekil- 4.5: ZigBee çalışma modları.....	38
Şekil- 4.6: AT komut formatı.....	39
Şekil- 4.7: Ağ geçidi donanımı	39
Şekil- 4.8: Ağ geçidi yazılımı şeması	41
Şekil- 4.9: Ağ geçidi çalışma modları.....	42
Şekil- 4.10: Ağ geçidi algoritması	43
Şekil- 4.11: Ağ geçidi kullanıcı grafik arayüzü ZigBee sekmesi.....	45
Şekil- 4.12: Ağ geçidi kullanıcı grafik arayüzü XMPP sekmesi.....	46
Şekil- 4.13: Ağ geçidi kullanıcı grafik arayüzü veri tabanı sekmesi	47
Şekil- 4.14: Ağ geçidi kullanıcı grafik arayüzü yapılandırma sekmesi	48
Şekil- 4.15 ZigBee arayüz algoritması.....	49
Şekil- 4.16: XMPP dinleyici algoritması	51
Şekil- 4.17: Kullanıcı yazılım algoritması	52
Şekil- 5.1: SCADA uygulama şeması.....	53
Şekil- 5.2: Düğüm modeli.....	54
Şekil- 5.3: Arduino güç şeması	55
Şekil- 5.4: Mikrodenetleyici ve seri haberleşme şeması.....	55
Şekil- 5.5: Buton, LED, XBee modül, sıcaklık sensörü ve LCD bağlantıları	56
Şekil- 5.6: Düğüm mikrodenetleyici algoritması.....	57
Şekil- 5.7: SCADA uygulaması XMPP kullanıcı yazılımı grafik arayüzü.....	59

TABLULAR DİZİNİ

	Sayfa
Tablo- 2.1: IEEE 802.15.4 frekans bantları	6
Tablo- 4.1: XBee modül pin bilgileri	31
Tablo- 4.2: API çerçeve çeşitleri.....	33
Tablo- 4.3: Koordinatör ve son cihaz birleşme parametreleri.....	36
Tablo- 4.4: XBee uyku modlarına giriş ve çıkış şekilleri	38

SİMGELER VE KISALTMALAR DİZİNİ

6LoWPAN	:IPv6 over Wireless Personal Area Network
ACK	:Acknowledgement Message
ADC	:Analog to Digital Converter
AES-128	:Advanced Encryption Standard 128 bits
API	:Application Programming Interface
ASCII	:American Standard Code for Information Interchange
Bps	:Bits Per Second
CAP	:Contention Access Period
CCA	:Clear Channel Assessment
CFP	:Contention Free Period
cmdData	:Command Data
cmdID	:Command Identifier
CS	:Carrier Sense
CSMA-CA	:Carrier Sense Multiple Access with Collision Avoidance
CSMA-CD	:Carrier Sense Multiple Access with Collision Detection
dBm	:Decibel Milli
DIFS	:Distributed Inter Frame Spaces

DIN	:Data In
DOUT	:Data Out
DSL	:Digital Subscriber Line
EIFS	:Extended Inter Frame Spaces
EUI-64	:Extended Unique Identifier
FCS	:Frame Check Sum
FFD	:Full Function Device
FTDI	:Future Technology Devices International
FTP	:File Transfer Protocol
GHz	:Giga Hertz
GPRS	:General packet Radio Service
GTS	:Guaranteed Time Slot
HEX	:Hexadecimal
HTTP	:Hypertext Transfer Protocol
HTTPS	:Hypertext Transfer Protocol Secure
ID	:Identifier
IEEE	:Institute of Electrical and Electronics Engineers
IETF	:Internet Engineering Task Force
IFS	:Inter Frame Spaces

IP	:Internet Protocol
IPv4	:IP version 4
IPv6	:IP version 6
ISM	:Industrial, Scientific and Medical
JRE	:Java Runtime Enviorenment
JID	:Jabber Identifier
kbps	:Kilo Bits Per Second
kHz	:Kilo Hertz
LAN	:Local Area Network
LCD	:Liquid Crystal Display
LDAP	:Lightweight Dirctory Access Protocol
LED	:Light Emitting Diode
LLC	:Logical Link Control
LR-WPAN	:Low Rate Wireless Personel Area Network
LSB	:Least Significant Bit
mA	:Milli Amper
MAC	:Media Access Control
Mbps	:Mega Bits Per Second
MHz	:Mega Hertz

MSB	:Most Significant Bit
MTU	:Maximum Transmission Unit
OEM	:Original Equipment Manufacturer
O-QPSK	:Offset Quadrature Phase Shift Keying
OSI	:Open Systems Interconnection
PAN	:Personal Area Network
PAN-ID	:Personal Area Network Identifier
PCS	:Physical Carrier Sense
PIFS	:Point Inter Frame Spaces
PSDU	:Physical Layer Service Data Unit
PWM	:Pulse Width Modulation
RF	:Radio Frequency
RFC	:Request for Comments
RFD	:Reduced Function Device
RSSI	:Received Signal Strength Indication
SASL	:Simple Authentication and Security Layer
SCADA	:Supervisory Control and Data Acquisition
SIFS	:Short Inter Frame Spaces
SNMP	:Simple Network Management Protocol

SOAP	:Simple Object Access Protocol
SSCS	:Service Specific Convergence Sublayer
TCP	:Transmission Control Protocol
TCP/IP	:Transmission Control Protocol/Internet Protocol
TLS	:Trasnport Layer Security
TTL	:Transistor-Transistor Logic
uA	:Micro Amper
UART	:Universal Asynchronus Receiver/Transceiver
UDP	.User Datagram Protocol
V	:Volt
VCS	:Virtual Carrier Sense
WAN	:Wide Area Network
XML	:Extensible Markup Language
XMPP	:Extensible Messaging and Persence Protocol

1. GİRİŞ

Son yıllarda haberleşme uygulamalarının yaygınlaşmasıyla birlikte uygulama gereksinimlerine göre optimizasyon çalışmaları yeni standartların ortaya çıkmasını tetiklemiştir. Kablosuz haberleşme standartlarından IEEE 802.15.4, LR-WPAN'ların Fiziksel ve MAC katmanlarını tanımlamaktadır. OSI modeline göre Fiziksel ve MAC katmanları LR-WPAN'ların ilk iki katmanıdır. LR-WPAN'lar düşük maliyetli, uzun batarya ömrüne ihtiyaç duyan ve yüksek hızda haberleşmeye gereksinim duymayan uygulamalar için kullanılan ağ çeşididir. OSI modeline göre LR-WPAN'ların üst katmanlarını ZigBee, MiWi, WirelessHART ve 6LoWPAN gibi teknolojiler oluşturmaktadır.

ZigBee, kablosuz sensör ağı uygulamaları için kullanılan IEEE 802.15.4 standardını temel alan bir LR-WPAN teknik standardıdır. Teknik standartlar piyasanın ihtiyacı doğrultusunda genellikle özel kuruluşlar tarafından oluşturulan standartlardır. ZigBee standardı için teknik standart oluşturucu birliği ZigBee Alliance'dır. Kablosuz sensör ağları mekâna bağlı olarak dağılmış otonom sensör düğümlerinden oluşan ve çevreden bilgi toplamaya yarayan ağlardır. ZigBee sağladığı uzun pil ömrü, geniş kapsama alanı ve esnek ağ yapısı avantajları sebebiyle askeri, sağlık, robotik, sanayi ve ev otomasyonu uygulamalarında tercih edilmektedir. Kullanım alanı açısından çok geniş alana sahip olmasına rağmen ZigBee standardıyla çalışan ağlar merkezidir ve yerel bir ağ yapısına sahiptir. Yani ZigBee ile çalışan ağlar küçük alanlarda çalışmakta ve diğer ağlarla haberleşmemektedir [1].

Günümüzde İstenilen bilgiye uzaktan erişebilme gereksinimleri farklı teknolojilerin bir arada çalıştırılmasını ve en genel ağ türü olan internet ile ağlar arası haberleşme yapılmasını doğurmuştur. LR-WPAN'lar, özellikle uzun batarya ömrüne ihtiyaç duyan kontrol ve izleme tekniklerinin kullanıldığı askeri, çevre görüntüleme, endüstriyel uzaktan kumanda, ev otomasyonu ve tarım uygulamaları gibi alanlarda kullanılmaktadır. İhtiyaç doğrultusunda geniş kullanım alanına sahip kablosuz sensör ağlarının, IP tabanlı ağlarla birleştirilmesi birçok araştırmacının ilgisini çekmektedir. Kablosuz sensör ağlarında kullanılan ZigBee teknolojisinin adresleme yapısı, bellek kapasitesi, paket büyüklüğü ve düşük veri oranı, kablosuz sensör ağlarının IP tabanlı

ağlarla doğrudan haberleşmesini engellemektedir. Özellikle internetteki artan kullanıcı sayısı sebebiyle IPv4'ün yerini IPv6 tabanlı ağlara bırakacağı düşünüldüğünde adresleme, veri aktarım oranları ve paket genişliği ciddi sorun olmaktadır. Bu tezde, ZigBee standardının sağladığı avantajları koruyarak en verimli şekilde ağlar arası haberleşme yapılması amaçlanmaktadır.

Tasarlanan sistemde literatür taramasına dayanılarak ZigBee standardının korunması için sunucu tabanlı yöntem seçilmiştir. Ancak tasarlanan sistemde sunucu olarak web sunucusu yerine bir mesajlaşma sunucusu kullanılmıştır. Anlık mesajlaşma sunucusu kullanılmasıyla ZigBee düğümlerine, internet erişimi sağlanan her noktadan bir anlık mesajlaşma programı vasıtasıyla erişim hedeflenmektedir.

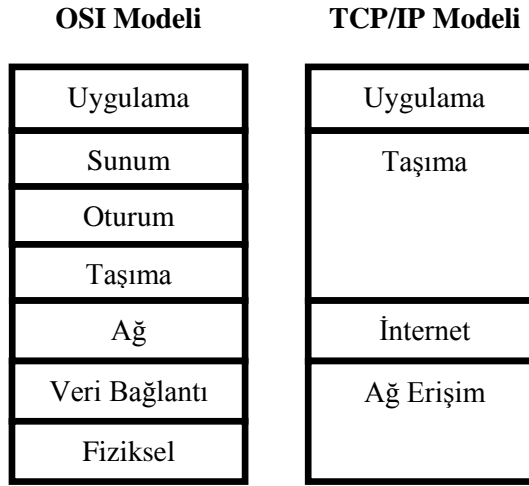
Tezde kullanılan sunucu tabanlı yöntemde klasik web sunucusu yerine bir anlık mesajlaşma sunucusu kullanılması farklı sunucu türlerinin ağlar arası haberleşmede nasıl çalıştığını görmek açısından önemlidir. Ayrıca sistemde ZigBee standardının korunarak ağlar arası haberleşme yapılması, ZigBee standardının sağladığı avantajlardan faydalanabilmek ve her ZigBee standardıyla çalışan ağ ile çalışabilmek açısından önemlidir.

Tezin literatür taraması kısmında TCP/IP, IEEE 802.15.4, ZigBee ve tezde kullanılacak olan XMPP protokolü hakkında genel bilgi verilmektedir. Üçüncü bölümde ağlar arası haberleşme problemleri ve problemlerin çözülmesi için kullanılan tekniklerle incelenmektedir. Dördüncü bölümde tasarlanan ağlar arası haberleşme sistemi hakkında bilgi verilmektedir. Beşinci bölümde uygulamada kullanılan program ve özellikleri tanıtılmıştır. Sonuç ve öneriler bölümüyle tez son bulmaktadır.

2. GENEL BİLGİLER

2.1. TCP/IP ve Özellikleri

TCP/IP, internetin çalışmasını sağlayan iletişim protokolüdür. Yollanan verilere, katmanlara göre başlık ekleme işlemleri yapılmaktadır. Veriler tüm katmanlardaki paketleme işlemi tamamlandıktan sonra hedefe gönderilmektedir. Alıcıda bu paket katmanlara göre teker teker açılıp veri aktarımı tamamlanmaktadır. Bu yöntem kapsülleme olarak adlandırılmaktadır. Kapsülleme veri yollama şekli ile veri yolunu birbirinden ayırmakta ve birlikte çalışmayı kolaylaştırmaktadır. TCP/IP modeli uygulama, taşıma, internet ve ağ erişim olarak dört katmandan meydana gelmektedir. TCP/IP katmanları ve OSI modeli Şekil-1.1’de gösterilmektedir.



Şekil- 2.1: OSI modeli ve TCP/IP modeli

Uygulama katmanı, bilgisayar uygulamasıyla ağ arasındaki arabirim görevini yerine getiren katmandır. Uygulama katmanı Kullanıcı tarafına en yakın katmandır ve diğer katmanlara servis sağlamaktadır. Kullanıcının direk olarak karşılaştığı HTTP, FTP ve SNMP bu katmanda çalışan bazı protokollerdir.

Taşıma Katmanı, Uygulama Katmanından gelen veriyi ağda iletilecek segmentler haline getirmektedir. OSI modeline göre oturum, sunum ve taşıma katmanlarını kapsamaktadır. Bağlantı odaklı haberleşme, veri yönlendirme, akış denetimi, veri doğrulama, veri sıralama, tıkanıklık giderme, işlem portu belirleme ve veri güvenliği gibi işlemler bu katmanda gerçekleştirilmektedir. TCP ve UDP protokolleri bu katmanda tanımlıdır. UDP, verileri bağlantı kurmadan yollamaktadır. Yani UDP ile giden verinin hedefine ulaşıp ulaşmadığı kontrol edilmemektedir. Böylece yüksek

veri iletim hızı sağlanmaktadır. UDP, ses ve görüntü gibi gerçek zamanlı veri aktarımları için kullanılmaktadır. TCP, bilgisayar haberleşmesinde kayıpsız veri gönderimi sağlamak için kullanılmaktadır. Gönderilen veriler için özel bir kabul mesajı alıcıdan göndericiye yollanmaktadır. Bu mesaj verinin doğru iletilip iletilmediğini bildirmektedir. Hata çıkması durumunda veri tekrar gönderilmektedir.

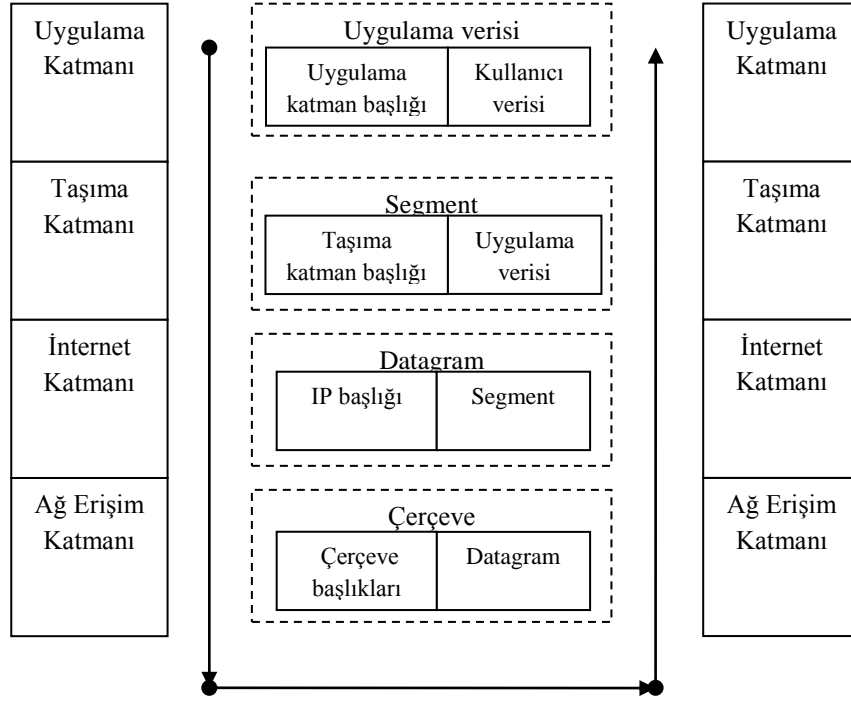
İnternet Katmanı, kaynaktan hedefe paketin iletilmesiyle sorumludur. Haberleşmenin bağlantı odaklı yapıya yapılmayacağı bu katmanda tanımlıdır. Geniş alan ağlarını alt ağlara bölme işlemi bu katmanda gerçekleştirilmektedir. Bu işlem için ağ geçitleri veya yönlendiriciler kullanılmaktadır. Bu cihazlar paketleri ağlar arasında yönlendirmede ve ağlar arası haberleşmede kullanılmaktadır. Veri bu katmanda datagram halindedir.

Ağdaki her cihaza hedefi ve kaynağı belirlemek için bir adres atanmaktadır. Bu adres IP adresi olarak adlandırılmaktadır. Şu an kullanmakta olduğumuz adresleme IPv4 olarak adlandırılmaktadır. Ancak 32 bitlik adres yapısına sahip olan IPv4 bu gün adreslemede yetersiz kalmaktadır. Bu adresleme sıkıntısını ortadan kaldırmak için IPv6 oluşturulmuştur. IPv6'nın 128 bitlik adresleme yapısıyla IPv4'deki 4.3×10^9 adres yerine 3.4×10^{38} gibi çok büyük bir adresleme kapasitesine ulaşılmaktadır. Bunun yanında IPv4'de kullanılan MTU değeri en az 576 byte iken IPv6'da en az 1280 byte olmaktadır.

Ağ Erişim Katmanı, en alttaki katmandır. OSI modeline göre veri bağlantı katmanı ve fiziksel katmanı kapsamaktadır. Veri bu katmanda çerçeveler halindedir yani artık hedefe gönderilmeye hazırdır. Ağ üzerindeki diğer bilgisayarları tanıma, veri gönderirken hata ve adres denetimi, veri alırken verinin tekrar istenmesi ve veri akış denetimi işlemleri ağ erişim katmanında gerçekleştirilmektedir. Bu işlemlerin haricinde ağ erişim katmanının en önemli işlevi verinin aktarılacağı ortama veri iletmek ve ortamdan veri almaktır.

TCP/IP katmanlarının çalışmasını ve yaptıkları işlemleri bir örnekle özetleyecek olursak; uygulama katmanında uygulama çıktısı oluşur ve sistemde hangi veriyi, hangi adrese, hangi porttan yollayacağını söylemektedir. Uygulama Katmanında oluşturulmuş uygulama verisine taşıma katmanında port ve paket boyu bilgileri eklenerek paketler oluşturulmaktadır. Ardından bu pakete ağ katmanında kaynak ve hedef IP adres bilgileri eklenmektedir. Fiziksel katmanda ise paket MAC adresleri yazılmakta ve paketin son boyu eklenmektedir. Daha sonra paket, iletim ortamına

aktarılmaktadır. Buraya kadar yapılan kapsülleme işlemleriyle oluşturulan paket istenen hedefe ulaştırılmaktadır, Hedefe ulaşan paketler katmanlardan tırmanırken kapsüllemeye yapılan işlemlerin tersi yapılarak çözülmektedir ve son olarak yine alıcının uygulama katmanına kadar ulaşmaktadır. Böylece veri aktarımı tamamlanmakta ve veriler uygulamada işlenmektedir. TCP/IP katmanlarına göre verinin kapsülleme ve çözülme işlemleri Şekil-1.2’de gösterilmektedir[2].



Şekil- 2.2: TCP/IP kapsülleme işlemi

2.2. IEEE 802.15.4 Standardı ve Özellikleri

Kablosuz haberleşme standartlarından IEEE 802.15 kablosuz kişisel alan ağlarını tanımlamaktadır. IEEE 802.15.4 ise LR-WPAN yani düşük veri aktarım oranlı kablosuz kişisel alan ağı standardıdır. IEEE 802.15.4, LR-WPAN'ların fiziksel katman ve ortam erişim katmanı (MAC) standartlarını belirtmektedir. IEEE tarafından oluşturulan IEEE 802.15.4 standardı Şekil-1.3'deki OSI modelinde gösterildiği gibi ilk iki katman olan fiziksel ve MAC katmanlarını tanımlamaktadır.

LR-WPAN aygıtlarında, Fiziksel katman RF alıcı-verici mekanizmasını barındırmaktadır. MAC katmanı ise üst katmanlardan gelen verinin fiziksel katmana erişimini sağlamaktadır. Üst katmanlarda yer alan ağ katmanı, ağın yapılandırma, değişiklik algılama ve mesaj yönlendirme işlemlerini yerine getirmektedir. Uygulama katmanı ise aygıtın ağdaki görev ve yeteneklerine yönelik işlemlerin

yapıldığı katmandır. IEEE 802.2 mantıksal bağlantı denetimi (LLC) ile üst katmanlar MAC katmanına SSCS kullanarak erişmektedir [1].

OSI Modeli	ZigBee	MiWi	6LoWPAN	
Uygulama	Uygulama	Uygulama	Uygulama	
Sunum				
Oturum				Taşıma
Taşıma				
Ağ	Ağ	Ağ		IPv6
				Uyumlandırma
Veri Bağlantı	MAC			} IEEE 802.15.4
Fiziksel	PHY			

Şekil- 2.3: OSI modeli ve IEEE 802.15.4-ZigBee modeli

2.2.1. IEEE 802.15.4 fiziksel katmanı

IEEE 802.15.4 standardı Fiziksel Katmanı temelde iki hizmet sunmaktadır. Bunlar veri servisi ve fiziksel katman yönetim servsidir. Veri servisi, fiziksel radyo kanalı üzerinden veri birimlerinin alınması ve gönderilmesini sağlar. Fiziksel katman radyo alıcı-vericisini etkinleştirme, haberleşme kanalı enerji seviye ölçümü, hat kalite sınama, kanal seçme, temiz kanal sınama (CCA) ve veri alma-verme işlemlerinden sorumludur.

IEEE 802.15.4, fiziksel katmanda farklı frekans bandı seçenekleri sunmaktadır. Tablo-1.1'de özetlenen bu frekanslardan ISM 2.4GHz frekansı dünya genelinde en yaygın olarak kullanılmaktadır.

Tablo- 2.1: IEEE 802.15.4 frekans bantları

Frekans	Bölge	Band	Veri Aktarım Oranı (kbps)	Kanal Sayısı
868 MHz	Avrupa	868–868.6	100	1
915 MHz	Amerika	902–928	250	30
2.4 GHz	Küresel	2400–2483.5	250	16

Bu standart ISM 2450 MHz frekansında 250 kbps veri aktarım oranı sağlamaktadır. Bu frekansta O-QPSK modülasyonu kullanılmaktadır. Veri önce 4 bit sembollere

ayrılır, sonra da semboller 32 bit uzunluğunda parçalar haline getirilir ve modüle edilir. Farklı frekans bantlarındaki birçok kanalın bulunması spektrum içinde yer değiştirme olanağı sağlamaktadır. Ayrıca IEEE 802.15.4 standardı kanal tarama işlemiyle, çalışılabilecek kanalları belirleyerek aktif kanal değiştirme olanağı sağlamaktadır. Kanal tarama işlemi esnasında kanaldaki enerji seviyesi ölçülerek kanal yoğunluğu ve kanal kalitesi belirlenmektedir [1,3].

Alıcı enerji seviye ölçümü, kanal seçme algoritmasının bir parçasıdır. Enerji seviye ölçümü, tarama için tanımlanmış olan kanallarda sinyal gücünün ölçülmesidir. Ancak bu ölçüm, ölçüm yapılan kanaldaki tahmini güç değerini vermektedir. Enerji seviyesi ölçüm sonucu, 0x00 ile 0xff arasında 8 bit bir değer olarak belirtilmektedir [3].

Hat kalite bildirimini, alınan paketin sağlamlık ve kalite karakteristiğidir. Hat kalite bildirimini enerji seviye ölçümü ve sinyal gürültü oranı ölçümünden oluşmaktadır. Paket alındıktan sonra fiziksel katman servis veri birim (PSDU) uzunluğu gönderilmektedir. Bu PSDU değeri hat kalite bildirimini içermektedir. Kalite bildirimini 0x00 ve 0xff arasında bir 8-bitlik değer ile bildirilir. Burada 0x00 en düşük kalite 0xff ise en yüksek kaliteyi belirtmektedir [3].

Temiz kanal sınaması (CCA) eşik değeri, taşıyıcı ve eşik seviyesi üzerinde taşıyıcı olmak üzere üç farklı şekilde yapılmaktadır. Eşik değeri üzerinde enerji algılamasında, taranan kanalda eşik değerinin üzerinde enerji olup olmadığına bakılmaktadır. Bu durum tespit edildiğinde meşgul kanal bildirimini yapılmaktadır. Ortamdaki taşıyıcı varlığının sınanması, kanalda modülasyon taşıyıcısının olup olmadığına bakılarak yapılmaktadır. Taşıyıcı algılanması durumunda meşgul kanal bildirimini yapılmaktadır. Bu durumda sinyal enerjisinin eşik seviyesi üzerinde veya altında olup olmadığına bakılmamaktadır. Eşik seviyesi üzerinde taşıyıcı algılamada ise, taranan kanaldaki eşik seviyesinin üzerinde enerjiye sahip taşıyıcıların olup olmadığına bakılmaktadır. Eşik seviyesinin üzerinde taşıyıcı algılanırsa meşgul ortam bildirimini yapılmaktadır [1,3].

Fiziksel katman veri paketleri alıcı cihazın senkronize olmasını ve bit katarına kilitlenmesini sağlayan senkronizasyon başlığı, çerçevenin fiziksel özellik bilgisini içeren fiziksel başlık ve fiziksel katman yükünden oluşmaktadır. Fiziksel katman yükü, MAC katmanından gelen verilerden oluşmaktadır. Şekil-1.4'de veri paketlerinin yapısı gösterilmektedir[3].

Başlangıç (8 bit)	Senkronizasyon (8 bit)	Çerçeve Uzunluğu (7 bit)	Ayrılmış Kısım (1 bit)	PSDU (Değişken uzunlukta)
Senkronizasyon		Fiziksel Özellik		Fiziksel Katman Yüğü

Şekil- 2.4: Fiziksel katman veri paketi

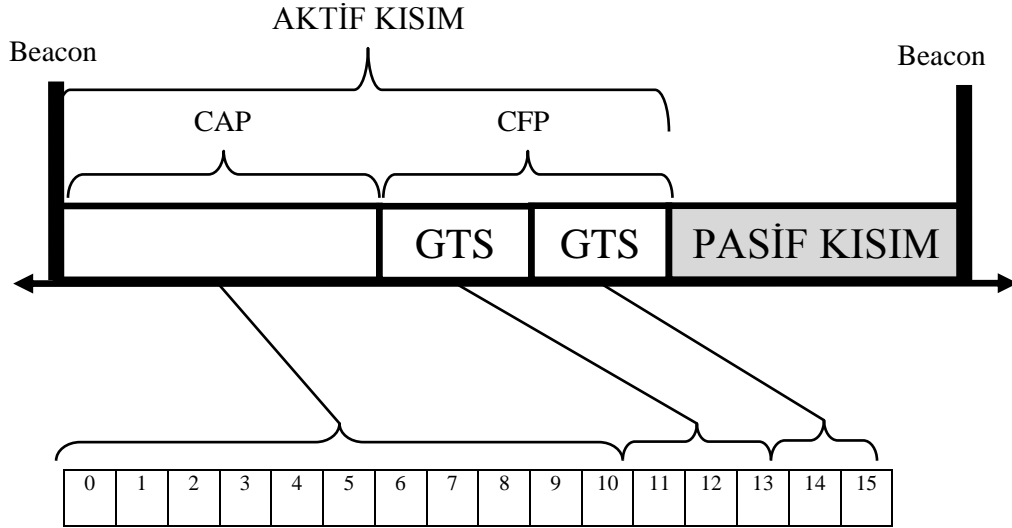
2.2.2. IEEE 802.15.4 MAC katmanı

MAC Katmanı kanal erişimi ve çerçeve iletiminin gerçekleştiği kısımdır. Beacon yönetimi, GTS yönetimi, çerçeve doğrulama, kabul mesajı gönderme, ağa düğüm eklenmesi ve çıkarılması gibi işlemler bu katmanda gerçekleştirilmektedir [1].

2.2.2.1. Süper çerçeve yapısı

Süper çerçeve yapısı LR-WPAN'larda isteğe bağlı olarak kullanılmaktadır. Süper çerçeve formatı ağ koordinatörü tarafından belirlenmektedir. Bu çerçeveler beacon'lar arasında ve 16 eşit slot halindedir. Süper çerçevenin ilk parçası beacon çerçevesidir. Koordinatör süper çerçeveyi yollamaktan vazgeçerse beacon iletimini kapatabilir. Beaconlar ağa ekli cihazları senkronize etmek, WPAN'ı ayırtırmak ve süper çerçeve yapısını belirlemek için kullanılmaktadır. Süper çerçeve yapısı kullanmadığı zaman koordinatör gerekli olmadıkça beacon göndermez tüm iletimler slotsuz CSMA-CA ile yapılır ve ek olarak GTS tahsisi yapılmaz. Şekil-1.5'de süper çerçeveler ve slot dağılımları gösterilmektedir.

Süper çerçeve'nin aktif ve pasif kısımları bulunabilmektedir. Pasif kısımda koordinatör kendi WPAN'ı ile etkileşimde olmamaktadır. Aktif kısım CAP ve CFP periyotlarını kapsamaktadır. CAP alanı, beacondan hemen sonra başlayan ve CFP alanına kadar olan alandır. CAP alanı veri iletimi için çekişmenin yapıldığı alandır. CAP içinde iletilen çerçeveler CSMA-CA mekanizması kullanarak kanalar erişmektedir. CFP alanı, CAP alanından sonra başlar ve pasif kısma kadardır. CFP alanı iletim için çekişmenin olmadığı alandır. Düşük gecikme gerektiren veya özel veri hızı gerektiren uygulamalarda koordinatör CFP alanının bir kısmını bu işlemler için ayırabilmektedir. Bu işlemler için ayrılan kısımlara GTS denir. GTS'ler süper çerçevenin aktif kısmının sonunda yer almaktadır. Yani CFP'nin sonunda yer işgal etmektedir [3,4].



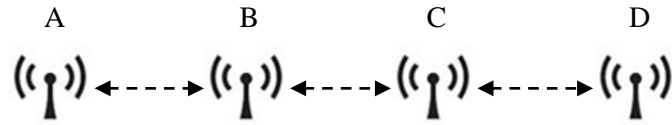
Şekil- 2.5: Süper çerçeve yapısı

2.2.2.2. Kanal erişimi

CSMA-CD, veri iletimi yoluna erişmek için kullanılan bir tekniktir. Veri iletim yoluna bağlı tüm birimlerin haberleşme ortamına erişimi bu teknikle sağlanmaktadır. Veri iletim yolu, bağlı olan tüm birimlerin veri aktarımına açıktır. Veri yoluna bağlı farklı birimler aynı anda iletme geçmek istediğinde veri aktarım yolunda çarpışma (collision) meydana gelmektedir. Çarpışma durumunda veriler bozulur ve yeniden aktarılması gerekir bu nedenle verici aktarım sonrası hattı dinlemektedir ve çarpışma durumunu algılamaktadır. Çarpışma, verici tarafından algılandıktan belli bir süre sonra hat kontrol edilir ve veri tekrar gönderilir. Bekleme süresi belli limitler içinde rasgeledir. İletişime geçecek herhangi iki birimin bekleme süresinin eşit olması düşük bir ihtimaldir. Eşit olsa dahi hat uzunluklarından kaynaklanan gecikmeler bu süreleri farklı kılmaktadır. Oluşan bu farklı süreler sayesinde çarpışma durumu çarpışma tekrar çarpışma yaşanmadan algılanmış olur. Bu mekanizmaya CSMA-CD denir. CSMA-CA ise CSMA-CD'nin aksine haberleşme ortamında çarpışmayı önleyerek erişim sağlayan mekanizmadır. CSMA-CD mekanizması LAN yapıları için uygun olmasına rağmen kablosuz yapılarda kullanışsızdır. Bu durumun üç sebebi vardır bunlar:

- Gizli istasyon problemi: herhangi iki kablosuz istasyonun birbirini göremedikleri için haberleşememesidir. Yani birbiriyle başka bir cihaz kullanarak haberleşmeleri durumudur.

- Uyarının hedef şaşırması problemi: Şekil-1.6'de görüldüğü gibi dört kablosuz cihazdan B cihazı A cihazına veri gönderdiğinde, B cihazının yaydığı sinyaller C cihazında gelecektir ve bir haberleşmenin olduğunu anlayacaktır böylece iletme geçmeyecektir. Fakat aynı sinyali D cihazı duyamadığı için B ve C cihazları arasındaki alanda çakışma durumudur.
- Yakın/uzak etkisiyle ilişkili olarak sinyal zayıflamasıyla sinyallerin iletilmemesi ve çakışmanın oluşması durumu.



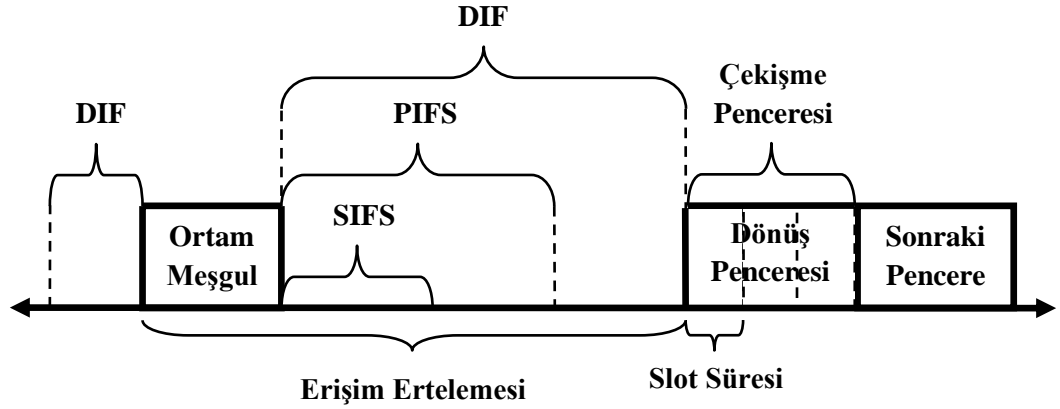
Şekil- 2.6: Uyarının hedef şaşırabileceği düğüm yerleşmi

CSMA-CA, sinyal zayıflamasıyla oluşan durum haricindeki iki durum için kullanılmaktadır. CSMA-CA, CS prosedürü ile iletim ortamının algılanması, çerçeveler arası boşluk zamanı, pozitif kabul, çakışma önleyici yaklaşım, geri çekilme ve çoklu erişim işlemlerini gerçekleştirmektedir.

Çerçeveler arası zaman boşlukları (IFS) veri iletim hızından bağımsızdır ve iletilen çerçeveler arasındaki bölgeleri temsil eder. IFS her fiziksel katman için sabittir. MAC protokolünün ortama erişebilmesi için çerçeveler arasındaki boşluk çok önemlidir çünkü çerçeveler arası boşluklar ortama erişimi belirleyen geri çekilme algoritmasındaki slot sürelerini etkilemektedir. Boşluk hesaplamada kullanılan slot süresi geri çekilme algoritmasında her zaman diliminde ortamın meşgul olup olmadığı kontrol eden süredir. Ortam erişimi için dört farklı IFS tanımlanmaktadır. Şekil-1.7'de bu IFS süreleri gösterilmektedir.

- En kısa çerçeveler arası boşluk (SIFS): Acil mesaj gönderiminde kullanılmaktadır. Ortam erişimini kazanan istasyon SIFS ile yüksek öncelikli olarak iletimi gerçekleştirmektedir.
- Nokta koordinasyonlu çerçeveler arası boşluk (PIFS): Koordinatör yönetiminde erişim mekanizmasıyla ortam erişimi kazanmak için kullanılmaktadır. SIFS ve slot süresi toplamına eşittir.

- Dağıtık koordinasyonlu çerçeveler arası boşluk (DIFS): ardışık veri paketleri arasındaki en az gecikmedir. Ortamın boş olduğundan kesinlikle emin olmak için istasyonlar boşluk süresince erişimlerini bekletmektedir. PIFS ve slot süresi toplamına eşittir.
- Genişletilmiş çerçeveler arası boşluk (EIFS): en uzun çerçeveler arası boşluktur. Hatalı ve gereğinden uzun süre bekletilmiş paketlerin iletiminde kullanılır. Geri çekilme algoritması çarpışmadan kaçınmak için iletimin bekletilmesinde kullanılan algoritmadır. Burada kullanılan üstel geri çekilme ise slot sayısı ve slot numarasına göre değişkenlik gösteren bir geri çekilme algoritmasıdır.



Şekil- 2.7: IFS süreleri

İletim ortamı dinleme işlemi, fiziksel katman dinleyicisi olan PCS prosedürü ile ve MAC Katmanı VCS prosedürüyle yerine getirilmektedir. PCS’de ortamdaki sinyallerin enerjilerini karşılaştırarak diğer istasyonların yüzdesini belirlenmektedir. VCS’de ise kablosuz ortamın kullanılmaya yakın olduğunu bildiren rezervasyon bilgisinin kullanıcılar arasında dağıtılmasına dayanmaktadır. VCS’de bu işlem için bir istek mesajı gönderilmekte ve bu mesaja karşılık bir boş mesaj gönderilerek kabul mesajı gönderilmiş olmaktadır [2,3].

2.2.2.3. Veri aktarım modeli

Koordinatörden son cihaza, son cihazdan koordinatöre ve son cihazlar arası olmak üzere üç farklı veri aktarım çeşidi bulunmaktadır. Her aktarım çeşidi beacon kullanan ve kullanmayan olmak üzere iki farklı aktarım gerçekleştirilmektedir.

Beacon kullanılmayan bir ağda cihazlar veri aktarımlarında slotsuz CSMA-CA kullanılmaktadır. Burada veri iletmek isteyen cihaz veriyi direk olarak göndermektedir

ve isteğe bağılı olarak alıcıdan bu mesaj için bir onay mesajı döndürülmektedir. Beacon kullanılmayan ağlarda koordinatör bir cihaza veri aktarmak istediğinde koordinatör doğru cihazın kendisiyle iletişime geçmesi ve veri istemesi için veriyi depolamaktadır. Cihaz koordinatörle iletişime geçmesi MAC komut çerçevesi yollayıp kendisi için bekleyen mesajları slotsuz CSMA-CA ile istemesi yoluyla olmaktadır. İstek gerçekleştikten sonra koordinatör kendisinde bekleyen veri olduğunu onaylamaktadır ve veriyi hedef cihaza göndermektedir. Veri iletimi gerçekleştikten sonra cihaz onay mesajı göndermekte ve mesajın koordinatörden silinmesiyle işlem tamamlanmaktadır.

Beacon kullanılan ağlarda cihaz ilk önce ağı beacon yakalamak için dinlemektedir. Beacon yakalandığında cihaz süper çerçeve yapısına senkronize olmaktadır. Süper çerçeve yapısında veri iletme zamanı geldiğinde veri cihaz veri çerçevesini slotlu CSMA-CA kullanarak iletmektedir. Beacon kullanan ağlarda bu uygulama koordinatör tarafından yönetilmektedir ve böylece enerji tasarrufu sağlanmaktadır. Koordinatör bir cihaza veri göndermek istediğinde ise beacon'da bekleyen mesaj olduğunu belirtmektedir. Periyodik olarak ağdaki beacon'ları dinleyen cihaz bu beacon'u aldığıında bir MAC komut çerçevesiyle veriyi slotlu CSMA-CA ile istemektedir. Bunun ardından koordinatör yine slotlu CSMA-CA ile veriyi göndermektedir. Cihazın onay mesajından sonra ise koordinatör mesajı bekleyenler arasında silmektedir [3].

2.2.2.4. GTS ve GTS dağıtma

GTS'ler kanalda belli band genişliğini ayırmak için kullanılmaktadır. Bu slot süreleri sadece koordinatör tarafından yönetilmektedir. Garantilenmiş süreli slot birden fazla süper çerçeve üzerine yayılabilir dolayısıyla tekrarlayan bir sistem olabilmektedir. Band genişliği ayırma mekanizması uzunluğu ve yönü belirtilerek istendiğinde koordinatör mesajı kabul eder ve durumu değerlendirir. Eğer iletim için yeterli yer varsa sonraki beaconun ardından bunu gönderir. GTS istek komutu ağa katılmış herhangi bir düğüm tarafından yeni bir GTS yerleştirmek veya var olan GTS'yi kaldırmak için kullanılmaktadır.

Bir cihazın GTS isteğinde bulunması için beacon izlemesi yapması gerekmektedir. GTS dağıtım işlemi ise ağ koordinatörü tarafından yapılmaktadır. İhtiyaca göre bir GTS yedi süper çerçeve slotuna kadar doldurabilmektedir. Dağıtım işlemi ilk gelene

ilk servis sağlanması şeklinde çalışmaktadır. İhtiyaç bittiğinde koordinatör düğüm için ayırdığı GTS'yi geri almaktadır [3].

2.2.2.5. MAC çerçeve yapısı

Tüm MAC çerçeveleri fiziksel katmanda PSDU'yu oluşturmaktadır. MAC Katmanındaki veri birimini ise Ağ katmanından sağlanmaktadır. IEEE 802.15.4 standardı çerçeveleri dört kategoriye ayırmaktadır. Bunlar Beacon, Veri, Kabul (ACK) ve Komut çerçeveleridir. Beacon çerçevesi aynı ağdaki aygıtların saatlerinin ayarlanarak senkronize çalışmaları için kullanılmaktadır. Veri çerçevesi veri göndermek için kullanılmaktadır. Kabul çerçevesi ise gönderilen verinin başarılı şekilde ulaştığını bildirmek için kullanılmaktadır. Komut çerçeveleri ise MAC komutlarını taşımak için kullanılmaktadır. MAC çerçevelerinin yapısı Şekil-1.8'de gösterilmektedir. MAC çerçevelerinde çerçeve kontrol alanı uzunluğu 16 bit, sıra numarası uzunluğu 8 bit ve çerçeve kontrol toplamı 16 bit uzunluğundadır ve bu alanların uzunlukları değişmemektedir. Adres alanı uzunluğu beacon çerçevesinde 32 den 80 bit'e kadar, veri ve MAC komut çerçevesinde 32 den 160 bit uzunluğuna kadar olabilmektedir.

2.3. ZigBee Standardı ve Özellikleri

IEEE 802.15.4 standardı tarafından alt katmanları tanımlanan ZigBee, düşük maliyetli, uzun pil ömrüne sahip ve yüksek veri aktarım oranı gerektirmeyen uygulamalar için tasarlanmıştır. ZigBee daha çok ev uygulamalarında dikkat çekmektedir. Ancak ucuzluğu, kullanım kolaylığı, uzun batarya ömrü sağlaması ve güvenli ağ özellikleri sebebiyle sanayi, askeri, sağlık, tarım ve robotik gibi alanlarda da kendine birçok kullanım alanı bulmuştur. ZigBee standartlarını tanımlama işlemini ZigBee Alliance yapmaktadır. ZigBee IEEE 802.15.4 standardının tanımladığı MAC katmanının üstünde yer alan Ağ ve Uygulama katmanlarını tanımlamaktadır [3].

Çerçeve kontrol alanı	Sıra Numarası	Adres Alanı	Süper Çerçeve Alanı	GTS Alanı	Bekleyen Erişim Alanı	Beacon Veri Yüğü	Çerçeve Kontrol Toplamı
-----------------------	---------------	-------------	---------------------	-----------	-----------------------	------------------	-------------------------

Beacon Çerçevesi

Çerçeve kontrol alanı	Sıra Numarası	Adres Alanı	Veri Yüğü	Çerçeve Kontrol Toplamı
-----------------------	---------------	-------------	-----------	-------------------------

Veri Çerçevesi

Çerçeve kontrol alanı	Sıra Numarası	Çerçeve Kontrol Toplamı
-----------------------	---------------	-------------------------

Onay Çerçevesi

Çerçeve kontrol alanı	Adres Alanı	Komut Tipi	Komut Verisi	Çerçeve Kontrol Toplamı
-----------------------	-------------	------------	--------------	-------------------------

MAC Komut çerçevesi

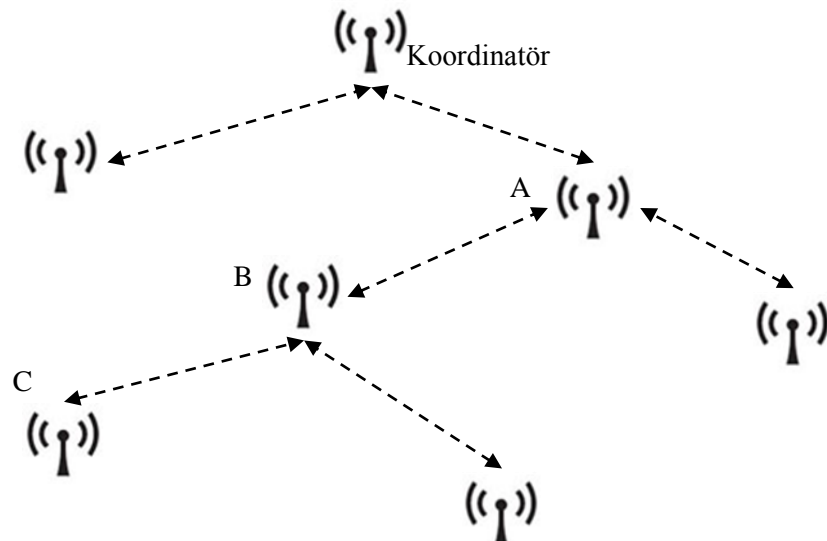
Şekil- 2.8:MAC katmanı çerçeveleri

2.3.1. Ağ topolojileri ve bileşenleri

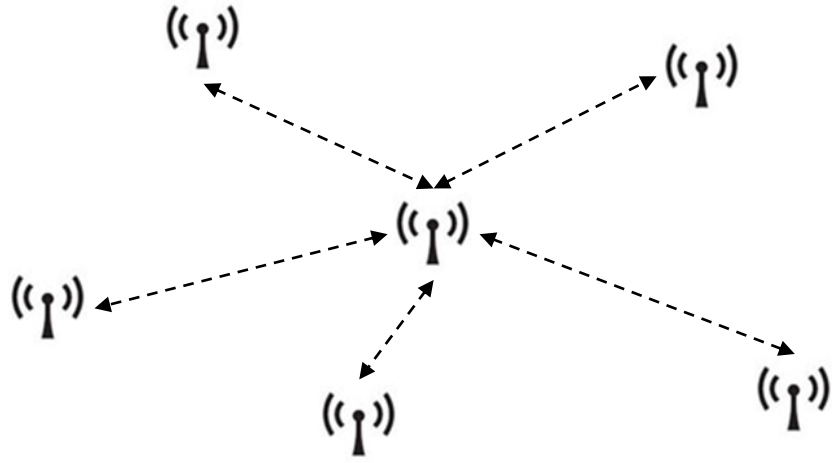
LR-WPAN'lar ilişkilerine, işlevlerine ve görevlerine göre farklı düğümler içermektedir. İlişkilerine göre cihazlar ebeveyn ve çocuk olmak üzere iki tiptir. Ebeveyn-çocuk ilişkisi düğümlerin ağda birbirlerini görmesi ve koordinatöre yakınlıklarına bağlıdır. Şekil-1.9'da gösterilen ve A düğümünün koordinatöre bağlantı açısından en yakın düğümdür. Bu ağda C düğümü A ve B düğümlerinin çocuğudur. B düğümü de A düğümünün çocuğudur. Benzer şekilde A düğümü B ve C düğümlerinin ebeveynidir. Ayrıca B düğümü de C düğümünün ebeveynidir. Düğümler görevlerine göre koordinatör, yönlendirici ve son cihaz olarak üçe ayrılmaktadır. Koordinatör bulunduğu PAN'ın yöneticisidir yani ağa düğüm katılması, ağ güvenliği, ağ parametreleri, düğüm listeleme gibi yönetsel işlemlerin yapıldığı düğümdür. Son cihazlar ağın uç kısımlarında bulunan ve sadece kendine gelen/giden alıp-vermekle ve bu bilgiyi işlemekle meşgul olan düğümlerdir. Yönlendiriciler ise birbiri ile iletişim kuramayan iki düğümün haberleşmesini sağlayan düğümlerdir. Yönlendiriciler, sensör düğümü işlevi de yapabilmektedir. Düğümler işlevlerine göre tam işlevli (FFD) ve kısıtlanmış/azaltılmış işlevli aygıt (RFD) olarak ikiye ayrılmaktadır. Tam işlevli cihaz tüm görevlerde çalışabilen ve hiç

bir işlevi kısıtlanmamış cihazdır. Burada bahsedilen kısıtlanmış işlevler, sensör düğümünün görevi gereği kullanmayacağı çeşitli ağ yönetim işlevleridir. Koordinatör ve yönlendirici olarak görevli aygıt mutlaka tam işlevli cihaz olmalıdır. Koordinatör olarak görev yapan aygıt kesinlikle uyku moduna geçirilmez. Bir başka deyişle ağda mutlaka uyanık bir tam işlevli cihaz bulunmaktadır. Böylece ağa katılmak isteyen ve ağ tarama işlemleri yapan cihazlar hataya düşmemektedir. Kısıtlanmış işlevli cihazlar ise ağ yönetim işlevleri kısıtlanmış cihazlardır. Kısıtlanmış işlevli cihazlar sadece tam işlevli cihazlarla haberleşebilmektedir. Bu cihazların işlevlerinin kısıtlanmasının sebebi güç tasarrufu sağlamaktır. Kısıtlanmış işlevli cihazlar sadece son aygıt olarak görev yapmaktadır [1,3].

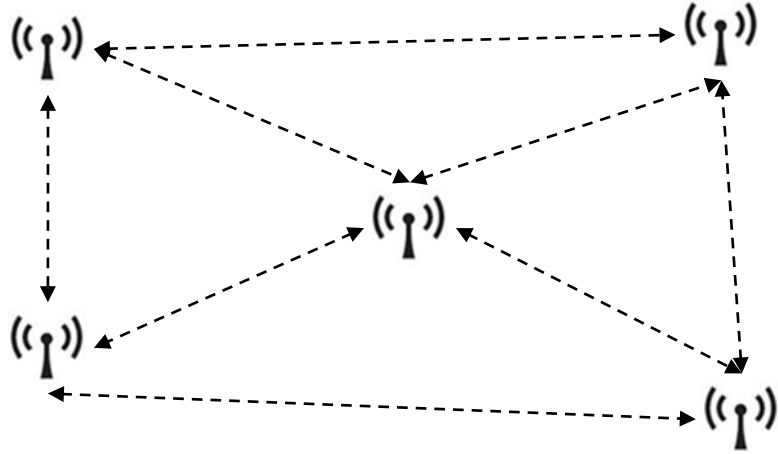
ZigBee ağ katmanı yıldız, saçaklı ağaç ve mesh ağ yapısını desteklemektedir. Yıldız ağ yapısında ağda Şekil-1.10'da görüldüğü gibi bir koordinatör ve etrafında son cihazlar barındırmaktadır. Mesh ve ağaç topolojilerinde bir koordinatör, yönlendiriciler ve son cihazlar bulunmaktadır. Yönlendiricilerin bulunduğu bu ağ yapılarında peer to peer haberleşebilir. Şekil-1.11'de gösterilen mesh ve Şekil-1.12'de gösterilen ağaç topolojilerinin birbirinde farkı ise ağdan bir cihaz ayrıldığında mesh ağlar kendilerini düzeltebilirken ağaç topolojilerde böyle bir durum söz konusu değildir. Yani ağaç topolojisinden bir yönlendirici kaldırıldığında ağın o yönlendiriciye bağlı düğümleri yetim kalır ve iletişimleri kopar. Ancak mesh ağlarda bir yönlendirici kaldırıldığında o yönlendiricinin çocuğu durumunda bulunan düğümler başka bir ebeveyn arar. Arama sonucu yeni ebeveyn bulunursa bu ebeveyn yetim düğümleri kabul eder ve ağ tamir edilmiş olur [3].



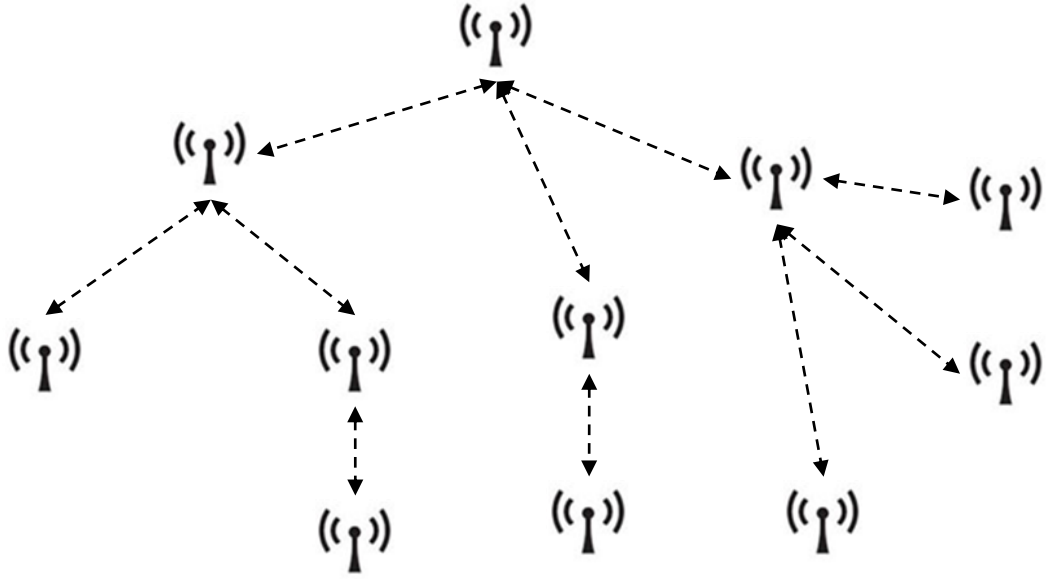
Şekil- 2.9: Kablosuz sensör ağlarında çocuk-ebeveyn ilişkisi



Şekil- 2.10: Yıldız ağ topolojisi



Şekil- 2.11: Mesh ağ topoloji



Şekil- 2.12: Ağaç ağ topolojisi

2.3.2. Ağ katmanı

Ağ Katmanı, Uygulama Katmanından gelen verileri IEEE 802.15.4 MAC Katmanına uygun bir şekilde aktarmakla yükümlü arayüz işlevi gören katmandır. Ağ katmanının temel görevleri ağ güvenliği, düğüm adresleme, mesaj yönlendirme, servis keşfi ve bağlantı işlemleridir.

Güvenlik servisi, bağlantı esnasında kimlik doğrulaması ve veri şifreleme işlemleridir. Şifreleme için AES-128 kullanılmaktadır. Veri şifreleme ağ ve aygıt seviyesinde sağlanabilmektedir. Ağ seviyesinde şifreleme yapıldığında ağda ortak şifreleme anahtarı bulundurulurken cihazlarda zaten az olan hafıza kapasitesinden tasarruf sağlanmaktadır. Aygıt seviyesinde şifrelemede ise iki aygıt arasında ortak bağlantı anahtarı kullanılmaktadır.

Adresleme bu ağlarda iki türdür. İlki 16 bitlik kullanıcı tarafından değiştirilebilen kısa adreslemedir. Bu adresleme kullanıldığında aynı WPAN'da aynı kısa adresli iki düğüm bulunmamasına dikkat edilmelidir. İkincisi ise 64 bit uzunluğundaki eşsiz adrestir. Üretici tarafından atanan bu eşsiz adrese uzun adres denmektedir. Uzun adresleme her ağ ve her düğümde sorunsuzca kullanılmaktadır.

Yönlendirme, ağın yapısı ve komşuluklara bakılarak oluşturulan yönlendirme tabloları sayesinde ağda birbirini doğrudan göremeyen cihazlar haberleşebilmektedir. Ağa yeni cihaz katıldığı veya ayrıldığı anlaşıldığında yönlendirme tabloları keşif

yapılarak düzenlenmektedir. Mesaj yönlendirme işlemleri sadece FFD cihazlar tarafından yapılabilmektedir.

Servis keşif görevi ilk olarak düğümleri keşfetmek içindir. Bunun için unicast mesajlarla koordinatör veya yönlendirici görevindeki düğüme adresi sorulur. Bu adres sorgusu sonucu ağa kayıtlı adresler elde edilmektedir. Bunun yanında broadcast mesajıyla koordinatör veya yönlendirici adresi sorulmaktadır.

Bağlantı işlemi ağa katılmak isteyen düğümün istekte bulunmasıyla başlamaktadır. İsteği alan koordinatör, ağda güvenlik parametreleri tanımlanmış ise ilk önce düğümün güvenlik parametrelerini ve PAN-ID'sini kontrol eder. Bu parametreler uygunsa düğüm ağa kabul edilmektedir. Eğer düğüme kullanıcı tarafından bir adres tanımlanmışsa bu adres, aksi halde koordinatörün vereceği adres düğüme atanmaktadır. Adres ve kabul bilgisi mesajla düğüme iletilmektedir. Ağa katılım işlemi yönlendirme tablosuna düğümün kaydedilmesiyle tamamlanmaktadır [1,3,4].

2.3.3. Uygulama katmanı

Uygulama Katmanı ağ katmanının üzerinde yer alan ve kullanıcıya en yakın katmandır. Bu katman paket filtreleme, uçtan uca tekrar ve kabul mesajı gönderme, bağlantı tablosu düzenleme, grup tablo düzenleme ve adres dönüştürme gibi işlemleri yerine getirmektedir.

Filtreleme işlemi, uygulama katmanının ağda olmayan düğümlerden gelen, PAN-ID'si uyuşmayan veya tekrarlardan doğan fazladan kopya paketleri süzüp atması işlemidir. Verici tarafından kabul istenirse paketin düzgün iletilip iletilmediğini bildirmek için otomatik olarak kabul mesajı Uygulama Katmanı tarafından gönderilir. Eğer kabul mesajı ulaşmazsa mesaj tekrarı gerçekleştirilir. Uygulama katmanı çeşitli tablo düzenleme işlemlerini yerine getirmektedir. Bağlantı tablosu bir cihazın diğerine veya diğerlerine olan bağlantısını göstermektedir. Grup tablosu, rasgele dağılmış düğüm kümelerindeki grupların toplamını barındıran tablodur. Adres dönüştürme 64 bitlik uzun adres yapısını 16 bit'lik kısa adres yapısına çevirme veya tersini yapma işlemidir [1,3].

2.4. XMPP ve Özellikleri

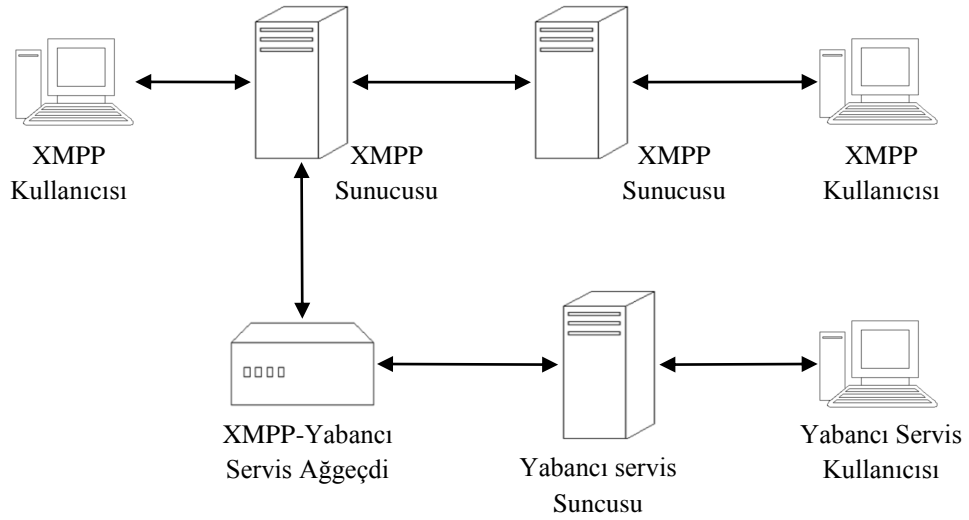
Türkçe olarak genişletilebilir mesajlaşma ve durum protokolü anlamına gelmekte olan XMPP, anlık mesajlaşma durum bilgisi, çoklu sohbet, ses ve görüntü aktarımı, içerik yayınlama için kullanılan küçük yazılımlı teknolojiler bütünüdür. XMPP ücretsiz, açık, genel ve kolay anlaşılabilir. Ek olarak birçok kullanıcı, sunucu, sunucu bileşeni ve kod kütüphanesi desteği bulunmaktadır. XMPP, IETF anlık mesajlaşma ve durum teknolojisi olarak resmen onaylamıştır. 2004 yılında XMPP özellikleri RFC 3920 ve RFC 3921 olarak yayınlanmış ve XMPP Standart Vakfı tarafından birçok yeni standart serisi yayınlanmaktadır. XMPP eski adıyla Jabber ilk olarak 1998 yılında Jeremie Miller tarafından geliştirilmiştir. Günümüzde çok kararlı halde olan bu teknoloji üzerinde yüzlerce geliştirici halen çalışmaktadır. XMPP sunucusu kullanan binlerce servis arasında Google Talk gibi büyük servisler de bulunmaktadır.

XMPP mimarisi e-mail'e benzemektedir. Dolayısıyla herhangi bir kişi kendi XMPP sunucusunu kurup istediği şekilde işletebilmektedir. XMPP sunucuları genel ağlardan yalıtılabilmektedir. XMPP çekirdeğinde SASL ve TLS olduğu için güçlü bir güvenliğe sahiptir. Ayrıca XMPP ağı spamsızdır ve veri şifreleme kullanılmaktadır. Açık kaynak oluşundan dolayı kullanıcılar kendi XML kodlarını yazarak istedikleri uygulamayı XMPP'ye ekleyebilmektedir. XMPP uygulamaları sohbetin dışında ağ yönetimi, içerik paylaşımı, dosya paylaşımı, oyun, uzaktan izleme, bulut hesaplaması gibi uygulamalara izin vermektedir. XMPP teknolojisini kullanan geniş bir proje geliştiricisi ve şirket yelpazesi bulunmaktadır.

XMPP belli bir ağ mimarisine sabitlenmemiştir. Genelde kullanıcı-sunucu mimarisine uygulanmaktadır. XMPP servisine ulaşmak isteyen kullanıcı TCP/IP bağlantısıyla XMPP sunucusuna erişmektedir. Sunucuya erişen kullanıcı yine TCP/IP ile diğer kullanıcılarla iletişim kurabilmektedir. Şekil-1.13'de XMPP ağ mimarisi gösterilmektedir. Şekilde görüldüğü üzere ağda birden fazla XMPP sunucusu çalışabilmekte ve XMPP'den farklı yabancı servis protokolleri XMPP servisine bir ağ geçidi aracılığıyla bağlanabilmektedir.

XMPP sunucularının XMPP haberleşmesi yaptığı için başlıca işler bağlantı-oturum yönetme ve XML akımlarıyla veriyi doğru adrese göndermedir. Bunların haricinde XMPP sunucusu isteğe bağlı olarak veri depolama işlemleri de gerçekleştirilmektedir.

XMPP sunucularını diğer mesajlaşma protokolleriyle ilişkilendirmek için ağ geçitleri kullanılmaktadır. SMTP, ICQ, SIMPLE ve MSN Messenger kullanımda olan ağ geçitlerinden bazılarıdır. XMPP sunucuları buldukları ağ adresine göre ayrılmaktadır. Pratikte sunucu-sunucu haberleşmesi, kullanıcı-sunucu haberleşmesinin basit bir uzantısıdır. Bu şekilde XMPP servis ağları bir sunucu ağı şeklindedir. Böylece iki farklı XMPP servis sağlayıcısına üye olan kullanıcılar birbiriyle kolayca haberleşebilmektedir. Bu durum seçime bağlı olarak sınırlandırılabilir veya kaldırılabilir. Sunucuların birbiriyle haberleşmesi için 5269 nolu port kullanılmaktadır.



Şekil- 2.13: XMPP ağ mimarisi

Kullanıcılar XMPP servisine TCP/IP ile direk olarak bağlanabilmektedir. Birden çok kullanıcı servise aynı anda bağlanabilmektedir dolayısıyla kullanıcılar birbirinden kullanıcı ayraçları olan JID ile ayrılmaktadırlar. Genellikle kullanıcılar için XMPP servis portu 5222 olarak kullanılmaktadır.

XMPP servis veri akımlarının dinlenmesi ve kurcalanmasını önlemek amacıyla TLS protokolü kullanılmaktadır. TLS, TCP/IP taşıma katmanı seviyesinde simetrik şifreleme ve mesaj doğrulama gerçekleştirmektedir. XMPP, kimlik doğrulama için SASL protokolünü kullanmaktadır. SASL, bağlantı tabanlı protokollere kimlik doğrulama desteği sağlayan bir sistemdir [5,6].

3. AĞLAR ARASI HABERLEŞME

Ağlar arası haberleşme, ağ geçidi cihaz veya cihazları kullanarak çeşitli yöntemler ile farklı standartlarda çalışan yerel ağlardan geniş alan ağı oluşturmaktır. Ağ standartlarından kaynaklanan farklar ağ geçitleri tarafından çözülmektedir. Ağ geçitleri iki ağ arasında arayüz görevi yapan ve OSI modeline göre farklı katmanlarda çalışabilen ağ cihazlarıdır. Ağ geçitleri içinde ihtiyaca göre protokol tercümanı, empedans eşleyici, oran çevirici, hata önleyici veya sinyal çevirici gibi birimler bulundurabilmektedir.

Tüm ağlar arası haberleşme sistemleri gecikme toleranslı uygulamalarda kullanılabilir. Bu durumun sebebi ağlar arası haberleşmede araya giren eleman sayısı arttıkça ağın büyümesi ve yavaşlamasıdır. Sunucu tabanlı ağlar arası haberleşme sistemlerinde ağın yavaşlamasına, ağ geçitleri sebep olmaktadır. Ağ geçitleri üzerinde gerçekleştirilen ağ uyumlandırma işlemleri veri aktarımında gecikmelere sebep olmaktadır.

3.1. IEEE 802.15.4/ZigBee ile TCP/IP Ağları Arasındaki Farklar ve Ağlar Arası Haberleşmede Karşılaşılan Sorunlar

Çerçeve büyüklüğü, veri parçalama-birleştirme, veri aktarım oranı, LR-WPAN tasarım kısıtlamaları, adresleme, servis keşfi ve güvenlik işlemleri TCP/IP ve LR-WPAN ağları arasında haberleşmede karşılaşılan başlıca sorunlardır. TCP/IP ve LR-WPAN ağları arasındaki en belirgin problem LR-WPAN ağların TCP/IP ağların en büyük paket uzunluğunu karşılayamamasıdır. LR-WPAN Fiziksel veri birimi 133 byte uzunluğundadır ancak bundan 6 byte başlangıç kısmı atıldığında en büyük paket 127 byte olmaktadır. Bu 127 byte'lık paketten 25 byte uzunluğundaki çerçeve kontrol, sıra numarası, adresleme ve FCS kısımları çıkarıldıktan sonra geriye 102 byte kalmaktadır. Bunun haricinde pakete güvenlik için 21 byte uzunluğundaki AES-128 eklendi ise geriye sadece 81 byte'lık yer kalmaktadır. Bu durumda IPv4'ün 576 byte ve IPv6'nın 1280 byte uzunluğundaki MTU büyüklüklerine göre çok yetersiz kaldığı görülmektedir [7,8].

IEEE 802.15.4 paketleri ve IP paketleri arasında büyük fark bulunması ve uygulamaların fiziksel hattın kısıtlamalarını bilmemesi sebebiyle paketleme ve parçalama işlemleri önem taşımaktadır. Paketleme ve parçalama işlemi esnasında eklenen başlıklar ağa göre farklılıklar göstermektedir. Parçaların uygun şekilde

parçalanıp birleştirilmesi IP tabanlı haberleşme kullanan cihazlarda donanım ve performans kısıtlaması olmaması sebebiyle bu cihazlarda büyük bir sorun değildir. Ancak parçalama ve birleştirme işlemleri LR-WPAN cihazları için yüksek işlem gücü gerektirmektedir. Düğüm üzerinde kullanılacak paket parçalama birleştirme algoritmalarının uzun oluşu sebebiyle cihazlar normalden fazla güç harcamakta ve düğümlerin tasarım hedeflerinden uzaklaşmaktadır. Ayrıca LR-WPAN cihazların enerji tasarrufu için uyku moduna geçmesi ağlar arası haberleşmeyi veri kayıplarına sebep olarak sekteye uğratabilmektedir.

LR-WPAN'larda uzun ve kısa adresleme olmak üzere iki adresleme kullanılmaktadır. TCP/IP ağlarda 32 bitlik IPv4 veya 128 bitlik IPv6 adres kullanılmaktadır. IPv4 adreslemesinin yetersiz kaldığı günümüzde IPv6 adreslemesi TCP/IP adreslemesinde hedef alınmaktadır. Şu anki LR-WPAN adreslemesi IPv4 için yeterlidir. Fakat LR-WPAN'larda yüksek sayıda düğüm olduğunda düşünüldüğünde zaten geçilmesi planlanan IPv6 için LR-WPAN adreslemesi yetersiz kalmaktadır.

Kablosuz teknolojilerde en büyük sorunlardan biri güvenlik olduğu için ağlar arası haberleşmede kullanılacak teknik önem taşımaktadır. Uygulanacak teknik kablosuz teknolojilere yapılan tipik man-in-the-middle ve servis engelleme saldırılarına engel olmalıdır. Özellikle TCP/IP tabanlı ağların Mbps seviyesindeki yüksek veri aktarım oranını kullanarak kbps seviyesindeki daha düşük veri oranlı LR-WPAN düğümlerinin küçük veri oranlarının şişirilmesi ve uyku modunda depolanan mesajların silinmesi yoluyla yapılan saldırılar önem teşkil etmektedir. TCP/IP ağlarında yapılan XML tabanlı SOAP gibi servis keşif işlemleri LR-WPAN için çok ağırdır ve uygun değildir. LR-WPAN'larda basit servis keşif işlemleri yapılmaktadır [7–10].

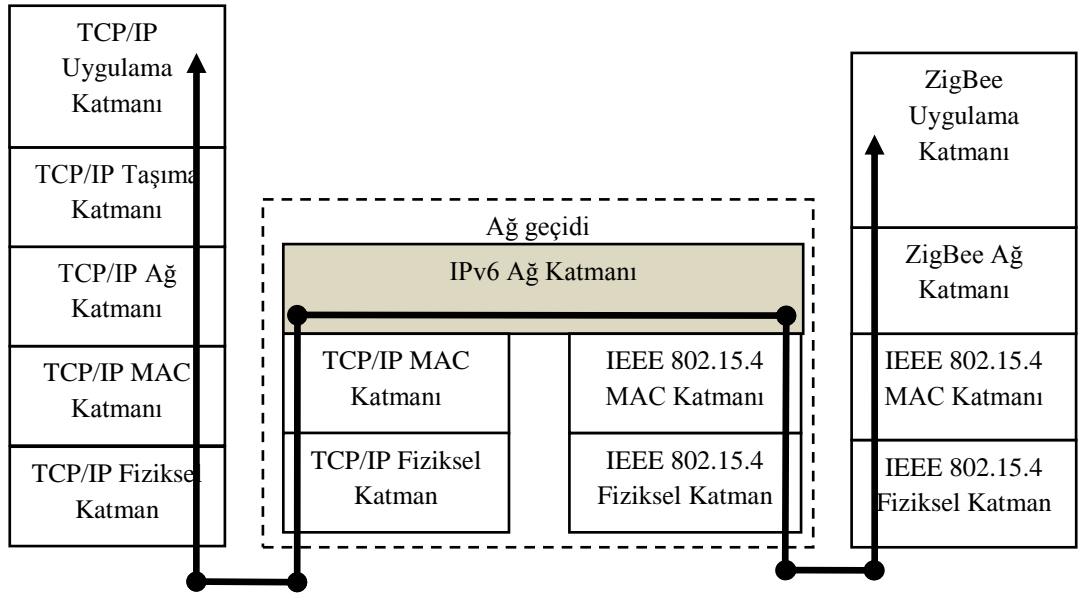
3.2. Ağlar Arası Haberleşme Yöntemleri

Ağlar arası haberleşme ağ geçitleri kullanılarak yapılmaktadır. Ağ geçitlerinde, ağlar arası haberleşme sorunlarını aşmak için IEEE 802.15.4 veya ZigBee standartlarının üzerine uyumlandırma olmak üzere iki ana yöntem kullanılmaktadır. Burada dikkat edilmesi gereken ZigBee ve IEEE 802.15.4'ün birbiriyle çalışabilen fakat birbiriyle tamamen farklı standartlar oluşudur. IEEE 802.15.4 daha çok fiziksel ortamla ilgili işlemlerle ilgilenirken ZigBee daha çok ağ yapılandırması ve yönetimi üzerinedir.

Uyumlandırma işlemlerinin hangi standart veya hangi katmandan sonra yapıldığı bu standartların farklı oluşu sebebiyle önemlidir.

3.2.1. IEEE 802.15.4 standart yığını üzerinden ağlar arası haberleşme

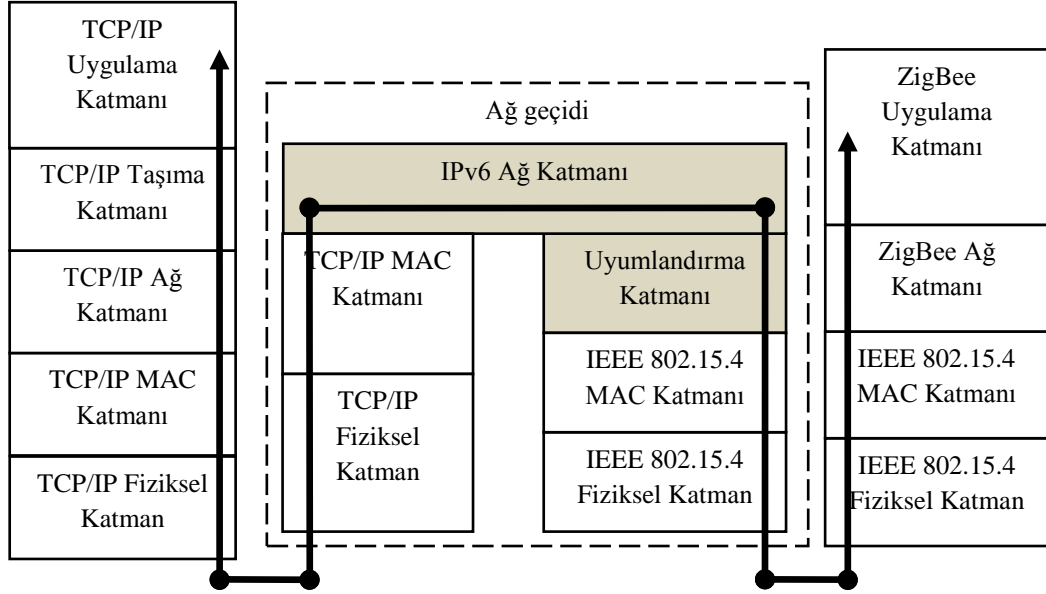
IEEE 802.15.4 standardının üzerine TCP/IP yığınının yerleştirildiği ağ geçitlerinde veri Şekil-2.1'deki yolu izlemektedir. Şekilde görüldüğü üzere ağ geçidinde ZigBee ile tanımlanmış katmanlara girilmeyip direk TCP/IP uyumlandırma katmanına geçilmektedir. Bu şekilde çalışan en bilindik teknoloji 6LoWPAN'dır. Şekil-2.2'de 6LoWPAN yığını gösterilmektedir. 6LoWPAN, IETF tarafından oluşturulmuştur. 6LoWPAN'da yapılan işlem temelde IEEE 802.15.4 MAC katmanıyla IPv6 ağ katmanı arasında bir uyumlandırma katmanı yerleştirmektir. 6LoWPAN için kullanılan ağ geçidi hem IEEE 802.15.4 MAC hem de TCP/IP Ağ Katmanı ile çalıştığı için çok katmanlıdır. Benzer şekilde iki ağa da bakan yüzleri olduğu için çok arayüzlüdür.



Şekil- 3.1: IEEE 802.15.4 yığını üzerine TCP/IP yığını yerleştirilmesi

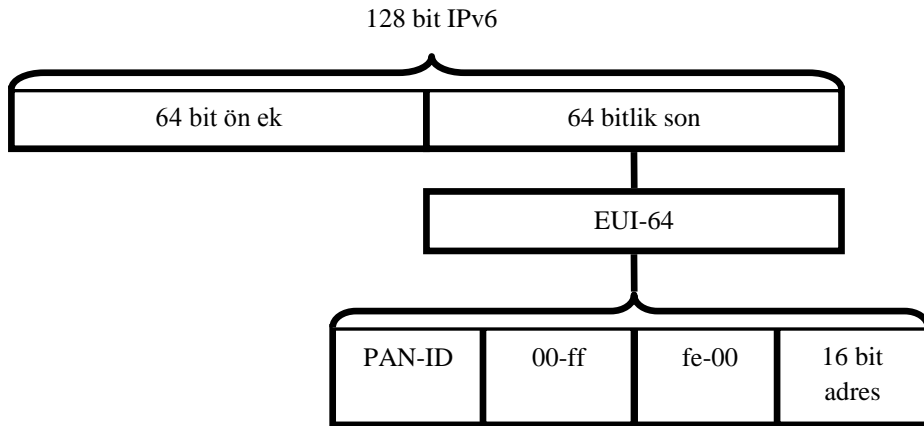
6LoWPAN'larda paket büyüklüğü problemini önlemek için paket sıkıştırma uygulanmaktadır. Paket sıkıştırma için paketlere sıkıştırma başlığı eklenip sabit veya elenebilir alanların neresi olduğu belirtilir. Örneğin TCP/IP tarafından gelen versiyon alanları genelde sabit alanlardır. Hedef ve kaynak adresleri 128 bit IPv6 yerine 64 bit MAC adresinden türetilerek düzenlenebilmektedir. Paket uzunluğu Fiziksel Katman veri biriminden türetilenmektedir. Trafik sınıfı ve akış etiketlerine ihtiyaç yoksa

bunlarda sabit düşünölebilmektedir. Sıkıştırma işlemlerinin belirtildiđi başlık uygulamalara göre deđişiklik gösterebilmektedir.



Şekil- 3.2: 6LoWPAN ağ geçidi

IEEE 802.15.4 düğümlerini IPv6 için adresleme işlemlerinde IEEE 802.15.4 tarafındaki düğümlerde eđer 64 bitlik uzun adres kullanılıyorsa bu adres direk olarak EUI-64 ayracı olarak kullanılmaktadır. 16 bitlik kısa adresleme kullanıldığında ise Şekil-2.3'de gösterildiđi gibi yüksek kısma PAN-ID eklenir sonra 32 bit uzunluğunda 00-FF-FE-00 serisi son olarak 16 bitlik kısa adres ile EUI-64 oluşturulmaktadır.



Şekil- 3.3: IPv6 ve EUI-64

6LoWPAN ile servis keşfi IPv6 servis keşfi kullanılarak yapılmaktadır. Bu durumda mekanizmaların multicast desteği vermesi beklenmektedir. Ancak IEEE 802.15.4 cihazları multicast desteği verememektedir. Buradaki problemin aşılması için IEEE 802.15.4 MAC katmanının broadcast özelliğinden faydalanılmaktadır.

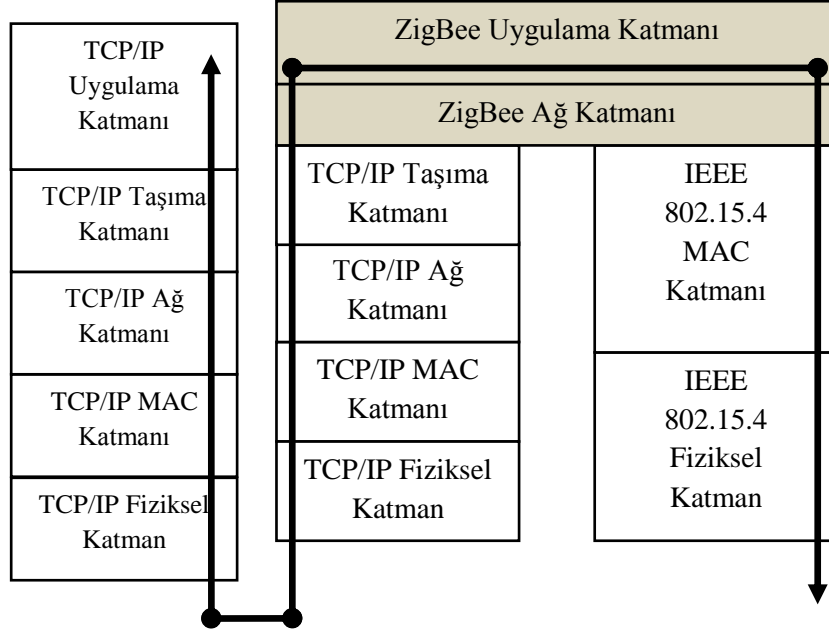
6LoWPAN'larda mesh düğümler üzerinden yönlendirme sağlanabilmektedir. Mesh ağlarda veri yönlendirilirken her düğümdeki yönlendirme tablolarına bakarak bir düğümden diğerine birçok atlama yaparak iletilmektedir. Yönlendirme tabloları sonraki düğümün hangisi olacağına karar verdiği için 6LoWPAN verilerini yönlendirmede ek başlığa gerek yoktur.

6LoWPAN'lar kullanılırken ZigBee tamamen bir kenara bırakıldığı için özellikle paket sıkıştırması yüzünden 6LoWPAN ve ZigBee düğümleri birlikte çalışmamaktadır. Servis keşfi ZigBee'de ağ katmanında gerçekleştirilirken 6LoWPAN'da IEEE 802.15.4 MAC katmanında gerçekleşmektedir. Ek olarak servis keşfi için broadcast mesajlarının kullanılması hem band genişliği hem de güç ihtiyaçlarını arttırmaktadır. Ayrıca her cihazın yüksek paket sıkıştırma algoritmasını çözebilmesi için işlevsel olması gerekmektedir dolayısıyla ZigBee'deki işlevsel görevler 6LoWPAN'da yoktur [7–9].

3.2.2. ZigBee standart yığını üzerinden ağlar arası haberleşme

ZigBee yığını kullanan temel iki yöntem bulunmaktadır ilki ZigBee yığını genişletip ZigBee'nin temel özellikleri bozmadan ağlar arası haberleşmeyi sağlama diğeri ise ZigBee yığının en üst katmanı olan uygulama katmanından sonra uyumlandırma katmanı eklemektir.

ZigBee Alliance, IETF'nin 6LoWPAN'ına alternatif olarak bir ZigBee genişletme aygıtı geliştirmektedir. Bu aygıtın mimarisi Şekil-2.4'de gösterilmektedir. Bu genişletme aygıtı ZigBee'ye ait olan yönlendirme ve ağ katmanlarını TCP/IP katmanlarının üzerine genişleterek ağlar arası haberleşmeyi sağlamayı amaçlamaktadır. Böylece hem ZigBee hem de TCP/IP yığınları birlikte enkapsüle olarak çalışmaktadır [7,9,10].

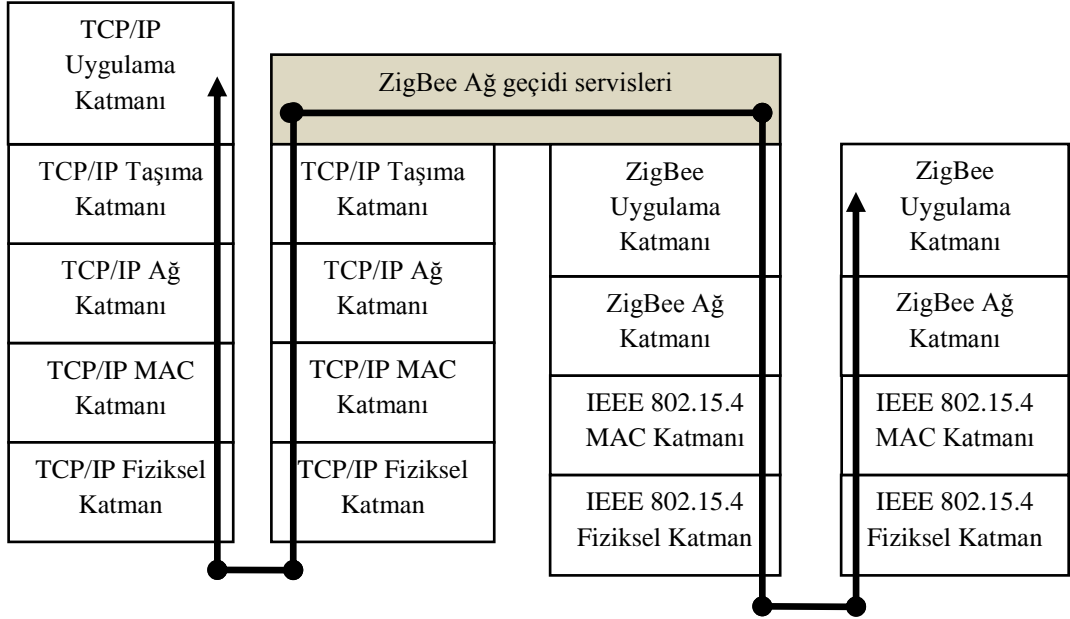


Şekil- 3.4: ZigBee yığınının genişletilerek TCP/IP yığına erişim

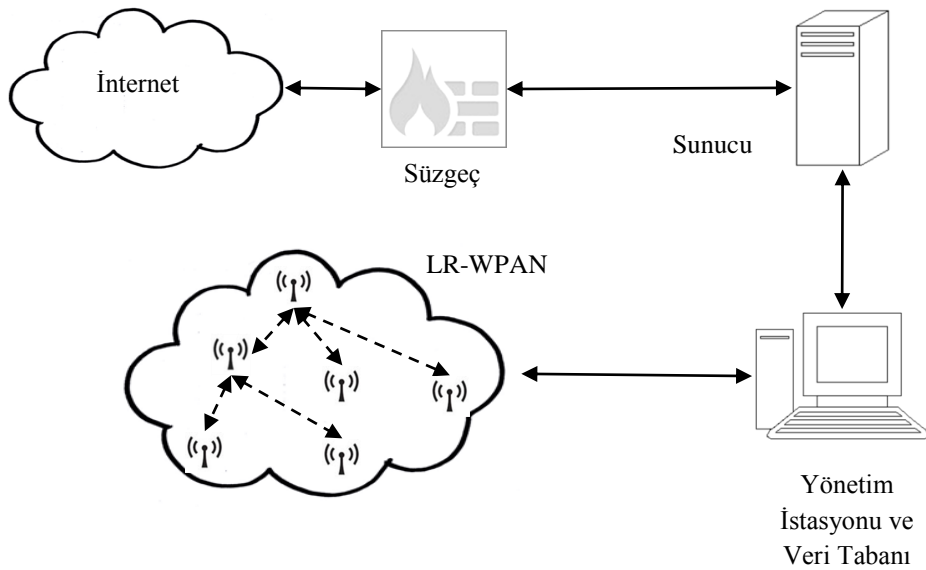
Şekil-2.5’de ZigBee yığını üzerinden ağlar arası haberleşmede verinin izlediği yol gösterilmektedir. Şekilde de görüldüğü üzere veri ilk önce IEEE 802.15.4 yığındaki katmanlardan geçmekte daha sonra ZigBee yığınının tepesine kadar çıkmakta ve daha sonra uyumlandırma katmanına girmekte ve buradan TCP/IP yığına geçmektedir. ZigBee yığının üzerine yerleştirilen uyumlandırma katmanı ZigBee karakteristiklerini koruyarak haberleşmeyi amaçlamaktadır. Tüm paket dönüşümleri, adresleme, yönlendirme, servis keşfi vb. İşlemler uyumlandırma katmanında gerçekleştirilmektedir. ZigBee yığının üzerine uyumlandırma katmanı yerleştirilerek ağlar arası haberleşmede en çok tercih edilen teknik sunucu-ağ geçidi tekniğidir.

Sunucu tabanlı yöntemlerde sistem yönetim ve sensör ağı olmak üzere iki ağdan meydana gelmektedir. Şekil-2.6’de sunucu tabanlı sistem mimarisi gösterilmektedir. Yönetim ağı sunucu, süzgeç, veri tabanı ve yönetim istasyonundan oluşmaktadır. Kablosuz sensör ağı yönetimi, yönetim ağı yapılandırması, internet erişim şifreleri ve verileri kontrolü bu ağda yapılmaktadır. Sensör ağı ağ geçidi ve sensör ağı düğümlerinden oluşmaktadır. Süzgeç farklı süzme yöntemleri ile ağın gelen giden veri trafiğini kontrol altında tutar. IP süzme, port süzme, içerik süzme yaptığı işlemlerden bazılarıdır. Veri tabanı ZigBee ağında veri kaybı yaşanmaması ve istenen verilerin depolanması için kullanılmaktadır. Yönetim istasyonu yönetim ağını yapılandırmak, verileri okumak, adresleme ve paket dönüşümü için kullanılmaktadır. Sunucu ağdan alınan verileri internetteki kullanıcılara sunmak ve kullanıcılardan

gelen verileri yönetim istasyonuna iletmekle yükümlüdür. Sensör ağı yönetim ağına ağ geçidiyle bağlıdır. Ağ geçidi sensör ağının yapılandırma ve iki ağ arasında veri transferini sağlamaktadır. Şekil-2.6'de görüldüğü üzere sensör ağına bağlanmak isteyen kullanıcı önce süzgeç ile karşılaşır ve erişim yetkisi var mı bakılmaktadır. Sonra yönetim ağına erişim sağlanmaktadır. Buradan sunucuya bağlanılmakta ve kablosuz sensör ağına erişilmektedir [7,8,9,11].



Şekil- 3.5: ZigBee yığını üzerine TCP/IP yığını yerleştirilmesi



Şekil- 3.6: Sunucu tabanlı sistem

4. AĞLAR ARASI HABERLEŞME SİSTEMİ

Ağlar arası haberleşme sistemi için ZigBee'nin karakteristik özelliklerini korumak amacıyla sunucu tabanlı bir sistem tercih edilmektedir. Sistemde kullanacağımız sunucu tabanlı sistemin genel yapısı Şekil-3.1'de gösterilmektedir. Sistem üç ana kısımdan oluşmaktadır bunlar XMPP sunucusu ve ağ geçidi ve LR-WPAN'dır.

Sistem daha önce anlatılan sunucu tabanlı sistemlerle temelde aynı olmasına karşın şekilde de görüldüğü üzere küçük farklar içermektedir. Öncelikle sistemde sunucu olarak klasik web sunucusu yerine anlık mesajlaşma sunucusu kullanılmaktadır. Bunun sebebi sunucu tabanlı yöntemlerde web sunucusu yerine başka teknolojilerin kullanılabilirliğine bakmaktır. Sistemde kullanılan sunucu ve ağ geçitleri internete farklı noktalardan bağlanabildikleri gibi aynı noktadan da bağlanabilmektedir. Mesajlaşma, internet tarafındaki güvenlik, kullanıcı hesapları ve veri depolama işlemleri XMPP sunucusunda gerçekleştirilmektedir. Anlık mesajlaşma sunucu olarak XMPP sunucusunun tercih edilmesinin temel nedenlerini şöyle sıralayabiliriz:

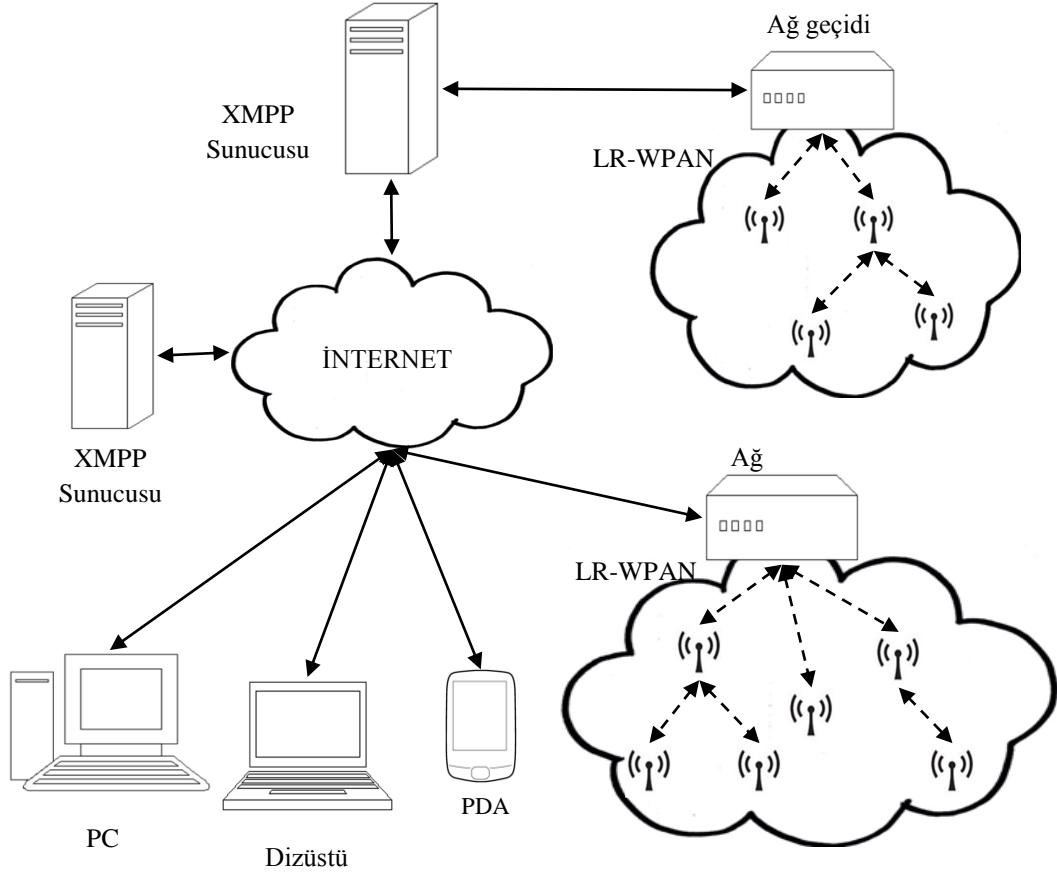
- Birçok XMPP servis sağlayıcısının var olması sebebiyle sunucu barındırma, bakım, yönetim ve güvenlik işlemlerini büyük servis sağlayıcılarına bırakılabilmektedir.
- İstenildiği takdirde, gerekli XMPP servis sunucusunun açık kaynaklı sistemler kolayca kurularak sistem oluşturulabilmektedir.
- XMPP sunucularına kullanıcı erişimi bir web sayfasından veya basit bir XMPP kullanıcı yazılımıyla zahmetsizce yapılabilmektedir
- İsteğe bağlı olarak kurulacak olan XMPP sunucusuna kullanıcı hesaplarının LDAP ile kolayca aktarılabilmesi, mesajların süzülüp, saklanabilmesi.
- Çevrim dışı olan kullanıcılara mesajların çevrim içi oldukları anda veriler gönderilebilmektedir.
- XMPP, gerek duyulduğu takdirde anlık mesajlaşma işlevine ek olarak görüntü, ses ve dosya transferi de sağlayabilmektedir.
- Her programlama dili için birçok XMPP Kütüphanesi bulunması sayesinde istenilen platformda istenilen işlevde program yazılabilmektedir.

- Birçok XMPP servis sağlayıcısı bulunmaktadır. Ayrıca XMPP servisini isteyen istediği şekilde yapılandırarak kullanabilmektedir.
- İnternet tarafındaki güvenlik işlemlerini üstlenmektedir. Taşıma Katmanı güvenliği sağlamaktadır. Spam koruması sağlamaktadır.
- XMPP'nin XML kodlarıyla oynanarak genişletilebilmektedir.
- Tek XMPP sunucusuyla 100.000 kullanıcıya kadar servis sağlanabilmektedir. Birden fazla XMPP sunucusu tek servis sağlamak için kullanılarak bu sayı daha yukarılara çekilebilmektedir.
- Açık standart lisanslıdır ve ücretsizdir.
- XMPP sunucusuna bağlanılabilen her noktadan servise erişilebilmektedir.

İnternet üzerinde birçok XMPP servis sağlayıcısı bulunmaktadır. Google Talk, Nimbuzz ve Ovi gibi büyük, genel ve iyi bilinen servisler yanında daha küçük ve özel amaçlı servislerde bulunmaktadır. Bunların yanında Openfire, Tigase ve ejabberd gibi özelleştirilebilir hazır yazılımlarla servis sağlama çözümleri de bulunmaktadır. Bu çözümlerde sunucu yönetim işlemi web arayüzü ile yapılabilmektedir. Bu arayüze 9090 (HTTP) veya 9091 (HTTPS) portlarından ulaşılabilir. XMPP sunucusu kullanılmasıyla eklenti arayüzü, özelleştirme, SSL/TLS desteği, veri tabanı bağlantısı ve LDAP bağlantısı sağlanabilmektedir.

Ağ geçidi, iki ağ arasındaki arayüzleme, paketleme, adresleme ve veri depolama işlemlerini yerine getirmektedir. Ağ geçidinin donanımı seri portu ve internet bağlantısı bulunan bir bilgisayar ve bir ZigBee düğümüdür. İsteğe bağlı olarak ağ geçidi ve sunucu aynı bilgisayarda toplanabilmektedir.

LR-WPAN, yıldız, ağaç veya mesh ağ yapısında ve içinde çeşitli işlev ve görevlerde çalışan ZigBee düğümlerinden oluşan ZigBee ağıdır. Bu ağ koordinatörü ile ağ geçidine bağlanmaktadır. Düğümlerde olmazsa olmaz olarak bulunacak en az iki temel birim mikrodenetleyici ve ZigBee birimidir. Mikrodenetleyici bulunduğu çevreden veri toplamaya yarayan sensörleri okuyabilmekte ve bulunduğu çevreye etki edebileceği donanımı yönetilebilmektedir. Düğüm ZigBee birimi ile kablosuz haberleşmeyi sağlamaktadır.



Şekil- 4.1: ZigBee ve İnternet ağları arası haberleşme sistemi

4.1. ZigBee Modülü

Piyasada satılan ZigBee modülleri, dâhili mikrodenetleyici kontrollü alıcı-verici modülleri ve sadece alıcı-verici modülleri olarak satılmaktadır. Alıcı-verici modüllerinde işlem birimi bulunmamaktadır ve mikrodenetleyicili alıcı-verici modüllerinden daha ucuzdurlar. Alıcı-verici modüllerin çalışması için mutlaka bir işlemciye ihtiyaç duyulmaktadır. ZigBee düğümleri için mikroişlemci kullanmak gereksizdir bu yüzden düğümlerde mikrodenetleyici kullanılmaktadır. Fakat herhangi bir mikrodenetleyici alıcı-verici modüllerle direk olarak çalıştırılması uğraş gerekmektedir. Çünkü ZigBee yığınının işlemciye uyarlanması ve gerekli tanımlamaların yapılması gerekmektedir. Her mikrodenetleyici ZigBee yığın programını destekleyememektedir. Bu uğraştan kullanıcıyı kurtarmak için mikrodenetleyicili alıcı-verici modülleri geliştirilmiştir. Bu modüller içlerinde buldukları mikrodenetleyici sayesinde hem haberleşme işlemlerini yapabilmekte hem de tek başlarına bir sensör düğümü olarak çalışabilmekte hem de yetersiz kaldıklarında başka mikrodenetleyicilerle birlikte çalışabilmektedirler. Ağlar

arası haberleşmede işlem gücü gerektiğinden ve mikrodenetleyici ile alıcı-verici uyumluluğunu sağlama işlemlerinden kurtulmak için Digi firmasının XBee-PRO OEM mikrodenetleyicili alıcı-verici modülü kullanılmıştır.

4.1.1. XBee modül özellikleri

XBee-PRO OEM mikrodenetleyicili alıcı-verici modüllerin pin bilgisi Tablo-3.1’da verilmektedir. Modülleri yapılandırmak için gerekli referans tabloları Ek-A’da verilmektedir [12]. Tablo-3.1’da verilen VCC, GND, DIN ve DOUT pinleri haberleşme için doğru şekilde bağlanmalıdır. XBee-PRO OEM mikrodenetleyicili alıcı-verici modüllerin kapsama menzili kapalı alanda 100m, açık alanda 1500m civarındadır. Modüller uyku modunda 10uA’den az akım çekmektedir. Ayrıca modüllerde dokuz adet giriş çıkış birimi ve yedi adet 8 bitlik analog-sayısal çevirici bulunmaktadır.

Tablo- 4.1: XBee modül pin bilgileri

PİN	ADI	YÖN	TANIMI
1	VCC	-	Güç kaynağı
2	DOUT	ÇIKIŞ	UART veri çıkışı
3	DIN	GİRİŞ	UART veri girişi
4	DO8	ÇIKIŞ	Sayısal çıkış 8
5	RESET	GİRİŞ	Modül sıfırlama
6	PWM0/RSSI	ÇIKIŞ	PWM çıkışı 0/ alınan sinyal gücü göstergesi
7	PWM1	ÇIKIŞ	PWM çıkışı 1
8	[AYRILMIŞ]	-	Boş (bağlanmaz)
9	UYKU_RQ/DI8	GİRİŞ	Uyku modu pini veya sayısal giriş 8
10	GND	-	Toprak
11	AD4/DIO4	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 4
12	DIO7	GİRİŞ-ÇIKIŞ	Sayısal giriş-çıkış 7
13	ON	ÇIKIŞ	Modül durum göstergesi
14	VREF	GİRİŞ	Analog veya sayısal girişler için referans gerilimi
15	AD5/DIO5	GİRİŞ-ÇIKIŞ	Analog giriş 5 veya sayısal giriş-çıkış 5/ ağa katılım göstergesi.
16	AD6/DIO6	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 6.
17	AD3/DIO3	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 3
18	AD2/DIO2	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 2
19	AD1/DIO1	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 1
20	AD0/DIO0	GİRİŞ-ÇIKIŞ	Analog giriş 4 veya sayısal giriş-çıkış 0

4.1.1.1. Şeffaf (Transparent) mod

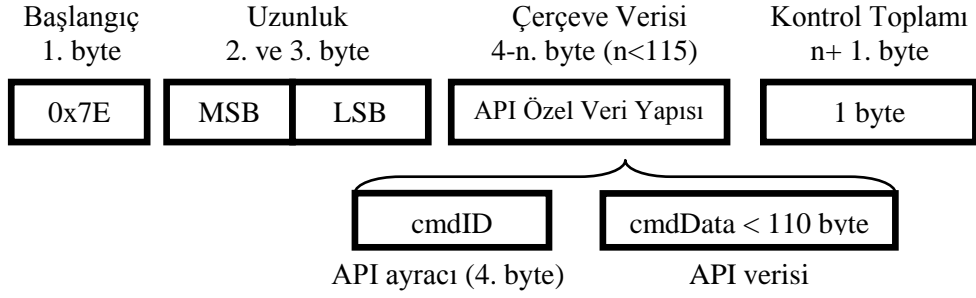
Modüller varsayılan olarak Şeffaf (Transparent) modda çalışmaktadır. Tüm UART verisi DI tamponundan alınır ve RF antenden yollanmaktadır. Modül RF paket

aldığında ise bilgi DO tamponuna alınır ve buradan UART'a yollanmaktadır. Verinin paketlenip gönderilmesi için paketleme süresinin dolması, paketleme limitinin dolması veya paket gönderme komut setinin alınması gerekmektedir. Veri alınırken ise antene gelen sinyal kontrol edildikten sonra paket çözme işlemleri yapıp doğrudan DO pine aktarılmaktadır. Şeffaf modda modül parametre kaydı değiştirilmek veya bu kayıt sorgulanmak istenirse komut moduna geçiş yapılması gerekmektedir. Komut moduna UART'dan “+++” gönderilerek girilmektedir. Bir noktadan çok noktaya veri gönderen sistemlerde uygulama alıcıları belirlemek için ek paket içermelidir [12].

4.1.1.2. API modu

API işlemi uygulama programlama arayüz işlemi anlamına gelmektedir ve şeffaf mod işlemine alternatif olarak çıkarılmıştır. API modu çerçeve tabanlı haberleşme sağlamaktadır. Çerçeveler sayesinde uygulamayla ilgili bilgiler haricinde birçok özelliğin kullanılması sağlanmaktadır. Gönderilen veri çerçevesinde giden veri çerçevesi ve komut çerçevesi bulunmaktadır. Alınan veri çerçevesinde gelen veri çerçevesi, komut cevabı ve olay bildirimleri (sıfırlama, ağa katılım v.b.) bulunmaktadır.

API modu kullanıcı uygulama katmanında alternatif yapılandırma ve yönlendirme olanakları sunmaktadır. API modu sayesinde, şeffaf modda komut moduna girmeden yapılamayan birden fazla adrese veri gönderme, veri ulaştı mesajı, kaynak adres ayrıştırma, alınan sinyal seviyesi gibi işlemler yapılabilmektedir. UART'dan alınan API veri çerçeve yapısı Şekil-3.2'da gösterilmektedir. API çerçevesinin başladığı 0x7E değerine sahip bir başlangıç byte'ı ile belirtilmektedir. Başlangıç byte'nın ardından çerçeve uzunluğunu gösteren iki adet uzunluk byte'ı gelmektedir. Bunun sonrasında çerçeve verisi gelmektedir. Çerçeve verisinin içindeki cmdID çerçevesi, cmdData çerçevesinin içerdiği API mesajının hangisi olduğunu belirtmektedir. cmdData çerçevesi modem durum bilgisi, veri, adres ve komut gibi bilgileri içermektedir. cmdData çerçevesinin içerdiği bilgiler ve uzunlukları Tablo-3.2'de gösterilmektedir. API çerçevesinin en sonunda da verinin doğruluğunu kontrol etmek için 1 byte uzunluğundaki kontrol toplamı bulunmaktadır [12].



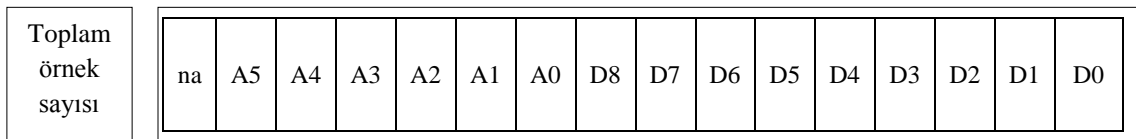
Şekil- 4.2: API çerçeve yapısı

Tablo- 4.2: API çerçeve çeşitleri

İçerik	Uzunluk	cmdID	cmdData				
Modem Durumu	6 byte	0x8a	Durum 0: Donanım sıfırlama 1: Watchdog zamanlayıcısı sıfırlama 2: Ağa katıldı 3: Ağdan ayrıldı 4: Senkronizasyon kaybedildi 5: Koordinatör yeniden düzenlemesi 6: Koordinatör başladı (1 byte)				
Komut	Parametre olup olmamasına göre 8 veya 12 byte	0x08	Çerçeve Ayracı Sonraki onay mesajı için UART verilerini ayırtmaktadır (1byte)	AT Komutu AT komutunu tanımlayan iki ASCII karakter (2 byte)	Parametre Değeri AT komutuyla parametre atanabildiği durumda parametrenin aldığı değer. (4 byte)		
Komut Sorgulama	Parametre olup olmamasına göre 8 veya 12 byte	0x09			Komut sorgusu yapılırken parametre atanmaz (4 byte)		
Komut Cevabı	Durum değerine göre 9 veya 13 byte	0x88			Durum 0: Tamam 1: Hata (1 byte)	Değer İstenen kaydın HEX değeri (4 byte)	
64 Bitlik Adrese Gönderme İsteği	115 byte	0x00	Hedef adres 64 bitlik adres Broadcast: 0x000000000000ffff kullanılmaktadır. (8 byte)	Seçenek 0x01: Onay mesajı yok 0x04: Paketi broadcast PAN-ID ile gönder (1 byte)	Veri 100 byte'a kadar veri aktarılabilir. ktedir.		
16 Bitlik Adrese Veri Gönderme İsteği	109 byte	0x01					Hedef Adres 16 bitlik adres Broadcast: 0xffff kullanılmaktadır. (2 byte)
Gönderi Durumu	7 byte	0x89					Durum 0: Başarılı 1: Hiç onay mesajı alınmadı 2: CCA başarısız 3: Tasfiye (1 byte)
64 Bitlik Adresten Alınan Veri	115 byte	0x80	Kaynak Adresi 64 bit uzunluğunda kaynak adresi. (8 byte)	RSSI Alınan sinyal güç seviyesi (1 byte)	Seçenek 1: adres broadcast 2: PAN broadcast (1 byte)	Veri En fazla 100 byte uzunluğunda veri	
16 Bitlik Adresten Alınan Veri	109 byte		Kaynak Adresi 16 bit uzunluğunda kaynak adresi. (2 byte)				

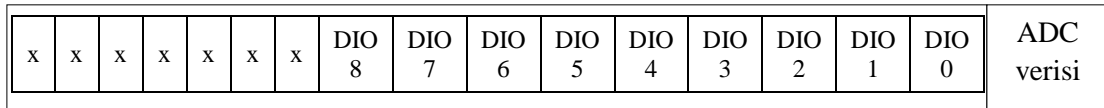
4.1.1.3. Giriş-çıkış birimi ve analog sayısal çevirici

Giriş- çıkış verisini başlatan başlık iki kısımdan oluşmaktadır. Başlık 1 byte uzunluğunda örnek sayısı toplamıyla başlamaktadır. Ardından 2 byte uzunluğunda hangi girişin aktif olduğunu gösteren kanal göstergesi gelmektedir. Kanal göstergesinde her bit bir sayısal giriş çıkışı veya analog girişi göstermektedir. Giriş-çıkış verisinin başlık yapısı Şekil-3.3’de gösterilmektedir.



Şekil- 4.3: XBee giriş-çıkış pin başlık yapısı

Veri örneği başlığın hemen ardından gelmektedir. Eğer herhangi bir sayısal giriş-çıkış hattı kullanılabilir durumdaysa ilk iki byte sayısal giriş-çıkış hatlarını belirtmekte kullanılmaktadır. Sonra gelen iki byte ise analog girişleri göstermede kullanılmaktadır. Giriş-çıkış veri formatı Şekil-3.4’de gösterilmektedir [12].



Şekil- 4.4: XBee giriş çıkış pin veri formatı

4.1.1.4. XBee ağı

XBee modülleri ZigBee standardının karakteristik ağ yapılarına ve düğüm özelliklerine sahiptir. XBee modüllerinin ağa katılım veya birleşme işlemi son cihazın koordinatörden üyelik edinmesi şeklindedir. Bu birleşme işlemi esnasında olmazsa olmazlar koordinatör, PAN-ID ve Kanal –ID’dir.

Bir son aygıt koordinatörün adresini, Kanal-ID’sini veya PAN-ID’sini bilmeden birleşebilmektedir. XBee modüllerindeki koordinatör birleşme A2 parametresi ile son cihaz birleşme ise A1 parametresi ile ayarlanmaktadır. Tablo-3.3’da A2 ve A1 parametrelerinin değerlerine göre birleşme işlemleri açıklanmaktadır. Koordinatör çalıştırılırken izlenen işlemler şöyledir:

- 1- A2 parametresinin kontrolü.

2- Koordinatör başla: koordinatör seçilen kalan ve PAN ID ile görevine başlar. Dikkat edilmesi gereken nokta bu parametrelerin 1. ve 2. basamaklarda seçilmiş olmasıdır. Koordinatörün A2 parametresi kuruluysa sadece son cihazların kendisiyle birleşmesine izin verir.

3- Koordinatör değişiklikleri: koordinatör başladıktan sonra A2, ID, CH veya MY parametresini değiştirme koordinatörün MAC'inin sıfırlanmasına sebep olur. A2nin değişmesi koordinatörün MAC inin değişmesine sebep olmaz. İşaretsiz sistemde son cihaz koordinatöre amacı ile bağlanır. Dolayısıyla eğer koordinatör ID, kanal veya MY değerleri değişir. Son cihaz bu andan sonra koordinatörle haberleşemez. Koordinatör başladıktan sonra ID, CH, MY veya A2 parametreleri kesinlikle değiştirilmemelidir.

Son cihaz çalıştırılırken şu işlemleri yapmaktadır:

1- A1 parametresinin kontrolü.

2- Koordinatörü keşfet: Otomatik birleş biti kurulduğunda çalışır. Son cihaz Aktif taramaya başlar. Aktif tarama önceden bahsedildiği şekilde tüm kanallardaki PAN'ları tarar. Son cihaz A1 parametresine göre bir koordinatör seçer.

3- Doğru koordinatöre bağlanmak için 2. adımdaki şekilde bir koordinatör bulunduğu son cihaz bir birleşme isteği gönderir. Sonra onay mesajı bekler.

4- Son cihaz değişimlerinin birleşmeye etkisi: A1, PAN-ID veya Kanal-ID parametrelerinin değişimi son cihazın bağlantısını sonlandırır ve birleşme sürecini yeniden başlatır. Eğer son cihaz birleşmede sorun yaşarsa A1 hata içeriği yollar.

Her RF veri paketi kaynak ve hedef adreslerini başlık alanlarında taşınmaktadır. RF modülü IEEE 802.15.4 standardının sağladığı 16 bit ve 64 bit adreslemeyi desteklemektedir. Eşsiz 64 bit IEEE kaynak adresi fabrika üretimi esnasında atanmaktadır. SL ve SH komutlarıyla bu adresin alçak ve yüksek kısımları okunabilir. Kısa adresleme elle MY komutu kullanılarak yapılmaktadır. Bir paketi özel bir adrese göndermek için DL ve DH komutları kullanılmaktadır. Bu komutlar kullanılarak 64 bitlik hedef modül adresinin alçak ve yüksek kısımları yazılmaktadır. 16 bit adres için ise sadece DL komutu kullanılmaktadır. Bu durumda DH=0 yapılmaktadır.

Tablo- 4.3: Koordinatör ve son cihaz birleşme parametreleri

Parametre	Bit	Görev	Değer	Açıklama
A2	0	PAN-ID tekrar atanma izni	0	Koordinatör aktif tarama yayını yapar. Aktif tarama bir kanal seçer ve yayın mesajı (0xffff) olarak işaret tepkisi bekler ve PAN ID sini yayımlar. Sonra seçili kanalı dinler ve işaret tepkilerini toplar. Bu kanalı dinleme süresi SD (tarama süresi) parametresiyle belirlenir. Bir kere zaman dolduğunda aktif tarama bu kanalı bırakıp başka kanalı tarar ve aynı denemeyi tekrar yapar. Bu süreç tüm kanallar tamamlanana veya 5 PAN keşfedilene kadar devam eder. Aktif tarama tamamlandığında tüm PAN ID'lerin ve kanalların listesi çıkarılmış olur. Bu liste sayesinde koordinatörün eşsiz PAN ID almasında kullanılır. ID parametresi aktif tarama sonucu bulununcaya kadar korunur. Eğer bulunursa parametre ayarında güncelleme olur.
			1	Koordinatör ID ayarını korur. Aktif tarama olmaz.
	1	Kanal-ID yeniden atanma izni	1	Koordinatör enerji taraması için yayın yapar. Bir kanal seçilir ve kanaldaki enerji seviyeleri taranır. Tarama süresi parametresi tarama süresini belirler. Bu süre dolduğunda seçili kanal bırakılıp diğer kanala geçilir. Bu tarama tüm kanallar taranana kadar devam eder. Enerji taraması tamamlandığında kanalların enerji seviyelerinin bulunduğu bir sonuç listesi oluşur. Eğer aktif tarama çalıştıysa, kanallar PANların tespiti gerçekleşir. Enerji taraması ve aktif tarama sonucunda en az güç tespit edilen kanal ve en az PAN barındıran seçimi yapılarak en iyi haberleşme seçimi gerçekleşir.
			0	Koordinatör kanal ayarlarını korur. Enerji taraması gerçekleşmez.
	2	Birleşme izni açık/kapalı	0/1	
A1	0	PAN-ID yeniden atama izni	1	Son cihaz herhangi bir PAN-ID ile bir ağa üye olabilir.
			0	Son cihaz önceden belirlenen bir ID ile PAN a üye olabilir.
	1	Kanal-ID yeniden atama izni	0	Son cihaz kanal değeri önceden ayarlanır ve sadece eşleşen değerdekiyle çalışır.
			1	Son cihaz Herhangi bir kanal değeriyle PAN a üye olabilir.
	2	Otomatik birleş	0	Son cihaz koordinatörle birleşmeye çalışmaz. Son cihaz önceden belirlenmiş olan ID, CH ve MY parametreleriyle çalışır. Birleşme tamamlandığında birleşme LED'i yanar (saniyede beş defa). Otomatik birleşme kurulmadığında 2. ve üçüncü adımlar uygulanmaz.
			1	Son cihaz koordinatörle birleşmeye çalışır.

Varsayılan olarak RF modülleri unicast modunda çalışmaktadır. Unicast modu tekrar yapmayı sağlayan tek moddur. Bu modayken alıcı modül yeni mesaj aldığı anda kaynağa ACK mesajı gönderir. Eğer verici modül ACK mesajı almazsa üç kere daha benzer şekilde ACK bekleyerek paketi tekrar gönderir. 16 bit kıs adresleme

kullanılırken MY komutuyla modüle 0xFFFFE den küçük 16 bit adresler verilebilmektedir. DH=0 seçilerek DL komutuyla hedef olarak 16 bit adres seçilebilmektedir. MY parametresi kullanılmadığı zaman SH ve SL komutlarıyla okunabilen seri numara kullanılmaktadır. Son cihaz koordinatörle birleşirken son cihazın MY parametresi 0xffffe olarak ayarlanarak 64 bit adres kullanılmaktadır.. Hedef adresi olarak seri no kullanılacaksa bu seri no DL ve DH parametreleriyle yazılmaktadır.

RF modülleri kapsama alanı içindeki adres bilgisi içeren broadcast almaktadır. Broadcast modunda çalışmaya ayarlanan modül ACK bildirimini göndermemektedir. Gönderici modül ACK beklemediği için unicast deki gibi mesaj tekrarlanmamaktadır. Broadcast mesaj göndermek için hedef adresi 16 bit ve 64 bit adreslemede DL: 0x0000ffff DH:0x00000000 şeklinde ayarlanmaktadır [12].

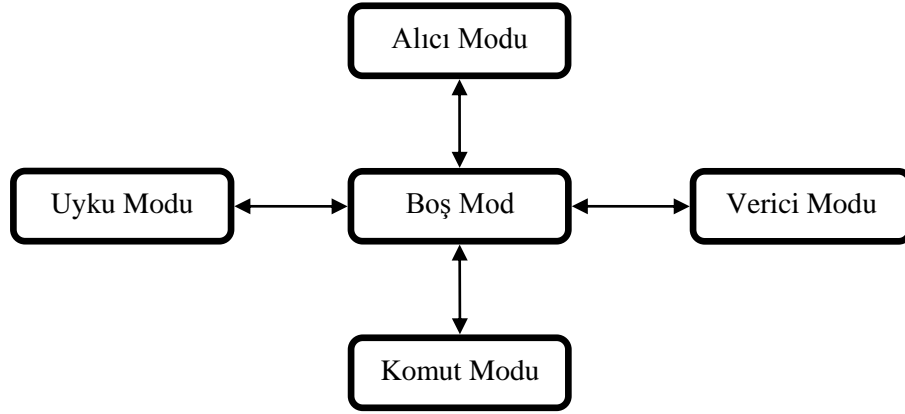
4.1.1.5. Çalışma modları

Boş, alıcı-verici, komut ve uyku modu olmak üzere beş çalışma modu bulunmaktadır. Şekil-3.5’da çalışma modlarının geçiş durumları gösterilmektedir. Veri alınmadığı veya gönderilmediği zaman RF modülün boş çalışma modudur. DI tamponundan veri alındığında verici moduna, RF ortamdan veri geldiğinde alıcı moduna, uyku tetiklendiğinde veya periyodik uyku zamanı geldiğinde uyku moduna ve komut seti geldiğinde komut moduna girilmektedir.

Uyku modu RF modülün düşük güç harcama haline geçmesi halidir. Uyku modlarına giriş ve çıkış şekilleri Tablo-3.4’de gösterilmektedir. Modülün uyku durumuna geçmesi için uyku pininin sürülmesi veya uyku süresi (ST) kadar boş modda kalması gerekmektedir.

Pin uykusu SM=1 için gücü minimize ederek yapılmaktadır. Bu durum gerilim seviyesi ile tetiklenmektedir. Uyku pini sürüldüğünde modül veri alma/verme ve birleşme işlemlerini tamamlar ve ardından boş durumda düştüğünde doğrudan uyku durumuna geçer. Modül, pin tetiklemeyle uyandırılana kadar uyku modunda kalmaktadır. Modül uyku modunda RF ve seri etkilere cevap vermemektedir. Pin uyuklama fonksiyonu SM=2 iken pin yarı çalışır durumdadır. Bu durumda modül SM=1’e göre daha hızlı uyanmaktadır. Ancak SM=2’de modül daha fazla güç harcamaktadır.

Döngüsel uyku durumu modülün RF veriyi döngüsel olarak denetlemesini sağlar. SM=4 olduğunda otomatik olarak modül koordinatörden kendine ait mesaj olup olmadığını kontrol eder. Eğer kendisi için bekleyen mesaj varsa bunu ister[12].



Şekil- 4.5: ZigBee çalışma modları

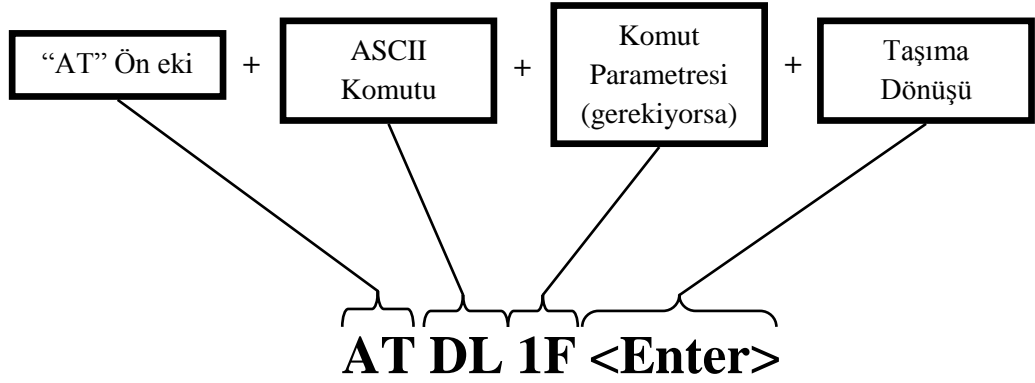
Tablo- 4.4: XBee uyku modlarına giriş ve çıkış şekilleri

Uyku Modu	SM (Uyku Modu) değeri	Uyku moduna geçiş	Uyku Modundan Çıkış
Pin uykusu (kış uykusu)	1	9. pin yükseğe çekilmektedir.	9. pin alçağa çekilmektedir.
Pin uykusu (uyuklama)	2	9. pin yükseğe çekilmektedir.	9. pin alçağa çekilmektedir.
Periyodik uyku	4-5	ST süresi dolduğunda otomatik olarak uyku moduna girmektedir	SP (Uyku Periyodu) süresi dolduğunda otomatik olarak uyku modundan çıkmaktadır.

4.1.2. XBee modül yapılandırması

XBee modüllerini yapılandırmak için AT komutları kullanılmaktadır. Komut moduna girmek için “+++” karakterleri gönderilmekte ve AT komutları sırasıyla gönderilmeye başlanmaktadır. AT komutları Şekil-3.6’da gösterildiği şekilde oluşturulmaktadır.

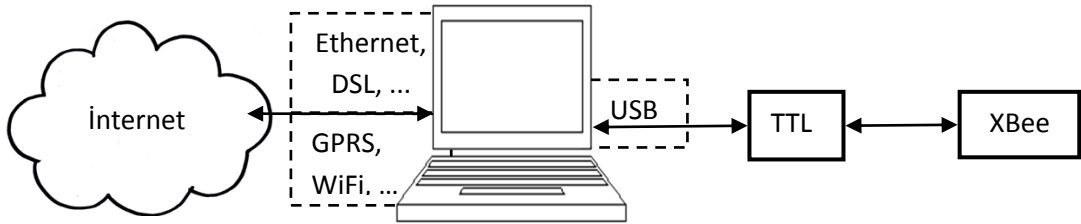
Komutlar arka arkaya girildikten sonra ATWR komutuyla kalıcı belleğe yazma işlemi gerçekleştirilmektedir. Komut modundan ATCN komutu girilerek çıkılabilmektedir. Uzun süre komut girilmediği takdirde de modül kendiliğinden komut modundan çıkmaktadır [12].



Şekil- 4.6: AT komut formatı

4.2. Ağ Geçidi Donanımı ve Gereksinimleri

Ağ geçidi, XMPP sunucusuna bağlanabilmek için internet arayüz kartlı ve XBee koordinatörü ile haberleşebilmek için seri haberleşme portu bulunan bir bilgisayardır. Ağ geçidi donanımı Şekil-3.7’de gösterilmektedir. Bilgisayarın seri portu 5V seviyesinde buna karşılık XBee’ler 3.3V lojik seviyesinde haberleşmektedir. XBee voltaj farkı sebebiyle donanımına zarar vermek için araya bir TTL entegresi konulmaktadır. Çalışmamızda TTL entegresi olarak olan FTDI FT232RL entegresi kullanılmıştır.



Şekil- 4.7: Ağ geçidi donanımı

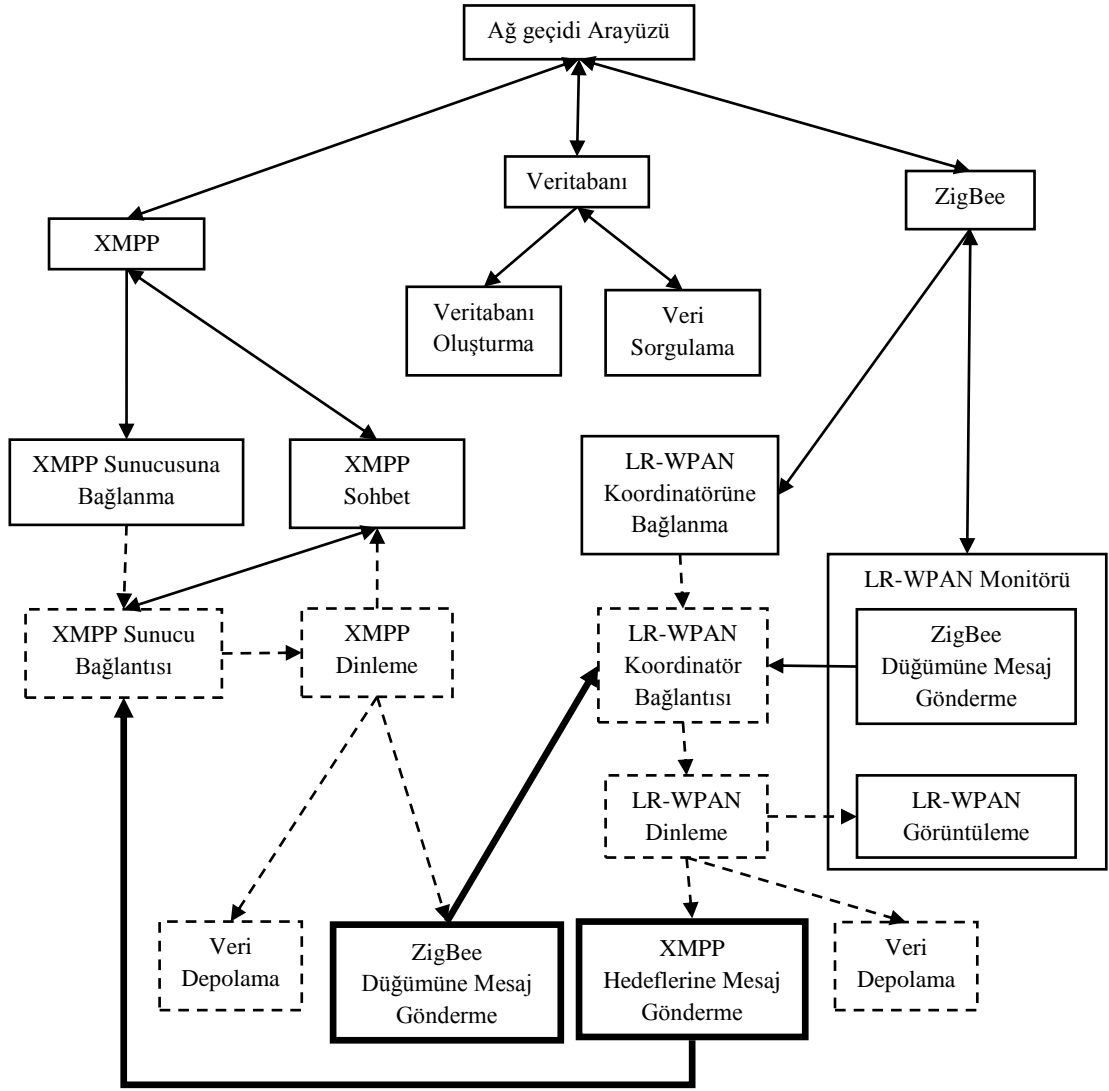
Ağ geçidi yazılımı Java dilinde yazıldığı için ağ geçidi bilgisayarında hangi işletim sisteminin kullanıldığı önemli değildir ancak kullanılan işletim sistemine uygun JRE bilgisayarda kurulu olmalıdır. Ayrıca ağ geçidinde gelen verilerin depolanması isteniyorsa bir veritabanı sistemi gerekmektedir. Çalışmada ağ geçidindeki depolama sistemi için MySQL veritabanını kullanılmıştır.

4.3. Sistem Yazılımı ve Yönetimi

Sistem ağ geçidi yazılımı ve kullanıcı yazılımı olarak ikiye ayrılmaktadır. Ağ geçidi yazılımı ağ geçidinde yapılan paketleme, yönlendirme, adresleme, bağlantı ve veri transferi işlemlerinin yanı sıra veri depolama ve ağ geçidi yönetimi işlemlerinin yerine getirildiği yazılımdır. Kullanıcı yazılımı ise XMPP kullanıcı arayüzü sağlamakla yükümlü yazılımdır. Bu yazılım sıradan bir XMPP kullanıcı mesajlaşma yazılımı olabilmekte beraber amaca uygun bir yazılımda olabilmektedir. Kullanıcı yazılımı XMPP sunucusundan gelen veriyi analiz etmek ve kullanıcının grafik arayüzüyle sistemi kontrol edebilmesini sağlamaktan sorumludur.

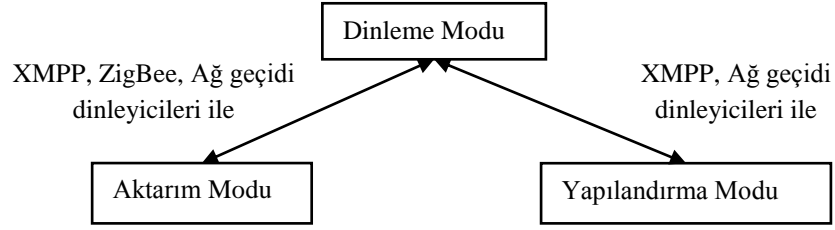
4.3.1. Ağ geçidi yazılımı

Ağ geçidi yazılımı Java dilinde yazılmıştır. Ağ geçidi yazılımı XMPP, ZigBee ve Ağ geçidi olmak üzere üç ana kısımdan oluşmaktadır. XMPP kısmında temel olarak XMPP bağlantısı, sisteme güvenli giriş işlemleri ve XMPP kullanıcılarına veri gönderip alma işlemleri gerçekleştirilmektedir. XMPP kısmı yazılırken XMPP için hazırlanmış birçok Java kütüphanesinden biri olan Smack kütüphanesinden faydalanılmıştır. ZigBee kısmı ZigBee koordinatörüne seri port bağlantısı sağlamak, ZigBee düğümlerini koordinatör üzerinden dinlemek ve bu düğümleri yönetmek ile görevlidir. ZigBee kısmında seri arayüz için en genel seri haberleşme kütüphanesi olan RXTX kütüphanesinden faydalanılmıştır. Ağ geçidi kısmı ise XMPP ve ZigBee kısımlarından gelen paketlerden verileri çıkarma, paketleme ve mesajların veri-kod ayrıştırma işlemlerini üstlenmektedir. Bunlara ek olarak ağ geçidindeki veri tabanı yönetimi de ağ geçidi kısmından yapılmaktadır. Şekil-3.8’de ağ geçidi yazılımının şeması gösterilmektedir. Şekilde kesik çizgilerle gösterilen işlemler yazılımda kendiliğinden çalışmaktadır. Şekilde normal çizgilerle gösterilen işlemler kullanıcı kontrolünde arayüz yardımıyla yapılmaktadır. Kalın çizgi ile gösterilen işlemlerde ise ağlar arası haberleşme için gerekli paketleme ve adresleme dönüşümleri gerçekleştirilmektedir.



Şekil- 4.8: Ağ geçidi yazılımı şeması

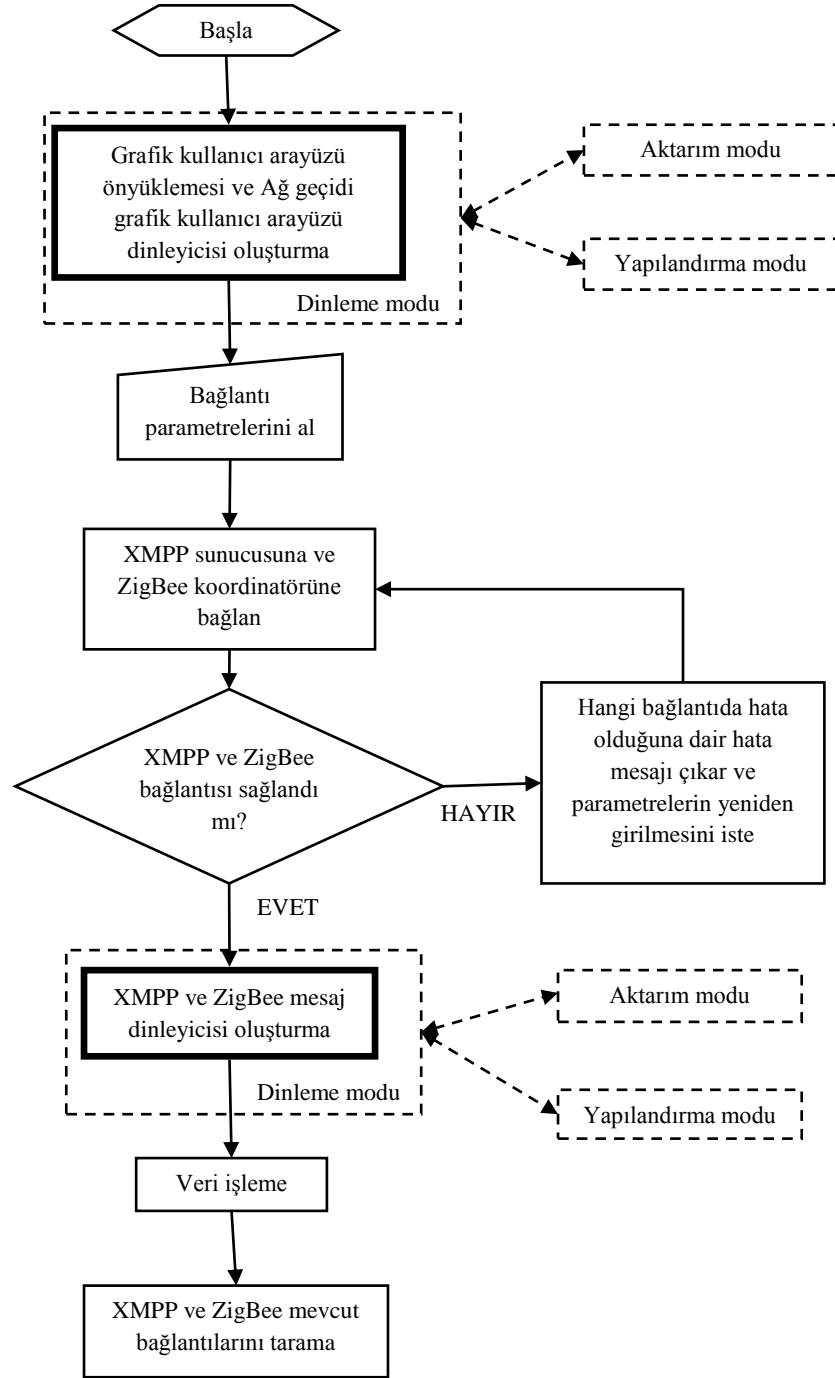
Ağ geçidi yazılımı dinleme, aktarım ve yapılandırma modu olmak üzere üç modda çalışmaktadır. Bu modlar Şekil-3.9’da gösterilmektedir. Dinleme modunda yazılıma yerleştirilmiş olan XMPP ve ZigBee dinleyicileri ile ağlar dinlenmektedir. Ağ geçidi dinleyicisi, kullanıcı arayüzü dinlemesi yapılmaktadır. Dinleyiciler bağlı oldukları kısımdan gelen etkileri dinlemekte ve bir etki olduğunda içinde tanımlanan işlemleri gerçekleştirmektedir. Dinleyiciler tetiklendiklerinde program okunan mesaja göre aktarım veya yapılandırma moduna girmektedir. Aktarım moduna her dinleyici erişebilmektedir ve dinleyicilerden gelen mesajlar direk olarak bir ağdan diğer ağa gönderilmektedir. Yapılandırma modu ağ geçidi yapılandırmasına olanak sağlayan moddur. Yapılandırma moduna sadece ağ geçidi ve XMPP dinleyicilerinden erişilebilmektedir çünkü yapılandırma yapacak kullanıcı veya yöneticiler sadece bu dinleyicileri tetikleyebilmektedir.



Şekil- 4.9: Ağ geçidi çalışma modları

Şekil-3.10’da ağ geçidi programının genel algoritması gösterilmektedir. Algoritmada görüldüğü üzere yazılım çalıştığında ilk önce ağ geçidi önyüklemesi yapılmaktadır. Ön yüklemede yazılım çalışmakta, sistem portlarını denetlemekte ve görsel arayüz çalıştırılmaktadır. Ön yüklemenin ardından ağ geçidi dinleyicisi eklenmektedir. Ağ geçidi grafik kullanıcı arayüzünden gelen tetiklemeler ile ağ geçidi, XMPP ve ZigBee ağı yapılandırma ve yönetim işlemleri yapılabilmektedir. Ayrıca bu arayüzden her iki ağa da bu ağ geçidinden mesaj gönderilebilmektedir. Temel ağ geçidi arayüz bileşenlerinin önyükleme işlemlerinden sonra yöneticinin isteğine bağlı olarak ağ geçidi bağlantı tetiklemeleriyle XMPP ve ZigBee bağlantıları sağlamaktadır. XMPP bağlantısı sağlanması için port, kullanıcı adı ve şifre bilgileri alınmaktadır. ZigBee ağına bağlanmak için ise seri port adı ve baud oranı bilgileri alınmaktadır.

Bağlantılar tamamlandıktan sonra her iki taraftan gelen verilerin işlenmesi gerekmektedir. Ancak önce verilerin geldiğini anlamak için XMPP ve ZigBee dinleyicilerinin oluşturulması gerekmektedir. Bu dinleyiciler kendi ağlarından gelen veriler ile tetiklenmekte ve bu ağlardan gelen verileri ayırtarak yükümlüdür. XMPP dinleyicisi programın başında bir MessageListener ile sistemde otomatik olarak dinlenirken ZigBee dinleyicisi seri port üzerine bir PacketListener eklenmesi suretiyle oluşturulmaktadır. PacketListener veri geldiğinde otomatik olarak tetiklenir ve seri porttan gelen veriyi String olarak direkt programa gönderir. ZigBee tarafından gelen veri paketleri seri porttan API mod çerçeveleri halinde geldiği için Şekil- 4.2 ve Tablo- 4.2 ‘de gösterilen kalıplara göre veri, kaynak adres ve sinyal seviyesi byte byte olarak ayrıştırılıp okunmaktadır. XML olarak gelen XMPP verilerine ilk olarak MessageListener uygulamasının oluşturduğu processMessage metodunun içinde ulaşılabilir. Bu metodun getirdiği Chat nesnesinin participant özelliğinin çekilmesi ile sohbet kaynak adresi çekilebilmektedir. Yine aynı metod içindeki Message nesnesinin body özelliği ile mesaj içeriğine erişilebilmektedir.



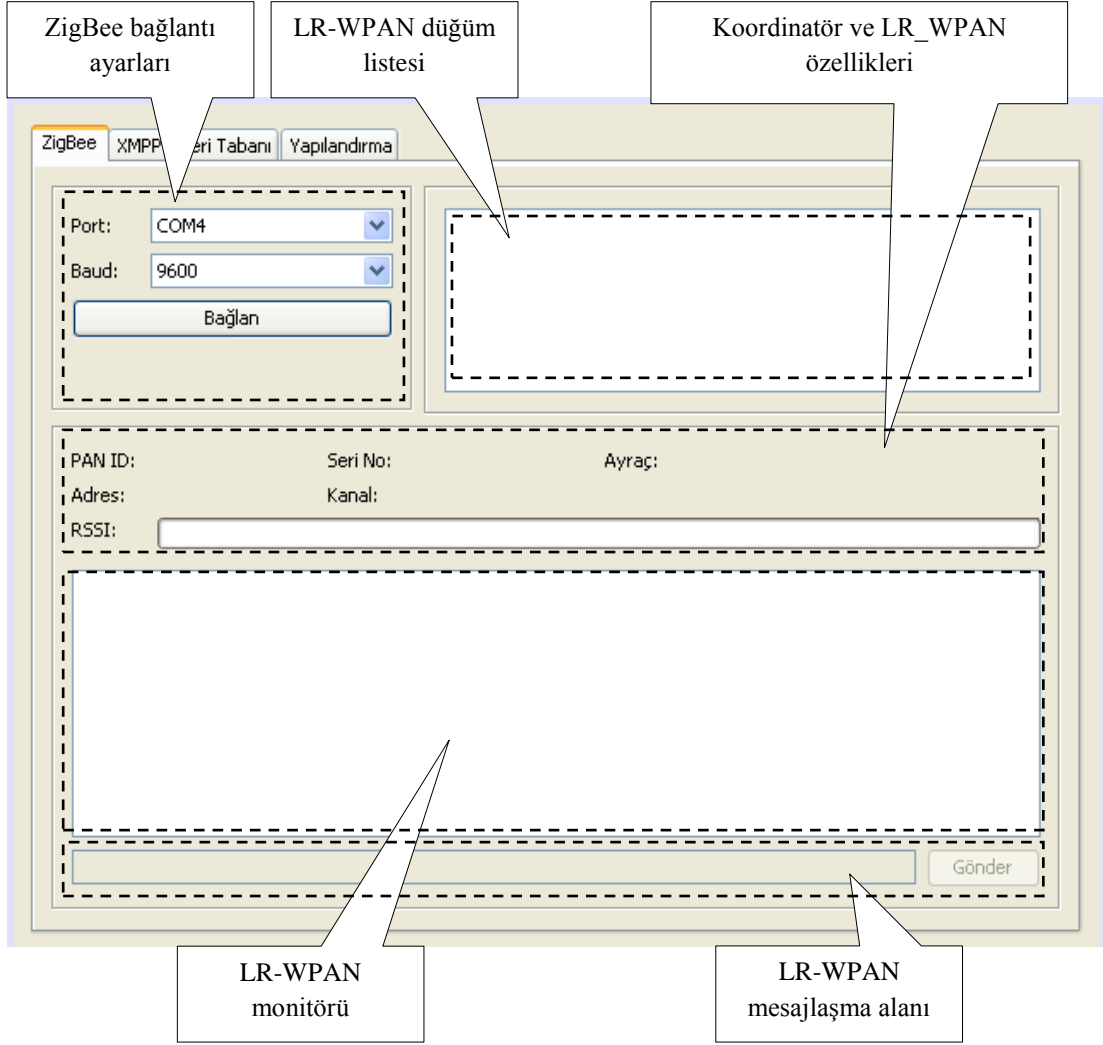
Şekil- 4.10: Ağ geçidi algoritması

Veri işlemede veri gönderme kısmı alma kısmından daha basittir. ZigBee tarafına veri gönderilmek istendiğinde API modunda kullanılan 16 bit adresli veri gönderme çerçeve kalıbı kullanılmaktadır. Burada önce verinin önüne 0x7E eklenmektedir sonra 2 byte uzunluğunda veri uzunluğu alanı, 1 byte uzunluğunda 0x01 komut ayraç ardından 2 byte uzunluğundaki 16 bitlik kısa adres eklenmektedir bunun ardından cevap istenmediğine dair 0x01 değeri ve son olarak en fazla 100 byte

uzunluğundaki veri eklenmektedir. Paket son olarak 1 byte uzunluğundaki kontrol toplamıyla tamamlanıp seri porttan gönderilmektedir. XMPP hedeflerine mesaj göndermek için ise xmpp bağlantı nesnesinin chatManager özelliğine hedef adres ve mesaj tanımlanarak oluşturulmaktadır. Burada hedef adres ve mesaj String türündendir.

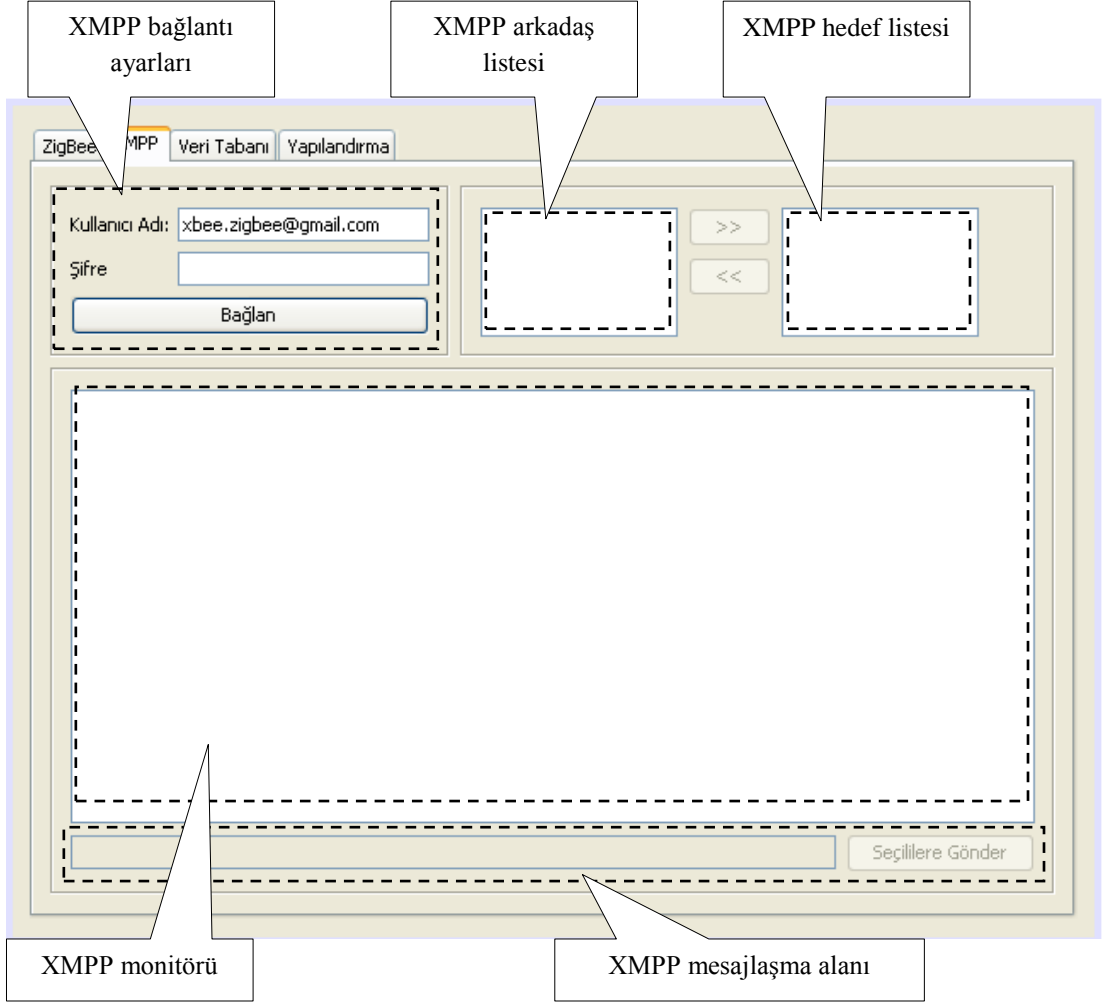
ZigBee bağlantı taramasında ZigBee ağına üye olan düğümler koordinatördeki düğüm listesinden çekilmekte ve ağ geçidinde tüm ZigBee düğümleri listelenmektedir. XMPP bağlantı taraması adımıyla bağlantının sağlanıp sağlanmadığını denetlemek için XMPP tarafında tarama yapılmaktadır. XMPP tarafından ağ geçidiyle arkadaş olan kullanıcıların listesi istenmekte ve bu kullanıcılara ağ geçidi kullanıcısının bir ağ geçidi olduğunu belirten bir mesaj gönderilmektedir. Bu mesaj içinde ağ geçidine kayıtlı olan ZigBee düğümleri gönderilmektedir. Örneğin zigbee1@xmpp.com adresli ağ geçidindeki 16 bit lik adresi 1111 olan bir düğüm zigbee1@xmpp.com:1111 olarak ifade edilmektedir. Bu ağ geçidi bildirimini sayesinde internetteki tüm ağ elamanları servis hakkında bilgi sahibi olmaktadır. Böylece internet taraflı servis bildirim işlemi gerçekleştirilmiş olmaktadır. ZigBee taraflı keşif işlemi ise ağ geçidindeki ZigBee düğümünün servis keşfi ve düğüm taraması ile yapılmaktadır. Oluşturulan sistemde düğümlerin internet adreslerini tanıması gerekmemektedir ZigBee düğümlerinden XMPP ağına giden veriler ağ geçidi tarafından yönlendirilmektedir.

Ağ geçidi kullanıcı grafik arayüzü ZigBee, XMPP, yapılandırma ve veritabanı olmak üzere dört sekmeden oluşmaktadır. ZigBee sekmesi ZigBee bağlantısını sağlamak, LR-WPAN'ı yönetmek ve ZigBee ağdan gelen ve ağa giden verileri görüntülemek için kullanılmaktadır. Şekil-3.11'de ZigBee sekmesi ve bileşenleri gösterilmektedir. Bu sekmede bağlan butonuyla ağ geçidi dinleyicisindeki ZigBee bağlantı ve ZigBee dileyicisi oluşturma fonksiyonları tetiklenmektedir. Bağlantı sağlandıktan sonra ZigBee sekmesindeki bileşenler aktifleşmektedir. Bu sekmenin alt kısmında bulunan gönder butonuna basıldığında mesaj alanına yazılan içerik listeden seçilen düğüm varsa o düğüme yoksa tüm düğümlere gönderilmektedir.



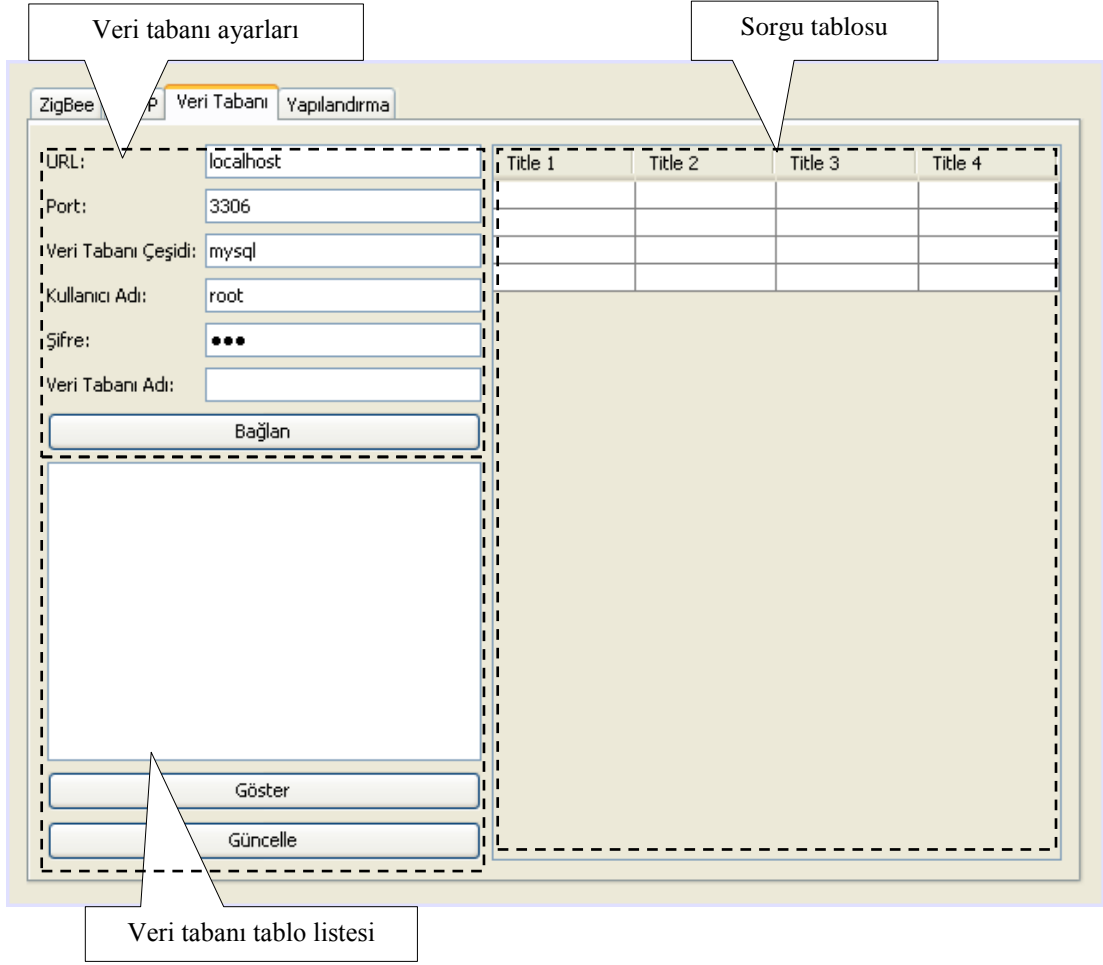
Şekil- 4.11: Ağ geçidi kullanıcı grafik arayüzü ZigBee sekmesi

XMPP sekmesi XMPP bağlantısı sağlamak, XMPP'den gelen giden tüm veriyi görüntülemek ve XMPP arkadaş listesindeki arkadaşlarla haberleşebilmek için kullanılmaktadır. Şekil 3.12'de XMPP sekmesi ve bileşenleri gösterilmektedir. Bu sekmede en altta bulunan gönder butonuna basıldığında mesaj alanında bulunan veri eğer XMPP hedef listesine ekli adreslerine varsa bu adres veya adreslere, yoksa arkadaş listesinin tamamına gönderilmektedir. Ağ geçidine ZigBee ağından gelen verilerde aynı şekilde hedeflere gönderilmektedir.



Şekil- 4.12: Ağ geçidi kullanıcı grafik arayüzü XMPP sekmesi

Veri tabanı sekmesi ağ geçidinin veritabanı ayarlarının yapıldığı ve veritabanındaki verilerin görüntülenebildiği sekmedir. Burada girilen verilere göre bağlantılar sağlandıktan ve sınılandıktan sonra veri tabanı oluşturulmaktadır. Eğer veritabanı parametreleri hatalı girilmiş veya parametreler girilmemiş ise veritabanı oluşturulmaksızın sistem işleme devam etmektedir. Şekil 3.13’de veri tabanı sekmesi gösterilmektedir.



Şekil- 4.13: Ağ geçidi kullanıcı grafik arayüzü veri tabanı sekmesi

Yapılandırma sekmesi LR-WPAN cihazlarının her birini uzaktan programlayabilmek ve özelliklerini okuyabilmek için oluşturulmuş bir arayüzdür. Bu sekme düğümdeki XBee modülünün temel özellikleri olan 16 bitlik kısa adres, Kanal-ID, PAN-ID, hedef adresi, Seri numarası, şifreleme, RF iletim güç seviyesi, RF sinyal eşik değeri, uyku modu ve uyku özellikleri bilgilerini okuma ve uzaktan programlayabilmeyi amaçlamaktadır. Şekil-3.14 'da gösterilen arayüzde listeden bir düğüm seçilerek oku butonuna basıldığında bu düğümün özellikleri okunmaktadır. Yapılandırma sekmesindeki değiştirilebilir alanlardan istenene parametre girilip hedef düğüm seçildikten sonra yaz butonuna basıldığında koordinatör üzerinden bu düğüm programlanır. Eğer hedef düğüm seçilmezse bu işlemler direk olarak koordinatöre uygulanmaktadır.

The image shows a software interface for configuring a ZigBee network. The main window has a tabbed interface with 'Yapılandırma' (Configuration) selected. The configuration area is divided into two sections: 'LR-WPAN düğüm listesi' (LR-WPAN node list) on the left and 'Düğüm özellikleri' (Node properties) on the right. The 'Düğüm özellikleri' section contains the following fields:

- PAN-ID: [Text input]
- KANAL-ID: [Text input]
- ADRES: [Text input]
- SERİ NO: [Text input]
- HEDEF: [Two text inputs]
- ŞİFRELEME: [Checkbox] [Password field]
- RF GÜÇ: [Dropdown menu]
- RF EŞİK: [Text input]
- UYKU MODU: [Dropdown menu]
- UYKUDAN ÖNCEKİ SÜRE: [Text input]
- PERİYODİK UYKU SÜRESİ: [Text input]

At the bottom of the configuration area, there are two buttons: 'OKU' (Read) and 'YAZ' (Write). A callout box points to these buttons with the text 'Düğüm yapılandırması okuma ve yazma butonları' (Node configuration read and write buttons).

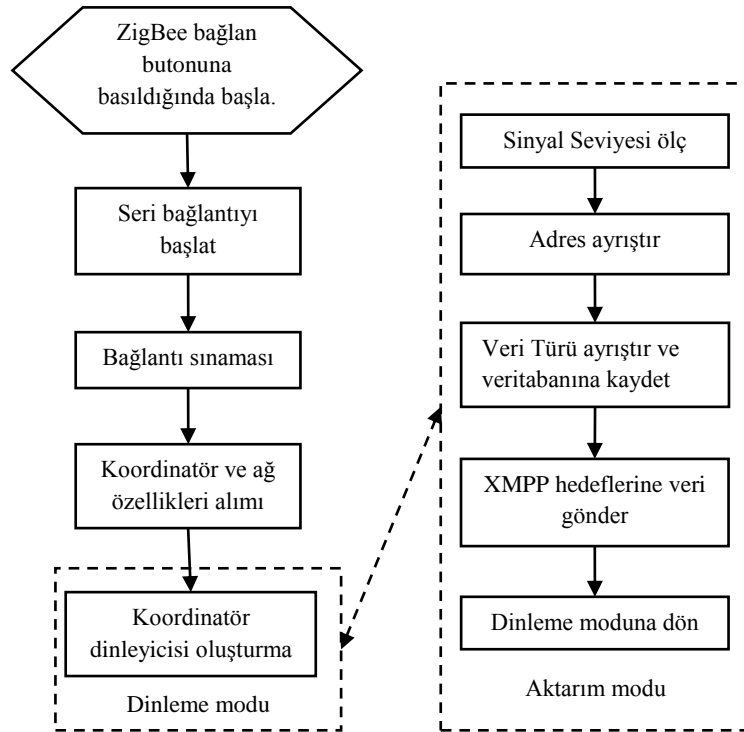
Şekil- 4.14: Ağ geçidi kullanıcı grafik arayüzü yapılandırma sekmesi

4.3.1.1. ZigBee arayüzü ve dinleyicisi

Ağ geçidi arayüz yazılımındaki ZigBee sekmesi sayesinde ZigBee ağına bağlanmak için gerekli olan seri haberleşme parametreleri alınmaktadır. Şekil-3.10'de verilen algoritmadaki ZigBee ağına bağlantı, grafik kullanıcı arayüzündeki bağlan butonuyla girilen seri port parametrelerine bağlı olarak başlanmaktadır. Ağ geçidindeki ZigBee düğümünün yani koordinatörün işlem kolaylığı ve işlevsellik açısından API modunda çalışması gerekmektedir. Diğer ZigBee düğümler şeffaf veya API modda çalışabilmektedir. ZigBee arayüz ve dinleyici algoritması Şekil-3.15'da gösterilmektedir. Bağlantı yapılmaya çalışırken oluşabilecek herhangi bir hatayı yakalamak için try-catch yöntemi kullanılmaktadır. Burada program açıldığında oluşturulmuş olan XBee nesnesine (XBee) bağlantı parametreleri aktarılıp seri bağlantı çalıştırılmaktadır. Daha sonra eğer bağlantı sağlanmışsa önce ZigBee sekmesindeki görsel arayüz bileşenleri aktif hale getirilmekte ardından ZigBee dinleyicisi zigbeeDinleyicisiEkle() fonksiyonuyla eklenmekte ve son olarak ta yerel özelliklerin alınması için yerelOzellikleriAl() fonksiyonu çağırılmaktadır.

yerelOzellikleriAl() fonksiyonu koordinatörün karakteristikleri ve ZigBee ağının temel karakteristikleri olan Kanal-ID ve PAN-ID özellikleri alınmaktadır. ZigBee dinleyicisi sayesinde koordinatöre gelen her mesaj dinleyici için bir tetik oluşturmaktadır. Dinleyici eklemek için zigbeeDinleyiciEkle() fonksiyonun içinde XBee nesnesine yeni bir paket dinleyici eklenmekte ve processResponse() metodu çalışmaktadır. Bu metodun içinde veri depolama, XMPP hedeflerine veri gönderme ve sinyal gücü, kaynak adresi, veri türü bilgilerinin alınması işlemleri gerçekleştirilmektedir. Sinyal seviyesi, kaynak adresi ve veri türü bilgilerinin alınmasında bölüm 3.1.2.1.2’de anlatılan API çerçeve formatlarından faydalanılmaktadır.

Ağ geçidi arayüz yazılımının ZigBee sekmesinde ağa katılan her düğümün adresi bağlantı panelinin sağındaki listede yer almaktadır. Eğer bir düğüm uzun süre ulaşılamazsa düğüm listeden kaldırılmaktadır. ZigBee sekmesinin alt tarafında yer alan mesaj kutusuna yazılan mesajlar hedef listesinde yer alan düğümlere gönderilmektedir. Eğer hedef listesi boş ise tüm düğümlere broadcast olarak gönderilmektedir.



Şekil- 4.15 ZigBee arayüz algoritması

4.3.1.2. XMPP arayüzü ve dinleyicisi

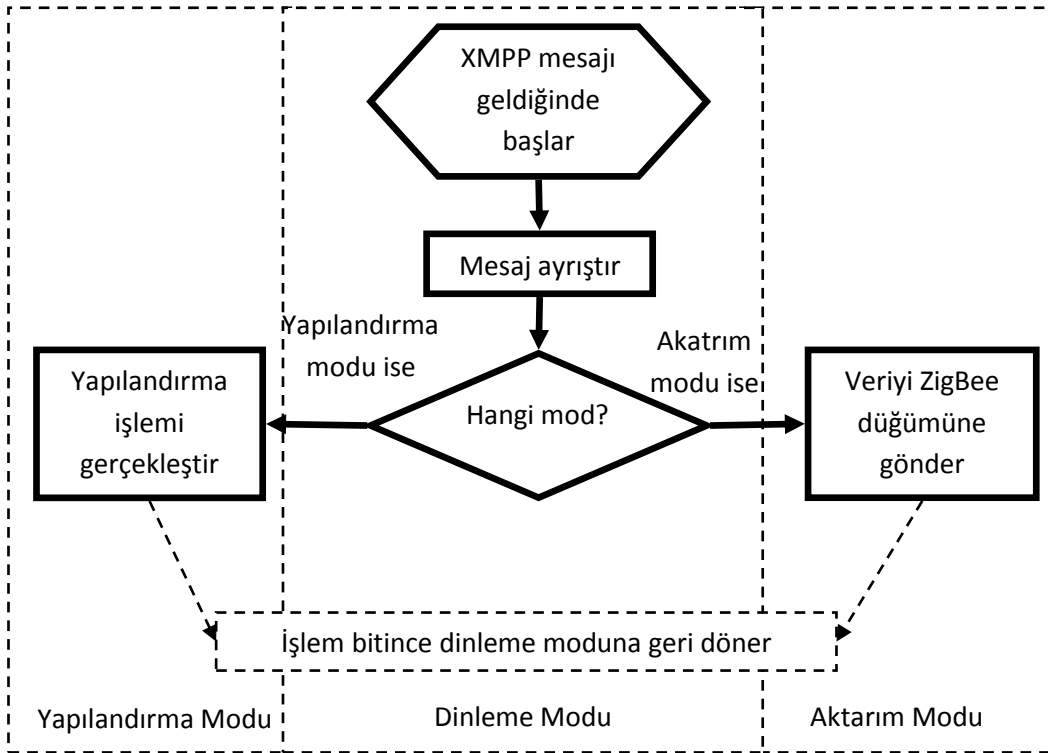
Ağ geçidinde XMPP bağlantı parametreleri XMPP sekmesinden girilmektedir. XMPP sekmesinde kullanıcı adı ve şifre parametreleri girildikten sonra bağlan butonuna basılarak ağ geçidi dinleyicisindeki XMPP sunucusuna bağlanma fonksiyonu çalıştırılır. Şekil-3.10'daki algorithmada da görüldüğü üzere bağlantı sağlandıktan sonra bağlantı tarama adımında XMPP sunucusundan arkadaş listesi istenir ve bu arkadaş listesi arayüzdeki arkadaş listesine aktarılır. Arkadaş listesi alındıktan sonra listedeki tüm arkadaşlara önce ağ geçidi bildirimini gönderilir ardından ağ geçidine kayıtlı olan ZigBee düğümlerini gönderme işlemi yapılır.

XMPP bağlantı butonuna basıldığında ilk önce bağlantı oluşturulurken oluşabilecek bir hatayı yakalamak amacıyla try-catch yapısı uygulanmaktadır. Bu try-catch yapısının içine hata oluşturma önceliğine göre önce xmppBaglan() fonksiyonu çalıştırılmakta ve XMPP bağlantı yapılandırma nesnesi (ConnectionConfiguration) "host" olarak oluşturulmaktadır. Bağlantı yapılandırma nesnesi oluşturulduktan sonra XMPP bağlantı nesnesi (XMPPConnection) oluşturulmakta ve nesneye yapılandırma nesnesi eklenmektedir. Bağlantı nesnesiyle önce sunucuya bağlanılmakta sonrada kullanıcı bilgileriyle bağlantı açılmaktadır.

Bağlantı sorunsuz oluştuysa program kendiliğinden XMPP mesaj dinleyicisini (MessageListener) ekler ve gelen mesajlar processMessage() fonksiyonun içine gider. Yani gelen mesaja ilk bu fonksiyondan erişilebilir. Dinleyicinin oluşturulmasının ardından XMPP sekmesinin arayüz bileşenlerini etkinleştiren ve pasifleştiren xmppGuiBileşenleri() fonksiyonu çalışmaktadır. Arayüz fonksiyonun gerekli görsel öğeleri aktif/pasif hale getirmesinin ardından XMPP sunucusundan arkadaş listesi çekilmekte ve arayüzde listelenmektedir. XMPP bağlantısı sağlandıktan sonra processMessage() fonksiyonunun içine gelen mesajlar direk olarak hedefe gönderilmektedir.

Dinleyici içindeki fonksiyonlar yani processMessage() fonksiyonun algoritması Şekil-3.16'da gösterilmektedir. Algorithmada görüleceği üzere gelen mesajın aktarım modu mu yoksa yapılandırma modu mu olduğu mesaj ön ekiyle belirtilmektedir. Ön ek yoksa normal sohbet işlemleri yapılmaktadır. Eğer mesaj "\$\$\$" ön ekiyle başlıyorsa aktarım moduna geçilmektedir. Mesajda "###" ön eki varsa yapılandırma moduna geçilmektedir. Aktarım modunda ön ekin ardından hedef 16 bitlik adres ve düğüme gönderilecek mesaj bulunmaktadır.

Aktarım modunda gelen veri önce veri yığına sokulup belleklenmekte sonra hedef adres ve veri ayrıştırılıp koordinatör üzerinden hedef düğüme gönderilmektedir. Böylece ZigBee düğümlerine internette gelebilecek yüksek miktardaki veri durumunda oluşabilecek veri kaybının önüne geçilmektedir. Aktarım modunda gelen veriler hem ZigBee hem de XMPP sekmelerindeki ekranlarda yazılmaktadır. Yapılandırma için tanımlı komutlar “####” ile başlamaktadır. Yapılandırma modu için tanımlanmış olan fonksiyonlar örnek amaçlı olup ZigBee ağ bağlantısını kapatma/açma ve hedef listesine ekleme örnekleri olarak yapılmıştır. Yapılandırma modunda gelen veriler sadece XMPP sekmesindeki ekranda yazılmaktadır.



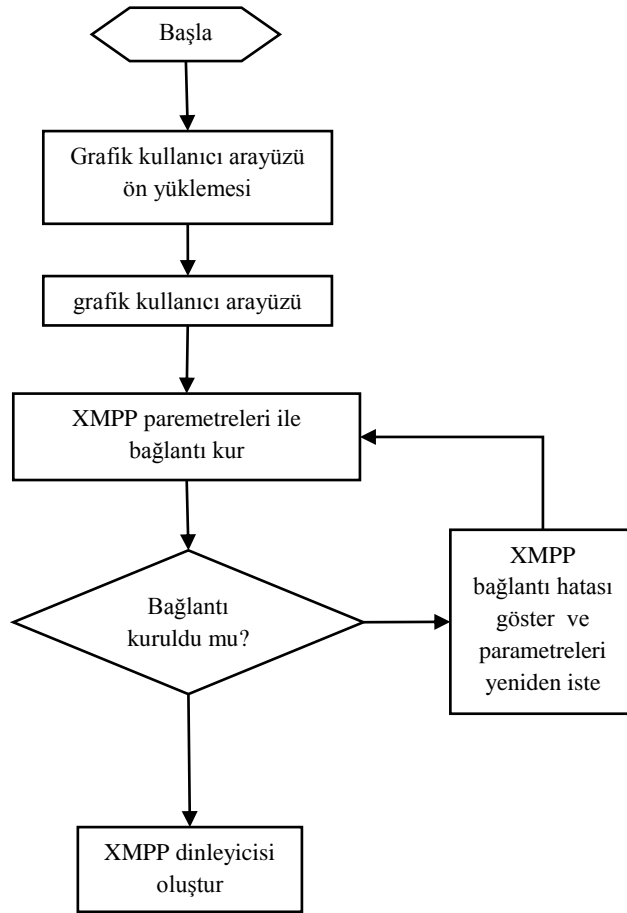
Şekil- 4.16: XMPP dinleyici algoritması

4.3.2. Kullanıcı yazılımı

Kullanıcı yazılımını LR-WPAN sistemini gözleyecek ve yönetecek kullanıcılara basit kullanım sağlamak için grafik arayüzü sunan yazılımdır. Bu yazılımın işlevi hali hazırda bulunan bir XMPP kullanıcı yazılımları ile de yapılabilmektedir fakat uygulama kapsamında kullanacağımız düğümleri daha kolay gözleyebilmek ve yönetebilmek için uygulamaya özel yazılım oluşturulması gerekmektedir.

Kullanıcı yazılımı ağ geçidi yazılımına göre çok daha basit bir yazılım olup sadece gelen verileri çözümlenmektedir. Gelen verilerin hangi türde olduğunu anlayıp grafik olarak kullanıcıya anlaşılır şekilde yansıtılması ve grafik arayüzden yapılmak istenen işlemi alıp gereken ön ekleri ekleyip ağ geçidine gönderme kullanıcı yazılımıyla gerçekleştirilebilmektedir.

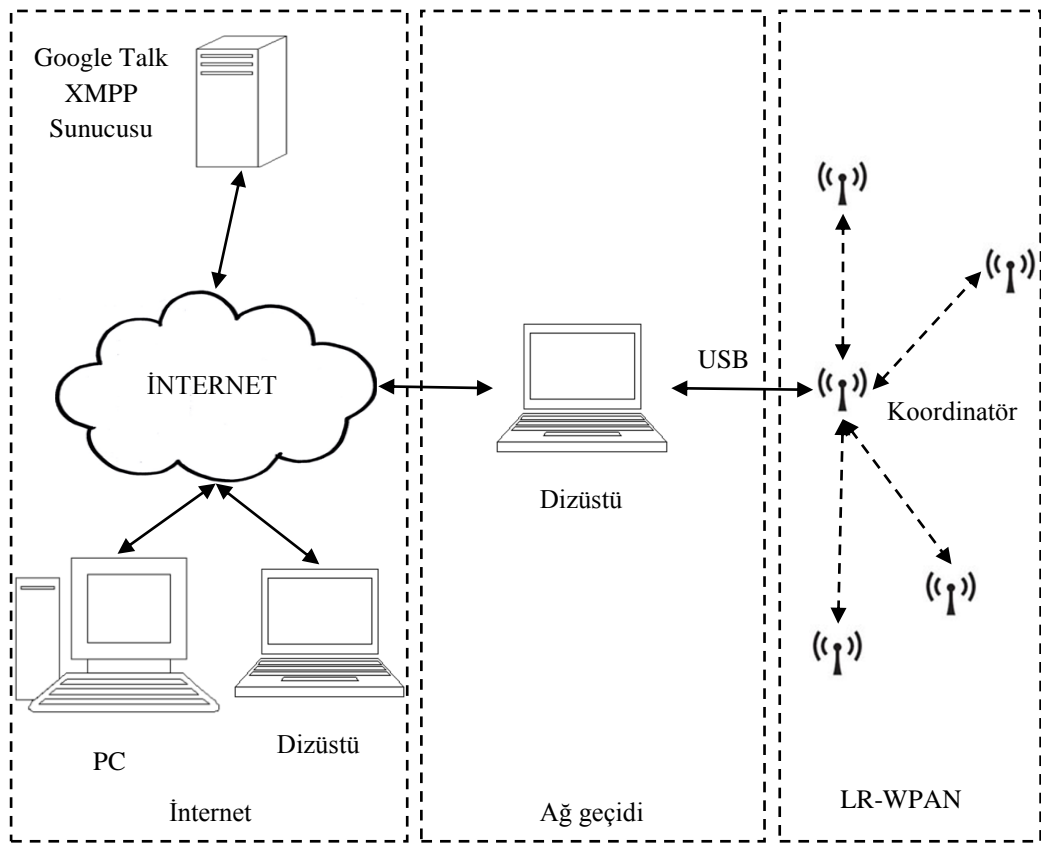
Şekil-3.17’de kullanıcı yazılımının algoritması gösterilmektedir. Burada görüleceği üzere temel olarak iki dinleyici bulunmaktadır. Bunlar kullanıcı grafik arayüz dinleyicisi ve XMPP dinleyicisidir. Kullanıcı grafik arayüz dinleyicisinin görevi grafik arayüzüyle yapılan işlemleri tetiklemektir. XMPP dinleyicisinin işi de ağ geçidinden gelen verileri analiz etmek ve kullanıcı grafik arayüzüne göndermektir.



Şekil- 4.17: Kullanıcı yazılım algoritması

5. SCADA UYGULAMASI

SCADA uygulaması ZigBee ve İnternet ağları arası haberleşme için oluşturulan ağ geçidi ve ağ geçidi yazılımını bir uygulamayla örneklemek amacıyla oluşturulmuştur. Bu uygulamada kullanılacak sistem Şekil-4.1’de gösterilmektedir. Sunucu olarak şu anda en yaygın olarak kullanılan Google Talk sunucusu seçilmiştir. İnternet tarafındaki kullanıcı cihazları ise bir dizüstü ve bir masaüstü bilgisayardır. Ağ geçidi olarak bir dizüstü bilgisayar seçilmiş olup LR-WPAN ağında beş XBee modülü bulunmaktadır. Bu düğümlerden ikisi gözlem amaçlıdır. Diğer ikisi ise ölçüm yapmak ve XMPP den gelen verilere tepki vermek üzere kullanılmaktadır.

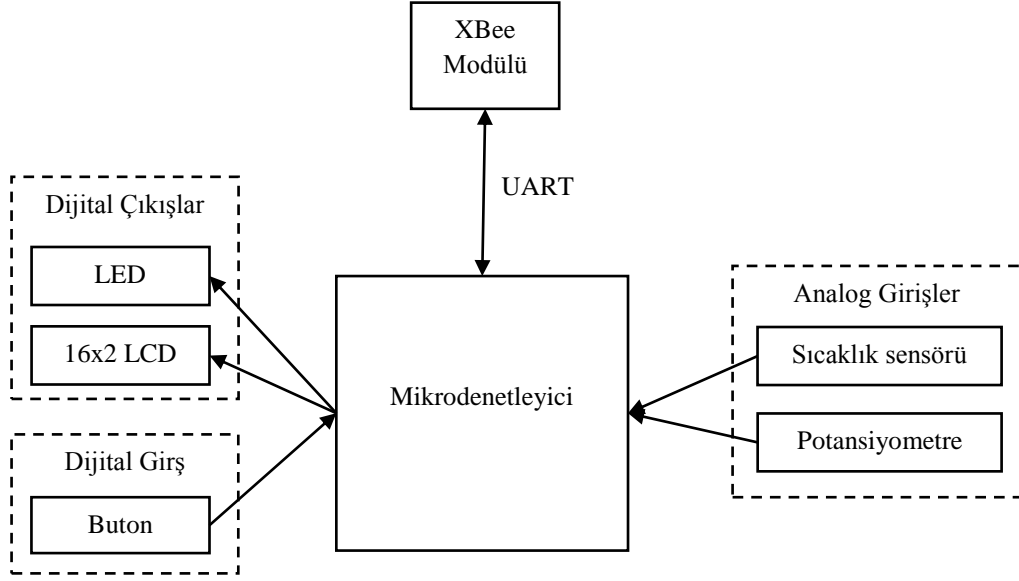


Şekil- 5.1: SCADA uygulama şeması

5.1. Kablosuz Sensör Ağı Düğüm Donanımı

Düğümler, Şekil-4.2’de gösterilen modül şemalarına gösterildiği üzere LED, buton, LCD, potansiyometre, sıcaklık sensörü, mikrodenetleyici ve XBee modülünden oluşmaktadır. Düğüm donanımındaki LED ve LCD alınan veriye göre çıkış vermek için kullanılmaktadır. Buton, potansiyometre ve sıcaklık sensörü uygulama kapsamında örnek veri oluşturmak için kullanılmıştır. Mikrodenetleyici, XBee

modülü ile UART üzerinden haberleşmektedir. XBee modülü gelen veriyi DOUT pininden mikrodnetleyicinin alıcı pinine gönderilmektedir. Mikrodnetleyici UART üzerinden alınan veriyi işlemekte ve buna göre çıkış birimlerini yönetmektedir. Girişlerden alınan veya ölçülen veri ise mikrodnetleyicinin verici pininden, XBee modülünün DIN pinine gönderilmektedir. XBee modülü de DIN pininden aldığı veriyi RF ortama iletmektedir.



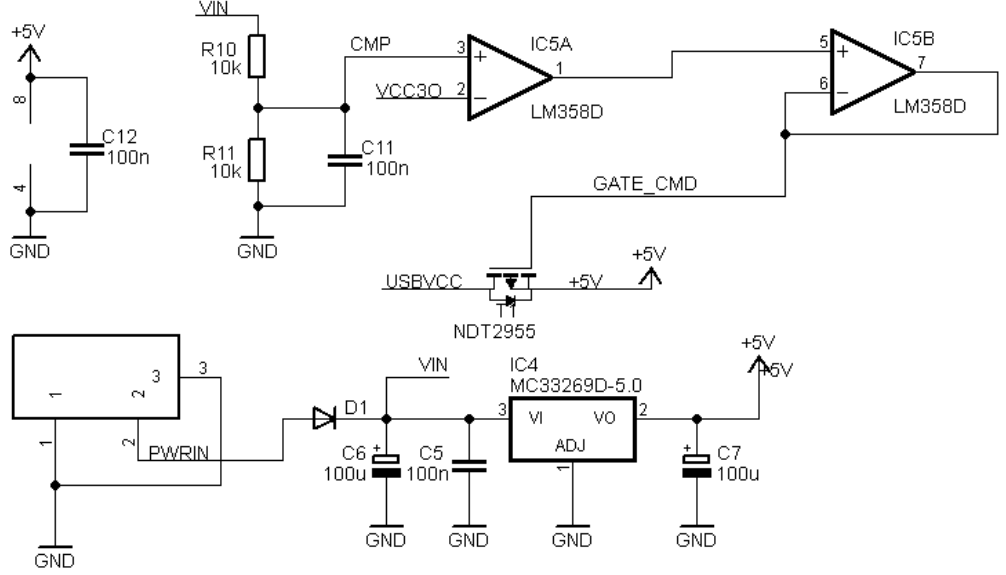
Şekil- 5.2: Düğüm modeli

5.1.1. Mikrodnetleyici özellikleri ve yazılımı

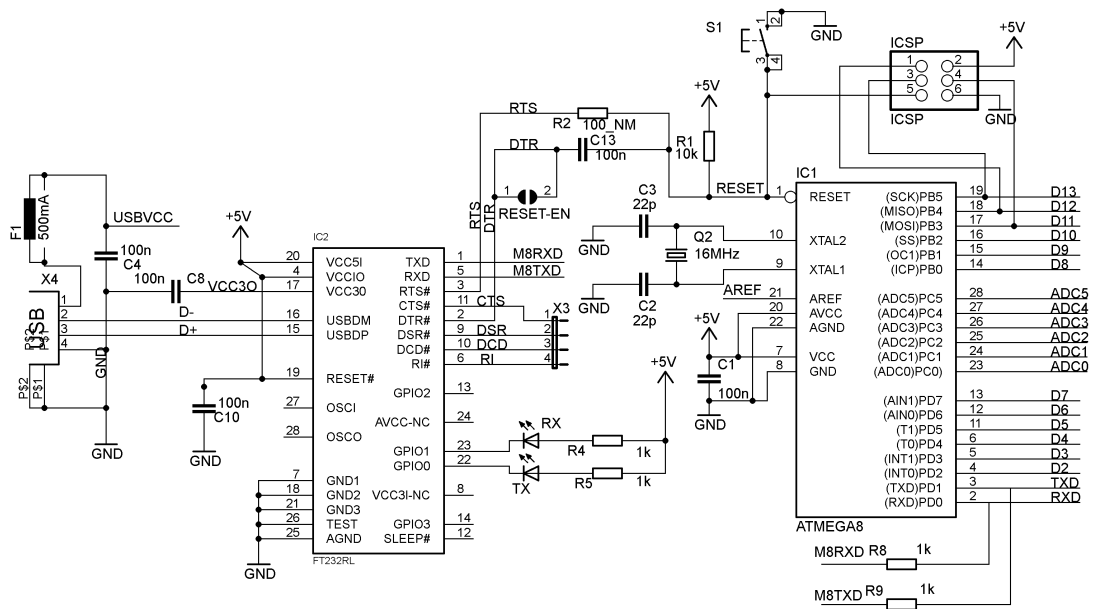
Düğümelerde mikrodnetleyici olarak seri haberleşme yapabilen herhangi bir mikrodnetleyici kullanılabilir. Uygulamada deneme ve kullanım kolaylığı sebebiyle Arduino Duemilanove deneme kiti kullanılmıştır. Bu kit üzerinde ise mikrodnetleyici olarak ATMEL firmasının ATmega168 mikrodnetleyicisi bulunmaktadır. Kit içinde Şekil-4.3'de gösterilen güç katı olarak 5V'dan ve 9V'dan 3.3V'a dönüştürücü bulunmaktadır. Seri haberleşme için Şekil-4.4'de gösterilen FDTI TTL entegresi bulunmaktadır. Modül içinde kullanılacak olan sensör, buton, XBee modül ve LCD bağlantıları Şekil-4.5'da gösterilmektedir.

Düğümelerde kullanılan mikrodnetleyici algoritması Şekil-4.6'da gösterilmektedir. Algoritma buton denetimi ile başlamaktadır. Butona basıldığında düğüm adını UART'dan göndermektedir. Sonraki adımda analog girişler okunup dönüşümler yapıldıktan sonra UART'dan gönderilmektedir. Son olarak UART'dan bilgi gelip gelmediği kontrol edilmektedir. Bilgi geldiyse LED yakılmakta ve gelen veri

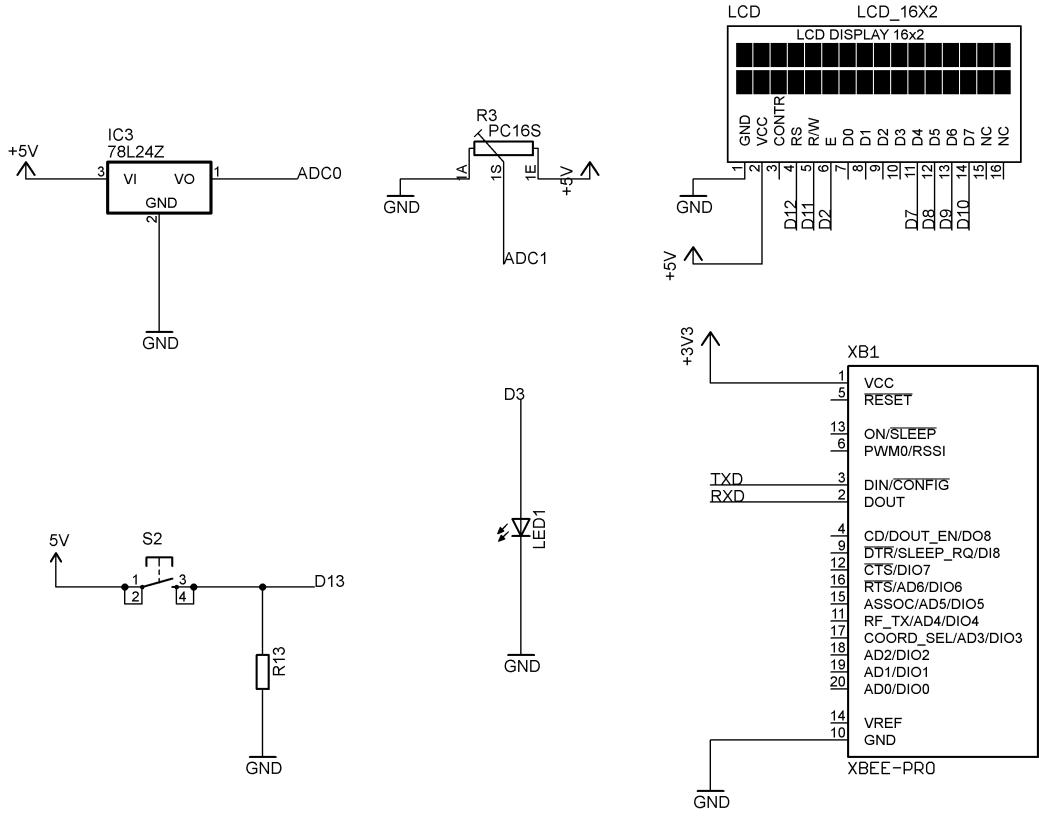
LCD’de gösterilmektedir. Dügümde algoritma başladıktan sonra sürekli bir döngü içine girilmektedir yani butona denetimi ile başlayıp UART dinlemeyle biten algoritma sürekli olarak dönmektedir.



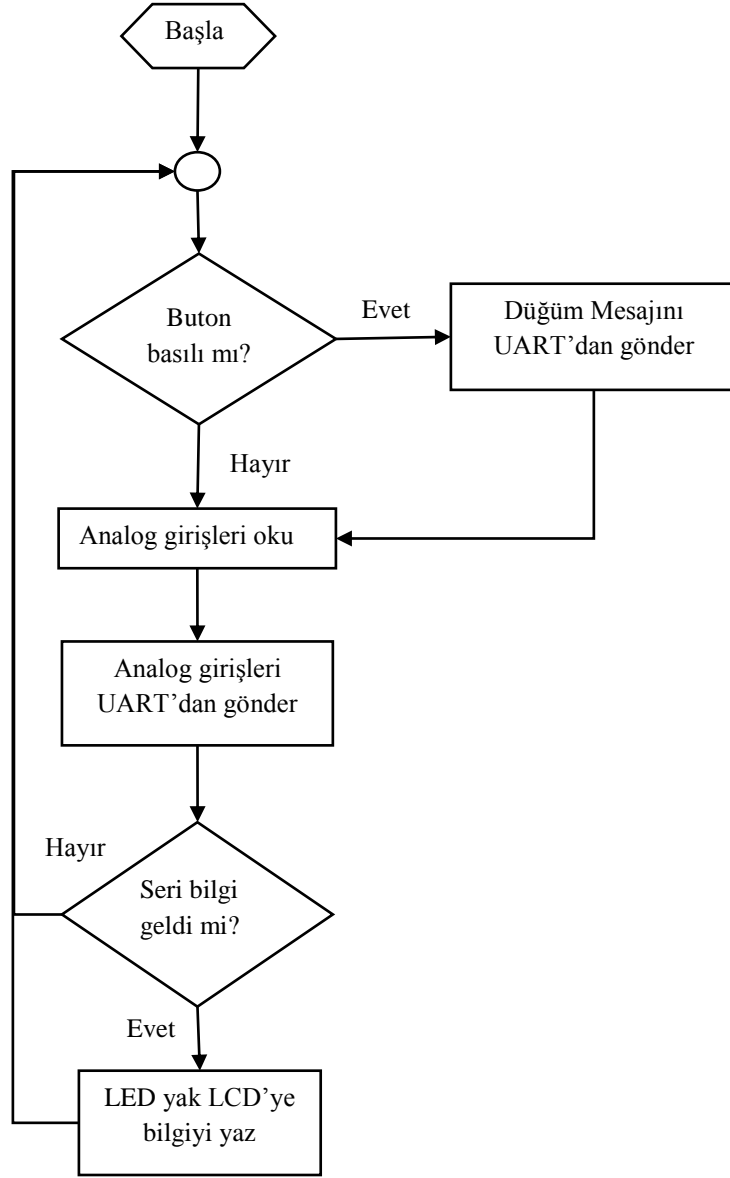
Şekil- 5.3: Arduino güç şeması



Şekil- 5.4: Mikrodenetleyici ve seri haberleşme şeması



Şekil- 5.5: Buton, LED, XBee modül, sıcaklık sensörü ve LCD bağlantıları



Şekil- 5.6: Düğüm mikrodenetleyici algoritması

5.1.2. XBee modül yapılandırması

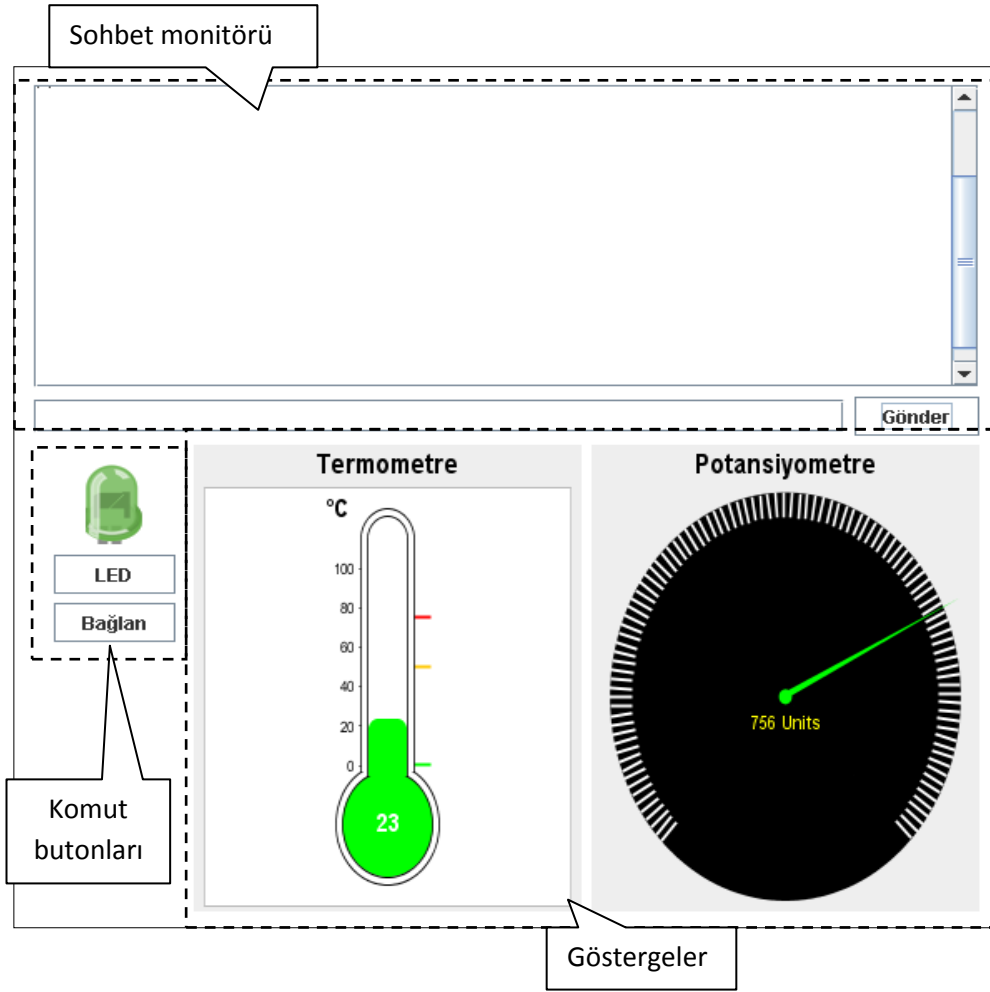
XBee modülleri, Digi firmasının modülleri programlamak için sunduğu X-CTU programıyla, seri porttan AT komutlarıyla veya ağ geçidi programındaki yapılandırma arayüzü yardımıyla programlanabilmektedir. Bu modül programlama yöntemlerinin hepsi aslında seri porttan AT komutu gönderme işlemine dayanmaktadır. Seri porttan programlama ile sadece bağlı olan modül programlanabilmektedir. Sadece ağ geçidi programıyla direk olarak uzaktan programlama yapılabilmektedir. Diğer yöntemlerde API çerçevelerinin tamamı elle yazılmak durumundadır. Uygulama için modül yapılandırması için işlenecek kodlar sırasıyla şöyledir:

- **+++** : AT komut moduna giriş.
- **ATCH 12** : Kanal-ID 12 olarak atama.
- **ATID 1111** : PAN-ID 1111 olarak atama.
- **ATDH 0000** :Hedef cihaz adresinin yüksek kısmı. (16 bitlik kısa adresleme kullanılacağı zaman yüksek kısım 0000 olarak atanır)
- **ATDL** :Hedef cihaz adresin alçak kısmı boş bırakılan yere yazılmaktadır. 16 bit adreslemede hedef adres direk olarak buraya girilmektedir. (Koordinatörün tüm düğümlere veri gönderebilmesi için FFFF yapılıır)
- **ATMY** : Modülün kendi 16 bit adresi boş bırakılan yere yazılmaktadır.
- **ATNO 1** : Düğümler için 1 koordinatör için 0 değerini almaktadır.
- **ATCE 0** : Koordinatör için 1 son cihaz için 0 değerini almaktadır.
- **ATAP 0** : Düğümlerde Şeffaf mod kullanıldığı için 0 Koordinatörde API modu kullanıldığı için 1 değerini almaktadır.
- **ATWR** : Modüle yazılan bilgilerin kaydedilmesi.
- **ATCN** :AT programlama modundan çıkış.

Eğer çalışma esnasında programlama yapıyorsa XBee modül programla esnasında veri göndermeyi kesmekte sadece kendine gelen AT komutlarına cevap mesajları göndermektedir. Programla tamamlandıktan sonra XBee modülü görevine yeni parametreleriyle geri dönmektedir.

5.2. XMPP Kullanıcı Yazılım Uygulaması

XMPP kullanıcı ağ geçidinden gelen verileri okumak ve grafiğe dökmekle yükümlüdür. Uygulamada düğümlerdeki sıcaklık ve potansiyometre değerleri ile buton durumunu grafik arayüze aktarmaktadır. Ayrıca grafik arayüzdeki mesaj gönderme alanıyla düğümlere mesaj gönderebilmekte ve butonlarla ağ geçidi yazılımına yapılandırma kodu gönderebilmektedir. Kullanıcı yazılımı arayüzü Şekil-4.7'de gösterilmektedir.



Şekil- 5.7: SCADA uygulaması XMPP kullanıcı yazılımı grafik arayüzü

6. SONUÇ VE ÖNERİLER

Bu çalışmada ZigBee protokolüyle haberleşen kablosuz sensör ağlarına internet üzerinden erişebilmek için sunucu tabanlı çalışan bir kontrol sistemi tasarlanmıştır. Tasarlanan sistemde, sunucu tabanlı ağlar arası haberleşme tekniği kullanılmasıyla ZigBee'nin sağladığı avantajlar korunmaktadır. Tasarlanan sistemde IP tabanlı ağlar ve kablosuz sensör ağları XMPP teknolojisi yardımıyla birleştirilmiştir. Sistemde, XMPP teknolojisinin kullanılmasıyla kablosuz sensör ağına kolay erişim sağlanmış ve XMPP'nin sağladığı yapısal avantajlardan faydalanılmıştır.

Kablosuz sensör ağı ile IP tabanlı ağların haberleşmesinde öne çıkan başlıca sorunlar adresleme, veri aktarım oranı, servis keşfi ve güvenlidir. Tasarlanan sunucu tabanlı sistemde bu sorunları aşmak için her iki ağla da aynı anda haberleşebilen bir ağ geçidi oluşturulmuştur. Sistemde adresleme sorunu uygulama katmanı seviyesinde çözülmüştür. IP tabanlı ağlarda adres olarak kullanıcı adı kullanılmıştır. Kablosuz sensör ağı düğümlerinde ise 16 bit'lik kısa adres kullanılmıştır. Her iki taraftaki ağ elemanları birbirlerinin adreslerini ağ geçidi sayesinde öğrenebilmektedir. Paketleme sorunu, ağ geçidinde verinin tamamen paketten çıkarılması ve iletileceği ağ için yeniden paketlenmesiyle çözülmüştür. Servis sağlayıcılarına saldırı amaçlı yapılan veri bombardımanı gibi işlev ve veri kaybına neden olan uygulamalara internette sık rastlanmaktadır. Tasarlanan sistemde ağ geçidinde verilerin böyle bir saldırıda kaybedilmemesi için çözüm olarak veriler üzerinde ön bellekleme uygulanmıştır. Servis keşif problemi, ağ geçidinin kendinde, ZigBee düğümlerinde ve XMPP ağında meydana gelen değişikliklere tepki olarak servis bildirimini yayınlaması ile çözümlenmiştir. İki ağ arasındaki veri aktarım oranı farkı sebebiyle oluşabilecek veri kayıpları paketleme esnasında yapılan önbellekleme ve veri depolama işlemleriyle çözümlenmektedir. Ağlar arası haberleşmede internet kaynaklı güvenlik problemleri XMPP'de bulunan TLS ve SASL protokolleri kullanılarak giderilmektedir.

Tasarlanan sistemde XMPP, uzak ve dağınık bir ağ yapısı üzerinde gerçek zamanlı çalışmalarda yüksek başarımla sağlayan bir alt yapı teknolojisi olarak kullanılmıştır. Gerçekleştirilen ağ geçidi yazılımı ile ZigBee düğümlerine hem seri port üzerinden hem de RF sistem üzerinden yapılandırma yapılabilmektedir. XMPP teknolojisi ile özel olarak yazılmış herhangi bir yazılım gereksizdir herhangi bir XMPP sohbet programından ZigBee düğümlerine erişim sağlanabilmektedir. Projede gerçekleştirilen yazılımlar SCADA uygulamalarında ihtiyaç duyulan yapıya uygun

olarak tasarlanmıştır. Bu sayede uygulamaya görsel nitelikler kazandırılmış ve kullanıcı için kolay bir arayüz oluşturulmuştur. Oluşturulan kullanıcı yazılımı sayesinde hem ağ geçidine hem de ayrı ayrı tüm ZigBee düğümlerine komut ve mesaj gönderilebilmektedir.

Kablosuz sensör ağında kullanılacak düğümler sistem performansı açısından büyük önem arz etmektedir. ZigBee alıcı-verici modülü ve mikrodenetleyicisi ayrı ayrı iki parça şeklinde alınıp birleştirilmesi durumunda mikrodenetleyici içine gömülecek ZigBee protokol yığının iyi bilinmesi ve buna göre kontrol edilmesi gerekmektedir. Buna ek olarak ağ geçidine gönderilecek paketlerin istenildiği şekilde işlenebilmesi için bu paketlerin iyi belirlenmesi gerekmektedir. Tasarlanan sistemde kullanım kolaylığı sağlaması sebebiyle dâhili mikrodenetleyici kontrollü ZigBee modülleri (XBee) tercih edilmiştir. Kullanılan modüllerin işlem kolaylığı sağlamasının yanında sağladığı en büyük avantaj tek başlarına bir sensör düğümü olarak görev yapabilmeleridir. Yani bu modüller harici bir mikrodenetleyici birimi olmadan tek başlarına kendisine bağlı giriş ve çıkış birimlerini yönetebilmektedir. Bunun yanında isteğe bağlı olarak sisteme harici mikrodenetleyici veya mikrodenetleyiciler eklenebilmektedir. Bu sayede modül dahili mikrodenetleyicisinin sistem üzerindeki kısıtlı kontrol imkanları genişletilebilmektedir.

Şeffaf mod, modüllerin seri hat gibi davranmasını sağlayan moddur. Bu modda modül kontrolü tek tek AT komutlarıyla yapılmaktadır. Ağ geçidindeki düğüme gönderilecek komut miktarı arttıkça şeffaf modda komut satırlarının miktarı artmaktadır dolayısıyla sistem hantallaşmaktadır. API modu ise şeffaf modun geliştirilmiş halidir. API modu sayesinde birçok işlem tek bir API çerçevesiyle yerine getirilebilmektedir. Bu sebepten dolayı ağ geçidi API modunda çalışacak şekilde tasarlanmıştır. Sistem gereği ağ geçidindeki modül yalnız API modunda çalışabilmektedir. Ancak ağda bulunan diğer modüller her iki modda da çalışabilmektedir. Ayrıca ağ geçidinde paketleme algoritması çok karmaşık olmadığı için ağ geçidi yazılımında yapılacak ufak değişikliklerle ağ geçidi şeffaf modda da çalışır konuma getirilebilir.

Tezde oluşturulan sistemde XMPP teknolojisi yardımıyla video ve ses gibi büyük veriler taşınabilmektedir. Bu özellik sayesinde ileride yapılacak çalışmalar ile yüksek veri yoğunluklu uygulamaların sistemde çalışması mümkündür. Günümüzde sosyal paylaşım uygulamalarında da XMPP teknolojisi kullanılmaktadır. Bu sayede

gelecekte kablosuz sensör ağı uygulamalarının sosyal paylaşım platformlarına taşınması planlanmaktadır. Ayrıca tezde yapılan uygulamaya benzer çalışmalarda bulunmak isteyenlere sunmak amacıyla yazılan ağ geçidi programının bir kütüphane formatına getirilmesi planlanmaktadır.

KAYNAKLAR

- [1] **Labioud, H., Afifi, H., ve Santis, C.D.**, 2007, *WiFi, Bluetooth, ZigBee and WiMax*, Springer, Dordrecht, Hollanda, Sayfa:109-122.
- [2] **Kozierok, C.M.**, 2005. *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*, SanFransisco Resmi baskı yok.
- [3] **Farahani, S.**, 2008, *ZigBee Wireless Networks and Transceivers*, Newnes Elsevier, NewYork, ABD.
- [4] **Akyildiz I.F., Su W., Sankarasubramaniam Y., ve Cayirci E.**, Mart 2002, Wireless sensor networks: a survey, *Elsevier Computer Networks*, Cilt: 38, No: 4, s393-422.
- [5] **Shigeoka, I.**, 2002, *Instant Messaging in Java: The Jabber Protocols*, Manning Publications, ABD.
- [6] **Saint-Andre P.**, Nisan 2009, *XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies*, O'Reilly Media, ABD.
- [7] **Wang R.C., Chang R.S., ve Chao H.C.**, Ağustos 2007, "Internetworking between ZigBee/802.15.4 and IPv6/802.3 Network", *IPv6'07*, Kyoto, Japonya.
- [8] **K. Mayer, and W. Fritsche**, 30-31 Mayıs 2006, IP-enabled wireless sensor networks and their integration into the Internet," *ACM InterSense'06*, Nice, Fransa.
- [9] **Hossen, S., Kabir A.F.M.S., Khan R.H., ve Azfar, A.** Ocak 2010, Interconnection between 802.15.4 Devices and IPv6 Implications and Existing Approaches, *International Journal of Computer Science Issues*, Vol. 7, Issue 1, N1. 1, s19-31
- [10] **Luo X.M.W.**, Aralık 2008, The Analysis of 6LoWPAN Technology, *Pacific-Asia Workshop on Computational Intelligence and Industrial Application PACIIA'08*, Wuhan, Çin H.C.
- [11] **Sakane, S., Ishii, Y., Toba, K., Kamada, K., ve Okabe N.A.**, Ocak 2006, A translation method between 802.15.4 nodes and IPv6 nodes,

Symposium on Applications and the Internet Workshops SAINT 2006,
Phoenix-Arizona, ABD, s34-37.

[12] Digi MaxStream XBee / XBee-Pro OEM Modules Product Manual v1.xAx –
802.15.4 Protocol.

EKLER

EK-A: AT Komut Referans Tablosu

Tablo-A.1: AT referans tablosu

AT Komutu	Komut kategorisi	Açıklama	Parametre aralığı	Varsayılan
WR	Özel	Parametre değerlerini geçici olamayan hafızaya yazar		
RE	Özel	Varsayılan – fabrika ayarlarına döndürür		
FR	Özel	Yazılımı sıfırlar.		
CH	Ağ	Haberleşme kanalının ayarlanması ve okunması	0c0b-0x1a (xbee) 0x0c-0x17 (pro)	0x0c
ID	Ağ	PAN ID ayarlama ve okuma (0xffff yapılarak tüm panlara broadcast yapılabilir)	0-0xffff	0x3332 (13106d)
DH	Ağ	Hedef adresin yüksek kısmının okunup yazılması 16 bit adresleme için 0 yapılmalı	0-0xffffffff	0
DL	Ağ	Hedef adresin alçak kısmının okunup yazılması. 16 bit için broad cast 0xffff olmalı	0-0xffffffff	0
MY	Ağ	16 bit adres yazma ve okuma için. Broadcast için 0xffff 64 bit adres kullanılacağı zaman 0xfffe olmalı	0-0xffff	0
SH	Ağ	Seri numaranın yüksek kısmını okumak için		
SL	Ağ	Seri numaranın alçak kısmını okumak için		
RR	Ağ	Xbee mesaj tekrar sayısı oku yaz	0-6	0
RN	Ağ	Rastgele gecikme slotları, geri dönüş üstelini CSMA-CA oku yaz	0-3	0
MM	Ağ	MAC modu durumuna izin verme	0-2 0: maxstream 1: 802.15.4 no ACK 2: 802.15.4 with ACK	0
NI	Ağ	Düğüm ayracı	20 karakter ASCII	-
ND	Ağ	Tüm RF modülleri keşfeder ve raporlar	Seçeneğe bağlı olarak NI parametresi aratılabilir	
NT	Ağ	Düğüm keşif süresinin okunup yazılması	0x01-0xfc	0x19
DN	Ağ	Hedef düğümün NI parametresini hedef yapar	20 karakter ASCII	
CE	Ağ	Koordinatör moduna izin verme	0-1	0

Tablo-A.1: AT referans tablosu (Devamı)

SC	Ağ	Kanal taraması ayarları. 15 bit küçükten büyüğe doğru 0b, 0c, 0d, 0e, 0f, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 1a kanallarını tarar.	0-0xffff 14. ve 15. bitler pro modüllerde kullanılmaz	0x1ffe
SD	Ağ	Tarama süresini ayarlar. Son cihaz: işaretli sistemde koordinatör SD:BE olduğundan min BE olmalı	0-0xf	4
A1	Ağ	Son cihaz birleşmesi seçeneklerini ayarlar Bit 0 0 : PAN ID si ve eşleşen koordinatöre bağlanır. 1: PAN ID si herhangi bir koordinatöre bağlanır. Bit 1 0: Kanal parametresi (CH) eşleşen koordinatöre bağlanır. 1: herhangi bir kanalda çalışan cihaza bağlanır. Bit 2 0: aygıt birleşme gerçekleştirmez 1: başarılı olana kadar bir ağa bağlanmaya çalışır Bit 3 0: modül uyandığında koordinatörden kendine gelen mesaj kontrolü yapmaz. 1: uyandığında koordinatörü sorgular. Bit 4-7 kullanılmamaktadır	0x0f	0
A2	Ağ	Koordinatör birleşmesi Bit 0 0: koordinatör PAN ID tespiti için aktif tarama gerçekleştirmez. ID bilgisi eşleşen modüllerle çalışır. 1: Aktif taramayla PAN ID ler belirlenir ID çakışması olursa ID parametresi değiştirilir. Bit 1 0 : Koordinatör enerji taraması gerçekleştirmez 1: enerji taraması gerçekleştirilir ve serbest kanal bulunup orda çalışır. Bit 2 0: koordinatör herhangi bir cihazın kendisiyle birleşmesine izin vermez 1: koordinatör cihazların kendisiyle birleşmesine izin verir Bit 3-7 kullanılmamaktadır.	0-7	0

Tablo-A.1: AT referans tablosu (Devamı)

AI	Ağ	Birleşme belirtisi: birleşme sırasında oluşan hataları okur. 0x01 aktif tarama zaman aşımı 0x02 aktif taramada herhangi bir PAN bulunamadı 0x03 aktif taramada PAN bulundu fakat birleşmeye izin verilmiyor. 0x04 aktif taramayla PAN bulundu ancak koordinatör ve son cihazlar işaret desteği vermiyor 0x05 aktif taramayla PAN bulundu ancak ID parametreleri eşleşmiyor. 0x06 aktif taramayla PAN bulundu ancak kanal parametreleri eşleşmiyor. 0x07 enerji taraması zaman aşımı 0x08 koordinatör başlama isteği başarısız 0x09 koordinatör doğru parametrelerle başlayamadı 0x0a koordinatör yeniden düzenleniyor 0x0b birleşme isteği gönderilemedi 0x0c birleşme isteği zaman aşımına uğradı veya cevap alınamadı 0x0d birleşme isteğinde geçersiz parametre var 0x0e birleşme isteği kanal erişim hatası/ CCA hatası 0x0f uzak koordinatör birleşme isteğinden sonra ACK göndermedi 0x10 uzak koordinatör birleşme isteğine cevap vermedi ancak ACK gönderdi 0x12 senkronizasyon kayboldu 0x13 ağ üyeliğinden çıkıldı	0-0x13	
DA	Ağ	Üyelikten ayrılmaya zorlama. Derhal ağdan ayrıl.		
FP	Ağ	Endirek mesajların sorgulanmasını zorla		
AS	Ağ	Aktif tarama: işaret cevabını tüm ağa yayınla . Parametre her kanalı tarar. Her işaret alınışında PAN tanımlayıcı oluşur. PAN tanımlayıcıda aşağıdaki parametreler yer alır. Koordinatör adresi, koordinatör PAN ID, Koordinatör adres modu, kanla, güvenlik, ACLEntry, güvenlik hatası, super çerçeve özellikleri (15-birleşme izni, 14-PAN koordinatör,12- pil ömrü, 8-11-son CAP slotu, 4-7-super çerçeve isteği,0-3- işaret isteği) Gts izni, RSSI(sinyal seviyesi), zaman damgası	0-6	
ED	Ağ	Enerji taraması: tüm kanalların enerji seviyelerini ölçer. Her kanalın tarama uzunluğunu ayarlar	0-6	
EE	Ağ	AES şifreleme kurma	0-1	0

Tablo-A.1: AT referans tablosu (Devamı)

KY	Ağ	AES şifresi	0-(16 byte değer)	-
PL	RF Arayüz	RF modülün aldığı ve gönderdiği sinyallerin güç seviyesini okur	0-4 0: -10/10 dbm 1: -6/12 dbm 2: -4/14dbm 3: -2/16dbm 4: 0 / 18 dbm	4
CA	RF Arayüz	CCA eşiğini kurar ve okur. (okunacak en düşük enerji seviyesi)	0-0x50 [-dbm]	0x2c (-44dbm)
SM	Uyku	Uyku modu ayarlarını okuyup yazar	0-5 0: uyanık 1 : kış uykusu 2: uyuklama 4: dögüsel uyku 5: dögüsel uyku pin yandırmalı 6: koordinatör uykusu	0
ST	Uyku	Uyumadan önceki süreyi ayarlar ve okur. (SM = 4-5)	1-0xffff	0x1388
SP	Uyku	Dögüsel uyku modunun periyodunu ayarlar	0-068b0	0
DP	Uyku	Birleşmeden uyku periyodunu okur yazar	1-0x68b0	0x3e8
BD	Seri Arayüz	Seri arayüzün baud oranını okur yazar	0: 1200 bps 1: 2400 2 : 4800 3: 9600 4: 19200 5: 38400 6:57600 7:115200	3
RO	Seri Arayüz	Paketleme zaman aşım süresini okuyup yazar	0-0xff	3
AP	Seri Arayüz	API moduna izin verme	0-2 0: izinsiz 1: izinli 2: izinli kaçış kontrollü	0
PR	Seri Arayüz	Pinlerin Pull up dirençlerin kurulması Bit0: pin 11 Bit 1: pin 17 Bit 2: pin 18 Bit 3: pin 19 Bit 4: pin 20 Bit 5: pin 16 Bit 6: pin 9 Bit 7: pin 3	0xff	0xff

Tablo-A.1: AT referans tablosu (Devamı)

D(0-8)	Giriş/Çıkış	(0-8) hangi pin yazıldıysa onun görevini ayarlar / okur	0-1 0: kullanılmayacak 1: CTS/RTS/birleşme bildirimi/yok 2: ADC/ yok 3: DI 4: DO düşük/ yok 5: DO yüksek/ yok	
IU	Giriş/Çıkış	Giriş çıkış birimlerini aktifleştir/pasifleştir	0-1	1
IT	Giriş/Çıkış	İletimden önce örnekleme sayısı	1-0xff	1
IS	Giriş/Çıkış	İzinli tüm girişleri okumaya zorlar	8 bit Bitmap	
IO	Giriş/Çıkış	Sayısal çıkış seviyesi: sayısal çıkış seviyesini düşük yapar.		
IC	Giriş/Çıkış	Giriş çıkış denetimi: giriş çıkışların değişimlerini denetleme bitlerinin kurulumu	0xff	0
IR	Giriş/Çıkış	Örnek oranını kurma/ okuma	0-0xffff	0
AV	Giriş/Çıkış	ADC voltaj referansı (sadece pro modüllerde)	0-1 0: Vref pininden 1 : aralık	0
IA	Giriş/Çıkış	Giriş çıkış adresi: çıkışların bağlı olduğu modül adresini okur/yazar. Çıkışlar 0xff izinsiz/0xffff izinli	0xffffffffffffff	0xffffffffffffff
T0-T7	Giriş/Çıkış	Çıkış zaman aşımı süresinin okunması / yazılması	0xff [x100ms]	0xff
P0	Giriş/Çıkış	PWM0 ayarları.	0-2 0: yok 1:RSSI 2: PWM çıkışı	1
P1	Giriş/Çıkış	PWM1 ayarları	0-2 0: yok 1:RSSI 2: PWM çıkışı	0
M0	Giriş/Çıkış	PWM0 çıkış seviyesi	0-0x03ff	-
M1	Giriş/Çıkış	PWM1 çıkış seviyesi	0-0x03ff	
PT	Giriş/Çıkış	PWM çıkış zaman aşımı süresinin okunması/yazılması	0-0xff [x100ms]	0xff
RP	Giriş/Çıkış	RSSI PWM zamanlayıcısı. PWM zamanlayıcı kaydını akor/yazar	0xFF [x100ms]	0x28
VR	Teşhis	Versiyon bilgisi okur	0-0xffff	
VL	Teşhis	Versiyon bilgisi okur (üretim tarihi, MAC, PHY vb bilgileri)	0-0xffff	
HV	Teşhis	Donanım versiyonu	0-0xffff	
DB	Teşhis	Alınan sinyalin güç seviyesini verir	0-0x64	
EC	Teşhis	CCA hataları: CCA hata sayısını sıfırlar/okur	0-0xffff	
EA	Teşhis	ACK hataları: ACK hatalarını sıfırlar/okur	0-0xffff	

Tablo-A.1: AT referans tablosu (Devamı)

ED	Teşhis	Enerji taraması: enerji bulma taraması uzunluğunu belirler.	0-6	
CT	AT komut modu seçeneği	Komut modu zaman aşımı süresini okur/yazar	2-0xffff	0x64
CN	AT komut modu seçeneği	Komut modundan çıkma		
AC	AT komut modu seçeneği	Değişiklikleri uygula		
GT	AT komut modu seçeneği	Koruma süresi: komut dizisinden önce gerekli süreyi kurar	2-0x0ce4 [x 1ms]	0x3e8
CC	AT komut modu seçeneği	Komut dizisi karakteri	0-0xff	0x2b (“+”)

ÖZGEÇMİŞ

Ad Soyad : Ahmet Çağdaş SEÇKİN

Doğum Yeri ve Yılı : Ankara, 1985

Adres : Gültepe Mah. 4565 sok. No:5 Gümüşler /
DENİZLİ

Lisans Eğitimi ve Mezuniyet Tarihi :Süleyman Demirel Üniversitesi Elektronik ve
Haberleşme Mühendisliği, 2008

Çalıştığı Kurum :Uşak Üniversitesi