

**BLUETOOTH KABLOSUZ HABERLEŞME
TEKNOLOJİSİ VE KULLANIM ALANI ÖRNEKLERİ**

**YÜKSEK LİSANS TEZİ
Müh. Hande ERKOÇ
(504961415)**

**Tezin Enstitüye Verildiği Tarih : 24 Aralık 2002
Tezin Savunulduğu Tarih : 17 Ocak 2003**

**Tez Danışmanı : Prof.Dr. Günsel DURUSOY
Diğer Jüri Üyeleri Doç.Dr. Tamer ÖLMEZ
Yrd.Doç.Dr. Demir ÖNER (İ.Ü.)**

OCAK 2003

ÖNSÖZ

Yeni nesil mobil teknolojiler konusunda çalışmam için beni yönlendiren ve yüksek lisans tez konum olan Bluetooth teknolojisi üzerine yaptığım çalışma boyunca benden desteklerini esirgemeyen sayın danışmanım Prof.Dr.Günsel Durusoy'a, hayatımın her döneminde beni daima destekleyen sevgili anneme, babama ve kardeşime, tez hazırlama sürecimdeki özverili katkılarından dolayı müstakbel eşim Erkut Uzun'a sonsuz teşekkür ederim.

Ocak, 2003

Hande Erkoç

İÇİNDEKİLER

KISALTMALAR.....	xi
TABLO LİSTESİ.....	xiv
ŞEKİL LİSTESİ.....	xv
ÖZET.....	xvii
SUMMARY.....	xix
1. GİRİŞ.....	1
2. GENİŞ BANTLI KABLOSUZ HABERLEŞME TEKNOLOJİLERİ.....	3
2.1 Lisanslanmamış Bölgede Çalışan Kablosuz Ağlar.....	3
2.1.1 IEEE 802.11b.....	4
2.1.2 Açık hava (Open Air).....	4
2.1.3 EvRF (HomeRF).....	5
2.1.4 Bluetooth.....	5
2.1.5 HiperLAN.....	6
2.2 Bluetooth Kablosuz Haberleşme Teknolojisine Giriş.....	6
2.2.1 2.4 GHz. Frekans Spektrumunda RF Haberleşmesi.....	6
2.2.2 RF Haberleşmesinde Saçılmış (Spread) Spektrum.....	8
2.2.3 Yönetici-Köle (Master-Slave) Roller.....	9
2.2.4 Temelbant Modları ve Enerji-Korumalı Özellikler.....	10
2.2.5 Bağlantı Kurulumları.....	12
2.2.6 Haberleşme Topolojileri.....	14
3. BLUETOOTH RADYO SPESİFİKASYONU.....	17
3.1 Frekans Bantları ve Kanal Düzenlemesi.....	17
3.2 Verici Karakteristikleri	17
3.2.1 Modülasyon Karakteristikleri.....	18
3.2.2 Sahte Yayınlar.....	19
3.2.2.1 Bant-İçi Sahte Yayınım.....	19
3.2.2.2 Bant-Dışı Sahte Yayınım.....	20
3.2.3 Radyo Frekans Toleransı.....	20
3.3 Alıcı Karakteristikleri.....	21
3.3.1 Gerçek Duyarlık Derecesi.....	21

3.3.2 Girişim Performansı.....	21
3.3.3 Bant-Dışı Bloklama.....	22
3.3.4 Intermodülasyon Karakteristikleri.....	22
3.3.5 Maksimum Elverişli Seviyeler.....	23
3.3.6 Sahte Emisyonlar.....	23
3.3.7 Alıcının İşaret Güç İndikatörü (Seçime Bağlı).....	23
3.3.8 Referans İşaret Tanımlaması.....	24
4. BLUETOOTH PROTOKOL MİMARİSİ.....	25
4.1 Giriş.....	25
4.1.1 Protokol Tanımı.....	25
4.1.2 Bluetooth Protokol Mimarisi.....	26
4.1.3 Bluetooth Protokol Yığınındaki Protokoller.....	27
4.1.3.1 Bluetooth Ana Protokolleri.....	28
4.1.3.2 Kablo Yerine Geçen Protokol.....	30
4.1.3.3 Telefon Kontrol Protokolü.....	30
4.1.3.4 Uyarlanmış Protokoller.....	31
4.2 Temelbant Protokolü.....	33
4.2.1 Giriş.....	33
4.2.2 Fiziksel Kanal.....	33
4.2.2.1 Kanal Tanımlaması.....	33
4.2.2.2 Zaman Slotları.....	34
4.2.3 Fiziksel Linkler.....	35
4.2.3.1 SCO Linki.....	35
4.2.3.2 ACL Linki.....	36
4.2.4 Paketler.....	37
4.2.4.1 Genel Format.....	37
4.2.4.2 Erişim Kodu.....	38
4.2.4.3 Paket Başlığı.....	40
4.2.4.4 Taşınan Bilgi (Payload).....	43
4.2.4.5 Paket Tipleri.....	43
4.2.5 Hata Düzeltme.....	49
4.2.5.1 FEC Kodu: 1/3 Hızlı.....	50
4.2.5.2 FEC Kodu: 2/3 Hızlı.....	50
4.2.5.3 ARQ Algoritması.....	50
4.2.5.4 Hata Kontrolü.....	51
4.2.6 Konuşma Kodlama.....	52
4.2.6.1 CVSD Konuşma Kodlama Tekniği.....	52
4.2.6.2 LogPCM Konuşma Kodlama Tekniği.....	53
4.2.7 Veri Beyazlatma.....	53
4.2.8 Doğrulama ve Şifreleme.....	53
4.2.9 Lojik Kanal Tanımlaması.....	54
4.2.9.1 Giriş.....	54
4.2.9.2 Link Kontrol (LC) Kanalı.....	55
4.2.9.3 Link Yöneticisi (LM) Kanalı.....	55
4.2.9.4 Kullanıcı Kontrol (UC) Kanalı.....	55

4.2.9.5 Kullanıcı Asenkron Veri (UA) Kanalı.....	55
4.2.9.6 Kullanıcı Isonkron Veri (UI) Kanalı.....	55
4.2.9.7 Kullanıcı Senkron Veri (US) Kanalı.....	55
4.2.9.8 Kanal Adresleme.....	55
4.2.10 İşlemsel Prosedürler.....	56
4.2.10.1 Sorgu Prosedürü.....	56
4.2.10.2 Bağlantı Kurulum Prosedürü.....	56
4.2.11 Güç Yönetimi.....	57
4.2.11.1 Giriş.....	57
4.2.11.2 Alınan Paket Prosesi.....	58
4.2.11.3 Çağrı (Page)/Sorgu Durumu.....	58
4.2.11.4 Bekleme (standby) Durumu.....	58
4.2.11.5 Aktif Yönetici Durumu.....	59
4.2.11.6 Aktif Köle Durumu.....	59
4.2.12 Kimlikler.....	60
4.2.12.1 Bluetooth Adresleri.....	60
4.2.12.2 Erişim Kodları.....	60
4.2.12.3 MAC Adresi	61
4.2.13 Pikonet İçi Bağlantılar.....	62
4.2.13.1 Yönetici-Köle Bağlaşması.....	63
4.2.14 Bluetooth Saati.....	64
4.2.15 Güç Tüketimi.....	65
4.2.15.1 Güç Tüketimini Azaltmak.....	66
4.2.15.2 Düşük Veri Hızları.....	66
4.3 Link Yönetim Protokolü.....	67
4.3.1 PDU Tipleri.....	69
4.3.2 Genel Cevap Mesajları.....	69
4.3.3 Doğrulama.....	69
4.3.4 Çiftleme (Pairing).....	70
4.3.5 Link Anahtarının Değişmesi.....	71
4.3.6 Mevcut Link Anahtarının Değişmesi.....	72
4.3.7 Şifreleme.....	72
4.3.8 Saat Ofset Talebi.....	74
4.3.9 Zaman Aralığı (Slot) Ofset Bilgisi.....	74
4.3.10 Zamanlama Doğruluk Bilgisi Talebi.....	74
4.3.11 LMP Versiyonu.....	75
4.3.12 Desteklenen Özellikler.....	76
4.3.13 Yönetici-Köle Roller Değişimi.....	76
4.3.14 İsim İsteği.....	76
4.3.15 Bağlantı Bitişi.....	77
4.3.16 Durağan Mod.....	77
4.3.17 Koklama Modu.....	77
4.3.18 Park Modu.....	78
4.3.19 Güç Kontrolü.....	79
4.3.20 Kanal Kalitesi Temelli Veri Hızı Değişimi.....	80
4.3.21 Servis Kalitesi (Quality of Service-QoS).....	80
4.3.22 SCO Linkleri.....	80
4.3.23 Çok Slotlu Paketlerin Kontrolü.....	82

4.3.24 Çaęrı Yapma (Paging) Planı.....	82
4.3.25 Link Denetimi.....	83
4.3.26 Baęlantı Kurulumu.....	83
4.3.27 Test Modları.....	83
4.3.28 Hatanın İřleniři.....	84
4.3.29 Özet.....	85
4.4 Lojik Link Kontrolü ve Adaptasyon Protokolü (L2CAP).....	85
4.4.1 L2CAP Fonksiyonları.....	87
4.4.2 Temel Çalışma.....	88
4.4.2.1 Kanal Tanımlayıcıları.....	89
4.4.2.2 Ayırıştırma ve Tekrar Birleřtirme.....	89
4.4.3 Durum Makinesi.....	91
4.4.3.1 Olaylar.....	92
4.4.3.2 Hareketler.....	96
4.4.3.3 Kanal Çalışma Durumları.....	98
4.4.4 Veri Paket Formatı.....	99
4.4.4.1 Baęlantı Yönelimli Kanallar.....	100
4.4.4.2 Baęlantısız Veri Kanalı.....	100
4.4.5 İřaretleřme.....	101
4.4.5.1 Paket Yapısı.....	102
4.4.5.2 İřaretleřme Komutları.....	102
4.4.6 Konfigürasyon Parametre Opsiyonları.....	104
4.4.6.1 Paket Yapısı.....	105
4.4.6.2 Opsiyonlar.....	105
4.4.6.3 Konfigürasyon Prosesi.....	106
4.4.7 Servis Primitifleri.....	107
4.4.7.1 Olay Göstergesi.....	107
4.4.7.2 Baęlantı.....	108
4.4.7.3 Baęlantı Cevabı.....	108
4.4.7.4 Konfigüre.....	108
4.4.7.5 Konfigürasyon Cevabı.....	108
4.4.7.6 Baęlantı Sonlanma.....	108
4.4.7.7 Yazma.....	109
4.4.7.8 Okuma.....	109
4.4.7.9 Grup Yaratılması.....	109
4.4.7.10 Grup Kapatılması.....	109
4.4.7.11 Gruba Üye Ekleme.....	109
4.4.7.12 Gruptan Üye Çıkarmak.....	109
4.4.7.13 Grup Üyelięi Alma.....	109
4.4.7.14 Ping.....	110
4.4.7.15 Bilgi Alma.....	110
4.4.7.16 Baęlantısız Trafik Olanaksız Kılınması.....	110
4.4.7.17 Baęlantısız Trafik Olanaklı Kılınması.....	110
4.4.8 Özet.....	110
4.5 Servis Keřif Protokolü (SDP).....	111
4.5.1 SDP Geliřimi.....	112

4.5.2 SDP Temel Özellikleri.....	113
4.5.3 SDP Kullanımı.....	117
4.6 RFCOMM.....	119
4.6.1 RFCOMM Protokol Gelişimi.....	120
4.6.2 RFCOMM Protokol Özellikleri.....	121
4.7 IrDA Uyumluluğu.....	124
4.7.1 Giriş.....	124
4.7.1.1 OBEX ve Bluetooth Mimari Yapısı.....	125
4.7.1.2 Bluetooth OBEX ile İlişkili Spesifikasyonlar.....	126
4.7.1.3 Diğer IrOBEX Uygulamaları.....	127
4.7.2 OBEX Objesi ve Protokolü.....	127
4.7.2.1 Obje.....	127
4.7.2.2 Oturum Protokolü.....	128
4.7.3 RFCOMM Üzerinde OBEX.....	130
4.7.3.1 RFCOMM Üzerinde OBEX Sunucu Başlangıcı.....	131
4.7.3.2 Seri Porttan OBEX Paketlerini Almak.....	131
4.7.3.3 Bağlantının Kurulması.....	132
4.7.3.4 Bağlantının Çözülmesi.....	132
4.7.3.5 RFCOMM Üzerinden OBEX Paketlerini İtmek ve Çekmek.....	132
4.7.4 TCP/IP Üzerinden OBEX.....	132
4.7.4.1 TCP/IP Üzerinde OBEX Sunucu Başlangıcı.....	133
4.7.4.2 Bağlantının Kurulması.....	133
4.7.4.3 Bağlantının Çözülmesi.....	133
4.7.4.4 TCP Üzerinden OBEX Paketlerini İtmek ve Çekmek.....	134
4.7.5 OBEX Kullanan Bluetooth Uygulama Profilleri.....	134
4.7.5.1 Senkronizasyon.....	134
4.7.5.2 Dosya Transferi.....	135
4.7.5.3 Obje İtme.....	135
4.7.6 IrDA ve Bluetooth.....	135
4.7.6.1 IrDA ye Genel Bakış.....	135
4.7.6.2 Bluetooth'a Genel Bakış.....	137
4.7.6.3 IrDA ve Bluetooth Uygulama Kesişmesi.....	138
4.8 Ses ve Telefon Kontrolü.....	142
4.8.1 Ses ve Telefon Kontrol İşleyişi.....	143
4.8.1.1 TCS Protokol Gelişimi.....	144
4.8.2 TCS Protokolü.....	145
4.8.2.1 TCS Çağırma (Call) Kontrolü.....	145
4.8.2.2 TCS Grup Yönetimi.....	145
4.8.2.3 Bağlantısız TCS.....	147
4.8.3 Bluetooth Ses Özellikleri Gelişimi.....	147
4.8.3.1 Bluetooth Ses İncelemesi.....	148
4.8.3.2 Ses ve Telefon Kontrol Kullanımı.....	148

4.9 Host Kontrolör Arayüzü (Host Controller Interface (HCI)).....	149
4.9.1 HCI_PDU Paket Sınıfları.....	151
4.9.2 HCI_PDU ları.....	154
4.9.2.1 Link Kontrol HCI_PDU ları.....	155
4.9.2.2 Link İlke (Policy) HCI_PDU ları.....	156
4.9.2.3 Host Kontrolör ve Temelbant HCI_PDU ları.....	156
4.9.2.4 Bilgi Parametreleri HCI_PDU ları.....	156
4.9.2.5 Durum Parametreleri HCI_PDU ları.....	157
4.9.2.6 Test amaçlı HCI_PDU ları.....	157
5. BLUETOOTH GÜVENLİK MİMARİSİ.....	158
5.1 Giriş.....	158
5.2 Fonksiyonlar ve Sınırlamalar.....	158
5.2.1 Güvenlik Kademeleri.....	158
5.2.2 Esneklik ve Kullanılabilirlik.....	159
5.2.3 Gerçekleştirme ve Bluetooth'a Özel Sorunlar.....	160
5.2.4 Riskler ve Kısıtlamalar.....	160
5.3 Gereksinimleri Karşılacak Güvenlik Mimarisi.....	161
5.3.1 Genel Bakış.....	162
5.3.2 Güvenlik Kademeleri.....	163
5.3.2.1 Doğrulama ve Yetkilendirme.....	163
5.3.2.2 Cihaz Güvenlik Derecesi.....	164
5.3.2.3 Servislerin Güvenlik Dereceleri.....	164
5.3.3 Bağlantı Kurulum Prosedürü.....	165
5.3.3.1 Genel Kavramlar.....	165
5.3.3.2 Temelbant Bağlantı Linki Kurulumunda Doğrulama.....	166
5.3.3.3 Protokol Yığını İşlenmesi.....	166
5.3.3.4 Kayıt Prosedürleri.....	168
5.3.3.5 Harici Anahtar Yönetimi.....	169
5.3.4 Erişim Kontrol Prosedürleri.....	169
5.3.5 Bağlantısız L2CAP.....	172
5.4 Güvenlik Yöneticisinin Arayüzü ve Fonksiyonları.....	173
5.4.1 Veri Tabanları.....	173
5.4.1.1 Servis Veri Tabanı.....	173
5.4.1.2 Cihaz Veri Tabanı.....	174
5.4.1.3 Geçici Depolama.....	174
5.4.2 L2CAP Arayüzü.....	175
5.4.3 Diğer Çoğullama (multiplexing) Protokolleri Arayüzü.....	175
5.4.4 ESCE Arayüzü.....	176
5.4.5 Kayıt Prosedürleri.....	177
5.4.6 HCI / Link Yöneticisi Arayüzü.....	177
5.4.6.1 Doğrulama Talebi.....	177

5.4.6.2 Şifreleme Kontrolü.....	178
5.4.6.3 Uzak Cihazdan İsim İsteme.....	178
5.4.6.4 Link Katmanında Şifreleme Politikası Ayarı.....	178
5.4.6.5 Link Katmanında Doğrulama Politikası Belirleme.....	178
6. BLUETOOTH PROFİLLERİ.....	179
6.1 Bluetooth Genel Profilleri.....	181
6.1.1 Genel Erişim Profili.....	181
6.1.1.1 Genel Parametreler.....	182
6.1.1.2 Boş Mod Prosedürleri.....	185
6.1.1.3 Bağ Kurma (Bonding).....	186
6.1.1.4 Kuruluş Prosedürleri.....	187
6.1.2 Seri Port Profili.....	189
6.1.2.1 Uygulama Seviyesi Prosedürleri.....	190
6.1.2.2 Güç Korunumu ve Kayıp Link Durumu.....	192
6.1.2.3 RS-232 Kontrol İşaretleri.....	192
6.1.2.4 L2CAP Uygunluk Gereksinimleri.....	193
6.1.2.5 SDP Uygunluk Gereksinimleri.....	194
6.1.2.6 Link Yöneticisi Uygunluk Gereksinimleri.....	194
6.1.3 Servis Keşif Uygulama Profili.....	195
6.1.3.1 İstemci ve Sunucu Roller.....	196
6.1.3.2 Çiftleme (Pairing).....	198
6.1.3.3 Servis Keşif Uygulaması.....	198
6.1.3.4 Mesaj Dizisi.....	199
6.1.3.5 Servis Keşfi.....	200
6.1.3.6 İşaretleşme.....	200
6.1.3.7 Konfigürasyon Seçenekleri.....	200
6.1.3.8 SDP Hareketleri (Transaction) ve L2CAP Bağlantıları.....	202
6.1.3.9 Link Yöneticisi.....	203
6.1.3.10 Link Kontrolü.....	204
6.1.4 Genel Obje Değiş-Tokuş Profili (Generic Object Exchange Profile-GOEP).....	205
6.1.4.1 Profil Yığını.....	205
6.1.4.2 Sunucu ve İstemci.....	206
6.1.4.3 Profil Temelleri.....	206
6.1.4.4 Özellikler.....	207
6.1.5 Özet.....	210
7. BLUETOOTH KULLANIM MODELLERİ.....	212
7.1 Kablosuz Bilgisayar.....	212
7.2 Mikrofon-Kulaklık Seti.....	212
7.3 Bir Telefonda Üç Kullanım (Three-in-One Telefon).....	213
7.4 Dosya Transferi.....	214

7.5 İnternet Köprüsü.....	215
7.5.1 Çevirmeli Ağlar.....	215
7.5.2 Direkt Ağ Erişimi.....	216
7.5.3 LAN Erişimi.....	216
7.6 Konuşan Laptop.....	216
7.7 Otomatik Senkronizasyon.....	217
7.8 Kartpostal.....	218
7.9 Anlık (Ad Hoc) Ağlar.....	218
7.10 Gizli Hesaplama.....	219
8. BLUETOOTH’UN GLOBAL 3G SİSTEMİ İÇİNDEKİ YERİ.....	220
8.1 Global 3G Girişimi.....	220
8.1.1 Standartların Geliştirilmesi.....	220
8.1.2 IMT-2000 in Amaçları.....	221
8.1.3 Evrensel Mobil Haberleşme Sistemi (Universal Mobile Telecommunications System-UMTS)	222
8.2 Bluetooth’un Rolü.....	227
8.3 Özet.....	229
9. SONUÇLAR VE TARTIŞMA.....	230
KAYNAKLAR.....	234
ÖZGEÇMİŞ.....	236

KISALTMALAR

3G	: Third Generation
ACK	: Acknowledge
ACL	: Asynchronous Connectionless
AM_ADDR	: Active Member Address
ARQ	: Automatic Repeat Request
BCH	: Bose, Chaudhuri & Hocquenghem (bir kod tipi; bu kod tipini bulan kişilerin ismi verilmiştir)
BD_ADDR	: Bluetooth Device Address
BER	: Bit Error Rate
BPM	: Bluetooth Piconet Minder
CAC	: Channel Access Code
CBR	: Constant Bit-Rate
CCF	: Call Control Function
CDMA	: Code Division Multiple Access
CID	: Channel Identifier
CO	: Connection-Oriented
CRC	: Cyclic Redundancy Check
CTS	: Clear to Send
CVSD	: Continuous Variable Slope Delta Modulation
DAC	: Device Access Code
DCE	: Data Communications Equipment
DECT	: Digital Enhanced Cordless Telephone
DH	: Data-High Rate
DIAC	: Dedicated Inquiry Access Code
DLCI	: Data Link Connection Identifier
DM	: Data-Medium Rate
DSL	: Digital Subscriber Line
DTE	: Data Terminal Equipment
DTR	: Data Terminal Ready
DTS	: Data Set Ready
E1	: Avrupa’da kullanılan veri haberleşmesi standardı
EDGE	: Enhanced Data GSM Evolution
ESCE	: External Security Control Entity
ETSI	: European Telecommunications Standards Institute
FCC	: Federal Communications Commission
FCOFF	: Flow Control Off
FCON	: Flow Control On
FEC	: Forward Error Correction
FH	: Frequency Hopping
FHS	: Frequency Hop Synchronization
FHSS	: Frequency Hopping Spread Spectrum
FM	: Frequency Modulation
FTP	: File Transfer Protocol

GAP	: General Access Profile
GFSK	: Gaussian Frequency Shift Keying
GIAC	: General Inquiry Access Code
GOEP	: Generic Object Exchange Profile
GPRS	: General Packet Radio Service
GRPR	: Golden Receive Power Range
GSM	: Global System for Mobile Communications
HCI	: Host Controller Interface
HEC	: Header-Error-Check
HRFWG	: HomeRF Working Group
HSCSD	: High Speed Circuit Switched Data
HTTP	: Hyper Text Transfer Protocol
IAC	: Inquiry Access Code
IANA	: Internet Assigned Numbers Authority
IEC	: International Electrotechnical Commission
IEEE	: Institute of Electronic and Electrical Engineering
IETF	: Internet Engineering Task Force
IMT-2000	: International Mobile Telecommunications 2000
IR	: Infrared
IrDA	: Infrared Data Association
IrMC	: Infrared for Mobile Communications
ISDN	: Integrated Services Digital Network
ISM	: Industrial, Scientific, Medicine
ISO	: International Organization for Standardization
L2CA	: Logical Link Control and Adaptation
L2CAP	: Logical Link Control and Adaptation Protocol
LAN	: Local Area Network
LAP	: Lower Address Part
LC	: Link Controller
LIAC	: Limited Inquiry Access
LM	: Link Manager
LMP	: Link Manager Protocol
LocDev	: Local Device
LPO	: Low Power Oscillator
LSB	: Least Significant Bit
MSB	: Most Significant Bit
MSC	: Modem Status Command
MTU	: Maximum Transmission Unit
NAK	: Negative Acknowledge
NAP	: Non-Significant Address Part
OBEX	: Object Exchange Protocol
OCF	: Opcode Command Field
OGF	: Opcode Group Field
OSI	: Open Systems Interconnection
PAN	: Personal Area Network
PCM	: Pulse Coded Modulation
PDA	: Personal Digital Assistant
PDU	: Protocol Data Unit
PIN	: Personal Identification Number
PM_ADDR	: Parked Member Address

PPP	: Point-to-Point Protocol
PSM	: Protocol/Service Multiplexer
PSTN	: Public Switched Telephone Network
QoS	: Quality of Service
RemDev	: Remote Device
RF	: Radio Frequency
RSSI	: Received Signal Strength Indication
RTCON	: Real-time Transfer Control Protocol
RTS	: Request to Send
RTT	: Radio Transmission Technology
SAR	: Segmentation and Reassembly
SCF	: Service Control Function
SCO	: Synchronous Connection-Oriented
SDAP	: Service Discovery Application Profile
SDF	: Service Data Function
SDMA	: Space Division Multiple Access
SDP	: Service Discovery Protocol
SIG	: Bluetooth Special Interest Group
SPP	: Serial Port Profile
SSF	: Service Switching Function
SWAP	: Shared Wireless Access Protocol
TCP/IP	: Transmission Control Protocol/Internet Protocol
TCS	: Telephony Control Protocol Specification
TD-CDMA	: Time Division CDMA
TDD	: Time Division Duplex
TDMA	: Time Division Multiple Access
TMN	: Telecommunications Management Network
UA	: User Asynchronous
UAP	: Upper Address Part
UC	: User Control
UI	: User Isochronous
UMTS	: Universal Mobile Telecommunications System
UNII	: Unlicensed National Information Infrastructure
US	: User Synchronous
UTRA	: UMTS Terrestrial Radio Access
UUID	: Universal Unique Identifier
W-CDMA	: Wideband CDMA
WAE	: WAP Application Environment
WAN	: Wide Area Network
WAP	: Wireless Application Protocol
WECA	: The Wireless Ethernet Compatibility Alliance
WEP	: Wired Equivalent Privacy
WLAN	: Wireless Local Area Networks
WLIF	: Wireless LAN Interoperability Forum
WML	: Wireless Markup Language
WRC	: World Radio Conference
WRC 2000	: World Radio Conference 2000
WTA	: Wireless Telephony API
WUG	: Wireless User Group
XON/XOFF	: Transmitter On / Transmitter Off

TABLO LİSTESİ

Sayfa No

Tablo 2.1 Lisanlanmamış bölgede çalışan kablosuz ağ teknolojileri.....	3
Tablo 3.1 Çalışılan frekans bantları.....	17
Tablo 3.2 Emniyet bantları.....	17
Tablo 3.3 Güç sınıfları.....	18
Tablo 3.4 Transfer spektrum maskesi.....	19
Tablo 3.5 Bir paketteki frekans kayması.....	20
Tablo 3.6 Girişim performansı.....	21
Tablo 3.7 Bant-dışı bloklama gereksinimleri.....	22
Tablo 3.8 Bant-dışı sahte emisyonlar.....	23
Tablo 4.1 Bluetooth protokol yığınındaki protokol ve katmanlar.....	28
Tablo 4.2 Erişim kodları özeti.....	39
Tablo 4.3 SCO ve ACL link tipleri için tanımlanan paketler.....	44
Tablo 4.4 FHS paket içeriği.....	46
Tablo 4.5 Doğrulama ve şifreleme prosedürlerinde kullanılan nesneler.....	54
Tablo 4.6 LMP_Compld parametre kodları.....	75
Tablo 4.7 OBEX oturumu bağlantı talep formatı.....	128
Tablo 4.8 OBEX oturumu bağlantı cevap formatı.....	128
Tablo 4.9 OBEX oturumu bağlantı sonu talep formatı.....	129
Tablo 4.10 OBEX oturumu bağlantı sonu cevap formatı.....	129
Tablo 4.11 OBEX oturumu yerleştirme talep formatı.....	129
Tablo 4.12 OBEX oturumu yerleştirme cevap formatı.....	130
Tablo 4.13 OBEX oturumu alma talep formatı.....	130
Tablo 4.14 OBEX oturumu alma cevap formatı.....	130
Tablo 5.1 Servis veri tabanı güvenlik ile ilgili girişleri.....	174
Tablo 5.2 Cihaz veri tabanı.....	174

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1 Piconette yönetici ve köle rolleri.....	10
Şekil 2.2 Modların hassasiyet ve güç tüketimleri arasındaki ilişki.....	12
Şekil 2.3 Bağlantı prosesi.....	14
Şekil 2.4 Genel Bluetooth piconet yapısı.....	16
Şekil 2.5 Saçılmış ağ (scatternet) örneği.....	16
Şekil 3.1 Transfer modülasyonu.....	19
Şekil 3.2 RSSI dinamik aralık.....	23
Şekil 4.1 Bluetooth protokol yığını.....	27
Şekil 4.2 WAP çalışma şekli protokol yapısı.....	32
Şekil 4.3 Bluetooth sistemindeki fonksiyonel bloklar.....	33
Şekil 4.4 TDD ve zamanlama.....	34
Şekil 4.5 Çok slotlu paketler.....	35
Şekil 4.6 Standart paket formatı.....	37
Şekil 4.7 Erişim kodu formatı.....	38
Şekil 4.8 Başlangıç bilgisi.....	39
Şekil 4.9 CAC daki art bilgi (trailer). Senkronizasyon sözcüğünün MSB si 0 iken (a), ve 1 iken (b).....	40
Şekil 4.10 Başlık formatı.....	41
Şekil 4.11 HEC oluşumu ve kontrolü.....	43
Şekil 4.12 Paket tanımlaması.....	43
Şekil 4.13 FHS taşınan bilgi (payload) formatı.....	46
Şekil 4.14 CRC oluşturulması ve kontrolü.....	52
Şekil 4.15 “Hecese sıkıştırma” içeren CVSD kodlayıcının blok diyagramı.....	52
Şekil 4.16 “Hecese sıkıştırma” içeren CVSD kod çözücünün blok diyagramı.....	53
Şekil 4.17 Toplayıcı prosedürü.....	53
Şekil 4.18 Sorgu prosedürü.....	56
Şekil 4.19 İlk bağlantıda mesajlaşma.....	57
Şekil 4.20 Bekleme (standby) durumu, dinleme dizisi.....	59
Şekil 4.21 İki piconete dahil olan köle.....	63
Şekil 4.22 Kölenin iki piconete katılma zamanlaması.....	63
Şekil 4.23 Bluetooth saati.....	65
Şekil 4.24 İki cihaz arasında Link Yönetim Protokolü ile link kurulumu.....	68
Şekil 4.25 L2CAP in Bluetooth protokol mimarisindeki yeri.....	86
Şekil 4.26 L2CAP in Bluetooth protokol mimarisindeki diğer protokollerle ilişkisi.....	87
Şekil 4.27 Cihazlar arasında L2CAP tarafından belirlenen kanallar.....	90
Şekil 4.28 L2CAP etkileşimleri.....	91
Şekil 4.29 Farklı katmanların etkileşimini gösteren mesaj dizisi planı.....	93
Şekil 4.30 L2CAP paket formatı.....	100
Şekil 4.31 Grup yönelimli veri haberleşmesi için kullanılan bağlantısız paketler..	101

Şekil 4.32 Uzak cihazlardaki iki L2CAP varlığı arasında iletilen işaretleşme komutları formatı.....	102
Şekil 4.33 Konfigürasyon opsiyon paketi formatı.....	105
Şekil 4.34 SDP servis kaydının genel yapısı.....	114
Şekil 4.35 SDP iletimleri.....	118
Şekil 4.36 L2CAP üzerinde RFCOMM kullanan çoğullanmış seri haberleşme linkleri.....	122
Şekil 4.37 Bluetooth protokol yapısında OBEX protokolünün yeri.....	125
Şekil 4.38 Protokol yığınındaki ses ve TCS-BIN katmanları ile AT Komut Telefon Kontrol bileşeni.....	143
Şekil 4.39 Bluetooth referans modeli.....	150
Şekil 4.40 HCI içeren bir protokol yığını.....	152
Şekil 4.41 HCI_PDU sınıfları.....	153
Şekil 5.1 Bluetooth güvenlik mimarisi.....	163
Şekil 5.2 Güvenilir servise erişim için gereken bilgi akışı.....	165
Şekil 5.3 Gelen bağlantılar için protokollerin davranışı.....	167
Şekil 5.4 Giden bağlantılar için protokollerin davranışı.....	168
Şekil 5.5 Kayıt prosesleri.....	168
Şekil 5.6 Link Yöneticisi tarafından yapılan erişim kontrolü için örnek akış diyagramı.....	170
Şekil 5.7 Doğrulama prosedürü için örnek akış diyagramı.....	171
Şekil 5.8 Yetkilendirme prosedürü için örnek akış diyagramı.....	172
Şekil 6.1 Protokol yığını ilişkilerine göre sınıflandırılmış Bluetooth profilleri.....	180
Şekil 6.2 Servis tabanlı sınıflandırılmış Bluetooth profilleri.....	180
Şekil 6.3 Genel Erişim Profili'nin diğer Bluetooth profilleri ve kullanım modelleri ile ilişkisi.....	183
Şekil 6.4 Emüle edilmiş bir seri kablo bağlantısı için protokol modeli.....	190
Şekil 6.5 Servis Keşif Profili'nin içerdiği Bluetooth protokol yığını.....	197
Şekil 6.6 Servis Keşif Profili'ni destekleyen Bluetooth prosesleri.....	201
Şekil 6.7 Genel Obje Değiş-Tokuş Profili için protokol modeli.....	206
Şekil 6.8 Bir OBEX oturumunun doğrulama olmaksızın Connect operasyonu kullanılarak gerçekleştirilmesi.....	209
Şekil 6.9 Bir OBEX oturumunun doğrulama yapılarak gerçekleştirilmesi.....	210
Şekil 7.1 Mikrofon-kulaklık seti protokol yığını.....	213
Şekil 7.2 Telsiz telefon ve intercom kullanım modelleri protokol yığını.....	214
Şekil 7.3 Dosya transferi kullanım modeli protokol yığını.....	214
Şekil 7.4 Çevirmeli ağ kullanım modeli protokol yığını.....	215
Şekil 7.5 LAN erişimi kullanım modeli protokol yığını.....	216
Şekil 7.6 Senkronizasyon kullanım modeli protokol yığını.....	218

BLUETOOTH KABLOSUZ HABERLEŞME TEKNOLOJİSİ ve KULLANIM ALANI ÖRNEKLERİ

ÖZET

Günümüzde haberleşme alanında kullanılan cihazlar hızla çeşitlenmekte ve sayıları da günden güne artmaktadır. Buna paralel olarak bu cihazların birbirleri ile haberleşme yöntemlerinin nasıl olacağı konusu önem kazanmaktadır. Bu problemi gidermek için en çok kullanılan yöntemler cihazları birbirine kablo ile bağlamak veya bağlantıyı kızıl ötesi ışın kullanarak gerçekleştirmektir.

Kablo çözümü, bağlanacak cihazların tipine göre özelleştirilmiş kablo ve konfigürasyon yazılımı gerektirdiği için çoğunlukla zordur. Kızıl ötesi çözümü, kablo problemini elimine etmekle birlikte, ışık görüş çizgisi kısıtlaması içerir. Bluetooth teknolojisi tüm bu problemleri çözmek için geliştirilmiştir.

Bluetooth, sabit ve mobil cihazlar arasındaki iletişimde kablolarla duyulan ihtiyacı ortadan kaldıran, veri ve ses iletişimini kolaylaştıran global bir standarttır. Birçok şirketin ortak çalışması sonucu; düşük maliyetli, basit ve düşük güç tüketimli bir çözüm olarak 1999 yılının Aralık ayında piyasaya sunulmuştur.

Bluetooth ile özel amaçlı iletişim ağlarının kurulması ve tüm kişisel cihazlar arasında senkronizasyonun kablosuz bir şekilde sağlanması çok kolaydır. Bluetooth teknolojisi sadece donanım değil aynı zamanda yazılım ve birlikte çalışabilirlik gereksinimlerini de kapsar. Ayrıca Bluetooth'un kabul gördüğü tek sektör telekom sektörü değildir. Bilgisayar, ev elektroniği, otomotiv, sağlık ve daha pek çok farklı sektör, Bluetooth çözümlerine büyük ilgi göstermektedir.

Bluetooth spesifikasyonu, bir kısa (10 metre civarında) ve bir de opsiyonel olarak orta mesafeli (100 metre civarında) olmak üzere iki radyo bağlantısı tanımlar. Bu bağlantı üzerinden kanal başına maksimum 720 kbit/sn. lik veri ve ses iletişimi yapılabilir.

Bluetooth 2.40-2.48 GHz. ISM (Industrial, Scientific, Medical - Endüstriyel, Bilimsel, Tıbbi) bandında çalışır. Saçılmış bir spektrum, frekans atlama tekniği ve saniyede maksimum 1600 atlamaya izin veren tam dupleks bir yapı kullanılır. Gürültünün etkisi, haberleşme işaretinin 1 MHz. lik aralıklarda bulunan 79 frekans arasında atlamalar yapması sayesinde azaltılır. RF verimi, 10 metre mesafeli versiyonda 0 dBm (1 mW), daha uzun mesafeli versiyonda ise -30 ilâ +20 dBm (100 mW) olarak belirlenir.

Bluetooth ile, günümüzde birbirinden ayrı çalışan ve iletişim kanalları olarak kullandığımız masaüstü ve dizüstü PC, avuçiçi bilgisayar (PDA), mobil telefon, fotoğraf makinesi, video kamera gibi çeşili cihazlar, belirli bir frekans üzerinden birbirleriyle kablosuz haberleştirilerek, aralarında bilgi senkronizasyonu sağlanabilmektedir.

Bluetooth uyumlu olması istenen cihazlarda hangi tip yazılımların bulunması gerektiği de belirlenmiş ve standart haline getirilmiştir. Böylelikle, üretici farkı gözetmeksizin Bluetooth cihazları birbirlerine bağlanarak rahatlıkla çalışabilirler.

Bluetooth konseptinin en güçlü yönü, Bluetooth çiplerinin çok küçük boyutlu, ucuz ve düşük güç tüketimli çipler olmasıdır. Bunun yanısıra dünyanın önde gelen teknoloji şirketlerinin desteklediği bir teknoloji olduğu için kısa sürede yaygınlaşmaya başlamıştır.

Bu tezde Bluetooth teknolojisinin detaylı incelemesini vermek amaçlanmıştır. Donanım, yazılım ve Bluetooth uygulamalarının teknik gereksinimleri anlatılmıştır.

BLUETOOTH WIRELESS COMMUNICATION TECHNOLOGY and USAGE AREA EXAMPLES

SUMMARY

In these days, the number and variety of telecommunications devices is increasing rapidly. Consequently, the subject of how to connect them to each other gets more importance. The usual method to solve this problem is to connect the devices with a cable or to connect them using infrared light.

The cable solution is often complicated since it may require a cable specific to the devices being connected as well as configuration software. The infrared solution eliminates the cable, but requires line of sight. To solve these problems a new technology, Bluetooth, has been developed.

Bluetooth eliminates the need for cables in communication between fixed and mobile devices and make both data and audio transmission easier. It is the result of a co-operative effort among a number of companies all working for a cheap, simple, and low power-consuming solution and in 1999 December, was put into the market.

With Bluetooth, establishment of communication networks with personal aims and provide synchronization between personal devices without cables is very easy. The Bluetooth technology covers hardware, software and interoperability requirements. In addition to telecommunication; computer, home electronics, automotive, health and more different sectors interested in Bluetooth.

The Bluetooth specification defines a short range (10 m.) and a mid-range (100m.) radio connection. Over this connection data and audio transmission with a maximum rate of 720 Kbps per channel can be done.

Bluetooth operates in the international 2.40-2.48 GHz. ISM band. A spread spectrum and frequency hopping technique are used; a full duplex structure with 1600 hop per second is allowed. The signal hops between 79 channels in 1 MHz. intervals to reduce the effect of interference successfully. Transmitting power is between 1 mW and 100 mW.

With Bluetooth, communication devices like notebook and desktop PCs, personal digital assistants (PDA), mobile phones, photo machines and video cameras can communicate wirelessly at a specific frequency and synchronization between them can be provided.

Bluetooth also defines how certain applications should be mapped onto the hardware to be compatible with Bluetooth. Thus, the concept ensures that devices can operate with other Bluetooth applications and devices regardless of manufacturer.

The strength of the Bluetooth concept is that Bluetooth chips can be made very small; they are cheap and low power-consuming. Furthermore, there is a big support for the technique from a vast variety of companies and it starts to spread in a short time.

This thesis aims to give a detailed research of the Bluetooth technology. It strives to cover technical aspects, regarding hardware, software and Bluetooth applications.

1. GİRİŞ

Günümüzde haber işaretlerinin büyük çoğunluğu telefon hatları, koaksiyel kablo sistemleri, yerel alan ağları gibi teller ve kablolar içeren sistemler aracılığıyla taşınmaktadır. Çoğu televizyon sistemi kablo sistemlerine bağlanmıştır, ağ bilgisayarları ethernet ya da telefon hattı gibi fiziksel unsurlarla birbirlerine bağlıdır. Hatta telsiz ve mobil telefonlar bile sonlanma noktaları arasında aramayı taşımak ve yönlendirmek için fiziksel telefon şebekesini kullanmaktadır.

20. yüzyılda kablosuz haberleşme çok büyük bir gelişme göstermiştir. Yapılan araştırmalar bu büyümenin ses servisleri yanında, yüksek hızlı veri ve video servisleri tarafından daha da teşvik edileceğini göstermektedir; yüksek veri miktarları içeren bu servislerde daha geniş “Radyo Frekansı” (RF) spektrumu kullanılmaktadır.

Günümüzde birçok haberleşme şirketi ve GSM operatörü ses, veri ve videonun bütünsel olduğu servisler önermektedir. Bunun temelinde ses servislerinden elde edilen gelirlerin azalması yatmaktadır. Geniş bantlı kablosuz teknolojiler, kablolu ortama göre bu tip servisler için mobilite ve hızlı gelişim vadettiğinden daha çok tercih edilmektedir.

Gerçek zamanlı ses, veri ve video haberleşmesini sağlamak, yeni bir kavram olmamakla birlikte, birçok farklı sistem ve cihazı bir araya getirerek entegre etmeyi (PSTN üzerinden ses, E1 üzerinden veri, ISDN üzerinden video gibi) gerektirmektedir. Bu sebeple kısa süre öncesine kadar çoğu operatör büyük yatırım isteyen bu sistemlere geçiş yapmamıştır. Günümüzde bu durum iyiye gitmekte, çoklu servis erişim cihazları sayesinde ses, veri ve video servislerini entegre etmek kolaylaşmaktadır. Bir E1 devresi üzerinden, DSL bağlantısı üzerinden ya da geniş bantlı kablosuz bir düzenleme ile servislerin entegrasyonu mümkündür. Bu bütünselme aynı zamanda daha az teknik destek, yönetim, bakım ihtiyacı ve daha kolay ağ yönetimi gibi faydalar getirmektedir.

Düşük maliyetli ve mobil çözümlere olan ihtiyacın artması, geniş bantlı kablosuz teknolojilerin haberleşme teknolojilerini bütünleştirmede ideal yol olduğunu kanıtlamaktadır.

Bu çalışma, geniş bantlı kablosuz haberleşme teknolojilerine genel bakış ile Bluetooth teknolojisinin temel prensiplerin anlatıldığı bölüm ile başlamaktadır. Takip eden bölümlerde ise aşağıdaki ana başlıklara değinilmiştir:

Bluetooth radyo spesifikasyonu bölümünde, 2.4 GHz. frekans bandında çalışan radyo ünitesi özellikleri ile alıcı ve verici karakteristikleri verilmiştir.

Protokol mimarisi bölümünde, Bluetooth spesifikasyonuna uygun olarak geliştirilen uygulamaların birbirleri ile uyumlu olarak çalışmalarını sağlamak için oluşturulmuş protokoller detaylı olarak açıklanmıştır. Bu protokoller, Temelbant Protokolü, Link Yönetim Protokolü, Lojik Link Kontrolü ve Adaptasyon Protokolü, Servis Keşif Protokolü, RFCOMM, IrDA Uyumluluğu, Ses ve Telefon Kontrolü Protokolü ile Host Yönetim Arayüzü Protokolü'dür.

Bluetooth güvenlik mimarisi bölümü, link katmanında gerçekleştirilen güvenlik fonksiyonlarını, doğrulama ve şifreleme prensiplerini, gereksinimleri karşılayacak güvenlik mimarisi özelliklerini kapsamaktadır.

Bluetooth profilleri ve kullanım modellerinin açıklandığı bölümlerde, Bluetooth uygulamaları arasında uyumluluk sağlamak için geliştirilen profillerden Genel Erişim Profili, Seri Port Profili, Servis Keşif Uygulama Profili ve Genel Obje Değiş-Tokuş Profili detaylandırılmış; en popüler Bluetooth kullanım modelleri anlatılmıştır.

Son olarak Bluetooth'un global 3G sistemindeki yerine, olumlu-olumsuz yönlerine, Türkiye'deki ve dünyadaki güncel durumu ile gelecekteki beklentilere değinilmiştir.

2. GENİŞ BANTLI KABLOSUZ HABERLEŞME TEKNOLOJİLERİ

2.1 Lisanslanmamış Bölgede Çalışan Kablosuz Ağlar

Kablosuz yerel alan ağları (WLAN) fabrikalar ve ofisler gibi kurumsal ağı, bilgisayarları kablolarla birbirine bağlamanın yüksek maliyetli olduğu durumlarda tercih edilir. Bu tip sistemler daha çok birkaç yüz metrelik tek noktadan çok noktaya olan uygulamalarda tercih edilmekle birlikte, uygun kuvvetlendirici ve antenlerle desteklendiği zaman birkaç kilometrelik bir etki alanında tek noktadan tek noktaya ya da tek noktadan çok noktaya bağlantı sağlayabilirler. Tablo 2.1 deki “teknoloji/servis” bölümü bu teknolojilerin bu anlamdaki farklarını açıklamaktadır. IEEE 802.11b Amerika’da, HiperLAN ise Avrupa’da kabul gören WLAN standartlarıdır. Bluetooth ise yeni IEEE 802.15 kişisel alan ağına (PAN) temel teşkil ettiği için farklı bir öneme sahiptir. AçıkHava (Open Air) ve EvRF (HomeRF) teknolojileri de özel tip bazı uygulamalar için genişletilmiş kapasite olanakları sunmaktadır.

Tablo 2.1 Lisanslanmamış bölgede çalışan kablosuz ağ teknolojileri

Teknoloji/Servis	Veri Hızı (Kanal başına Mbit/sn.)	Maksimum Etki Alanı		Ürün Bulunurluğu
		Kapalı alan metre, nominal maksimum	Açık alan (km, anten sistemleri ile)	
2.4 GHz. ISM bandı				
IEEE 802.11b	1 - 11	100 - 150	3 - 30+	2000
AçıkHava(OpenAir)	0.8 - 1.6	100 - 150	3 - 30+	1996
EvRF (HomeRF)	1 - 2	30	NA	2000
Bluetooth	<1	10	NA	2000
5 GHz. ISM ve/veya UNII bantları				
IEEE 802.11a	6 - 54	60	50+	2001/2002
HiperLAN1	24	60	50+	?
HiperLAN2	6 - 54	60	50+	2001/2002
HiperAccess	20	NA	NA	?

2.1.1 IEEE 802.11b

IEEE 802.11b, 802.11 standart ailesinin üç üyesinden birisidir. Diğer ikisi 802.11 ve 802.11a dır. 802.11 in yerini 802.11b almıştır. 802.11a ise yüksek hızlı servis yönelimli bir versiyon olup halen geliştirme aşamasındadır. Bütün 802.11 teknolojileri tek noktadan çok noktaya haberleşme için tasarlanmış olup aynı zamanda tek noktadan tek noktaya haberleşmeyi de desteklemektedirler.

802.11b tek noktadan çok noktaya olan mimarinin hem altyapı tabanlı hem de anlık (ad hoc) şekillerini destekler. Aynı alt ağdaki (subnet) erişim noktaları uçlardaki cihazları bağlantıdan kesebilir fakat farklı alt ağdakileri (subnet'tekileri) kesemez. Çoğu WLAN cihazı alt ağlar (subnetler) arasındaki dolaşımı adresleyemez. Erişim noktaları birbirleriyle haberleşebilmektedirler fakat genellikle kablolu bir yapıya bağlı olarak çalışırlar.

802.11b cihazları orijinal 802.11 cihazları gibi 83.5 MHz. bant genişliğini kullanırlar fakat 802.11 de 2 Mbit/sn. olan veri hızı 802.11b de 11 Mbit/sn. lere çıkmıştır. Eğer bir erişim noktası ile istemci (client) cihaz arasındaki işaret yüksek veri hızlarını destekleyemeyecek kadar düşük seviyede ise, bağlantının devam edebilmesi için transfer hızı daha düşük seviyelere iner.

802.11b cihazları 1 ve 2 Mbit/sn. (802.11 e geriye dönük olarak uyumluluk için gereklidir), 5.5 Mbit/sn. ve 11 Mbit/sn. hızlarında çalışabilirler. 802.11b nin kapalı alandaki etki alanı uzaklığı 100-150 metredir.

802.11b cihazları 2000 yılının ilkbahar aylarında ilk defa piyasaya sürülmüştür. The Wireless Ethernet Compatibility Alliance (WECA) 802.11b cihazlarının uygunluğunu test eder ve onaylar. Cisco Systems, Lucent, 3Com, Nokia gibi üreticilerin cihazları bulunmaktadır.

802.11b Wired Equivalent Privacy (WEP) adlı bir şifreleme protokolü kullanır. Cihazların sertifikasyon almaları için WEP desteğine sahip olmaları gerekmektedir. WEP protokolünün 40 bit ve 128 bitlik şifre seçenekleri bulunmaktadır.

2.1.2 Açık hava (Open Air)

Çoğunlukla Açık hava (Open Air) teknolojisi el tipi bir tarayıcı ya da mobil veri terminali gibi bir istemci cihaza entegredir. Bu teknoloji 2.4 GHz. frekans atlamalı

WLAN temeline dayanır. Wireless LAN Interoperability Forum (WLIF) bu standardın sahibidir ve 1996 dan beri 40 kadar ürünü sertifikalandırmıştır.

2.1.3 EvRF (HomeRF)

HomeRF Working Group (HRFWG) mevcut WLAN ürünlerinin ev içi kullanım için fazla kompleks olduğunu düşünmüş ve EvRF (HomeRF) standardını kişisel bilgisayarlar, çevre birimleri, kişisel sayısal yardımcılar (PDA) ve telsiz cihazlar arasında çalışacak kablosuz bir ağ standardı olarak geliştirmiştir. EvRF (HomeRF) teknolojisi Shared Wireless Access Protokol (SWAP) üzerine kurulmuştur. SWAP, 802.11 in belirttiği frekans atlamalı protokolün basitleştirilmiş şekli ile, Digital Enhanced Cordless Telephone (DECT) in bir uzantısıdır. SWAP tabanlı cihazlar ses ve veri trafiğini taşırlar ve PSTN ve internetle haberleşirler.

SWAP tek noktadan çok noktaya haberleşmenin hem altyapı tabanlı hem de anlık (ad hoc) değişkenlerini destekler. Anlık (ad hoc) ağ sadece veri haberleşmesini destekler; tüm cihazlar aynıdır ve ağ kontrolü cihazlar arasında paylaştırılmıştır. Altyapı tabanlı yapıda ise hub veya bağlantı noktası PSTN ile haberleşmede bir geçiş kapısı görevi görür. Bağlantı noktası, cihazlar arasındaki veri haberleşmesini de sağlar.

EvRF (HomeRF) ürünleri 2000 yılının sonlarına doğru üretilmeye başlanmıştır ve çoğunluğu cihazların içine entegre edilmiştir. 2 Mbit/sn. lik veri hızını desteklerler. 10 Mbit/sn. ye kadar destekleyen ürünlerin üretilmesi de onaylanmıştır.

2.1.4 Bluetooth

Bluetooth mobil bilgisayarlar, PDA'ler, mobil telefonlar ve birbirlerine kısa kablolarla bağlanan cihazların kablosuz haberleşmesini sağlamak üzere geliştirilmiş en yeni ağ spesifikasyonudur. Bluetooth Special Interest Group (SIG) 1999 Aralık ayında Bluetooth Versiyon 1.0'ı duyurmuştur. Bluetooth uyumlu cihazlar bağımsız bir laboratuvar tarafından test edilmekte ve sertifika edilen cihazlar Bluetooth logosu almaktadırlar.

Bluetooth cihazları diğer PAN teknolojileri gibi pikonet olarak adlandırılan ve kullanıcı veya cihazın etrafında çalışan küçük ağlar oluşturur. Maksimum etkinlik mesafesi 10 m. dir, fakat bu mesafe opsiyonel olarak 100 m. ye kadar çıkarılabilmektedir.

2.1.5 HiperLAN

1991 yılında European Telecommunications Standards Institute (ETSI), yüksek performanslı bir radyo LAN (HiperLAN) standardı oluşturmak üzere bir alt komite oluşturmuştur. 1996 yılında IEEE 802.11 standardı tarafından karakterize edilen servisleri tanımlayan bir WLAN standardı olan HiperLAN1 standardı açıklanmıştır. HiperLAN1 teknolojileri 5 GHz. Industrial Scientific Medicine (ISM) bandı içinde çalışmaktadır. HiperLAN2 gelişmiş “Servis Kalitesi” (QoS), şifreleme ve doğrulama için güvenlik mekanizmaları içeren cihazlar üzerine odaklanmıştır. İlk HiperLAN2 ürünleri 2001 yılı sonlarında piyasaya sürülmüştür. [1]

2.2 Bluetooth Kablosuz Haberleşme Teknolojisine Giriş

Kablosuz haberleşme kavramı yeni bir kavram değildir. Radyo ve televizyon yayınları, uydu haberleşmesi, telsiz ve mobil telefonlar, uzaktan kumanda sistemleri, garaj kapı kumanda ve otomobil kilit sistemleri gibi bir çok örnek kablosuz haberleşme için verilebilir. Bu örneklerin çoğu radyo dalgaları, kızıl ötesi, ışığın görünmez bölge spektrumu gibi teknolojiler kullanmaktadır.

Bluetooth taşınabilir ya da sabit elektronik cihazları birbirine bağlayan kabloların yerine geçmek üzere tasarlanmış, kısa dalga radyo linkidir. Kısa mesafeli, düşük güçlü ve düşük maliyetli haberleşmeye imkan veren güçlü bir teknolojidir.

Bluetooth kablosuz haberleşme teknolojisi de radyo ve televizyon yayınlarına benzer şekilde RF teknolojisini kullanmaktadır. Bluetooth 2.4 GHz. deki lisanslanmayan ISM bandını kullanır. Yüksek katmanlarında ise kızıl ötesi kablosuz haberleşme teknolojisinde kullanılan transfer ve uygulama protokollerini kullanır.

Bu bilgilerin ışığı altında Bluetooth teknolojisinin kablosuz haberleşme ve taşınabilir cihazlarla bilgisayar haberleşmesi gibi konularda kullanımının ideal olduğu sonucuna varılmaktadır. Bu bölümde Bluetooth RF haberleşmesinin temel prensipleri açıklanacaktır.

2.2.1 2.4 GHz. Frekans Spektrumunda RF Haberleşmesi

RF teknolojileri gönderici ve alıcıların belirlenen bir frekans aralığında radyo dalgalarını alma ve göndermeye sırayla ayarlanması temeline dayanır. Göndericinin gücü ve alıcının duyarlılığı haberleşme uzaklığının belirlenmesine yardım eder. Kısa

mesafe haberleşmeleri genellikle düşük transfer gücü gerektirirken, televizyon yayınları gibi geniş alan haberleşmeleri ise yüksek transfer gücü gerektirir. Bu sebeple küçük bataryalı mobil cihazlarla sadece birkaç metrelik bir mesafe içinde haberleşme sağlanabilir. Haberleşme ile ilgili başka bir karakteristik de radyo dalgalarının birçok nesne içine penetre edebilmesidir. Kızıl ötesi gibi teknolojilerde ışık dalgalarının çeşitli engellerden yansımaları kullanılır. RF teknolojisinde kullanılan radyo dalgaları ise belli kısıtlamalar dahilinde engellere genellikle penetre ederler ve vücut, duvar, elbise gibi cisimlerin içine işlerler. Bu sebeple alıcı ve verici arasında bir “görüş hizalaması” na gerek duyulmaz.

RF teknolojileri belirli bir frekans spektrumu içerisinde radyo dalgaları üretmek için frekans modülasyonunu kullanırlar. İnfomasyon şifrelenir ve uygun frekansa ayarlanmış alıcılar tarafından alınır. Örneğin FM radyo yayınları 88 MHz.-108 MHz. arasında, bazı telsiz telefonlar 900 MHz. frekansında, Bluetooth ise 2.4 GHz. frekansında çalışır. Kullanılabilir radyo frekans spektrumunun sınırlı olması sebebiyle, çoğu ülke hükümeti bu spektrumun kullanımını düzenleyici yasalar çıkartmış, frekans spektrumunu parçalara ayırarak belirli güç seviyelerinde veri alışverişi yapılması için lisanslama yöntemi kullanılmıştır. Bazı frekansların kullanımı ise serbest bırakılmıştır. Yapılan uluslararası anlaşmalarla 2.4 GHz. frekansı birkaç ülke dışında dünya genelinde lisanslamaya gerek duyulmaksızın kullanılmaktadır. Bluetooth SIG ve IEEE, 2.4 GHz. lisanslanmayan spektrumun kablosuz haberleşme için kullanımını ortak olarak düzenlemekte ve sertifikasyon otoriteleri ile birlikte çalışmaktadırlar.

2.4 GHz. frekans spektrumu global olarak lisanssız kullanıma açık olduğu için birtakım düzenleyici kısıtlamalar içermektedir:

- Spektrum 79 kanala bölünmüştür. (İspanya ve Fransa’da sadece 23 kanal kullanılmaktadır. Japonya ise 2000 yılından itibaren 79 kanalın tamamını kullanmaya başlamıştır.)
- Kanal başına bant genişliği 1 MHz. ile sınırlandırılmıştır.
- Frekans atlamalı saçılmış spektrum kullanılmalıdır.
- Girişim konusu hesaba katılmalı ve uygun bir şekilde ele alınmalıdır.

EvRF (HomeRF) ve IEEE 802.11 gibi bazı diğer RF haberleşme teknolojileri ile mikrodalga fırınlar da bu spektrumu kullanmaktadırlar. Spektrum lisanssız olduğu için yeni kullanım alanlarının doğması da beklenmektedir. Ve spektrumun kullanımı arttıkça girişim oluşma ihtimali de artacaktır.

Bu spektrumu kullanan her teknoloji varolan sınırlamalar dahilinde bir tasarım seçimi yapmak durumundadır. Bluetooth kablosuz teknolojisi çok düşük güçte çalışırken RF girişimini ve etkilerini minimize etmek, kullanılabilen kanal bant genişliğini ise en avantajlı ölçüde kullanmak için tasarlanmıştır.

2.2.2 RF Haberleşmesinde Saçılmış (Spread) Spektrum

RF haberleşmesinde saçılmış (spread) spektrum mevcut uygun spektrumun frekans, zaman, bir kodlama şeması ya da başka bir yöntem ile bölümlenmesi anlamına gelmektedir.

Mesajlar çeşitli paketlere bölünerek bölümlenmiş spektrumdan gönderilirler. Bluetooth kablosuz haberleşmesinde kullanılan frekans bölümlemeli saçılmış (spread) spektrumun frekans atlama yönteminde spektrum değişik frekanslara ya da kanallara bölünür. Tek bir mesaj paketi seçilen kanal üzerinden iletilir, sonra Bluetooth ünitesi bir sonraki paketi iletmek için yeni bir kanal seçer (bu süreç yeni bir frekansa atlama şeklinde tanımlanır). Bu süreç mesajın tamamı uygun frekans spektrumu üzerinden gönderilene kadar tekrarlanır. Her teknoloji frekans atlama paterni oluşturmak için kendine özel bir yöntem kullanır. Bu çalışma şeklinde alıcılar her bir paketi ayrı ayrı alarak tüm mesajı doğru şekilde oluşturmak için kanalları doğru ayarlamalı ve atlama paternini bilmelidirler. Bu proses “Frekans Atlamalı Saçılmış Spektrum” (FHSS) olarak adlandırılır.

FHSS bazı faydalar sağlamasına rağmen seçilecek tek bir frekansın kullanımına oranla daha komplekstir. FHSS ile tüm üniteler bir frekanstan diğerine atladığı için (genelde rastgele ve hızlı şekilde) RF girişimi azalır. Spektrumdaki tüm taraflar FHSS’i kullandıklarında aynı frekansta gerçekleştirilen transferlerin çakışması yüzünden oluşan girişim büyük olasılıkla her ünitenin tek bir kanalı uzun bir süre kullanması ile oluşan girişime göre daha az olacaktır. Ayrıca ilk alternatifte çakışmaların oluşması durumunda sadece tek bir paket kaybolacağı ve kaybolan paket yeni bir frekansta tekrar gönderileceği için çakışmaların etkisi azaltılmış olur. Buna ek olarak sadece frekans atlama paternini bilen bir alıcının mesajın tüm

paketlerini birleştirebilmesi söz konusu olduğu için güvenlik açısından da daha avantajlıdır. Belirli bir spektrum için dahi bir atlama paterni belirlemek için birçok farklı yol olduğundan özellikle birçok ünite tarafından kullanılan bir spektrumda bilinmeyen bir paterni izleyerek sonuç çıkarmak pek mümkün değildir.

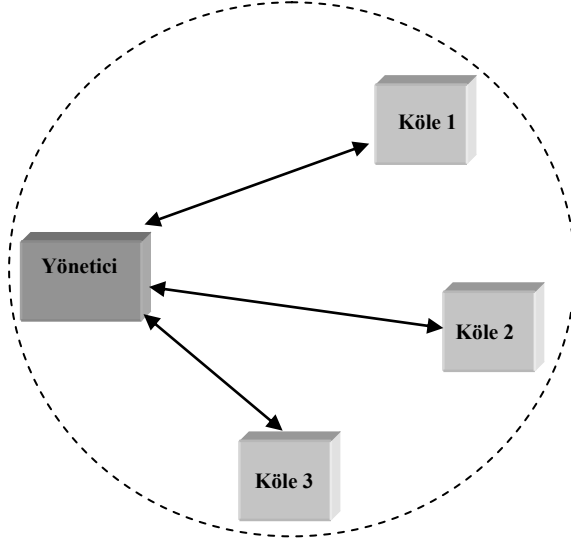
2.4 GHz. lik frekans kademesinde saçılmış spektrum kullanmak, spektrum lisanssız kullanıldığı için oluşması muhtemel girişim problemlerini minimize eder. Bluetooth teknolojisi çok hızlı (saniyede ortalama 1600 kere) frekans atlaması kullanır.

2.2.3 Yönetici-Köle (Master-Slave) Roller

Temelbant seviyesinde iki cihaz arasında bir Bluetooth linki kurulduğu zaman, cihazlardan biri yönetici, diğeri ise köle konumunda çalışır. Cihazlar iki konumdan birinde bulunabilirler. Bir haberleşme linkinde yönetici olarak çalışan bir cihaz, diğ bir haberleşme linkinde köle olarak çalışabilir. Yönetici cihazın köle cihazdan farklı bir yetki ya da ayrıcalığı yoktur; sadece cihazlar arasındaki FHSS haberleşmesinin senkronizasyonunu düzenler. Yönetici cihaz kendisinin Bluetooth cihaz adresine bağlı olarak frekans atlama paternine, yine kendisinin saatine bağlı olarak da atlama sıralamasının fazına karar verir. Bütün köleler yönetici ile uyumlu şekilde yönetici tarafından verilen atlama frekansı ile haberleşirler. Yönetici olma rolü genellikle haberleşmeyi başlatan cihaza verilir.

Yönetici cihaz 7 aktif ve 255 park modunda köleye kadar sayıda köle cihazla haberleşebilir. Tüm köleler tek bir yönetici ile haberleşebilir. Bu yapıya piconet adı verilir. Bir piconet içerisinde sadece bir tek yönetici bulunabilir.

Bluetooth'un düşük katmanlı haberleşmelerinde yönetici-köle ilişkisinin kurulması gereklidir fakat genellikle cihazlar eşdeğer olarak çalışır. Bir cihaz başka bir cihazla noktadan noktaya link kurarak haberleşmeye başladığında cihazların yönetici-köle konumları önemli değildir ve üst seviye protokoller ya da cihazı kullanan kişi için de bir etkisi yoktur. Bazı kullanım senaryolarında cihazlara özel roller vermek gerekebilir fakat genellikle her cihaz için tek bir spesifik rol tanımlamak kritik önem taşımaz.



Şekil 2.1 Piconette yönetici ve köle rolleri

2.2.4 Temelbant Modları ve Enerji-Korumalı Özellikler

Yukarıda anlatıldığı gibi bir piconette 7 aktif ve birçok park modunda köle bulunabilir. Bluetooth spesifikasyonu çeşitli temelbant modları tanımlar. Bu temelbant modları Bluetooth ünitelerinin düşük güçlü duruma geçmelerine izin vererek enerji korunmasını sağlarlar. Bu düşük güç modları bir düşük güç konumuna girmek ve çıkmak için üç farklı yöntem içerir ve mevcut Bluetooth bağlantısına uygulanırlar (bütünüyle bir cihaza uygulanmak yerine). Temelbant modları tüm cihazlar aynı anda aktif haberleşme linklerine ihtiyaç duymayacakları için aynı yakınlık mesafesine daha çok cihazın yerleşmesine izin verir. Mevcut 4 adet temelbant modlarının tamamı (aktif, koklama, durağan ve park) temelbant bağlantı durumuna geçtiğinde söz konusu olur; bağlantı yoksa temelbant bekleme (standby) konumunda kalır. Temelbant durumlarını bağlantı ve bekleme (standby) konumları olmak üzere ikiye ayırabiliriz.

Aktif modda köle sürekli olarak yöneticiden gelen transferleri dinler konumdadır. Aktif köleler yönetici ile senkronize kalmalarına yarayan ve yöneticiye paket iletme zamanlarına ilişkin bilgileri taşıyan paketleri alırlar. Başka bir aktif kölenin yönetici ile haberleşmekte olduğu süre içerisinde diğer aktif kölelerin yöneticiden gelen paketleri ya da sadece paket başlıklarını dinleme ihtiyaçları olmamasına rağmen, aktif bir köle sürekli olarak yöneticiden gelen tüm paketleri dinlemek zorundadır. Aktif konum en hızlı cevap süresine fakat bununla beraber en yüksek güç tüketim

miktarına sahiptir. Sürekli paket alındığı ve her zamana paket iletmeye hazır olduğu için çok fazla güç harcanır. [2,3]

Koklama modu güç tüketimini azaltmak için kullanılan bir yöntemdir. Koklama modunda köle periyodik olarak aktif konuma gelir. Yönetici belirli ve düzenli bir zaman aralığında belirli bir köleye paketleri iletmeye programlanır. Belirlenen her zaman aralığında paket iletilme mecburiyeti yoktur. Böylelikle köle de sadece belirlenen zaman aralıkları başlangıcında yöneticiyi dinlemeye başlar. Eğer zaman aralığı başlangıcında paket alınmaya başlanırsa dinleme ve paket alma süreci devam eder, aksi takdirde aralık boyunca “uyku” moduna geçilir. Böylelikle güç tüketimi düşer fakat duyarlılık da azalır. Güç tüketiminin ve duyarlılığın boyutu koklama aralığının uzunluğu ile ilgilidir.

Durağan modda köle belirlenen bir zaman aralığında yöneticiden gelen paketleri dinlemeyi tamamen keser. Yönetici ve köle durağan modda kalma süresini kararlaştırır ve bu süre içinde haberleşme linki kullanılmaz. Durağan mod süresi boyunca kölenin yöneticiyi dinlemeye ihtiyacı yoktur ve bu süre içinde başka cihazlarla bağlantı kurmak ya da uyku modunda kalmak gibi başka şeyler yapabilir. Durağan mod süresi bitiminde yöneticiden gelen paketler dinlenmeye başlanır. Durağan modu koklama moduna göre daha az hassas olmakla birlikte daha fazla enerji tasarrufu sağlar. Enerji tasarrufunun boyutu durağan modu süresinin uzunluğuna ve bu süre boyunca kölenin hangi işlerle ilgilendiğine bağlıdır.

Park modunda köle yönetici ile senkronizasyonunu devam ettirir fakat aktif olarak kabul edilmez (aktif, koklama ve durağan modları aktif modlar olarak kabul edilmiştir). Bir pikonette aynı anda 7 adet aktif köle olabileceğinden park modunun kullanımı ile yönetici cihaz 7 cihazdan fazla sayıda cihaz bulunan bir pikoneti aktif ve park modundaki kölelerin modlarını değiştirmek suretiyle yönetir duruma gelir. Park modundaki köle de yönetici ile olan senkronizasyonunu korumak zorunda olduğu için yöneticiyi periyodik olarak dinler. Park modu en az hassas mod olup, aynı zamanda da en az güç tüketiminde bulunur.

Şekil 2.2 de modların duyarlılık ve güç tüketimleri arasındaki ilişkiler anlatılmaktadır. Her iki faktör de haberleşme trafiği, durağan ve koklama süreleri gibi parametrelere bağlı olarak değişebilmektedir. Genel bir kural olarak aktif köleler en fazla gücü

tüketirken en hassas; park modundaki köleler ise en az gücü tüketirken en az hassas olan kölelerdir.



Şekil 2.2 Modların hassasiyet ve güç tüketimleri arasındaki ilişki

Enerji korunumunu sağlayan temelbant modlarına ek olarak adaptif transfer gücü özelliği de güç korunumu için etkilidir. Bu özellik yöneticinin transfer gücü uygun olmadığı durumda kölelerin yöneticiyi bilgilendirmesine ve böylelikle yöneticinin transfer gücünü düzenlemesine yardımcı olur. Bu özellik “Alınan İşaret Güç Göstergesi (RSSI)” kullanımı ile gerçekleşir. RSSI değeri belirlenen sınırların dışında ise köle yöneticiden gücü ayarlamasını isteyebilir. Bu durum özellikle iki cihaz birbirine çok yakınsa ve maksimum transfer gücü istenmiyorsa avantaj yaratır. (Tıpkı birbirine yakın duran iki insan da birinin diğeri ile yüksek sesle konuşması ve ikinci tarafın da yüksek sesli konuşan taraftan sesini alçaltmasını istemesi gibi) Bu durumun tersi de yani RSSI değeri çok zayıf olduğunda gücün artması da istenebilir. Yönetici her bir köle için transfer gücü değerlerini ayrı ayrı ayarlar. Böylelikle aynı pikonet içindeki bir kölenin transfer gücündeki değişikliğin diğer köleleri etkilememesi sağlanır.

2.2.5 Bağlantı Kurulumları

Bir ağın ilk kurulumunda veya bir pikonete yeni bir ünite eklenirken, ünite kimlikleri tanınmalıdır. Üniteler pikonete herhangi bir zamanda dinamik olarak katılıp ayrılabilirler. Bağlantı süresi tipik olarak 0.64 sn. dir. Bu süre ünitenin adresi bilindiği ve bir önceki bağlantıdan itibaren 5 saatten fazla süre geçmediği durumda geçerlidir. Ünite bağlantıda olmadığı durumlarda sadece bir düşük güç osilatörünün çalıştığı (LPO) bekleme (standby) durumunda olabilir. Bu çalışma şekli güç sarfiyatını minimize etmek içindir.

Bağlantı prosedürlerinin gösterildiği bir akış diyagramı Şekil 2.3 de verilmiştir.

Herhangi bir bağlantı yapılmadan önce, bütün üniteler bekleme (standby) konumundadır. Bu modda bağlantıda olmayan ünite gelen mesajları sadece 1.28 sn. de bir dinler. Bekleme modu sona erdiğinde, bu ünite kendisi için tanımlanan 32 atlama frekansından birisini dinler.

Bağlantı prosedürü yönetici konumunda olan ünite tarafından başlatılır. Bağlantı, bağlantı kurulacak ünitenin adresi biliniyorsa çağrı (page) mesajı ile, bilinmiyorsa sorgu mesajını takibeden bir çağrı (page) mesajı ile başlatılır. Başlangıçtaki çağrı (page) konumunda, çağrıyı yapan (paging yapan) ünite (yönetici), çağrı yapılan (paged) üniteye (köle) 16 değişik atlama frekansında birbirinin eşi olan 16 çağrı (page) mesajından oluşan bir dizi mesaj gönderir. Bu mesaj dizisi kölenin uyanabileceği frekans dizilerinin yarısını kapsar. Bu süre sonunda hiçbir cevap alınmazsa, yönetici kalan 16 atlama frekansında olan birbirinin eşi olan 16 çağrı (page) mesajından oluşan bir dizi mesaj daha gönderir. Yöneticinin köleye erişmesi öncesinde geçen maksimum gecikme 2.56 sn. dir.

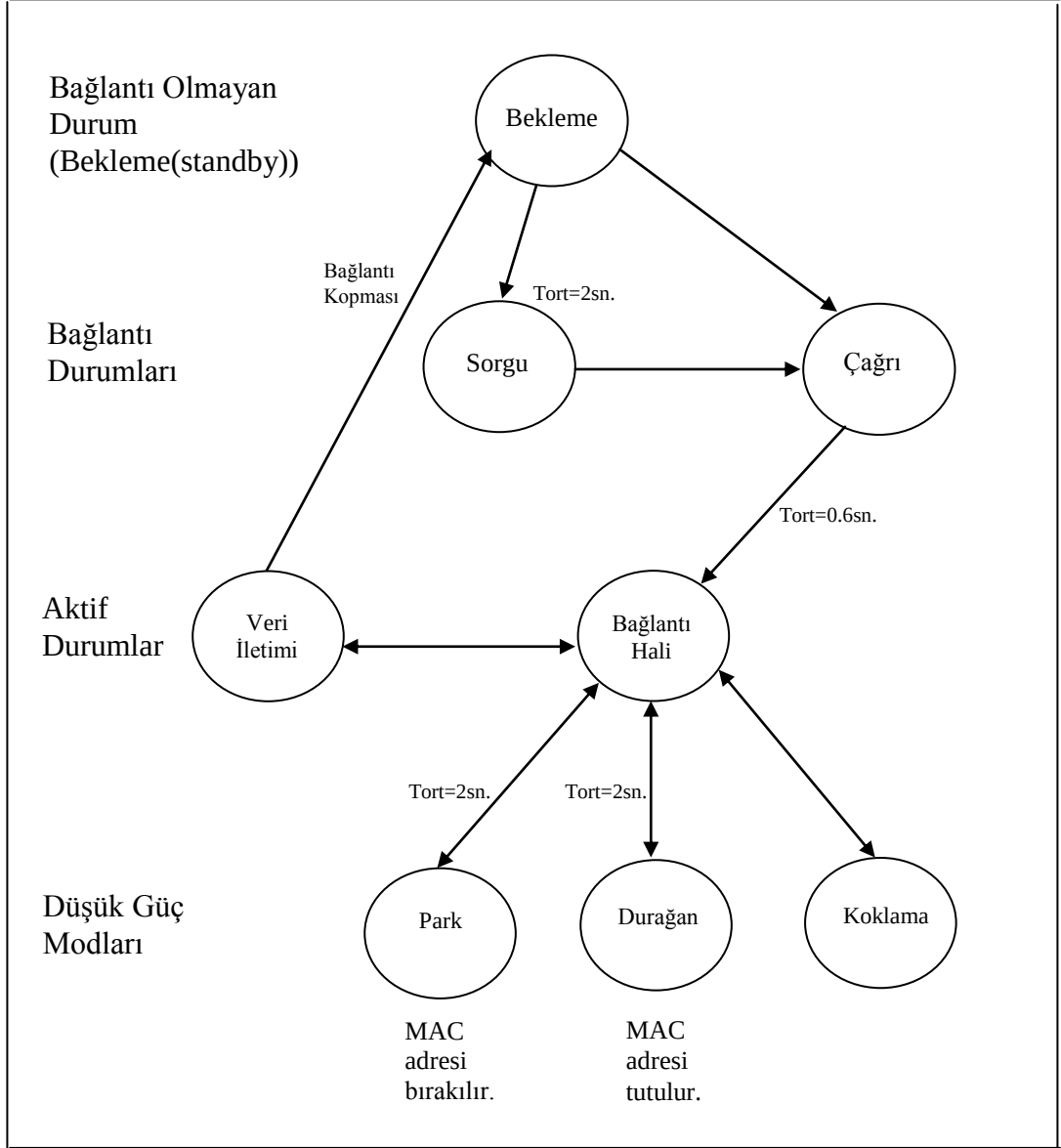
İlk çağrı (page) mesaj dizisindeki atlama frekansları yöneticinin köle için yaptığı saat tahminine dayanır. Mesaj dizisi tahmin edilen uyanma frekansını, bu frekanstan önceki 8 atlama frekansını ve sonraki 7 atlama frekansını içerir. Sonuç olarak, yapılan tahmin +/- 7 atlama hatalı olabilir ve yönetici köleye ilk çağrı (page) mesaj dizisi ile erişmiştir. Her bağlantı kurulumunda yapılan tahmin frekansı güncellendiği için, bağlantı kurulum gecikmesi ünitenin en son bağlantısında oluşan gecikmeye göre daha kısa olur. +/-250 ppm lik bir LPO hatasında, bağlantısız geçen 5 saatlik bir süre sonrasında ilk mesaj dizisi hala geçerlidir.

En son bağlantıdan sonra geçen 5 saatlik süre sonrasında elde edilen ortalama bağlantı süresi 0.64 sn. dir. Eğer ilk mesaj dizisi kölenin uyanma frekansını içermiyorsa, ikinci mesaj dizisi içerir ve ortalama bağlantı süresi 1.92 sn. olur.

Sorgu mesajı tipik olarak bilinmeyen adresli faks, yazıcı gibi cihazlar ile bağlantıya geçilirken kullanılır. Sorgu mesajı çağrı (page) mesajına benzer fakat bütün cevapları toplamak için gereken ek bir mesaj periyodu içerir.

Eğer herhangi bir veri transferi gerekmiyorsa, üniteler sadece dahili bir zamanlayıcının çalıştığı durağan moda girer. Üniteler durağan moddan çıktığında veri transferi hemen tekrar başlayabilir. Bu sebeple üniteler veri transferi olmaksızın

bir düşük güç modu olan durağan modda bağlantı durumunda kalabilirler. Durağan mod güç korunumunun önemli olduğu ve çok nadir veri transferi yapılan durumlarda da kullanılabilir. Bu modun kullanımına örnek olarak veri transferinin dakikada bir yapıldığı oda sıcaklık ölçümü verilebilir. [4]



Şekil 2.3 Bağlantı prosesi

2.2.6 Haberleşme Topolojileri

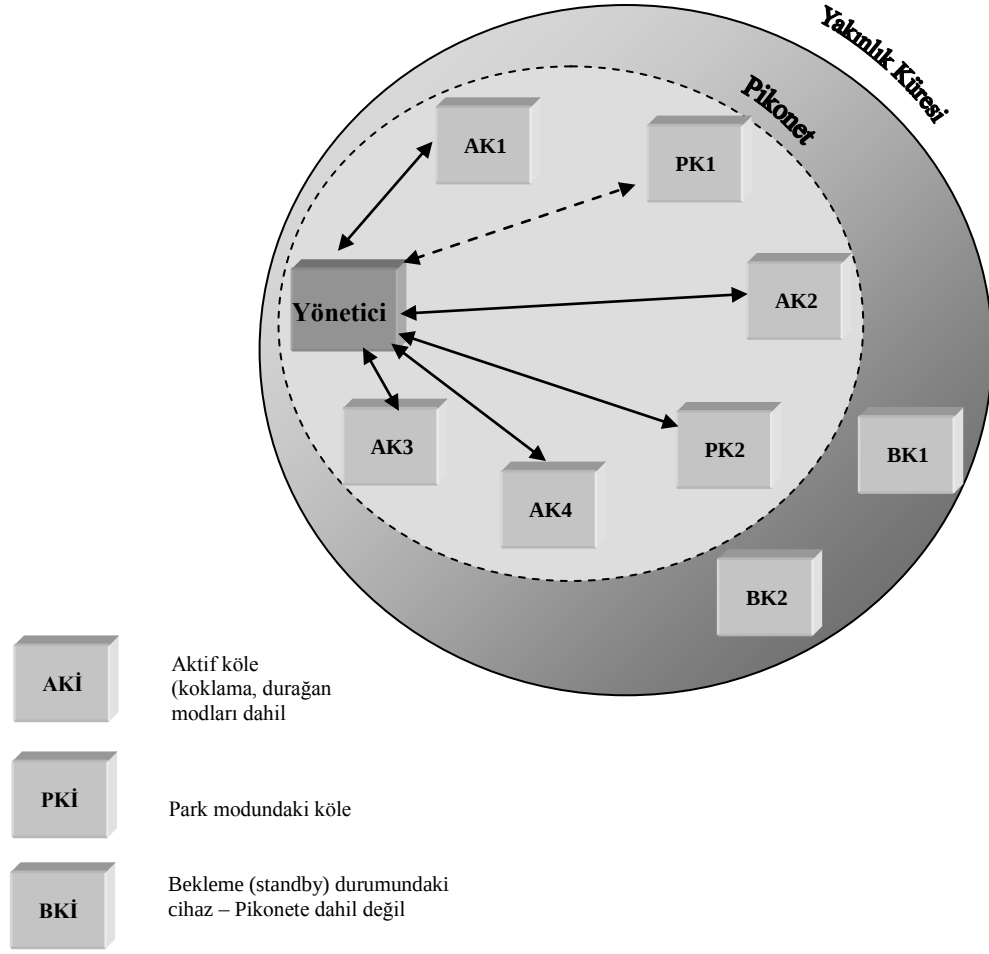
Bluetooth ağ modeli noktadan noktaya haberleşmeye dayalı bir ağ modelidir. İki cihaz birbirinin etki alanına (standart 0 dBm. Bluetooth cihazları için uzaklık 10 m., gücü arttırılmış 20 dBm. lik cihazlar için ise 100 m. ler civarındadır.) girdiğinde

otomatik olarak bir bağlantı linki kurulur. Ancak cihazlar birbirlerinin etki alanına girer girmez haberleşmeye başlamak zorunda değillerdir.

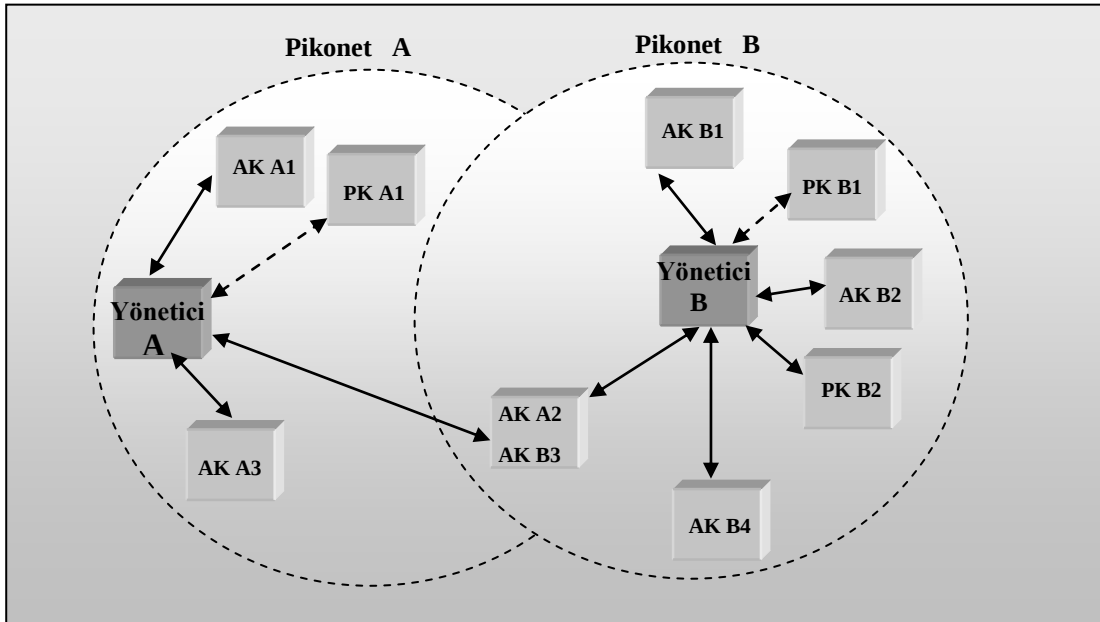
Kablosuz haberleşme ağları kişisel alan ağlarının, mobil telefon, cep bilgisayar, dizüstü bilgisayar gibi kişisel cihazların haberleşmesinin kolaylaşmasını sağlar. Bu tip cihazların haberleşmesi kablosuz hale geldiği zaman kullanım alanları da çeşitlenmektedir. Mobil cihazlarla kiosk, yazıcı, ağ erişim noktaları ve otomat cihazları gibi cihazların haberleşmesi de sadece aradaki mesafeye bağlı olarak mümkün hale gelmektedir.

Pikonet topolojisi biraz daha açılacak olursa; bir pikonet tek bir yönetici ve yönetici ile belirli bir yakınlık mesafesinde olan ve haberleşen çok sayıda köleden oluşur. Köleler aktif, koklama, durağan ya da park modlarından birinde olabilirler. Pikonetteki tüm cihazlar senkronize çalışır ve atlama frekansında haberleşirler. Aynı yakınlıkta yönetici ile haberleşmeyen (bekleme (standby) durumundaki cihazlar da dahil) başka cihazlar da olabilir fakat bunlar o pikonete ait değillerdir.

Bir cihazın birden fazla pikonet içinde yer alması da mümkündür. İki ya da daha fazla pikonet zamanda ve uzayda kısmi olarak örtüşüyorsa oluşan yapıya saçılmış ağ (scatternet) adı verilir. Pikonetler için geçerli olan prensipler saçılmış ağlar (scatternet) için de geçerlidir. Her pikonet tek bir yönetici ve aktif ya da park durumunda olan birçok köleden oluşur. Her pikonetin kendi yöneticisi tarafından belirlenmiş bir frekans atlama paterni vardır. Bir köle birden fazla pikonet içinde yer alabilir ve değişik yöneticilerle sırayla senkronize olabilir. Bir cihaz bir pikonet içinde köle iken, diğer bir pikonet içinde yönetici rolü üstlenebilir. Saçılmış ağ (scatternet) topolojisi sürekli hareket halinde olan ve diğer cihazlarla yakınlık mesafeleri değişen mobil cihazlar için çok kullanışlıdır. [2]



Şekil 2.4 Genel Bluetooth pikonet yapısı



Şekil 2.5 Saçılmış ağ (scatternet) örneği. A2/B3 kölesi her iki pikonette de aktif maddadır.

3. BLUETOOTH RADYO SPESİFİKASYONU

3.1 Frekans Bantları ve Kanal Düzenlemesi

Bluetooth'un çalıştığı 2.4 GHz. ISM bandı dünyadaki çoğu ülkede 2400-2483.5 MHz. arasındadır. Bazı ülkelerde bu frekans bandı ulusal kısıtlamalar içerir. Bu kısıtlamalarla uygunluk sağlamak için özel frekans atlama algoritmaları geliştirilmiştir. Daha dar bir frekans bandında çalışmak üzere tasarlanan cihazlar bandın tamamı için tasarlanan cihazlar ile birlikte çalışamazlar. Bluetooth SIG buna benzer karışıklıkları önlemek için aşağıdaki çalışmayı yapmıştır:

Tablo 3.1 Çalışılan frekans bantları

Coğrafi Konum	Regülasyon Kademesi	RF Kanalları
Kuzey Amerika, Avrupa ve diğer çoğu ülke	2.400-2.4835 GHz.	$f=2400+k$ MHz, $k=0,...,78$

Kanal boşluğu 1 MHz. dir. Bazı ülkelerdeki kısıtlamalar göz önüne alınarak bandın alt ve üst sınırlarında bir emniyet bandı bırakılır.

Tablo 3.2 Emniyet bantları

Coğrafi Konum	Alt Emniyet Bandı	Üst Emniyet Bandı
Kuzey Amerika, Avrupa ve diğer çoğu ülke	2 MHz.	3.5 MHz.

Bluetooth bazı ülkelerdeki ulusal kısıtlamalarla uygunluk göstermek için özel bir frekans atlama paterni içerir. Örneğin Fransa için 2.4465-2.4835 GHz. lik frekans aralığı ve buna karşılık gelen $f=2454+k$ MHz, $k=0,...,22$...RF kanalları kullanılır.

3.2 Verici Karakteristikleri

Bu bölümde belirtilen gereksinimler cihazların anten konektörlerinin güç dereceleri için verilmiştir. Eğer cihazın anten konektörü yoksa 0 dBm. kazançlı bir referans anteni olduğu varsayılır.

Güç kontrolü 1. güç sınıfına dahil olan cihazlar için istenir ve aktarılan gücün 0 dBm. üzerine çıkmasını sınırlamak için kullanılır. 0 dBm. in altındaki güç kontrolü seçime bağlıdır; güç tüketimini optimize etmek için kullanılabilir. Güç basamakları monotonik bir sıra izlemeli, en düşük basamak boyutu 2 dB., en büyük basamak boyutu 8 dB. olmalıdır. 20 dBm. yüksek transfer gücüne sahip bir 1. sınıf cihazın transfer gücünü 4 dBm. ya da altına düşürmesi gereklidir.

Güç kontrolü olan bir cihaz bir linkteki çıkış gücünü “Link Yönetim Protokolü” (LMP) komutları ile optimize eder. Bu optimizasyon RSSI ölçümü yapılarak çıkan sonuca göre artım ya da azaltım yapılarak sağlanır.

Eğer alıcı taraf verici tarafın güç kontrolünü sağlayacak gerekli mesajlaşmayı sağlayamıyorsa verici tarafta 1. güç sınıfı kullanılmalıdır. Bu durumda verici 2. ve 3. sınıf vericilerle uyum içinde olmalıdır. [5]

Tablo 3.3 Güç sınıfları

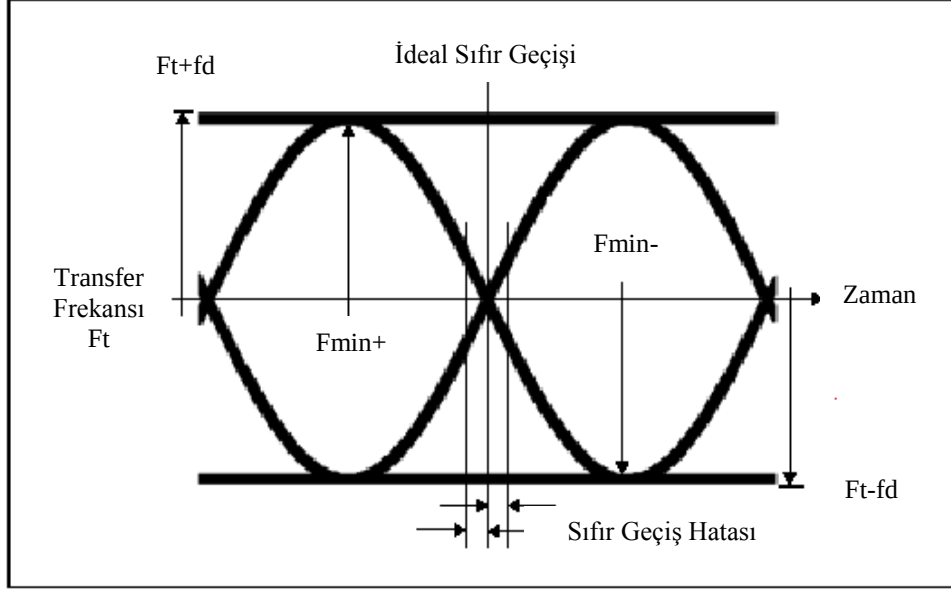
Güç Sınıfı	Maximum Çıkış Gücü(P _{max})	Nominal Çıkış Gücü	Minimum Çıkış Gücü (1)	Güç Kontrolü
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	P _{min} <+4 dBm- P _{max} Opsiyonel: P _{min} (2)’den P _{max} a kadar
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Opsiyonel: P _{min} (2)’den P _{max} a kadar
3	1 mW (0 dBm)	N/A	N/A	Opsiyonel: P _{min} (2)’den P _{max} a kadar

(1) Maksimum güç ayarındaki minimum çıkış gücü

(2) Düşük güç limiti P_{min}<-30 dBm önerilmekle birlikte zorunlu değildir. Uygulama gereklerine göre seçilebilir.

3.2.1 Modülasyon Karakteristikleri

Modülasyon BT nin 0,5 e eşit olduğu bir Gaussian Frequency Shift Keying (GFSK) modülasyonudur. Modülasyon indeksi 0,28 ile 0,35 arasında olmalıdır. Binary 1 pozitif bir frekans sapmasıyla; binary 0 ise negatif bir frekans sapmasıyla ifade edilir. Zamanlama sembolü ±20 ppm (part per million) den daha iyi olmalıdır.



Şekil 3.1 Transfer modülasyonu

Her gönderim kanalı için minimum frekans sapması ($F_{min} = \text{küçük}\{F_{min+}, F_{min-}\}$) 1010 sıralamasına karşılık gelir ve frekans sapmasının $\pm 80\%$ inden daha küçük olamaz.

Buna ek olarak minimum sapma 115 kHz. den küçük olamaz. Aktarılan verinin sembol hızı 1Mbit/sn. dir.

Sıfır geçiş hatası ideal sembol periyodu ile ölçülen geçiş zamanı arasındaki zaman farkıdır. Sembol periyodunun $\pm 1/8$ inden daha küçük olmalıdır.

3.2.2 Sahte Yayınım

Bant-içi ve bant-dışı sahte yayılım, tek frekansta atlama yapan bir frekans atlamalı verici ile ölçülür. Alış slotu ile veri slotu arasındaki frekans değiştirilmeli fakat her zaman aynı veri frekansına dönmelidir.

3.2.2.1 Bant-İçi Sahte Yayılım

Verici Tablo 3.4 de verildiği şekilde ISM bandı içinde bir spektrum maskesi geçirmelidir. Spektrum FCC nin 20 dB. bant genişliği tanımlamasına uygunluk göstermeli ve ona dayanarak ölçülmelidir. FCC gereksinimine ek olarak bitişik kanal gücü tanımlanmıştır. Bitişik kanal gücü 1 MHz. lik bir kanalda ölçülen güçlerin toplamı şeklinde tanımlanır. Aktarılan güç maksimum durağan mod kullanılarak 100 kHz. lik bant genişliği içinde ölçülür. Verici M kanalında transferi gerçekleştirmekte,

bitişik kanal gücü ise N kanalında ölçülmektedir. Verici test için gerçek olmayan bir veri paterni gönderir.

Tablo 3.4 Transfer spektrum maskesi

Frekans Ofseti	Transfer Gücü
± 500 kHz	-20 dBm
$ M-N = 2$	-20 dBm
$ M-N \geq 3$	-40 dBm

Çıkış gücü 0 dBm. den az ise, FCC nin 20 dB. kuralı Tablo 3.4 de gösterilen bitişik kanal gücü gereksiniminin önüne geçer.

3.2.2.2 Bant-Dışı Sahte Yayınım

Ölçülen güç mutlaka 100 kHz. bant genişliği içinde olmalıdır.

3.2.3 Radyo Frekans Toleransı

İletilen ilk merkezi frekans doğruluğu F_c den ± 75 kHz. olmalıdır. İlk frekans doğruluğu herhangi bir veri iletilmeden önceki frekans doğruluğudur. Frekans kayması gereksinimi ± 75 kHz. in içine dahil değildir.

Bir paketteki verici merkez frekans kayması Tablo 3.5 de verilmiştir. Farklı paketler temelbant spesifikasyonu kısmında tanımlanmıştır.

Tablo 3.5 Bir paketteki frekans kayması

Paket Tipi	Frekans Kayması
Tek-slot'luk paket	± 25 kHz
Üç-slot'luk paket	± 40 kHz
Beş-slot'luk paket	± 40 kHz
Maksimum kayma hızı ¹⁾	400 Hz/ μ sn.

(1) Maksimum kayma paket içinde herhangi bir yerde gerçekleşebilir.

3.3 Alıcı Karakteristikleri

Bit hata oranı (BER) performansını ölçebilmek için, cihaz mutlaka “geri döngü” özelliğine sahip olmalıdır. Cihaz şifresi çözülmüş bilgiyi geri gönderir.

Bu bölümde açıklanan referans duyarlık derecesi -70 dBm. dir.

3.3.1 Gerçek Duyarlık Derecesi

Gerçek duyarlık derecesi ham bit hata oranının (raw bit error rate=BER) %0.1 e eşit olduğu giriş seviyesidir. Bir Bluetooth alıcısı için gerçek hata derecesi -70 dBm. ya da daha iyi olmalıdır.

3.3.2 Girişim Performansı

Yan-Kanal (co-channel) ve bitişik 1 MHz. ve 2 MHz. kanallarındaki girişim performansı, referans duyarlık derecesinin 10 dB. üzerinde olan istenen işaret ile ölçülür. Bunun dışındaki tüm frekanslarda istenen işaret referans duyarlık derecesinin 3 dB. üzerindedir. Bir girişim işaretinin frekansı 2400-2497 MHz. lik bandın dışında olmalıdır. Girişim işareti Bluetooth modülasyonlu olabilir. $BER \leq \%0.1$ olmalıdır. Girişim oranları Tablo 3.6 da verildiği gibi olacaktır.

Tablo 3.6 Girişim performansı

Gereksinim	Oran
Yan-Kanal girişimi, $C/I_{\text{yan-kanal}}$	11 dB
Bitişik (1MHz) girişim, $C/I_{1\text{MHz}}$	0 dB
Bitişik (2MHz) girişim, $C/I_{2\text{MHz}}$	-30 dB
Bitişik ($\geq 3\text{MHz}$) girişim, $C/I_{\geq 3\text{MHz}}$	-40 dB
İmaj frekansı girişimi, C/I_{imaj}	-9 dB
İmaj frekansına bitişik (1 MHz) girişim, $C/I_{\text{imaj}\pm 1\text{MHz}}$	-20 dB

Bu oranlar normal sıcaklık koşullarında, tek alıcının tek bir frekansta atlaması dolayısıyla toplayıcının alıcı slot ve verici slot arasındaki frekansı değiştirmek zorunda olduğu fakat her zaman aynı alıcı frekansına döndüğü durumlarda test edilmiştir.

Gereksinimlerin karşılanmadığı frekanslar sahte cevap frekansları olarak adlandırılırlar. İstenen işareten ≥ 2 MHz. uzaklığındaki frekanslar içinden 5 adet sahte cevap frekansına izin verilir. Bu sahte cevap frekanslarında gevşek bir girişim gereksinimi ($C/I=-17$ dB) karşılanır.

3.3.3 Bant-Dışı Bloklama

Bant-dışı bloklama referans duyarlık derecesinin 3 dB. üzerindeki istenen işaret ile ölçülür. Girişim işareti sürekli bir dalga işareti şeklinde olacaktır. $BER \leq \%0.1$ olacaktır. Bant-dışı bloklama Tablo 3.7 de verilen gereksinimleri karşılamalıdır.

Verilen alıcı kanal frekanslarına bağlı olan 24 adet istisna frekansa izin verilir. Bu istisna frekanslar 1MHz. in tam katlarında yer alan frekanslardır. Bu frekansların 19 tanesinde BER in $\%0.1$ de kalmasını sağlamak için -50 dBm. gevşek güç seviyesi kullanılır. Geriye kalan 5 tanesinde güç seviyesi için herhangi bir kısıtlama yoktur.

Tablo 3.7 Bant-dışı bloklama gereksinimleri

Girişim İşareti Frekansı	Girişim İşareti Güç Kademesi
30 - 2000 MHz	-10 dBm
2000 - 2399 MHz	-27 dBm
2498 - 3000 MHz	-27 dBm
3000 MHz - 12.75 GHz	-10 dBm

3.3.4 Intermodülasyon Karakteristikleri

Referans duyarlık performansı, $BER=\%0.1$ aşağıdaki durumları karşılamalıdır:

- f_0 frekansında referans duyarlık derecesinin 6 dB. üzerinde istenen işaret.
- f_1 frekansında -39 dBm. lik güç seviyesinde bir statik sinüs dalgası
- f_2 frekansında -39 dBm. lik güç seviyesinde bir Bluetooth modülasyonlu işaret

$f_0=2f_1-f_2$ ve $|f_2-f_1|=n \times 1$ MHz. , $n=3,4,5$. Sistem yukarıdaki 3 alternatiften birini mutlaka sağlamalıdır.

3.3.5 Maksimum Elverişli Seviyeler

Maksimum elverişli giriş seviyesi için alıcı 20 dBm. den daha iyi çalışmalıdır. BER – 20 dBm. giriş gücünde %0.1 e eşit ya da küçük olmalıdır.

3.3.6 Sahte Emisyonlar

Bir Bluetooth alıcısı için sahte emisyonlar aşağıdaki değerlerden büyük olmamalıdır:

Tablo 3.8 Bant-dışı sahte emisyonlar

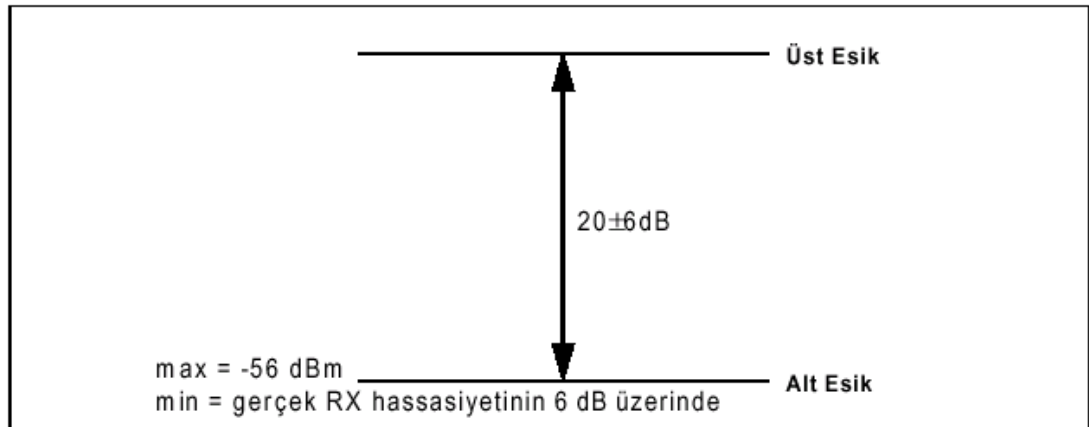
Frekans Bandı	Gereksinim
30 MHz - 1 GHz	-57 dBm
1 GHz - 12.75 GHz	-47 dBm

Ölçülen güç 100 kHz. lik bant genişliğinde ölçülmelidir.

3.3.7 Alıcının İşaret Güç İndikatörü (Seçime Bağlı)

Güç kontrollü linkleri desteklemek için alınan işaretin gücü ölçülebilmeli ve linkin diğer ucundaki vericinin kendi çıkış güç seviyesini artırması ya da azaltması gerektiğine karar vermesi sağlanmalıdır. RSSI ile bu mümkün hale gelir.

RSSI ölçümü alınan işaretin gücünü Altın Alıcı Güç Alanı (GRPR) olarak tanımlanan 2 eşik değeri ile kıyaslar. Alt eşik değeri –56 dBm. ile alıcının gerçek duyarlık değerinin 6 dB. üstündeki seviye arasında yer alır. Üst eşik değeri de alt eşik değerinin 20 ± 6 dB. üzerindedir.



Şekil 3.2 RSSI dinamik aralık

3.3.8 Referans İşaret Tanımlaması

Bluetooth modülasyonlu bir girişim işareti aşağıdaki şekilde tanımlanır:

Modülasyon=GFSK

Modülasyon indeksi = 0.32 ± 0.1

BT= 0.5 ± 0.1

Bit hızı= 1 Mbit/sn. ± 1 ppm

İstenen işaret için data modülasyonu= PRBS9

Girişim işareti için veri modülasyonu= PRBS15

Frekans doğruluğunun ± 1 ppm den iyi olması.

[6]

4. BLUETOOTH PROTOKOL MİMARİSİ

4.1 Giriş

4.1.1 Protokol Tanımı

Protokoller, cihazların bilgi alışverişi yapabilmeleri için üzerinde fikir birliğine varılan kurallardır. Ağ topolojilerinin bütün tipleri için mesajların linkler üzerinde nasıl iletileceğine ilişkin protokoller ve kurallar tanımlanmıştır. Protokoller bu mesajların formatları ile adres, hata kontrolü ve kullanıcı bilgisi gibi bilgiler için hangi alanların ayrıldığı bilgilerini de tanımlarlar.

Bilgi trafiğinin bir link üzerinden nasıl iletildiğine ilişkin örnekleri günlük hayatımızda da gözlemleyebiliriz. Örneğin araba kullanırken bir kavşağa geldiğimizde, trafik ışıkları tarafından yerine getirilen protokolü gözlemleyerek ne yapacağımız biliriz. Trafik ışığı ya da işareti olmayan durumlarda ise sürücüler arasında kimin ne zaman geçeceğine ilişkin bir karmaşa yaşanır. Böyle durumlarda trafik hızı yavaşlar ve problem çıkar.

Genel olarak kabul gören protokoller olmaz ise, donanım ve yazılım üreticileri kendi yöntemlerini geliştirerek üretim yapacakları için ağlar düzgün çalışmazlar. Aynı ağda bulunan cihazlar birbirleriyle haberleşemez duruma gelirler. 1960 ların sonuna doğru Transmission Control Protocol/Internet Protocol (TCP/IP) üzerine çalışılmaya başlanmış, bu tarihe kadar farklı üreticilerin ürettiği bilgisayarların birbirleri ile haberleşmelerini sağlamak mümkün olmamıştı. Bugün ise TCP/IP katmanını içeren bütün bilgisayar yapıları internete bağlanarak birbirleri ile haberleşebilmektedirler. Bütün bilgisayarlarda yüklü olan TCP/IP katmanı üzerinden bilgi alışverişi yapılabilmektedir.

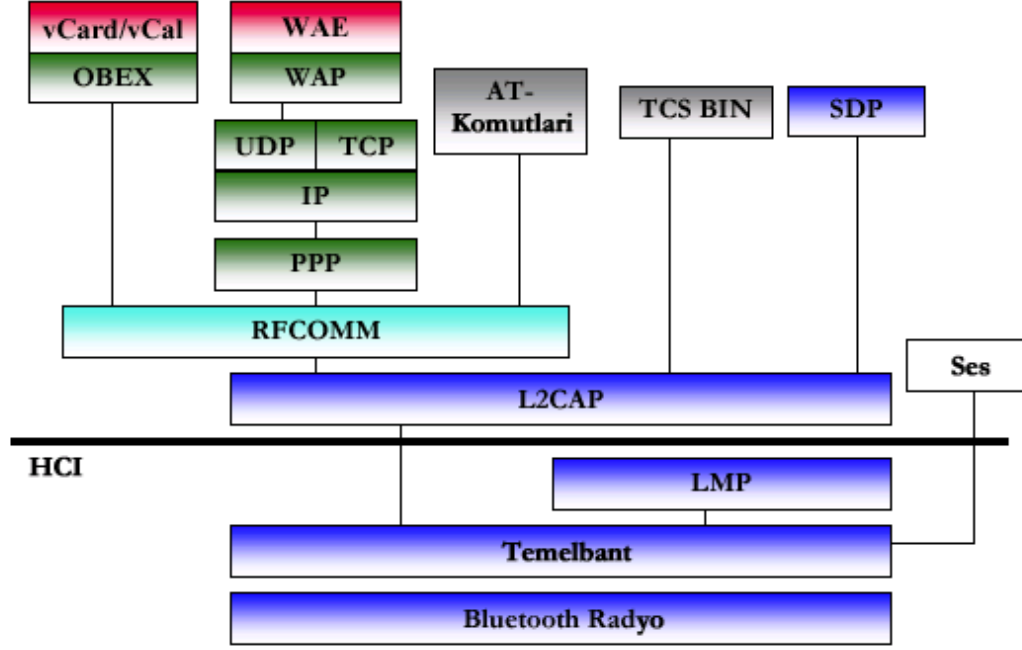
1970 lerin ortalarında, uluslararası standartlar organizasyonu Open Systems Interconnection (OSI) olarak adlandırılan genel referans modelini oluşturma görevini üstlenmiştir. OSI referans modeli haberleşme süreçlerini modellemek ve cihazların standartlara uyumluluk özelliklerini karşılaştırmak için bir model sunar. Ayrıca

üreticilerin de farklı haberleşme gereksinimlerini karşılarken doğru sınıflama yapmalarına yardımcı olur.

4.1.2 Bluetooth Protokol Mimarisi

Bluetooth spesifikasyonunun temel amacı, spesifikasyona uygun olarak geliştirilmiş uygulamaların birbirleri ile uyumlu olarak çalışmalarını sağlamaktır. Bu uyumluluğu sağlamak için, uzak cihazlardaki eşleşen uygulamalar (örneğin birbirlerine tekabül eden istemci-sunucu (client-server) uygulamaları) aynı protokol katmanı üzerinde çalışmalıdır. Örneğin vCard->OBEX->RFCOMM->L2CAP->Temelbant protokol listesi yukarıdan aşağıya doğru iş kartı değiş tokuş uygulamasını destekleyen protokol katman yapısını göstermektedir. Bu yapı hem dahili bir obje sunumu (vCard), hem de hava üzerinden olan transfer protokollerini içermektedir.

Farklı uygulamalar, farklı protokol katmanlarında çalışabilirler. Bununla birlikte, bu farklı protokol katmanlarının her biri ortak bir Bluetooth veri linki ve fiziksel katman kullanırlar. Şekil 4.1 de bütün Bluetooth protokolleri gösterilmektedir. Uygulamalar bütün protokolleri kullanmazlar, genellikle bir veya birden fazla dikey dilimi kullanırlar. Tipik olarak, ek dikey dilimler, ana uygulamanın destekleyicisi olan servislerdir. Şekil 4.1 taşınan bilgi (payload) verisi hava üzerinden iletilmek istendiğinde protokollerin diğer protokollerin servislerini nasıl kullandığını da göstermektedir. Bazı protokoller diğer protokollerle başka ilişkilerde de bulunurlar. Örneğin L2CAP, “Telefon Kontrol Protokolü (TCS) Binary” gibi protokoller link yöneticisini kontrol etmek gerektiğinde LMP yi kullanırlar.



Şekil 4.1 Bluetooth protokol yığını

Şekil 4.1’den görüleceği gibi, Bluetooth protokol yığını, LMP ve L2CAP gibi Bluetooth’a özel protokoller ve “Obje Değiş-Tokuş Protokolü” (OBEX) ve UDP gibi Bluetooth’a özel olmayan protokollerden oluşur. Protokol yığını geliştirilirken varolan protokollerin üst katmanlarda mümkün olduğu kadar çok kullanılmasına çalışılmıştır. Protokollerin tekrar kullanımı, bilinen mevcut uygulamaların da Bluetooth uygulamaları ile uyumluluk göstermesine yardımcı olur. Bluetooth spesifikasyonu açık bir altyapıya sahip olduğu için üreticiler kendi uygulama protokollerini Bluetooth’a özgü protokollere uygun hale getirebilirler. Böylece bir çok yeni uygulama geliştirilebilir.

4.1.3 Bluetooth Protokol Yığınındaki Protokoller

Bluetooth protokol yığını amaçlarına ve Bluetooth SIG in protokolleri belirlerken aldığı role göre dört bölüme ayrılır. Katmanlarda yer alan protokoller aşağıda belirtilmiştir.

Tablo 4.1 Bluetooth protokol yığınınındaki protokol ve katmanlar

Protokol Katmanı	Yığındaki Protokoller
Bluetooth Ana Protokolleri	Temelbant, LMP, L2CAP, SDP
Kablo Yerine Geçen Protokol	RFCOMM
Telefon Kontrol Protokolleri	TCS Binary, AT-komutları
Uyarlanmış Protokoller	PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

Yukarıdaki protokollere ek olarak, spesifikasyon temelbant kontrolörü ve link yöneticisine bir komut arayüzü ile donanım durumu ve kontrol kaydedicilerine erişim sağlayan Host Kontrolör Arayüzü (HCI) nü tanımlamıştır. Şekil 4.1 de HCI L2CAP in altında konumlandırılmıştır fakat üzerinde de olabilir.

Bluetooth ana protokolleri Bluetooth teknolojisine özeldir ve Bluetooth SIG tarafından geliştirilmişlerdir. RFCOMM ve TCS Binary protokolleri de Bluetooth SIG tarafından geliştirilmişlerdir ancak ETSI TS 07.10 ve ITU-T Q.931 temeline dayandırılmışlardır. Bluetooth ana protokollerine ve Bluetooth radyoya tüm Bluetooth cihazları tarafından gereksinim duyulurken; diğerleri sadece ihtiyaç duyulduğunda kullanılmaktadır.

Kablo yerine geçen protokol, telefon kontrol ve uyarlanmış protokol katmanları uygulamaların Bluetooth ana protokolleri üzerinde çalışmasını sağlayan uygulama yönelimli protokollerdir. Bluetooth spesifikasyonu açık bir altyapıya sahiptir ve “Hypertext Transfer Protokolü” (HTTP), “Dosya Transfer Protokolü” (FTP) gibi protokoller de Bluetooth’a özel transfer protokollerinin en üst seviyesi ile uyumluluk içinde çalışabilirler.

4.1.3.1 Bluetooth Ana Protokolleri

Temelbant

Temelbant ve Link Kontrol katmanı piconet oluşturan Bluetooth üniteleri arasında fiziksel RF linki oluşmasını sağlarlar. Bluetooth RF sistemi, paketlerin belirli frekanslardaki belirli zaman aralıklarında aktarıldığı FHSS yöntemini kullandığı için, bu katman farklı Bluetooth cihazlarının saatleri ve transfer atlama frekanslarının senkronize olmasını sağlayan sorgulama ve çağrı (paging) prosedürleri kullanır.

Temelbant aynı RF linki üzerinde çoğullama prensibine dayanarak aktarılabilen iki farklı fiziksel link tipi tanımlar: Senkron Bağlantı-Yönelimli (SCO) ve Asenkron Bağlantısız (ACL). ACL paketleri sadece veri için kullanılırken, SCO paketleri ses ya da ses ve verinin kombinasyonu için de kullanılabilirler. Bütün ses ve veri paketleri İleri Hata Düzeltme (FEC) veya Cyclic Redundancy Check (CRC) hata düzeltme tekniklerinin değişik seviyelerini içerebilir ve şifrelenebilirler.

Farklı veri tipleri (link yönetimi ve kontrol mesajları dahil) özel bir kanala tahsis edilirler.

Ses (Audio)

Ses bilgisi Bluetooth cihazları arasında aktarılabilir ve çeşitli kullanım modellerini mümkün kılar. SCO paketlerindeki ses verisi, temelbant üzerinden yönlendirilir; L2CAP'e geçmez. Bluetooth cihazları basit olarak bir ses linki açarak ses verisini taşıyabilirler.

Link Yönetim Protokolü

Link yönetim protokolü Bluetooth cihazları arasında bir link kurulmasını sağlar. Link ve şifreleme anahtarlarını oluşturup, kontrol ederek ve temelbant paket boyutlarını kontrol ederek doğrulama ve şifreleme işlemlerini yerine getirir.

Bluetooth radyo cihazının görev dönüşümlerini, bağlantı durumlarını ve güç modlarını kontrol eder.

L2CAP

L2CAP, temelbant üzerindeki üst katman protokollerini uyarlar. LMP ile paralel olarak çalıştığı düşünülebilir, fakat L2CAP farklı olarak LMP mesajlarında taşınan bilgi (payload) verisi gönderilmediğinde üst katmana servis sağlar.

L2CAP protokol çoğullama, ayrıştırma ve tekrar birleştirme işlemleri ile üst katman protokollerine bağlantı yönelimli ve bağlantısız veri servisleri sağlar. L2CAP, üst katman protokollerinin ve uygulamalarının 64 kilobyte uzunluğuna kadar L2CAP veri paketlerini iletmelerini sağlar.

Temelbant protokolünün SCO ve ACL link tiplerini desteklemesine rağmen, L2CAP sadece ACL linklerini desteklemektedir.

Servis Keşif Protokolü (SDP)

Keşif servisleri Bluetooth çalışma şeklinin kritik kısımlarıdır. Bu servisler tüm kullanım modelleri için temel teşkil ederler. “Servis Keşif Protokolü” (SDP) kullanarak cihaz bilgisi, servisleri, servislerin karakteristikleri sorgulanabilir ve bu sorguyu takiben iki veya daha fazla Bluetooth cihazı arasında bağlantı kurulabilir.

4.1.3.2 Kablo Yerine Geçen Protokol

RFCOMM

RFCOMM ETSI 07.10 spesifikasyonuna dayanan bir seri haberleşme emülasyon protokolüdür. Bu “kablo yerine geçen” protokol transfer mekanizması olarak seri haberleşme kullanan üst katman servisleri için (örneğin OBEX) transfer kabiliyeti sağlayarak RS-232 kontrolünü ve Bluetooth temelbandı üzerinden veri işaretlerini emüle eder.

4.1.3.3 Telefon Kontrol Protokolü

Telefon Kontrol-Binary

Telefon Kontrol Protokolü – Binary (TCS Binary veya TCS Bin); Bluetooth cihazları arasında konuşma ve veri çağrılarının kurulması için çağrı kontrol işaretleşmesini tanımlayan bit tabanlı bir protokoldür. Ayrıca, Bluetooth TCS cihaz gruplarını yönetmek için gereken mobilite yönetim prosedürlerini de tanımlar. TCS Binary ITU-T Q.931’e dayalı olan Bluetooth Telefon Kontrol Protokolü içinde tanımlanmıştır.

Telefon Kontrol-AT Komutları

Bluetooth SIG, çoklu kullanım modellerinde bir mobil telefon ya da modemin kontrol edilmesini sağlayan AT komut setini tanımlamıştır. Bluetooth’da kullanılan AT komutları ITU-T V.250 ve ETS 300 196 prosedürlerine dayanır. Ayrıca, faks servisleri için kullanılan komutlar da uygulama ile belirlenir. Aşağıdaki faks servislerinden birisi kullanılabilir:

- Faks Sınıfı 1.0 TIA-578-A ve ITU T.31 Servis Sınıfı 1.0
- Faks Sınıfı 2.0 TIA-592 ve ITU T.32 Servis Sınıfı 2.0
- Faks Servis Sınıfı 2 – Endüstri standardı yoktur.

4.1.3.4 Uyarlanmış Protokoller

PPP

PPP, RFCOMM üzerinde çalışarak noktadan noktaya bağlantı kurmak için tasarlanmıştır. PPP, IETF Noktadan-Noktaya protokolüdür ve PPP-Ağ Yapısı da IP paketlerini PPP katmanından alarak LAN'a yerleştirmek ya da tam tersini yapmak anlamına gelir.

TCP/UDP/IP

Bu protokol standartları Internet Engineering Task Force tarafından tanımlanmıştır ve internet üzerinden haberleşme için kullanılır. Şu an dünyada en çok kullanılan protokol olan TCP/IP katmanı birçok yazıcı, el bilgisayarı ve mobil cihazda bulunmaktadır. Bu protokollere erişim bir soket programlama arayüz modeli kullandığı halde işletim sisteminden bağımsızdır. Bluetooth cihazlarında bu standartların uygulanması internete bağlı olan herhangi bir cihaz ile haberleşmeyi mümkün kılar.

OBEX Protokolü

IrOBEX ya da kısaca OBEX, IrDA tarafından objeleri basit ve anında oluşan (spontane) bir yolla değiş tokuş etmek için geliştirilen bir oturum protokolüdür. OBEX, HTTP'ye benzer bir temel fonksiyonalityyi bir istemci-sunucu modeli kullanarak ve iletim API si ile iletim mekanizmasından bağımsız olarak daha basit şekilde gerçekleştirir. Protokolün kendisi de, cihazlar arasındaki OBEX konuşmaları için gramer, obje ve operasyonları tanımlamak için bir model sağlar. OBEX ayrıca, uzak cihazdaki dosyaların içeriğinde tarama yapmak (browse) için kullanılan bir dosya-listeleme objesi de tanımlar.

İlk aşamada RFCOMM OBEX için tek transfer katmanı olarak kullanılmıştır. İlerdeki uygulamaların TCP/IP kullanması da beklenmektedir.

İçerik Formatları

vCard, vCalender Internet Mail Consortium tarafından kontrol edilmekte olan açık uygulamalardır. Bu spesifikasyonlar sırası ile elektronik iş kartı ve kişisel takvim girdileri ile düzenlemelerinin formatını tanımlarlar. Herhangi bir iletim mekanizması tanımlamaksızın, aktarılan veriye bağlı olan formatı tanımlarlar. Tam

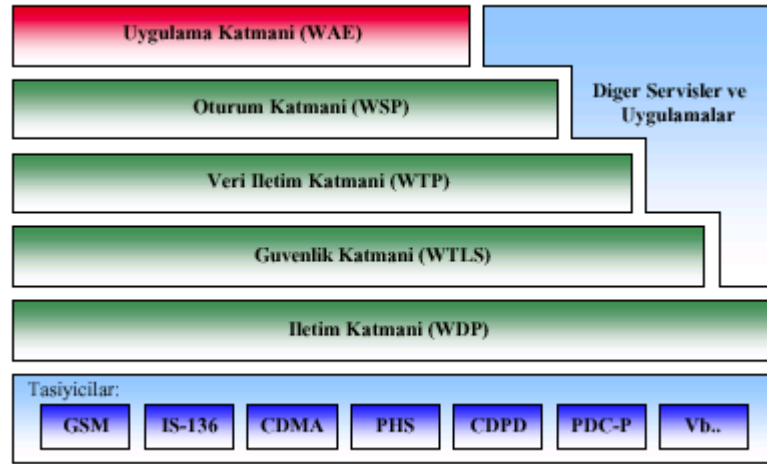
olarak tanımlanan bu formatlar yardımıyla kişisel bilginin deęiş tokuşunun daha kolay yapılması amaçlanmıştır.

Bluetooth da OBEX tarafından aktarılan dięer ierik formatları vMessage ve vNote dur.

WAP

Gizli hesaplama kullanım modelleri WAP zellikleri kullanılarak uygulanabilir.

Wireless Application Protokol (WAP) Forum, geniř alan kablosuz aęlarda alıřabilen bir kablosuz protokol spesifikasyonu inřa etmiřtir. Ama internetteki ierięi ve telefon servislerini mobil telefonlara ve dięer mobil cihazlara tařımaktır. řekil 4.2 de WAP alıřma modelinin protokol yapısı gsterilmektedir.



řekil 4.2 WAP alıřma řekli protokol yapısı

WAP seiminin arkasındaki fikir, WAP Application Environment (WAE) iin geliřtirilmiř üř seviye yazılım uygulamalarını tekrar kullanabilmektir. Bu uygulamalar PC uygulamaları ile alıřabilen WML ve WTA tarayıcılarını (browser) da ierir. WAP sunucuları ile PC ortamındaki bařka bir uygulama arasında bulunan uygulama arageitleri inřa ederek; uzaktan kumanda, bilgisayardan mobil telefona veri transferi gibi bađı gizli hesaplama fonksiyonları gerekleřtirilebilir. WAP sunucuları ayrıca bilgisayar ve mobil telefon arasında ierik transferine de imkan vermektedirler.

İerik formatları

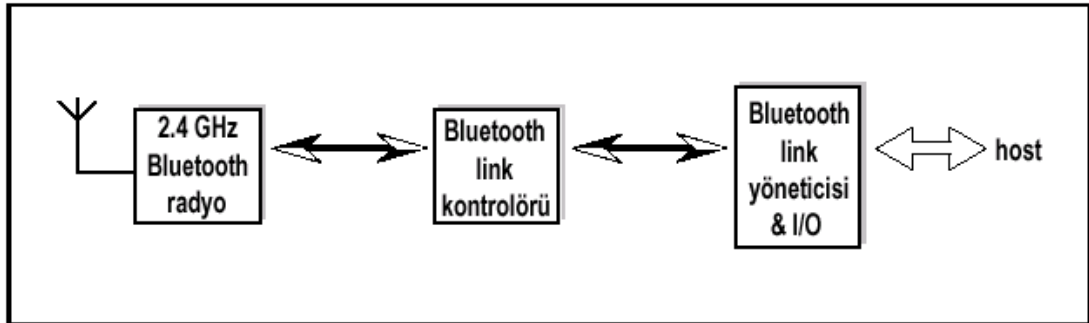
Bluetooth üzerinden WAP iin desteklenen ierik formatları WML, WMLScript, WTA, WBMP ve vCard/vCal dır. Tüm bu formatlar WAE'nin bir parasıdır. [7]

4.2 Temelbant Protokolü

4.2.1 Giriş

Bluetooth sisteminde girişim ve zayıflamayı azaltmak için bir frekans atlama alıcı-vericisi (transciever) kullanılır. Alıcı-vericiyi basitleştirmek için binary frekans modülasyonu (FM) kullanılır. Sembol hızı 1 Mbit/sn. dir. Nominal zaman aralığı (slot) uzunluğu 625 μ sn. olan slotlanmış bir kanal uygulanır. Tam duplex iletim için Zaman Bölmeli Duplex (TDD) şeması kullanılır. Bilgi kanal içinden paketler yardımıyla taşınır. Her paket farklı bir atlama frekansında taşınır. Bir paket normal olarak bir slot kapsar fakat 5 slot kapsayacak şekilde genişletilebilir. Bluetooth, devre ve paket bağlaşımlarının bir kombinasyonunu kullanır. Slotlar senkron paketler için rezerve edilebilir. Bluetooth asenkron bir veri kanalını, aynı anda maksimum 3 adet senkron ses kanalını veya asenkron veri ve senkron sesi aynı anda destekleyen bir kanalı desteleyebilir. Her ses kanalı her iki yönde de 64 kbit/sn. senkron ses kanalını destekler. Asenkron kanal ise maksimum 723.2 kbit/sn. asimetrik (dönüş yönünde 57.6 kbit/sn. dir) ya da 433.9 kbit/sn. simetrik transferi destekler.

Bluetooth sistemi bir radyo ünitesi, bir link kontrol ünitesi ve link yönetimi ile sunucu-istemci arayüz fonksiyonları için kullanılan bir destek ünitesinden oluşur.



Şekil 4.3 Bluetooth sistemindeki fonksiyonel bloklar

4.2.2 Fiziksel Kanal

4.2.2.1 Kanal Tanımlaması

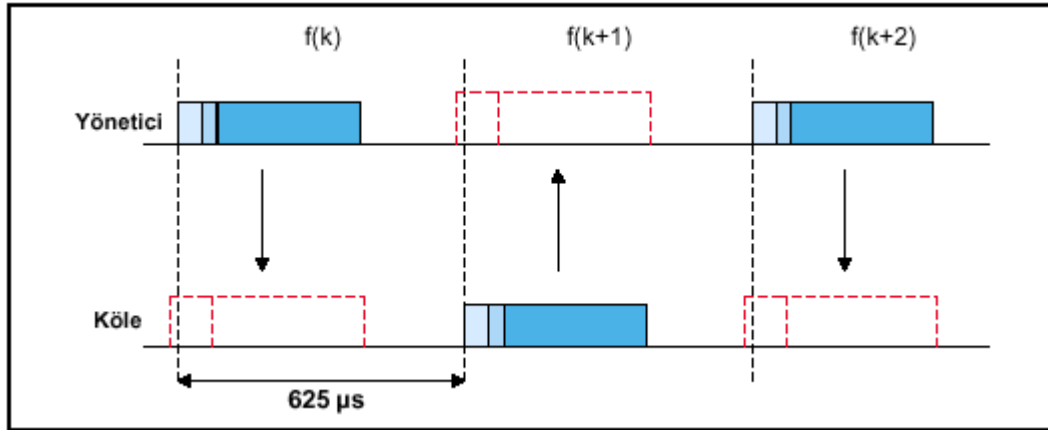
Kanal, 79 ya da 23 RF kanalı arasında atlama yapan bir rasgele atlama dizisi ile tanımlanır. Atlama dizisi pikonet için tektir ve yönetici cihazın Bluetooth adresi tarafından belirlenir. Atlama dizisi fazı da yöneticinin Bluetooth saati tarafından

belirlenir. Kanal her biri bir RF atlama frekansına denk gelen zaman slotlarına bölünür. Ardışık atlamalar değişik RF atlama frekanslarına tekabül ederler. Nominal atlama değeri 1600 atlama/sn. dir. Pikonete dahil olan tüm Bluetooth cihazları kanal ile zaman ve atlama açısından senkronizedirler.

4.2.2.2 Zaman Slotları

Kanal, herbirinin uzunluğu $625\mu s$ olan zaman slotlarına bölünür. Zaman slotları, pikonetteki yönetici cihazın Bluetooth saatine göre numaralanır ve 0 dan $2^{27}-1$ 'e kadar sayıda olabilir. Zaman slotlarında yönetici ve köle cihazlar paketleri iletebilirler.

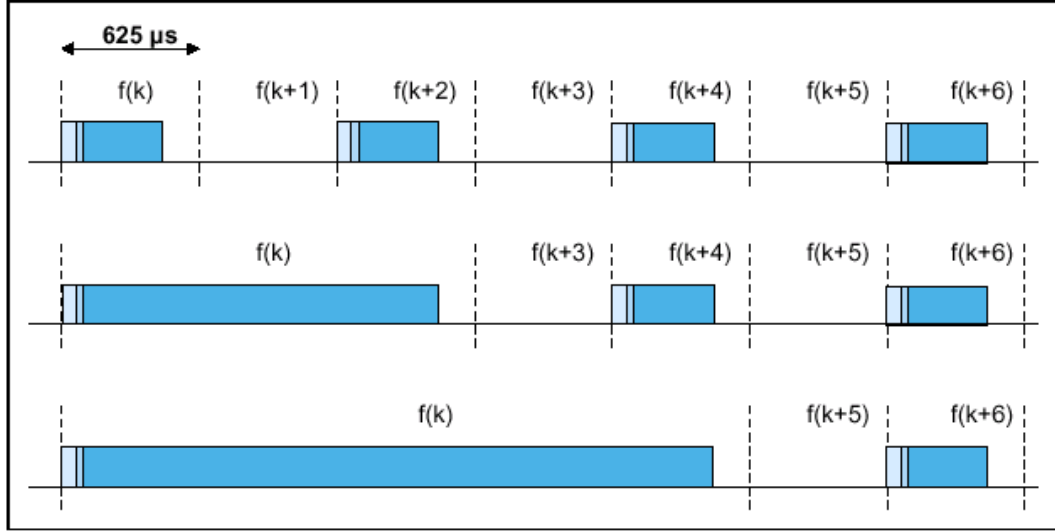
Şekil 4.4 de yönetici ve köle cihazların sıra ile ilettime geçtikleri durumda kullanılan bir TDD şeması gösterilmiştir. Yönetici cihaz çift numaralı zaman slotlarında, köle cihaz ise tek numaralı zaman slotlarında ilettime geçer. Paket başlangıcı slot başlangıcı ile birlikte meydana gelir. Yönetici ya da köle tarafından iletilen paketler en fazla 5 zaman slotundan iletebilirler.



Şekil 4.4 TDD ve zamanlama

RF atlama frekansı paket süresi için ayarlanmalıdır. Tek bir paket için kullanılan RF atlama frekansı mevcut Bluetooth saat değerinden elde edilir. Çoklu paket için kullanılan RF atlama frekansı ise paketin ilk slotundaki Bluetooth saat değerinden elde edilir. Çoklu bir paketten sonra gelen ilk slottaki RF atlama frekansı da mevcut Bluetooth saat değerinden elde edilen frekansı kullanır.

Şekil 4.5 de tek ve çoklu paketlerdeki atlama tanımlaması ifade edilmiştir. Eğer bir paket birden fazla zaman slotu içinde yer alırsa pakete uygulanacak atlama frekansı paketin iletiminin başladığı zaman slotunda uygulanan atlama frekansı olur.



Şekil 4.5 Çok slotlu paketler

4.2.3 Fiziksel Linkler

Yönetici ve köle(ler) arasında değişik tipte linkler kurulabilir. İki link tipi tanımlanmıştır:

- Senkron, Bağlantı Yönelimli (SCO) link
- Asenkron, Bağlantısız (ACL) link

SCO linki pikonetteki yönetici ve tek bir köle arasında kurulan tek noktadan tek noktaya çalışan bir link tipidir. Yönetici, düzenli zaman aralıklarında rezerve edilmiş slotları kullanarak SCO linkini kurar. ACL ise pikonetteki yönetici ve tüm köleler arasında kurulan tek noktadan çok noktaya çalışan bir link tipidir. SCO için ayrılmayan zaman slotlarında yönetici “slot başına” prensibine dayalı olarak ACL linklerini kurar. ACL linkleri bir SCO linkinde yer alan köleler ile dahi kurulabilir.

4.2.3.1 SCO Linki

SCO linki bir yönetici ve belirli bir köle arasında tek noktadan tek noktaya kurulan simetrik bir linktir. SCO linki slotları tuttuğu için yönetici ve köle arasındaki devre bağlaşmalı bir bağlantı gibi düşünülebilir. Bir SCO linki tipik olarak ses gibi zamana bağlı bilgi çeşidini destekler. Bir yönetici aynı köleye ya da farklı kölelere en fazla üç SCO linkini destekler. Bir köle aynı yöneticiden gelen en fazla üç SCO linkini ya da farklı yöneticilerden gelen en fazla iki SCO linkini destekler. SCO paketleri kesinlikle tekrar iletilmez.

Yönetici T_{SCO} denilen düzenli aralıklarda başka bir deyişle rezerve edilen yöneticiden köleye olan slotlarda SCO paketlerini gönderir. SCO köle, takip eden köleden yöneticiye olan slotta SCO paketi ile cevap verir. Bu durum sadece bir önceki yöneticiden köleye olan slotta farklı bir köle adreslenmişse geçerli olmaz. SCO köle paket başlığındaki köle adresinin kodunu çözmekte başarısız olursa, yine de tutulan SCO slotunda bir SCO paketi gönderebilir.

SCO linki yöneticinin LM protokolü yardımıyla bir SCO kurulum mesajı göndermesi ile kurulur. Bu mesaj SCO aralığı (T_{SCO}) ve rezerve edilen slotları belirtmek için kullanılan ofset değeri (D_{SCO}) gibi zaman parametrelerini içerir.

LMP kurulum mesajındaki bir başlangıç bayrağı başlangıç prosedürü olarak 1 ya da 2 nin kullanılıp kullanılmadığını belirler. Köle bu bayraktan aldığı veriye dayanarak bir başlangıç metodu uygular. Yönetici; yönetici saati (CLK_{27}) 0 iken başlangıç 1 i, yönetici saati (CLK_{27}) 1 iken ise başlangıç 2 yi kullanır. Yöneticiden köleye olan SCO slotları yönetici tarafından rezerve edilir ve saatin aşağıdaki eşitliği sağladığı slotlar için başlatılır:

$$CLK_{27-1} \bmod T_{SCO} = D_{SCO} \quad \text{başlangıç 1 için}$$

$$(\overline{CLK_{27}}, CLK_{26-1}) \bmod T_{SCO} = D_{SCO} \quad \text{başlangıç 2 için}$$

Köleden yöneticiye olan SCO slotları rezerve edilen yöneticiden köleye olan slotları takip eder. Başlangıç sonrasında bir sonraki yöneticiden köleye olan SCO slotunun saat değeri olan $CLK(k+1)$, mevcut yöneticiden köleye olan SCO slotunun saat değerine belirli bir değer olan T_{SCO} değeri eklenerek bulunur:

$$CLK(k+1) = CLK(k) + T_{SCO}$$

4.2.3.2 ACL Linki

SCO linkleri için rezerve edilmeyen slotlarda, yönetici herhangi bir köle ile “slot başına” temeline dayanarak paketleri değiş tokuş edebilir. ACL linki pikonetteki yönetici ile aktif olan tüm köleler arasında paket bağlaşmalı bir bağlantı oluşturur. Hem asenkron hem de senkron servisler desteklenir. Bir yönetici ve bir köle arasında sadece tek bir ACL linki bulunabilir.

Köleden yöneticiye olan slotta bir ACL paketini iade etmeye (return) yetkili bir köle, sadece önde bulunan yöneticiden köleye olan slotta adreslenmişse bu görevi yerine

getirebilir. Eğer köle paket başlığındaki köle adresinin kodunu çözmemişse, iletme izin verilmez.

ACL paketleri belirli bir köleye adreslenmezler; yayın amaçlı kullanılan paketlerdir ve her köle tarafından okunabilirler. ACL linki üzerinde hiçbir veri gönderilmemişse ve yoklama (polling) istenmiyorsa hiçbir iletim de gerçekleşmez.

4.2.4 Paketler

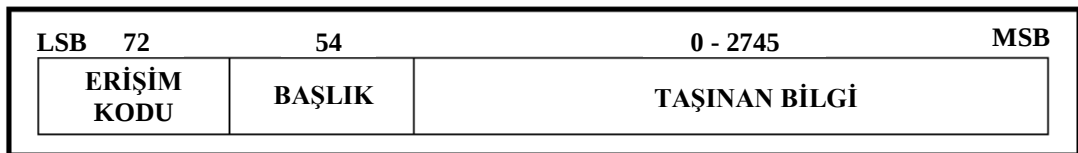
4.2.4.1 Genel Format

Temelbant spesifikasyonunda paket ve mesajları tanımlarken kullanılan bit sıralaması aşağıdaki kuralların uygulandığı “Little Endian Format” ı kullanır:

- En az ağırlığı olan bit (LSB) b_0 ile temsil edilir.
- Havadan gönderilen ilk bit LSB dir.
- Somut gösterimlerde LSB sol tarafta yer alır.

Link kontrolörü daha yüksek bir yazılım katmanından gelen ilk biti b_0 olarak yorumlar. Bu bit havaya gönderilecek ilk bittir. Temelbant seviyesinde dahili olarak üretilen paket başlık alanları ve taşınan bilgi (payload) başlık uzunluğu gibi veri alanları ilk olarak LSB ile iletilir. Örneğin $X=3$ şeklindeki 3-bitli bir parametre 0 1 2 şeklinde iletilir.

Pikonet kanalındaki veri paketler halinde taşınır. Genel paket formatı Şekil 4.6 da gösterildiği şekildedir. Her paket 3 parametreden oluşur: Erişim kodu, başlık ve taşınan bilgi (payload). Aşağıdaki şekilde her giriş için kullanılan bit sayısı gösterilmiştir.



Şekil 4.6 Standart paket formatı

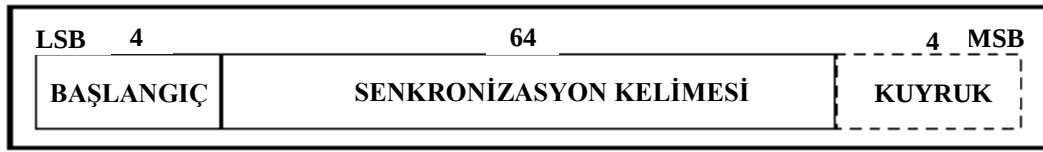
Erişim kodu ve başlık bölümleri sırasıyla 72 bit ve 54 bit olurlar. Taşınan bilgi (payload) ise 0 dan 2745 bite kadar olan aralıkta değişir. Değişik paket tipleri tanımlanmıştır: Sadece erişim kodunu içeren paketler, erişim kodu ve başlığı içeren paketler ve erişim kodu, başlık ve taşınan bilgiyi (payload) içeren paketler.

4.2.4.2 Eriřim Kodu

Her paket bir eriřim kodu ile bařlar. Eęer bunu bir paket bařlıęı takip ediyorsa eriřim kodu 72 bit uzunluęunda aksi durumda da 68 bit uzunluęunda olur. Eriřim kodu senkronizasyon, DC ofset kompenzasyonu ve kimlik tanıma için kullanılır. Eriřim kodu piconetteki kanalda alınıp gönderilen paketleri tanır. Aynı piconette bulunan tüm paketler aynı eriřim kodunu taşırlar. Alıcı olan Bluetooth ünitesinde sürme ilişkilendirici, bu eriřim koduna göre ilişki kurar ve bir eřik deęeri ařıldığında tetikleme yapar. Bu tetikleme işareti de alıř zamanını belirlemede kullanılır.

Eriřim kodu aynı zamanda çağrı (paging) ve sorgu prosedürlerinde de kullanılır. Bu durumda eriřim kodunun kendisi bir işaretleşme mesajı olarak kullanılır ve ne bařlık ne de taşınan bilgi (payload) bulunur.

Eriřim kodunun bir bařlangıç bilgisi, bir senkronizasyon kelimesi ve muhtemelen bir de kuyruk (trailer) bulunur.



Şekil 4.7 Eriřim kodu formatı

Eriřim Kodu Tipleri

Eriřim kodlarının üç farklı tipi mevcuttur:

- Kanal Eriřim Kodu (CAC)
- Cihaz Eriřim Kodu (DAC)
- Sorgu Eriřim Kodu (IAC)

Bu eriřim kodları bir Bluetooth ünitesinin deęişik modlarda çalışması için kullanılır. Kanal eriřim kodu bir piconeti tanımlar. Bu kod piconette alınıp gönderilen her pakette bulunur. Cihaz eriřim kodu çağrı (paging) ve çağrı (paging) cevabı gibi özel işaretleşme prosedürleri için kullanılır. Sorgu eriřim kodu için iki farklı durum söz konusudur. Genel Sorgu Eriřim Kodu (GIAC) tüm cihazlar için geçerlidir. GIAC hangi Bluetooth cihazlarının etki alanı içinde olduğunu belirlemede kullanılır. Dedike Sorgu Eriřim Kodu (DIAC) ise genel bir karakteristięi paylařan dedike bir

Bluetooth cihaz grubu tarafından kullanılır. DIAC sadece dedike olan Bluetooth cihazlarının etki alanı içinde olup olmadığını belirlemede kullanılır.

CAC başlangıç bilgisi, senkronizasyon kelimesi ve kuyruk (trailer) tan oluşur ve toplam uzunluğu 72 bittir. Başlıkları olmayan mesajlar için DAC ve IAC kuyruk (trailer) içermez ve 68 bitten oluşurlar.

Farklı erişim kodu tipleri senkronizasyon cümlesini oluşturmak için değişik Düşük Adres Bölümleri (LAP) kullanılır. Değişik erişim kodu tiplerinin bir özeti Tablo 4.2 de açıklanmıştır.

Tablo 4.2 Erişim kodları özeti

Kod Tipi	LAP	Kod Uzunluğu
CAC	Yönetici	72
DAC	Çağrılan (Paged) Ünite	68/72
GIAC	Rezerve	68/72
DIAC	Dedike	68/72

Başlangıç Bilgisi

Başlangıç bilgisi DC kompenzasyonunu gerçekleştirmek için kullanılan 4 sembolü bir 0-1 paternidir. Diziliş sırası, takip eden senkronizasyon kelimesinin LSB sinin 1 veya 0 olmasına bağlı olarak 1010 ya da 0101 olur. Başlangıç bilgisi Şekil 4.8 de gösterilmiştir.



Şekil 4.8 Başlangıç bilgisi

Senkronizyon Kelimesi

Senkronizasyon kelimesi 24 bit bir adresten (LAP) elde edilen 64 bitlik bir koddur. CAC için yöneticinin LAP'ı; GIAC ve DIAC için rezerve ve dedike LAP lar; DAC için ise köle ünitenin LAP'ı kullanılır. Senkronizasyon kelimesinin oto korelasyon özelliği zamanlama senkronizasyon prosesi üzerinde gelişir.

Kuyruk (Trailer)

Kuyruk (trailer), senkronizasyon kelimesi ile erişim kodunu takip eden paket başlığını ilişkilendirir. Bu tipik olarak CAC için gerekli olup; DAC ve IAC da da -bu kodlar çağrı (paging) cevabı ve sorgulama cevap prosedürleri esnasında alınıp gönderilen “Frekans Atlama Senkronizasyonu” (FHS) paketlerinde kullanıldığında-kullanılır.

Kuyruk (trailer), 4 sembollü bir 1-0 paternidir. Kuyruk (trailer) ile senkronizasyon kelimesinin 3 “En Yüksek Değerli Bit” (MSB) i genişletilmiş DC kompenzasyon için kullanılan 1 ve 0 ların değiştiği 7-bitli bir patern oluştururlar. Kuyruk (trailer) sırası senkronizasyon kelimesinin MSB sinin 0 veya 1 olmasına göre sırasıyla 1010 veya 0101 olabilir. Kuyruk (trailer) seçimi Şekil 4.9 da gösterilmiştir.



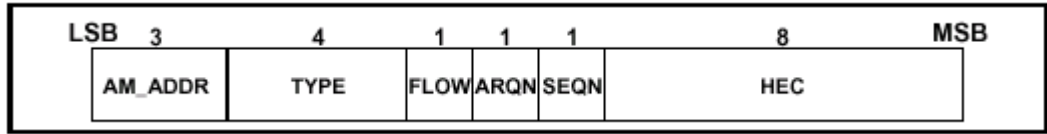
Şekil 4.9 CAC daki kuyruk (trailer). Senkronizasyon sözcüğünün MSB si 0 iken (a), ve 1 iken (b).

4.2.4.3 Paket Başlığı

Paket başlığı, link kontrolü (LC) bilgisini içerir ve 6 alandan oluşur:

- AM_ADDR: 3-bit aktif üye adresi
- TYPE: 4-bit tip kodu
- FLOW: 1-bit akış kontrolü
- ARQN: 1-bit alındı bilgisi göstergesi
- SEQN: 1-bit sıra numarası
- HEC: 8-bit başlık hata kontrolü

Başlık bilgisi Şekil 4.10 da da gösterildiği gibi HEC dahil toplam 18 bittir. Başlık bilgisi 1/3 hızlı FEC ile kodlanarak 54-bit durumuna gelir. “Aktif Üye Adresi” (Active Member Address-AM_ADDR) ve TYPE alanları LSB ile gönderilir.



Şekil 4.10 Başlık formatı

AM_ADDR

AM_ADDR bir üye adresini temsil eder ve pikonetteki aktif üyeleri ayırt etmek için kullanılır. Bir pikonette bir veya birden fazla köle tek bir yöneticiye bağlıdır. Kölelerin ayrı olarak tanımlanabilmesi için her köleye aktif olduğu zaman geçici olarak 3-bitlik bir adres atanır. Yönetici ile köle arasında iletilen tüm paketler o köleye ait AM_ADDR yi taşırlar. Kölenin AM_ADDR si hem yöneticiden köleye giden paketlerde hem de köleden yöneticiye giden paketlerde kullanılır. Tamamı sıfırlardan oluşan adres yöneticiden kölelere paket yayınlanması (broadcast) için rezerve edilmiştir. Sadece FHS paketi tamamı sıfırlardan oluşan üye adresini kullanmasına rağmen bir yayın (broadcast) mesajı değildir. Bağlantıda olmayan ya da park modunda olan köleler AM_ADDR lerini serbest bırakırlar. Pikonete tekrar bağlandıklarında ise yeni bir AM_ADDR alırlar.

TYPE

16 farklı paket tipi tanımlanmıştır. 4-bitli tip kodu ile hangi paket tipinin kullanıldığı belirtilir. Tip kodunun yorumu paket ile ilişkilendirilmiş olan fiziksel link tipine bağlıdır. Öncelikle paketin SCO linkinde mi ya da ACL linkinde mi gönderildiği tespit edilir. Sonra hangi tip SCO ya da ACL paketinin alındığı belirlenir. Tip kodu o an taşınan pakette kaç slot olduğu bilgisini de taşır.

FLOW

Bu bit ACL linki üzerinden taşınan paketlerin akış kontrolü için kullanılır. Alıcıdaki ACL linkinin RX ara belleği dolu olduğunda, veri akışını geçici olarak durdurmak için bir STOP göstergesi (FLOW=0) döndürülür. STOP işaretleri sadece ACL paketlerini ilgilendirir. Sadece link kontrol bilgisini (ID, POLL ve NULL paketleri) içeren paketler veya SCO paketleri ise alınmaya devam edilebilir. RX ara belleği boşaldığında bir GO göstergesi (FLOW=1) döndürülür. Hiç paket alınmadığında veya alınan başlıkta hata olduğunda GO göstergesi saklı (implicitly) varsayılır. Bu durumda köle RX ara belleği boşalmadığı halde CRC li yeni bir paket alabilir. Paket

CRC kontrolünü geçmiş olsa bile köle bu paket için bir “Negatif Alındı Bildirimi” (NAK) döndürür.

ARQN

1-bitlik alındı bildirimi (ACK) göstergesi olan ARQN, CRC li taşınan bilgi (payload) verisinin başarılı iletilip iletilmediği bilgisini taşımak için kullanılır. Pozitif alındı bildirimi ACK veya negatif alındı bildirimi NAK şeklinde olabilir. Alış işlemi başarılı olmuşsa ACK (ARQN=1), başarılı olmamışsa NAK (ARQN=0) döndürülür. ACK ile ilgili hiçbir dönüş mesajı alınmamışsa genel olarak NAK alınmış kabul edilir.

ARQN, dönüş paketinin başlık bilgisi ile birlikte (piggy-backed) bulunur. Alışın başarısı CRC kodu ile kontrol edilir.

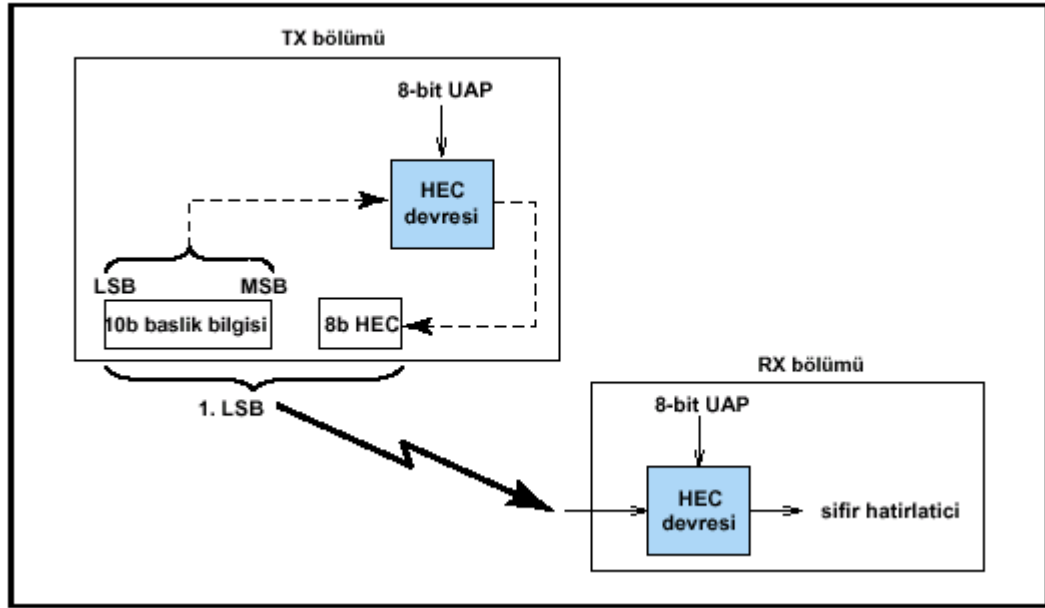
SEQN

SEQN biti veri paket sırasını ardışıl olarak numaralamak için kullanılır. CRC li veri içeren her yeni iletilen paket için SEQN bitinin tersi alınır. Bu bit iletilen paketlerin tekrar iletilmesini önlemek için kullanılır. ACK nın hata vermesi sonucu tekrar iletim gerçekleşirse, alıcı olan taraf aynı paketi ikinci kere almış olur. Ardışık paketlerin SEQN bitleri karşılaştırılarak, ikinci kere alınan paketler göz ardı edilebilir.

HEC

Her başlık bir başlık hata kontrol bilgisi içerir. HEC polynomial (çok terimli) 6 4 7 (oktal gösterim) tarafından üretilen 8-bitlik bir kelimedir. HEC üretilmeden önce, HEC jeneratörü 8-bitlik bir değerle başlatılır. Yönetici çağrı (page) cevap durumunda gönderilen FHS paketleri için köle üst adres bölgesi (UAP) kullanılır. Talep cevabı durumunda gönderilen HS paketleri için ise ilk (default) kontrol başlangıcı (DCI) kullanılır. Diğer tüm durumlarda yönetici cihazın UAP 1 kullanılır.

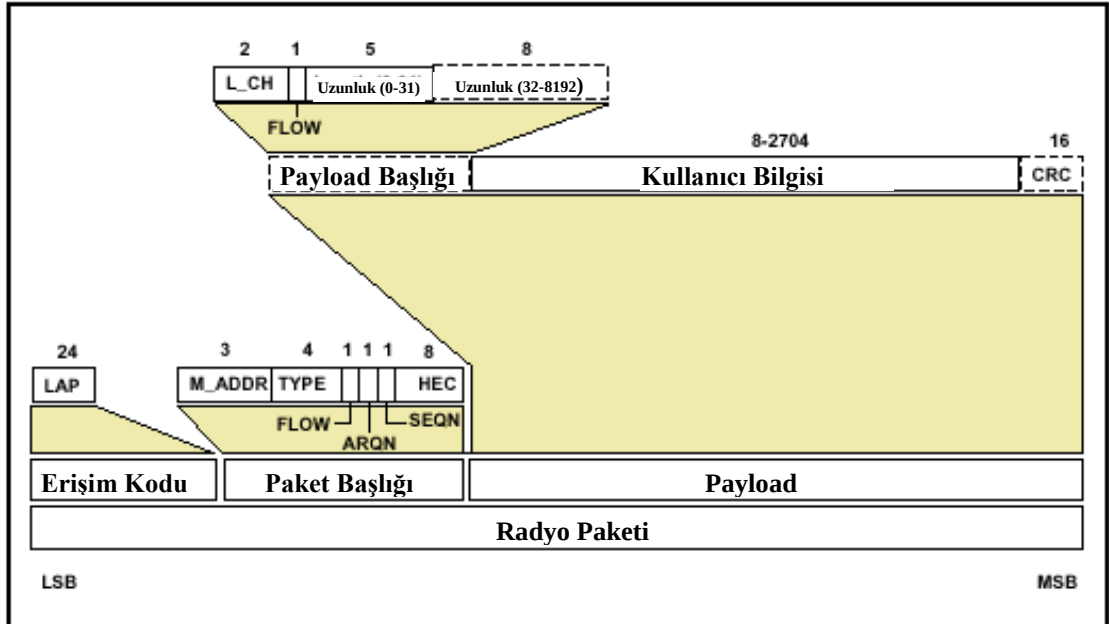
Başlangıç safhasından sonra HEC 10 başlık biti için hesaplanır. HEC kontrol edilmeden önce alıcı mutlaka uygun 8-bit UAP (DCI için) ile HEC kontrol devresini çalıştırmalıdır. HEC kontrol edilmezse paketin tamamı önemsenmez. [8]



Şekil 4.11 HEC oluşumu ve kontrolü

4.2.4.4 Taşınan Bilgi (Payload)

Taşınan bilgi (payload) daha yüksek katmanlar için gerçek kullanıcı bilgisini ve kontrol bilgisini taşır.



Şekil 4.12 Paket tanımlaması

4.2.4.5 Paket Tipleri

4-bitli TYPE kodu 16 farklı paket tipi tanımlar. Paket tipleri 4 farklı segmentte incelenir. İlk segment 4 paketten oluşur ve tüm fiziksel link tipleri için ortak olan

kontrol paketleri için rezerve edilmiştir. İkinci segment 6 paketten oluşur ve tek bir zaman slotunu işgal eden paketler için ayrılmıştır. Üçüncü segment 4 paketten oluşur ve üç zaman slotunu işgal eden paketler için ayrılmıştır. Dördüncü segment 2 paketten oluşur ve beş zaman slotunu işgal eden paketler için ayrılmıştır. Slot işgal etme durumu segmentasyonda belirtilir ve “type” kodunda direkt olarak elde edilebilir. Tablo 4.3 de SCO ve ACL link tipleri için tanımlanmış olan paket tipleri özetlenmektedir.

Tablo 4.3 SCO ve ACL link tipleri için tanımlanan paketler

Segment	TYPE kodu $b_3b_2b_1b_0$	Slot	SCO linki	ACL linki
1	0000	1	NULL	NULL
	0001	1	POLL	POLL
	0010	1	FHS	FHS
	0011	1	DM1	DM1
2	0100	1	TANIMSIZ	DH1
	0101	1	HV1	TANIMSIZ
	0110	1	HV2	TANIMSIZ
	0111	1	HV3	TANIMSIZ
	1000	1	DV	TANIMSIZ
	1001	1	TANIMSIZ	AUX1
3	1010	3	TANIMSIZ	DM3
	1011	3	TANIMSIZ	DH3
	1100	3	TANIMSIZ	TANIMSIZ
	1101	3	TANIMSIZ	TANIMSIZ
4	1110	5	TANIMSIZ	DM5
	1111	5	TANIMSIZ	DH5

Link Kontrol Paketleri

Beş genel paket vardır. Tablo 4.3 de segment 1 de listelenen tiplere ek olarak ID paketi mevcuttur.

- **ID paketi:** Kimlik ya da ID paketi kuyruksuz (trailer) erişim kodunu içerir ve kısaltılmış erişim kodu olarak anılır. 68-bit uzunluğundadır. Alıcı,

senkronizasyon kelimesinin 64 bitine karşın ilişki kurduğu için sağlam (robust) bir pakettir.

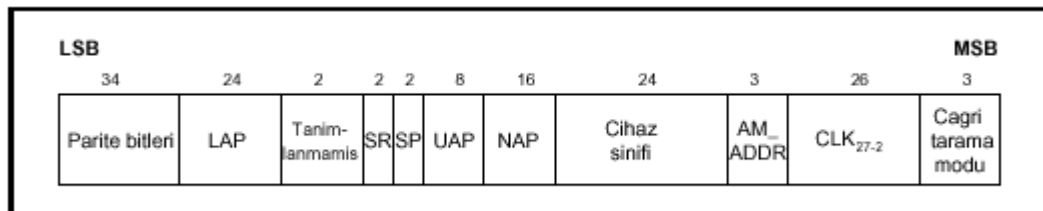
- **NULL paket:** NULL paket taşınan bilgi (payload) içermez ve bu sebeple sadece erişim kodu ile paket başlığından ibarettir. 126-bitten oluşur. NULL paket kaynağa bir önceki iletimin başarısı (ARQN) ve RX ara belleğinin durumu (FLOW) ile ilgili olarak link bilgisini geri döndürmek için kullanılır. NULL paketin kendisi alındı bilgisi almak zorunda değildir.
- **POLL paket:** POLL paket NULL pakete oldukça benzer. Taşınan bilgisi (payload) yoktur. NULL paketten farklı olarak alıcıdan alındı bilgisi alınmasına gerek duyar. Bu paket örneğin tek noktadan çok noktaya olan konfigürasyonda köleleri yoklamak (polling) için yönetici tarafından kullanılabilir. Ya da uzun bir süre herhangi bir bilgi akışı olmadığında bağlantının kontrol edilmesi için de kullanılabilir.
- **FHS paket:** FHS paketi, göndericinin saat statüsünü ve ünitelerin kimliğini açıklamak için kullanılan özel bir kontrol paketidir. Taşınan bilgi (payload), 18 bilgi byte ı ve 16-bitlik CRC den oluşur. Taşınan bilgi (payload) 2/3 hızındaki FEC ile kodlanmıştır. Bu sayede taşınan bilgi (payload) uzunluğu 240 bite çıkar. FHS paketi tek bir zaman slotunu kapsar. FHS paketinin içeriği Tablo 4.4 de özetlenmiştir. Ünite kimliğinden elde edilen düşük adres bölümü (LAP), 34 BCH parite bitleri ve 6 bit Barker kodu ile erişim kodunun 64-bitli senkronizasyon kelimesi direkt olarak inşa edilebilir.

FHS paketlerinin yönetici tarafından arama (call) kurulumu sırasında gönderilmesi durumunda, FHS taşınan bilgisindeki (payload) AM_ADDR alanı köle için ayrılmış olan MAC adresini de içerir. Bu MAC adresi yönetici ve köle arasında FHS paketinin kabul edilmesinden sonra başlayan bağlantı boyunca kullanılır. FHS paket başlığındaki AM_ADDR alanı halen 000 dır. FHS paketi bir çağrı (paging) prosedürü sırasında kullanıldığında FHS paketinin erişim kodu kölenin LAP ı ile kimliğinden elde edilir. FHS paketi alındığı bilgisi gelene kadar tekrar iletilir. Fakat saat bilgisi gerçek zamanlı bir değer olduğu için, her tekrar iletim durumundan önce yenilenir. FHS taşınan bilgisinin (payload) tekrar iletimi bu sebepten ötürü sıradan bir veri taşınan bilgisinin (payload) tekrar iletiminden farklıdır.

- **DM1 paket (Orta hızlı veri):** DM1 herhangi bir link tipindeki kontrol mesajlarını desteklemek için kullanılan segment 1 in bir parçasıdır. Bununla birlikte düzenli kullanıcı bilgisini de taşıyabilir. Ek olarak ACL linkinde olduğu gibi diğer veri paketleri de uygunsa, bu paketler de kontrol verisini taşıyabilirler. DM1 paketi aynı zamanda bir ACL paketi olduğu için ileriki bölümde detaylı olarak incelenecektir.

Tablo 4.4 FHS paket içeriği

Bilgi	Bitler
Barker kodu	6
Bluetooth ünitesinin IEEE kimliği	48
BCH parite bitleri	34
Servis sınıfı	24
M_ADDR	3
Ünitenin gerçek zamanlı Bluetooth saatinin en yüksek değerlikli bitleri	26
Gelecek kullanımlar için	3
TOPLAM	144



Şekil 4.13 FHS taşınan bilgi (payload) formatı

ACL Paketleri

ACL paketleri asenkron veya isenkron veriyi taşırlar. Tüm ACL paketleri asenkron I/O (veri) portuna yönlendirilmiştir. DM1 paketi dahil olmak üzere toplam yedi ACL paketi tanımlanmıştır. Bu paketlerin altısı CRC içerir ve uygun alım bilgisi gelmediği

sürece tekrar iletilirler. Yedinci ACL paketi olan AUX1 ise CRC içermez ve tekrar iletilmez.

- **DM1 paketi**

DM1 paketi sadece veri bilgisini taşıyan bir pakettir. Taşınan bilgi (payload), 18 bilgi byte ına kadar (1-byte lık taşınan bilgi (payload) başlığı dahil) byte ve 16-bit lik CRC bilgisini taşır. DM1 paketi sadece tek bir zaman slotunu kapsar. Bilginin tamamı ve CRC bitleri 2/3 hızlı FEC ile kodlanırlar. Bu kodlama sonucu her 10-bitlik segmente 5 adet parite biti eklenir. Gerekli görülürse, CRC bitlerinden sonra sıfırlar eklenebilir. DM1 paketindeki taşınan bilgi (payload) başlığı sadece 1 byte uzunluğunda olabilir. Taşınan bilgi (payload) başlığındaki uzunluk göstergesi kullanıcı byte larının sayısını belirler. (taşınan bilgi (payload) başlığı ve CRC hariç olmak üzere)

- **DH1 paketi (Yüksek hızlı veri)**

DH1 paketi DM1 paketine benzer fakat taşınan bilgideki (payload) bilgi FEC ile kodlanmamıştır. Bunun sonucu olarak da DH1 paketi 28 bilgi byte ı ve 16-bit CRC bilgisini taşıyabilir. DH1 paketi sadece tek bir zaman slotunu kapsar.

- **DM3 paketi**

DM3 paketi genişletilmiş taşınan bilgisi (payload) olan bir DM1 paketidir. DM3 paketi üç zaman slotunu kapsar. Taşınan bilgi (payload), 122 bilgi byte ına kadar (2-byte lık taşınan bilgi (payload) başlığı dahil) byte ve 16-bit lik CRC bilgisini taşır. DM3 paketindeki taşınan bilgi (payload) başlığı 2 byte uzunluğundadır. Taşınan bilgi (payload) başlığındaki uzunluk göstergesi kullanıcı byte ların sayısını belirler. (taşınan bilgi (payload) başlığı ve CRC hariç olmak üzere) Bir DM3 paketi gönderildiğinde ya da alındığında atlama kanalı 3 zaman slotu boyunca değişmez. (birinci zaman slotu paket erişim kodunun alındığı slottur) Bilgi ve CRC bitleri 2/3 hızlı FEC ile kodlanmıştır.

- **DH3 paketi**

DH3 paketi DM3 paketine benzer fakat taşınan bilgideki (payload) bilgi FEC ile kodlanmamıştır. Bunun sonucu olarak da DH3 paketi 182 bilgi byte ı ve 16-bit CRC bilgisini taşıyabilir. DH3 paketi üç zaman slotunu kapsar. Bir DH3 paketi gönderildiğinde ya da alındığında atlama kanalı 3 zaman slotu boyunca değişmez. (birinci zaman slotu paket erişim kodunun alındığı slottur)

- **DM5 paketi**

DM5 paketi genişletilmiş taşınan bilgisi (payload) olan bir DM1 paketidir. DM5 paketi beş zaman slotunu kapsar. Taşınan bilgi (payload), 226 bilgi byte ına kadar (2-byte lık taşınan bilgi (payload) başlığı dahil) byte ve 16-bit lik CRC bilgisini taşır. DM5 paketindeki taşınan bilgi (payload) başlığı 2 byte uzunluğundadır. Taşınan bilgi (payload) başlığındaki uzunluk göstergesi kullanıcı byte ların sayısını belirler. (taşınan bilgi (payload) başlığı ve CRC hariç olmak üzere) Bir DM5 paketi gönderildiğinde ya da alındığında atlama kanalı 5 zaman slotu boyunca değişmez. (birinci zaman slotu paket erişim kodunun alındığı slottur) Bilgi ve CRC bitleri 2/3 hızlı FEC ile kodlanmıştır.

- **DH5 paketi**

DH5 paketi DM5 paketine benzer fakat taşınan bilgideki (payload) bilgi FEC ile kodlanmamıştır. Bunun sonucu olarak da DH5 paketi 340 bilgi byte ı ve 16-bit CRC bilgisini taşıyabilir. DH5 paketi beş zaman slotunu kapsar. Bir DH5 paketi gönderildiğinde ya da alındığında atlama kanalı 5 zaman slotu boyunca değişmez. (birinci zaman slotu paket erişim kodunun alındığı slottur)

- **AUX1 paketi**

Bu paket DH1 paketine benzer fakat CRC içermemektedir. AUX1 paketi 30 bilgi byte ına kadar (1-byte lık taşınan bilgi (payload) başlığı dahil) byte taşıyabilir. AUX1 paketi sadece tek bir zaman slotunu kapsar.

SCO Paketleri

SCO paketleri ses gibi 64 kbit/sn. deki zamana bağlı bilgiyi taşırlar. Üç tip SCO paketi tanımlanmıştır. SCO paketleri CRC içermezler ve hiçbir zaman tekrar iletilmezler. Ek olarak, SCO paketleri asenkron veri alanı da taşıyacak şekilde tanımlanırlar.

- **HV1 paketi (High quality Voice)**

HV1 paketi saf bir ses paketidir. 1.25 msn. lik konuşmaya eşdeğer 10 ses byte ı içerir. HV1 paketinde 10 ses byte ı 1/3 hızlı FEC ile korunur. Taşınan bilgi (payload) uzunluğu 240 bit ve sabittir. Bir HV1 paketi her iki zaman slotunda bir gönderilmelidir.

- **HV2 paketi**

HV2 paketi de saf bir ses paketidir. 2.5 msn. lik konuşmaya eşdeğer 20 ses byte ı içerir. HV1 paketinde 20 ses byte ı 2/3 hızlı FEC ile korunur. Taşınan bilgi (payload) uzunluğu 240 bit ve sabittir. HV2 paketi 2.5 msn. lik konuşmaya eşdeğer bilgi içerdiğinden her dört zaman slotunda bir sadece bir HV2 paketi iletilir.

- **HV3 paketi**

HV3 paketi de saf bir ses paketidir. 3.75 msn. lik konuşmaya eşdeğer 30 ses byte ı içerir. HV1 paketinde 30 byte FEC ile korunmaz. Taşınan bilgi (payload) uzunluğu 240 bit ve sabittir. HV2 paketi 3.75 msn. lik konuşmaya eşdeğer bilgi içerdiğinden her altı zaman slotunda bir sadece bir HV2 paketi iletilir.

- **DV paketi (Veri ve Ses)**

DV paketi bütünleşik bir veri-ses paketidir. Taşınan bilgi (payload) 80 bitlik bir ses alanına ve 150 bitlik bir veri alanına bölünmüştür. 10 ses byte ı 10 “Darbe Kod Modülasyonu” (PCM) örneği içerir (1.25 msn. lik konuşma eşdeğeri). Ses alanı FEC ile korunmaz. Veri alanı 10 bilgi byte na kadar (1-byte lık taşınan bilgi (payload) başlığı dahil) byte taşıyabilir. Bilgi byte larına 16-bitlik CRC eklenmiştir. Bilgi ve CRC bitleri 2/3 hızlı FEC ile kodlanır. Kuyruk (trailer) bitleri FEC kodlaması için taşınan bilgi (payload) bitlerini 10 un katları yapmak için eklenir.

DV paketleri senkronize (ses) bilgi içerdiği için düzenli zaman aralıklarında gönderilmelidir ve bu sebeple SCO paket tipleri arasında incelenmektedir.

Ses ve veri alanları tamamen ayrı olarak işlem görür. Ses alanı senkron I/O portuna yönlendirilir ve hiçbir zaman tekrar iletilmez. Veri alanı ise ACL linkinin bir parçasıdır ve hata kontrolü yapıldıktan sonra gerekli görülürse tekrar iletilebilir. Veri alanı asenkron I/O portuna yönlendirilir.

4.2.5 Hata Düzeltme

Bluetooth için tanımlanmış üç hata düzeltme algoritması mevcuttur:

- 1/3 hızlı FEC

- 2/3 hızlı FEC
- Veri için “Otomatik Tekrarlama Talebi” (ARQ) algoritması

Veri taşınan bilgisindeki (payload) FEC algoritmasının amacı tekrar iletimlerin sayısını azaltmaktır. Fakat makul ölçüde hatasız çalışan bir cihazda FEC sisteme gereksiz bir yük getirdiği için verimi düşürür. Bu sebeple taşınan bilgide (payload) FEC kullanıp kullanmama konusu esnek bırakılmıştır. ACL linkinde DM ve DH paketlerinin; SCO linkinde de HV paketlerinin bulunma sebebi budur. Paket başlığı daima 1/3 hızlı FEC ile korunur çünkü değerli link bilgisini taşımaktadır ve daha çok bit hata olasılığı içerir.

4.2.5.1 FEC Kodu: 1/3 Hızlı

1/3 hızlı FEC kodunda basit bir tekrar kodu kullanılır. 3-bit tekrarlı kod uygulanır, örneğin her bit 3 kere tekrar edilir. Kod çözme ise alınan 3 bit üzerindeki çoğunluk kararına göre uygulanır. Tekrar kodu başlıkta uygulanır ve HV1 paketinde bulunur.

4.2.5.2 FEC Kodu: 2/3 Hızlı

2/3 hızlı FEC kodunda (15,10) kısaltılmış bir Hamming kodu uygulanır. Her 10 bitlik blok için 5 adet parite biti eklenir. Bu kodun serbest uzaklığı 4 tür ve bu sebeple tek bit hatasını düzeltebilirken; iki bit hatasını da dedekte eder. 2/3 hızlı kod HV2 paketi için, DV paketindeki veri için ve DM ile FHS paketleri için kullanılır.

4.2.5.3 ARQ Algoritması

Numaralanmamış bir ARQ şeması, bir slotta iletilen veri için alıcı tarafından bir sonraki slotta alındı bildirimi yapılıyorsa uygulanır. Alındı bilgisi alınan (ARQN=1) bir veri iletiminde hem HEC hem de CRC kontrol edilmelidir; aksi takdirde NAK (ARQN=0) döndürülür.

CRC li veri taşınan bilgisi (payload) içeren bir paketin alımında, alıcı ilk olarak HEC i kontrol eder. HEC kontrol edilirse CRC taşınan bilgisi (payload) de kontrol edilir. Eğer CRC de kontrol edilirse dönen paketteki ARQN alanı set edilir. (ARQN=1) Aksi takdirde ARQN alanı sıfırlanır (ARQN=0). HEC in kontrol edildiği durumda paket taşınan bilgi (payload) taşımıyorsa ya da CRC siz bir taşınan bilgi (payload) taşıyorsa önce dönen pakette gönderilen ARQN in aynısı gönderilir. HEC ve CRC kontrol edildiğinde ise taşınan bilgi (payload) kabul edilir ve paket başlığındaki

SEQN tarafından sağlanan link yöneticisine devredilir. Aksi takdirde taşınan bilgi (payload) dikkate alınmaz.

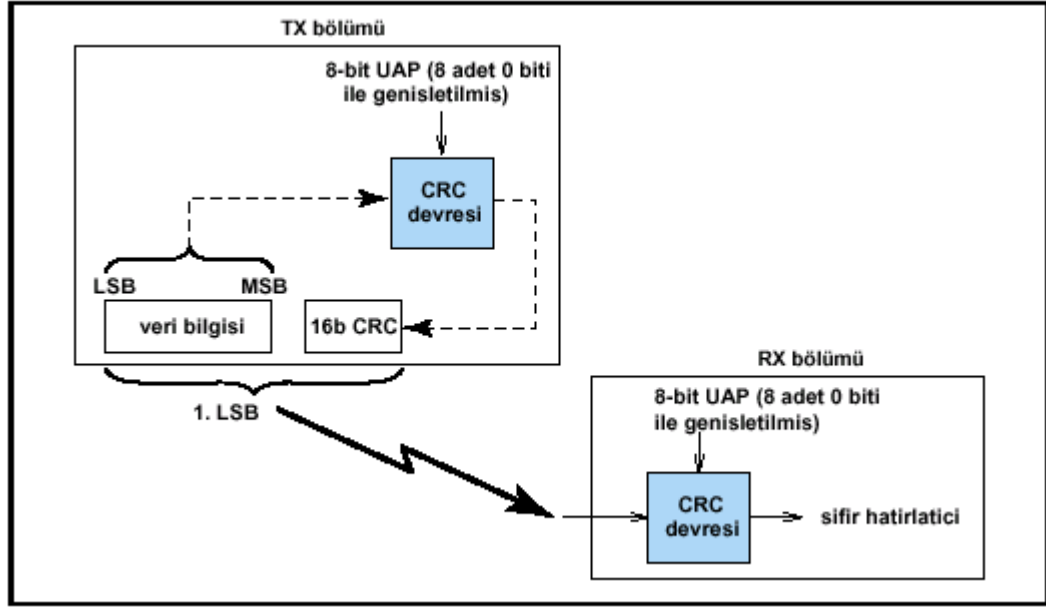
Dönen paket kabul edildiğinde, gönderen taraf ilk önce HEC i kontrol eder. HEC kontrol edilirse, başlıktaki ARQN alanı okunur. Bir ACK (ARQN=1) mevcutsa, gönderici bir sonraki paketteki SEQN i değiştirir (toggle) ve bir sonraki iletim slotunda yeni bir taşınan bilgi (payload) gönderir. HEC kontrol edilmezse ya da bir NAK (ARQN=0) alınırsa SEQN değiştirilmez (toggle) ve bir önceki taşınan bilgi (payload) tekrar gönderilir.

ARQ şeması yönetici ve her bir köle arasında ayrı ayrı uygulanır. Yönetici, yöneticiden köleye olan slotu takip eden köleden yöneticiye olan slottan direkt olarak yöneticiden köleye alındı bilgisini alır. Köleden yöneticiye bilgisinin alındı bilgisi yöneticinin köleyi adreslediği bir sonraki yöneticiden köleye olan slottan alınır.

4.2.5.4 Hata Kontrolü

Bir ünite mevcut taşınan bilgiyi (payload) atıp, yeni bir taşınan bilgi (payload) olarak tekrar iletimi engelleyebilir. Bu durum tipik olarak isonkron veri için kullanılır. Bir paketin ömrü dolarsa, o paket atılarak yani bir paket alınır. Bu atma işleminden sonra, gönderici eski taşınan bilgi (payload) bir önceki alım slotunda alındı bilgisi alınmamışsa SEQN i değiştirmez (toggle).

CRC, veri alanlarına HEC e benzer şekilde oluşturularak eklenir. CRC üretilmesinden ve kontrol edilmesinden önce, mevcut UAP kullanıcı verisi önüne eklenir. UAP nin kendisi iletilmez. CRC bitleri polynomial 210041 (oktal gösterim) tarafından üretilir.



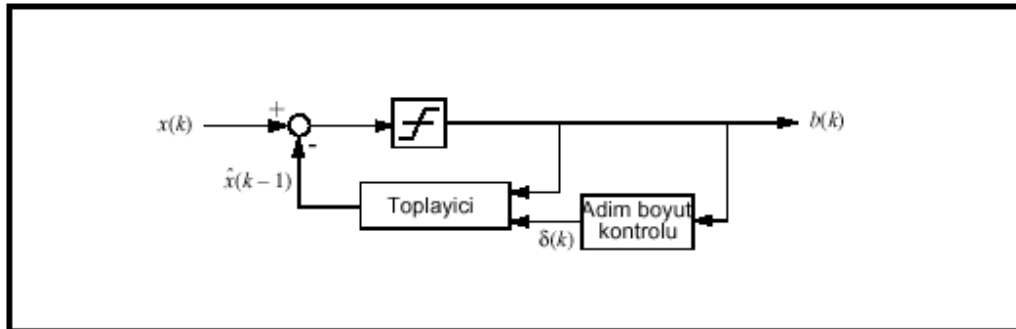
Şekil 4.14 CRC oluşturulması ve kontrolü

4.2.6 Konuşma Kodlama

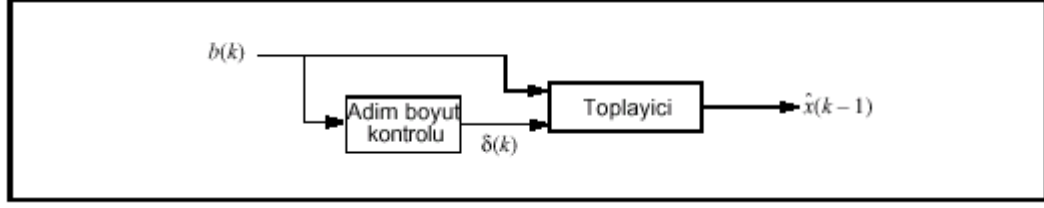
Bluetooth sisteminde 2 konuşma kodlama şeması desteklenir. Sürekli Değişken Eğim Delta (CVSD) Modülasyonu ve Logaritmik Darbe Kod (logPCM) Modülasyonu. Her iki şema da 64 kbit/sn. de çalışır. Varsayılan olarak kullanılan modülasyon türü CVSD dir.

4.2.6.1 CVSD Konuşma Kodlama Tekniği

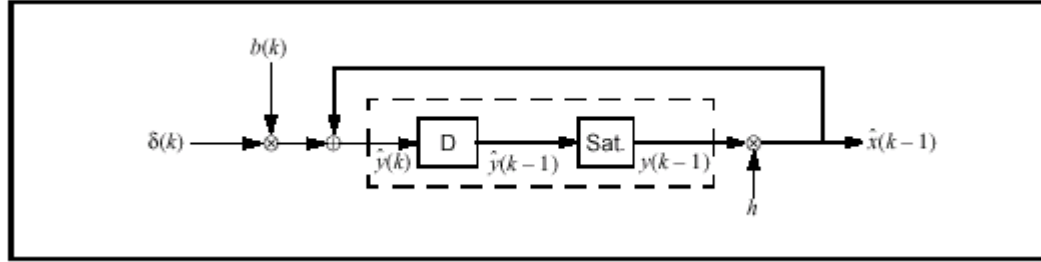
CVSD kodlama delta modülasyonu uygulayan bir dalga kodlayıcıdır. Eğim-aşırı yük etkisini azaltmak için “hecesel sıkıştırma (syllabic companding)” uygulanır. Delta adımının büyüklüğü ortalama işaret eğimine göre adapte edilir. CVSD konuşma kodlayıcının arayüzü 8000 örnek/sn lik lineer PCM dir. Artan girişim büyüyen bir arka plan gürültüsü olarak alınır.



Şekil 4.15 “Hecesel sıkıştırma” içeren CVSD kodlayıcının blok diyagramı



Şekil 4.16 “Hecesele sıkıştırma” içeren CVSD kod çözücünün blok diyagramı



Şekil 4.17 Toplayıcı prosedürü

4.2.6.2 LogPCM Konuşma Kodlama Tekniği

Alternatif konuşma kodlama tekniği temel logPCM dir. 8000 örnek/sn lik lineer PCM, logPCM de A-law ya da μ -law sıkıştırma algoritmaları kullanılarak sıkıştırılır.

4.2.7 Veri Beyazlatma

İletimden önce hem başlık hem de taşınan bilgi (payload) paketteki DC eğilimi (bias) minimize etmek ve verinin çok sayıda bulunan paternlerden etkilenmesini rasgele hale getirmek için bir veri beyazlatma kelimesi ile karıştırılır. Karıştırma işlemi FEC kodlama işleminden önce yapılır.

Alıcıda ise, alınan veri alıcıda üretilen aynı beyazlatma kelimesi kullanılarak eski haline getirilir. Eski haline getirme işlemi FEC kod çözme işleminden sonra yapılır.

4.2.8 Doğrulama ve Şifreleme

Kullanıcıyı korumak ve bilginin gizliliğini sağlamak için sistem hem uygulama katmanında hem de fiziksel katmanda güvenlik prosedürleri sağlamalıdır. Bu prosedürler eşdeğer ortamlar için geçerli olmalıdır. Her Bluetooth ünitesinde doğrulama ve şifreleme aynı şekilde yerine getirilmelidir. Bluetooth teknolojisi silikon uygulamalarına uygun olan temel seviyede bir şifreleme ve cihazları fazla komplikeleştirmeyen bir doğrulama algoritması kullanır. Geliştirilmekte olan şifre algoritmaları da geriye dönük olarak uyumludur.

Ana özellikler şunlardır:

- Doğrulama için deneme-cevap akışları
- Oturum anahtarı yaratma. Oturum anahtarları bir bağlantı sırasında herhangi bir zamanda değiştirilebilir.
- Akış şifresi

Genel güvenlik problemlerinde, üç ana nesne kullanılır: her kullanıcı için tek olan genel nesne; gizlilik nesnesi ve her yeni iletim için farklı olan rasgele nesne. Bu nesnelerin Bluetooth'da kullanılan boyutları aşağıda özetlenmiştir:

Tablo 4.5 Doğrulama ve şifreleme prosedürlerinde kullanılan nesneler

Nesne	Boyut
BD_ADDR	48 bit
Özel kullanıcı anahtarı, doğrulama	128 bit
Özel kullanıcı anahtarı, şifreleme, konfigüre edilebilir uzunluk (byte cinsinden)	8-128 bit
RAND	128 bit

Bluetooth adresi her Bluetooth ünitesi için farklı olan 48-bit IEEE adresidir. Bluetooth adresleri açık olarak bilinir ve MMI etkileşimleri ya da otomatik bir sorgu dizini tarafından belirlenebilir. Kullanıcı anahtarı 64-bit gizli bir anahtardır ve başlangıç aşamasında elde edilir. Fakat daha sonra kesinlikle açığa vurulmaz. RAND, Bluetooth ünitesindeki sahte ve rasgele bir proses sonucu elde edilen rasgele bir numaradır.

4.2.9 Lojik Kanal Tanımlaması

4.2.9.1 Giriş

Bluetooth sisteminde 6 lojik kanal tanımlanmıştır: 3 lojik kontrol kanalı (LC, LM ve UC) ve 3 lojik kullanıcı kanalı (UA, UI ve US).

Kontrol kanalları LC, LM ve UC sırasıyla link kontrol katmanında, link yönetim katmanında ve sunucu terminal katmanında kullanılırlar.

Kullanıcı kanalları UA, UI ve US sırasıyla asenkron, isonkron ve senkron kullanıcı bilgisini taşımak için kullanılırlar. LM, UC, UA ve UI kanalları taşıyan bilgi

(payload) başlığındaki L_CH alanında gösterilirler. Bu kanallar asenkron veri portuna yönlendirilmişlerdir. Sadece US kanalı senkron I/O portuna yönlendirilmiştir.

4.2.9.2 Link Kontrol (LC) Kanalı

LC kontrol kanalı paket başlığına adreslenmiştir. Bu kanal ARQ, akış kontrolü ve taşınan bilgi (payload) karakterizasyonu gibi düşük seviyeli link kontrol bilgisini taşır. LC kanalı paket başlığı olmayan ID paketi dışında her paket ile taşınır.

4.2.9.3 Link Yöneticisi (LM) Kanalı

LM kontrol kanalı yönetici ve kölelerin link yöneticileri arasında iletilen kontrol bilgisini taşır. Genel olarak LM kanalı korunumlu DM paketlerini kullanır.

4.2.9.4 Kullanıcı Kontrol (UC) Kanalı

UC kanalı kullanıcı protokolleri arasında iletilen kontrol bilgisini taşır.

4.2.9.5 Kullanıcı Asenkron Veri (UA) Kanalı

UA kanalı transparan asenkron kullanıcı verisini taşır.

4.2.9.6 Kullanıcı İsonkron Veri (UI) Kanalı

UI kanalı transparan isonkron kullanıcı verisini taşır. Taşınan bilgi (payload) başlığında bir başlangıç biti yeni bir isonkron mesajın başladığını gösterir. İsonkron kanalın zamanlaması pikoneteki yönetici tarafından kontrol edilir.

4.2.9.7 Kullanıcı Senkron Veri (US) Kanalı

US kanalı transparan senkron kullanıcı verisini taşır. Bu kanal senkron I/O portlarına yönlendirilmiştir.

4.2.9.8 Kanal Adresleme

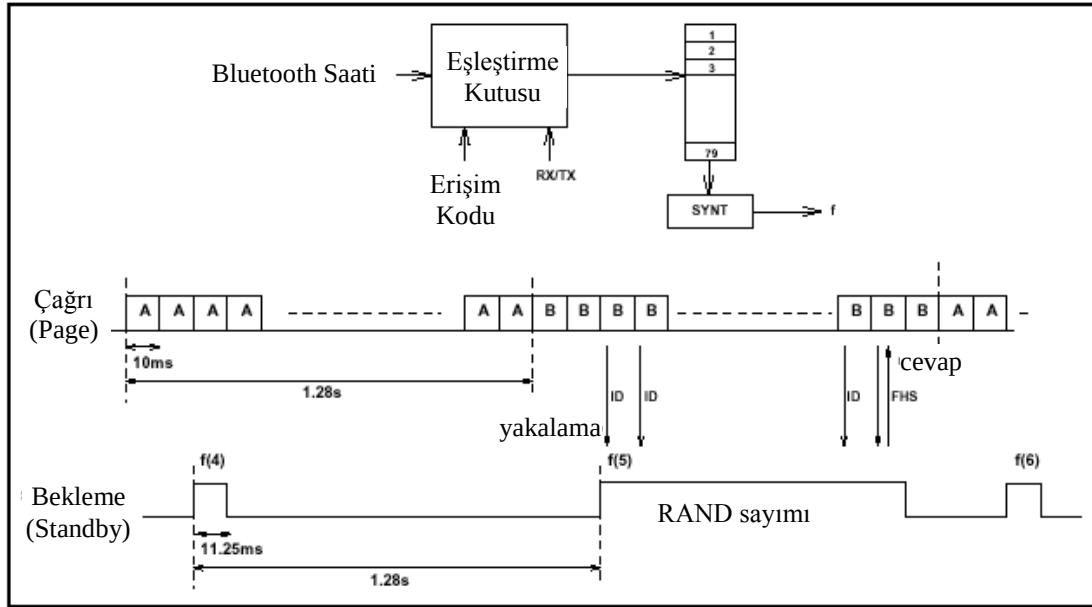
LC kanalı paket başlığına, tüm diğer kanallar ise taşınan bilgiye (payload) adreslenmiştir. Sadece US kanalı SCO paketleri üzerine adreslenebilir. Diğer tüm kanallar ise ACL paketleri üzerine ya da düşük bir ihtimalle SCO DV paketine adreslenmiştir. Kontrol kanalları rezerve edilmiş SCO slotlarındaki ortak DM1 paketi üzerinden kontrol bilgisi göndererek SCO linklerine müdahale edebilirler.

4.2.10 İşlemsel Prosedürler

4.2.10.1 Sorgu Prosedürü

Bluetooth ünitelerinin adreslerini sıralı olarak toplamak için, bir Bluetooth ünitesi periyodik olarak bir sorgu prosedürünü yerine getirir. Sorgu yapan ünite değişik RF atlama frekanslarında sorgu erişim kodunu tekrar tekrar iletir.

Sorgu erişim kodunu alan bir ünite 0 ile 63 arasında rasgele bir sayı üretir. Sonra, sorgu mesajının alındığı atlama frekansında sürekli bir tarama yaparak geçen sorgu mesajlarını sayar. Bu sayma sonucu önceden belirlenen rasgele sayıya ulaştığı zaman, işlemi yapan ünite bir sonraki köleden yöneticiye olan slotta ünitenin kimliğini, sistem saatini ve servisin sınıfını içeren bir FHS paketi geri döndürür. FHS paketi Erişim Kodu'ndaki sorgu erişim kodunu ve başlık ve taşınan bilgiyi (payload) işaretlemek için de UAP sorgusunu kullanır. FHS paketinin geri dönmesinden sonra, ünite sorgulanan ünitenin ünite erişim kodu tarafından belirlenen “Frekans Atlama” (FH) dizisine göre bir sonraki RF atlama frekansını tarar. Şekil 4.18 de bu prosedür açıklanmıştır. Sorgulanan ünite tüm FHS paketlerini toplamaktadır. Sorgulama prosedürü en az 4096 çerçeve boyunca devam eder.

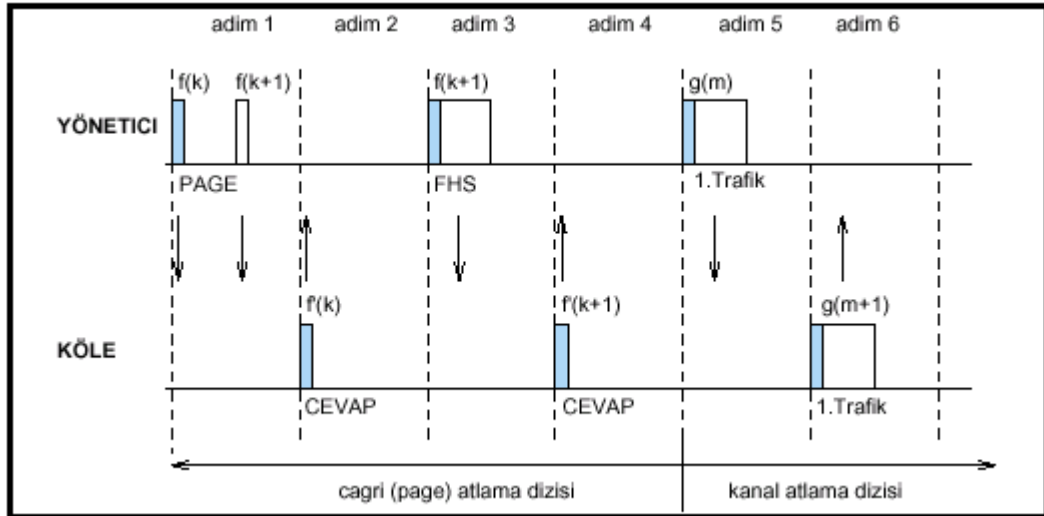


Şekil 4.18 Sorgu prosedürü

4.2.10.2 Bağlantı Kurulum Prosedürü

Sadece yönetici köleyi pikonete bağlayabilir. Pikonete katılmak isteyen bir köle öncelikle yöneticiyi bundan haberdar etmelidir; örneğin yönetici çağrı (paging) ya da

sorgu için dinlemede olduğunda farklı bir pikonetin yöneticisi gibi davranır. Böylelikle o ünite ilk yönetici tarafından pikonete bağlanır. Kurulum prosedürü Şekil 4.19 da açıklanmıştır. Yönetici, kölenin ünite_atlama dizisini kullanarak kölenin ünite_erişim kodunu bağlanacak köleye iletir. Köle olan ünite kendi erişim kodunu alınca, bir çağrı (page) tarama penceresi boyunca, uygun yöneticiden köleye pozisyonunda ünite_atlama dizisine uygun olan atlama frekansını kullanarak bir cevap döndürür. Bu cevap sadece kölenin erişim kodunu içerir. Kölenin cevabı alındıktan sonra yönetici kendi kimliği ve sistem saatini gösteren bir FHS paketi iletir. Köle erişim kodunu ikinci kere geri döndürerek FHS paketini aldığı bilgisini verir. FHS paketi pozitif alındı bilgisi alınana kadar tekrar gönderilir. (Bu esnada yöneticinin sistem saati her yeni iletim için yenilenmektedir.) Bu noktaya kadar tüm haberleşmeler kölenin erişim kodunu, köleye uygun olan ünite_atlama dizisini ve kölenin saatini kullanır. FHS paketi başarılı olarak alındıktan ve alındı bilgisi de geldikten sonra yönetici ve köle yöneticinin kimliği tarafından belirlenen kanal atlama dizisine ve kanal_erişim koduna değişirler.



Şekil 4.19 İlk bağlantıda mesajlaşma

4.2.11 Güç Yönetimi

4.2.11.1 Giriş

Genel olarak Bluetooth sisteminde kısa paketler (ID, NULL veya POLL paketleri) kullanılarak ve gönderilecek herhangi bir bilgi olmadığı durumda transfer yapılmayarak güç kaybı önlenir. Bağlantı kurulumu için mümkün olduğu kadar çok

RF atlama frekansında çağrı (page) mesajını iletmenin yükü çağrıyı yapan ünitededir. Aynı ünite bekleme (standby) modunda düşük güçlü tarama modunu devam ettirir.

4.2.11.2 Alınan Paket Prosesi

Alınan paketler gerçek zamanlı olarak proses edilir ve aşağıdaki durumlar gerçekleştiğinde proses işlemi durur:

- Paket başka bir alıcıya adreslenmişse
- Paket tipinin taşınan bilgisi (payload) yoksa veya kısa taşınan bilgi (payload) uzunluğu gösteriyorsa
- Paket düzeltilemeyecek hatalara sahipse

Alınan slotta ünite 64 bit için kanal_erişim koduna eşleşen ilişkilendiricisini (correlator) aktif eder. Bu zaman penceresinde ilişkilendirici (correlator) çıkışı eşik değerini (51 bitlik eşleştirme varsayılır) aşmadığında sonraki alımlar bir sonraki alım slotuna bırakılır.

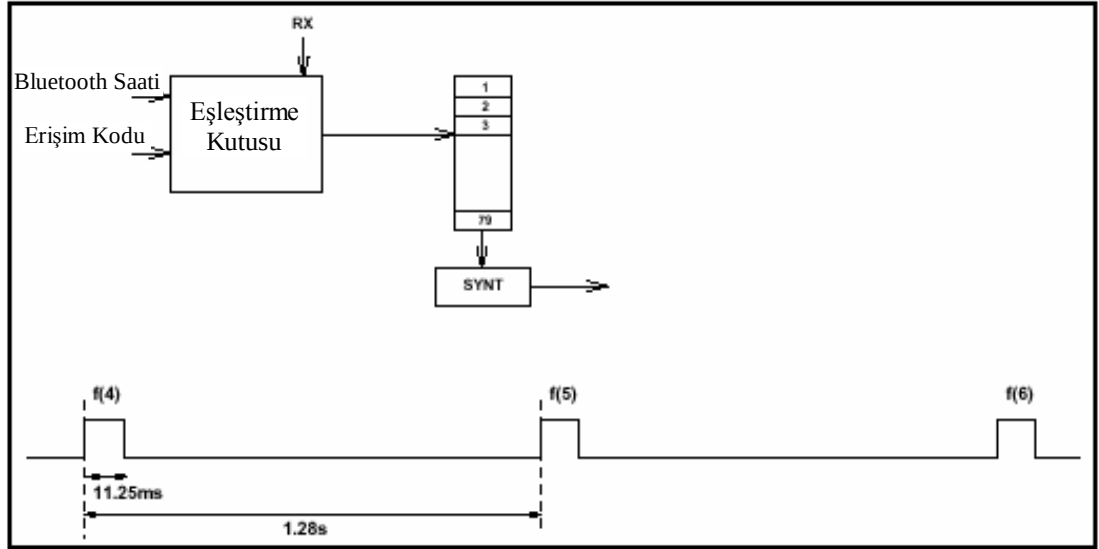
İlişkilendirici (correlator) geçerli bir pakete işaret ettiğinde, başlık kontrol edilir. HEC kontrolü başarılı olmazsa, sonraki alımlar bir sonraki alım slotuna bırakılır. Sonra M_ADDR alanındaki MAC adresi kontrol edilir. Alt (sub) adres, kölenin MAC adresine uygun gelmiyorsa sonraki alımlar bir sonraki alım slotuna bırakılır. Aksi durumda TYPE alanı okunur ve taşınan bilgi (payload) alınır.

4.2.11.3 Çağrı (Page)/Sorgu Durumu

Çağrı (page) ya da sorgu durumunda, Bluetooth ünitesi çerçeve başına 2 adet 64-bit erişim kodu iletir. Alım slotunda cevapların her biri için 88µsn 2 kere dinlenir.

4.2.11.4 Bekleme (standby) Durumu

Bekleme (standby) durumunda Bluetooth ünitesi her 1024 çerçevede bir (1.28sn.) 9 çerçeve (11.25 msn.) dinler. Sorgu cevap seçeneği aktif edilmişse, ünite ek olarak 9 çerçeve daha dinler. Şekil 4.20 de gösterildiği gibi bekleme (standby) durumu boyunca herhangi bir iletim gerçekleşmez.



Şekil 4.20 Bekleme (standby) durumu, dinleme dizisi

4.2.11.5 Aktif Yönetici Durumu

Bir kanal kurulduğunda yönetici farklı köleleri çeker. Eğer gönderecek hiç bilgi yoksa yoklama (poll) paketini kullanır. Gönderecek bilgi varsa, SCO ya da ACL paketleri dolaylı olarak köleyi çeker. Veri iletimi ve tarama istenmediği durumlarda yönetici iletim yapmaz. FH kanalı yönetici ve köleler atlama frekansını 1600 atlama/sn. de tuttukları ve tüm köleler yöneticiden köleye olan slotları dinlemeye devam ettikleri için sanal olarak bulunur.

Bazı durumlarda; yönetici, senkronizasyonu ayarlamak için paket göndermek zorundadır. Veri iletimine ihtiyaç yoksa yönetici FH kanalını durağan modda tutar. Bunun bir sonucu olarak tüm üniteler önceden tanımlanmış bir durağan mod periyodu boyunca bekleme (standby) durumuna geçerler. FH kanalındaki tüm gönderi ve alımlar durdurulur. Durağan mod süresi aşıldığında, yönetici sıra ile tüm köleleri tarar. Tüm üniteler senkronize olduğunda da çağrı (paging) ve bağlantı kurulumları istenmez.

4.2.11.6 Aktif Köle Durumu

Bir FH kanalına bağlı olan bir köle, yöneticiden köleye olan slotları dinler. Yöneticiden köleye olan slottaki adres eşleştğinde, köle paketleri almaya devam eder. Eğer köle adreslenmişse bir sonraki köleden yöneticiye slotunda bir paket geri döndürmelidir. (tamamı sıfır MAC adresi olan köle hariç) Eğer kölenin gönderecek bilgisi yoksa bir NULL paketi gönderir. Bu durumda yönetici köleyi önceden

belirlenmiş bir süre için durağan moda alabilir. Durağan mod süresi aşıldığında, köle FH kanalına geri döner ve her yöneticiden köleye slotunu dinler. Yönetici onu adresleyinceye kadar iletimde bulunmaz.

4.2.12 Kimlikler

4.2.12.1 Bluetooth Adresleri

Her Bluetooth ünitesi IEEE802 standardından elde edilen 48-bitlik bir Bluetooth adresine sahiptir. Bu 48-bitlik adres üç bölüme ayrılmıştır:

- LAP alanı: 24 bitten oluşan düşük adres bölümü
- UAP alanı: 8 bitten oluşan yüksek adres bölümü
- NAP: 16 bitten oluşan ağırlıksız adres alanı

LAP ve UAP Bluetooth adresinin ağırlıklı kısmını oluşturur. Bluetooth sisteminin toplam adres alanı 2^{32} dir.

Ünite kimliği atlama dizisini ve bekleme (standby) durumundaki bir ünitenin erişim kodunu belirler. Ünite kimliği, bu üniteyi beklemede (standby konumunda) çağrı (page) yapmak isteyen tüm üniteler tarafından kullanılır.

Tek bir Bluetooth adresi sorgu işlemlerinde kullanılmak üzere rezerve edilmiştir. Sorgu adresi tüm Bluetooth üniteleri için ortaktır.

4.2.12.2 Erişim Kodları

Bluetooth sisteminde işaretleşme amaçları için 72-bit erişim kodları kullanılır. Üç farklı erişim kodu tanımlamıştır:

- Ünite erişim kodu
- Kanal erişim kodu
- Sorgu erişim kodu

Sorgu erişim kodu dışındaki kodlar ünite kimliğinin LAP ından elde edilirler. Sorgu erişim kodu ise sorgu kimliğinden elde edilir. Ünite erişim kodu çağrı (paging) ve bekleme (standby) durumlarında kullanılır. Ünitenin kimliğinden elde edilen bir koddur. Kanal erişim kodu pikonetin kanalını karakterize eder. Kanal erişim kodu kanalda iletilen tüm paketlerin başlangıçlarına şekil verir. Kanal erişim kodu pikoneti

oluşturan Bluetooth ünitesinin LAP'ından elde edilir. Bu ünite pikonetin yöneticisi olacaktır. Sorgu erişim kodu da sorgu işlemlerinde kullanılır.

Erişim kodu alıcının bir paketin geldiğinin farkında olması için, zamanlama senkronizasyonu ve ofset kompenzasyonu için kullanılır. Kanal kurulumu sırasında kodun kendisi de bir ID paketi gibi kullanılır. Ek olarak PARK durumundaki rasgele erişim prosedürleri sırasında da kullanılır.

Erişim kodu başlangıç, senkronizasyon kelimesi ve kuyruk (trailer) tan oluşur.

Senkronizasyon Kelimesi Tanımlaması

Senkronizasyon kelimeleri genişletilmiş (64,30) bir BCH kodu temeline dayanır. Bu kod farklı adreslerdeki senkronizasyon kelimeleri arasında büyük Hamming uzaklığını ($d_{min}=14$) garanti eder. PN dizisi erişim kodunun oto korelasyon özelliklerini geliştirmiştir. Aşağıda senkronizasyon kelimesinin nasıl yaratıldığı adım adım açıklanmıştır:

1. Bilgi dizisi üretilir.
2. Bu bilgi dizisi PN dizisinin “bilgi kaplayan” bölümü ile XORlanır.
3. Genişletilmiş BCH kod kelimesi üretilir.
4. Kod kelimesi PN dizisinin bütün 64-bit'i ile XORlanır.

4.2.12.3 MAC Adresi

Piknete dahil olan her köleye bir MAC adresi ayrılır. Tamamı sıfırlardan oluşan adres yayın (broadcast) mesajları için ayrılır. Yöneticinin MAC adresi yoktur. Bir köle sadece eşleşen MAC adresi olan paketleri kabul eder. MAC adresi paket başlığının M_ADDR alanında bulunur.

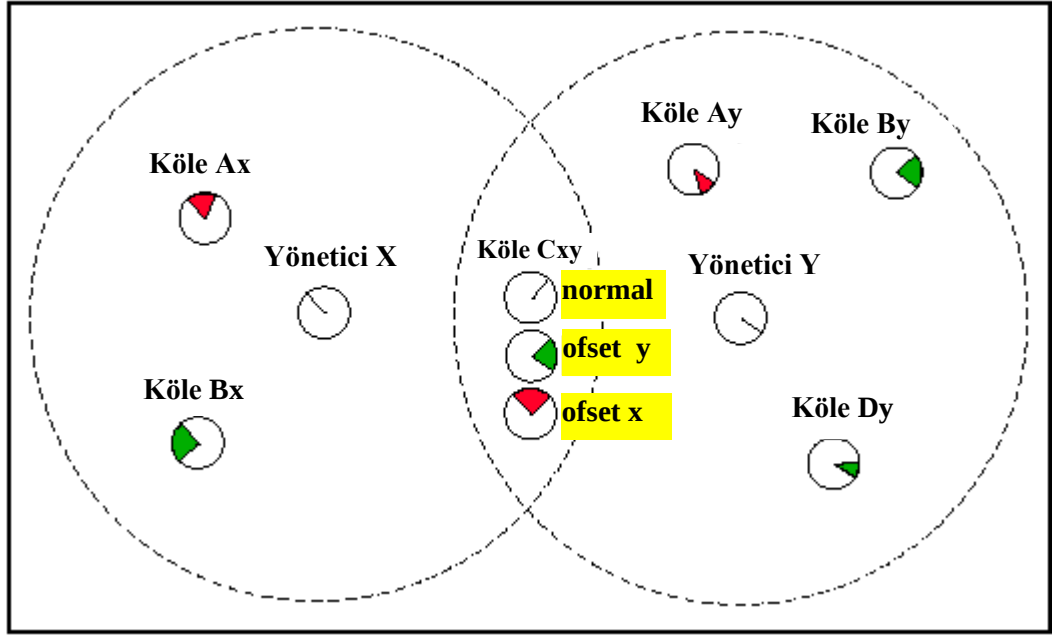
Bekleme (standby) ya da PARK modunda bulunan ünitelerin MAC adresi yoktur. MAC adresi arama kurulumu sırasında FHS paketinde bekleme (standby) durumunda olan köleye tahsis edilir. Arama kurulumunda, FHS paketi tamamı sıfır olan MAC adresini alır. PARK modundaki bir köle aktif hale geldiğinde, yönetici özel bir kontrol mesajı kullanarak bir MAC adresi belirler.

4.2.13 Piconet İçi Bağlantılar

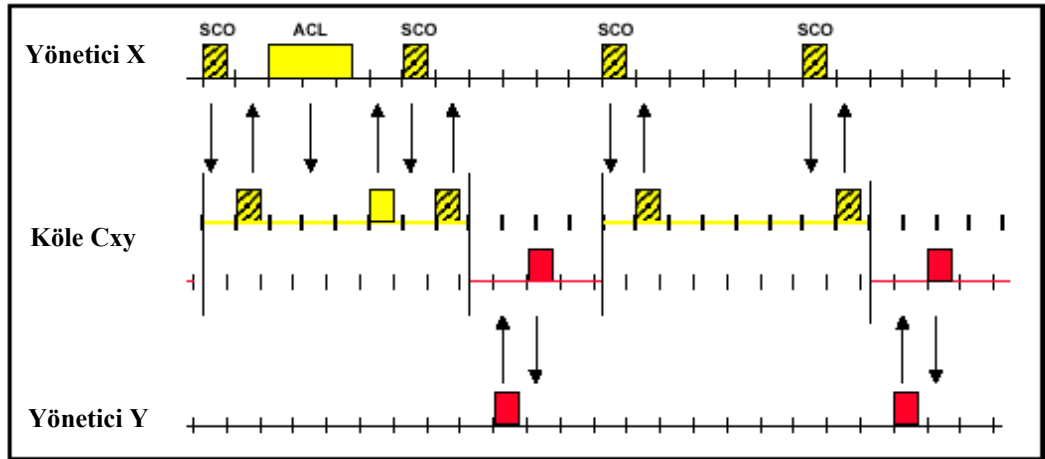
Birden fazla piconet aynı alanı kapsıyorsa, bir ünite zaman çoğullama uygulayarak iki ya da daha fazla piconete dahil olabilir. Uygun kanala katılabilmek için ilgili yönetici adresi ve uygun saat ofseti kullanılmalıdır. Bir Bluetooth ünitesi birçok piconette köle rolünde olabilir fakat yönetici olarak sadece tek bir piconette olabilir. Aynı yöneticiye sahip iki piconet senkronize olur ve aynı atlama dizisini kullanırlarsa tek bir piconete dönüşürler.

Bir yönetici ya da köle başka bir piconetin yöneticisi tarafından çağrılırsa (page edilirse) o piconetin kölesi olabilirler. Diğer taraftan bir piconete dahil olan bir ünite, başka bir piconetin yöneticisini ya da kölesini çağırabilir (page edebilir). Çağrı yapan (paging) ünite daima yönetici olarak başladığı için, köle rolü istenirse bir yönetici-köle rol değişimi yapılmalıdır.

Piconetler arasında bağlaşma yapmak için mutlaka zaman çoğullama kullanılmalıdır. Sadece ACL linklerinde bir ünite sadece kanal parametrelerini değiştirerek başka bir piconete katılması esnasında mevcut piconette de durağan moda girmeyi isteyebilir. Koklama modundaki üniteler koklama slotları arasında diğer piconetlere girmek için yeterli zamana sahiptirler. SCO linkleri kurulmuşsa diğer piconetler sadece rezerve olmayan slotlar arasında ziyaret edilebilirler. Bu durum sadece HV3 paketlerini kullanan tek bir SCO linki mevcutsa mümkündür. Çoğu piconetler senkronize olmadıkları için bozuk sıralı yerleşimleri saymak için bir emniyet süresi bırakılmalıdır. Bu nedenle HV3 paketleri arasında diğer piconeti ziyaret etmek için sadece 2 slot efektif olarak kullanılır.



Şekil 4.21 İki pikonete dahil olan köle



Şekil 4.22 Kölenin iki pikonete katılma zamanlaması

4.2.13.1 Yönetici-Köle Bağlaşması

Yönetici-köle bağlaşması iki yöntemle yapılabilir:

İlk yöntemde yönetici-köle bağlaşması sadece bir zamanlama bağlaştırmacısı (switch) gerektirir. Önceden köle olan ünite TX ve RX zamanlarını değiştirerek fakat önceki yönetici tarafından tanımlanan adres ve saat bilgilerini koruyarak yeni yönetici haline dönüşebilir. Kanal parametreleri değişmez, bu sebeple atlama önceden olduğu şekilde devam eder. Zamanlama bağlaşması bir pikonetteki kölenin aynı pikonette

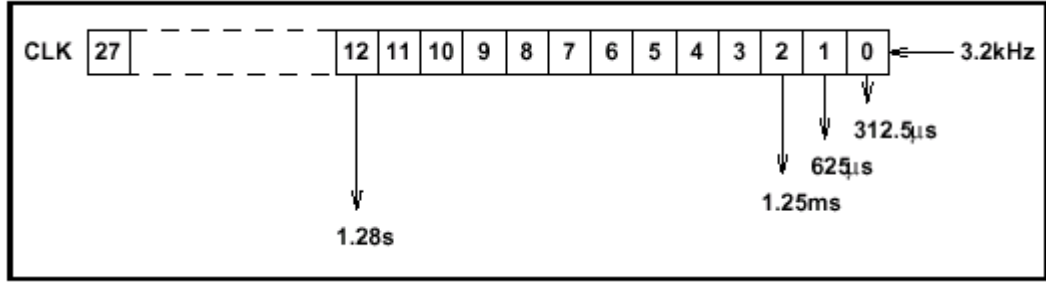
yönetici olması istemesi durumunda gereklidir. Yönetici o pikonet için köle durumuna gelir. Zamanlama bağlaşması ile pikonetteki diğer köleler için bir şey yapılmasına gerek kalmaz; bu köleler mevcut kanal parametrelerini korurlar ve yönetici slotunda iletilenleri dinlemeye devam ederler.

İkinci yöntemde ise, yönetici-köle bağlaşması hem bir zamanlama bağlaştırmacı (switch) hem de bir adres/saat bağlaşması gerektirir. TH bağlaştırmacı (switch) ile yeni yönetici (eski köle) nin parametreleri kanal parametreleri olarak kullanılır. Bu durum hem zamanlama hem de atlamayı etkiler. Eski yönetici ve tüm diğer köleler yeni yöneticinin adresi ve saati ile ilgili olarak bilgilendirilmeli ve bu yeni parametrelere değişmelidirler. TH bağlaştırmacı (switch) yeni bir ünite mevcut pikonete girmek istediğinde kullanılır. Önce pikonetin yöneticisi çağrılır (page edilir); sonra yeni ünitenin pikonetin yöneticisi, eski pikonetin yöneticisinin de köle olduğu bir pikonet kurar. [4]

4.2.14 Bluetooth Saati

Bluetooth saati her üniteye bulunur ve alıcı-vericinin zamanlama ve atlamasını belirler. Bluetooth saati hiçbir zaman kapanmayan ve hiçbir zaman ayarlanmayan doğal olarak çalışan bir saatten elde edilir. Diğer ünitelerle senkronizasyon için ofset değerleri doğal saatin üzerine eklenir. Bluetooth saati güncel zamanla ilişkili değildir; herhangi bir değerle başlatılabilir. Rezolüsyonu en az TX ya da RX slot uzunluğunun yarısı kadar ya da 312.5 μ sn. olmalıdır. Saat bir sayıcı ile uygulanırsa, $2^{28}-1$ çevresinde dolanan 28-bit bir sayıcıya ihtiyaç olur. LSB 312.5 μ sn. de bir atar ve 3.2 kHz. lik saati verir.

Saat kritik periyotları belirler ve Bluetooth alıcısındaki olayları tetikler. Bluetooth sisteminde dört periyot önemlidir: 312.5 μ sn., 625 μ sn., 1.25 msn. ve 1.28 sn. Bu periyotlar sırasıyla CLK₀, CLK₁, CLK₂ ve CLK₁₂ zamanlama bitlerine karşılık gelirler. Bir yönetici slotun başlangıcı CLK₀ ve CLK₁ in her ikisinin de sıfır olması ile anlaşılır. [2]



Şekil 4.23 Bluetooth saati

4.2.15 Güç Tüketimi

Bluetooth bekleme (standby) ve çağrı modu olmak üzere iki ana modda çalışır. Bekleme (standby) modu dört alt moddan oluşur: uyku, çağrı (page)-tarama, durağan ve park modları. Uyku modunda bütün Bluetooth linki pasifize olmuştur, sadece düşük güçlü bir alçak frekans osilatörü çalışmaktadır. Her 1.28 sn de bir link radyo alıcısı ile bir temelbant korelatörünün gelen bir çağrı için tarandığı çağrı (page)-tarama moduna geçer. Bu tarama periyodu 9 çerçeve boyunda yani 11.25 msn. dir. Gelen bir çağrı tespit edilirse Bluetooth çağrı moduna geçer, çağrı tespit edilmezse tekrar uyku moduna döner. Link asenkron olarak sunucu arayüzündeki UART yoluyla bekleme (standby) modundan çıkarılabilir. Park ve durağan modlarında link bir yönetici ile senkronize olmuştur ve düzenli tarama aralıklarında uyanır. Bu tarama aralıkları yönetici ile senkronize olmuşlardır ve saat kaymalarını kompanze edecek kadar uzun olmaktadır.

Çağrı modunda, link üç alt moda sahiptir: RX, FH ve TX modları. Tüm çağrı modlarında temelbant ve mikroişlemci devreleri aktiftir fakat radyo devresi sadece gerekli olan blokları kullanır. Bu sebeple RX modunda synthesizer ve alım zinciri; FH modunda sadece synthesizer ve TX modunda da synthesizer ve güç kuvvetlendiricisi aktiftir. Bekleme (standby) modunda çekilen akım aşağıdaki şekilde bulunabilir:

$$I_{\text{bekleme}} = I_{\text{uyku}} + I_{\text{RX}} = 0.03 + 0.3 \cong 0.3 \text{ mA.}$$

(tarama periyodu radyodaki başlangıç zamanlarını kompanze etmek için 12 msn. ye ayarlanmıştır.)

Benzer şekilde çağrı modunda çekilen akım da aşağıdaki şekilde bulunabilir:

$$I_{\text{call}} = I_{\text{RX}} + I_{\text{FH}} + I_{\text{TX}} = 10 + 10 + 10 = 30 \text{ mA.}$$

(başlangıç zamanlarını kompanze etmek için RX ve TX modlarına 20 µsn. eklenmiş ve saat kaymasını kompanze etmek için de RX moduna bir 10 µsn. daha eklenmiştir.)

100 ppm li uyku modu zamanlayıcısının doğruluğu ile, bir Bluetooth linki 4 sn. boyunca senkronizasyonu kaybetmeden durağan moda alınabilir. Eğer 4 sn. lik durağan periyot boyunca 3 paket iletilmişse, çekilen akım:

$$I = I_{uyku} + (3.75/4000) * (I_{RX} + I_{FH} + I_{TX}) \cong 60 \mu A.$$

olur.

4.2.15.1 Güç Tüketimini Azaltmak

Güç tüketimi radyo ve radyonun 2.4 GHz. lik kısımları tarafından domine edilmiştir. Bekleme (standby) ve uyku periyotlarını uzatmak bekleme modu (standby) güç tüketimini azaltır. Uyku modunu uzatmanın dezavantajı ise artan kazanma zamanıdır. Bluetooth ünitesi bir bağlantı talebini algılamak için en fazla iki adet sıkışık olmayan çağrı (page) dizisine ihtiyaç duyar. (ya da ≤ 2.56 sn.)

Bekleme (standby) moduna bir alternatif olarak hiçbir paket iletilmediğinde Bluetooth ünitesini durağan moda almak verilebilir. Durağan mod çağrı (page) taramaya ihtiyaç duymaz ve yönetici ve köle halen senkronize oldukları için paket iletimi aniden başlayabilir. Durağan moddaki güç tüketimi, bekleme (standby) uyku modundaki güç tüketimine eşittir. Durağan konumdaki bir link bağlantı taleplerine normal olarak servis veremez. Park modu da güç tüketimi ile ilgili olarak durağan mod ile benzerdir.

4.2.15.2 Düşük Veri Hızları

Bluetooth düşük veri hızı avantajını iki şekilde taşır. Birincisi, gönderilecek veri yoksa boş TX paketleri herhangi bir RX paketi alındısı almak zorunda olmadığı sürece gönderilmez. İkincisi, bir süreliğine iletilecek veri yoksa, link bağlantıyı kesmeksizin durağan moda ve uyku moduna geçer. Konuşma bağlantıları ise gecikme problemlerinin önüne geçebilmek için daima en yüksek veri hızında yapılır.

İletilecek veri yoksa, TX slotu için radyoda FH ve TX aktivitesi başlatılmaz. Her iki ünite de kendilerine gönderilecek veri için dinleme konumunda kalmak zorunda olduğu için her RX slotu için FH ve RX yerine getirilmelidir. Fakat eğer hiç veri ve

hatta hiçbir paket gönderilmeyecekse, alıcı sadece kendi başlangıcı için dinlemede kalır. Eğer başlangıç yoksa radyo bir sonraki RX slotu gelene kadar yani 88 µsn. sonra uyku moduna geçer.

Bir noktadan noktaya bağlantıda her iki Bluetooth ünitesi de düşük veri hızının avantajından yararlanmak için veri göndermeyi durdurmalıdır. Eğer iki uçtan birinin gönderecek verisi varsa, diğer ünite ona mutlaka alındı bilgisi göndermelidir ve böylece iki yönlü bir veri transferi oluşturulur. Fakat alındı bilgisi kısa NULL paketi içinde gönderilirse TX gücü azaltılmış olur. Konuşma işaretleri ise her zaman için sürekli bir veri akışına sebep olur.

Gönderilecek veri yoksa, çağrı modu akımı:

$$I_{call} = I_{RX} + I_{FH} + I_{TX} = 2 + 5 + 1 = 8 \text{ mA. olur.}$$

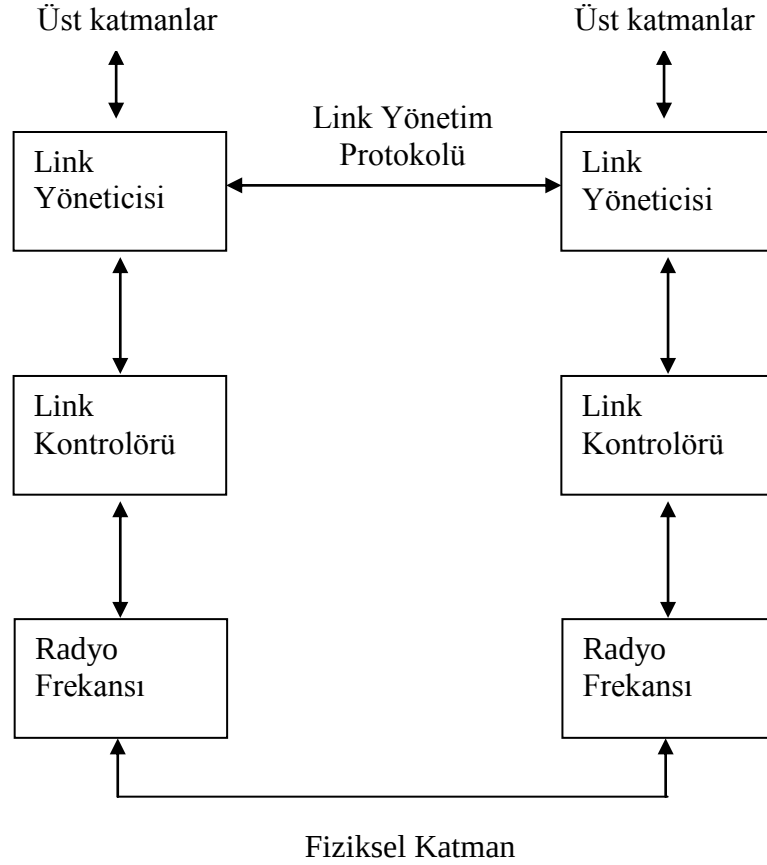
Bir Bluetooth linkinde maksimum veri hızında 30 mA. lik akım çekilir. Düşük veri hızlarında, çağrı modu akımı, asimptotik olarak, sıfır veri hızında 8 mA. e ulaşır. Örneğin 9600 bit/sn. lik veri hızında:

$$I_{call} = I_{fullrate} + I_{zerorate} = 30 * (9.6/172.8) + 8 * ((172.8 - 9.6)/172.8) = 2 + 8 = 10 \text{ mA.}$$

elde ederiz ve verinin sadece veri ara belleği dolu olduğunda gönderildiğini varsayalım. [4,8]

4.3 Link Yönetim Protokolü

İki Bluetooth cihazı birbirlerinin çalışma alanı içine girdiklerinde, her bir cihazdaki Link Yöneticisi diğer cihazı keşfeder. Link yöneticileri arasındaki noktadan noktaya bağlantıda mesajlar LMP sayesinde alınıp verilir. Bu mesajlar link kurulumunu yapar, doğrulama ve şifreleme gibi güvenlik işlevlerini yerine getirir ve temelbant paket boyutlarını kontrol ve değerlendirmeye alırlar. Bu mesajların alınıp verilmesi ile LMP, Bluetooth radyo cihazlarının görev durumlarını, piconetteki bağlantı durumlarını ve güç modlarını kontrol eder. Link Yönetim Protokolü ile diğer Bluetooth cihazları arasındaki ilişki Şekil 4.24 de gösterilmektedir.



Şekil 4.24 İki cihaz arasında Link Yönetim Protokolü ile link kurulumu

Link Yöneticisi Bluetooth ünitesindeki mikro işlemcide çalışan bir yazılımdır. Her Bluetooth cihazının kendine ait Link Yöneticisi vardır. Link Yöneticisi diğer uzak link yöneticilerini keşfeder ve link kurulumu, doğrulama, konfigüre etme ve diğer fonksiyonları gerçekleştirmek için onlarla haberleşir. [9]

Link Yöneticisi, servis sağlayıcısı görevini yerine getirebilmek için Link Kontrolörü (LC) tarafından sağlanan fonksiyonları kullanır. Link Kontrolörü tüm temelbant fonksiyonlarını yerine getiren ve Link Yöneticisini destekleyen bir yapıdadır. Veriyi gönderir ve alır, gönderen cihazın kimliğini sorgular, linki doğrular, linkin tipini (SCO veya ACL) belirler, paket bazında kullanılacak çerçeve tipine karar verir, cihazların diğer cihazlardan gelen iletim isteklerini kabul etme veya durağan moda alma gibi tavırlarını yönetir.

Link Yöneticileri arasında alınıp gönderilen mesajlar “Protokol Veri Üniteleri” (PDU) nin şeklini alırlar. Bu veriler kullanıcı verilerinden daha yüksek öneme

sahiptirler. Böylelikle Link Yöneticisi'nin göndermek istediği bir mesaj L2CAP trafiği tarafından geciktirilmez. PDU lar bireysel temelbant paketlerinin birçok defa tekrar gönderilmesi sonucu gecikmeye uğrayabilirler. Her durumda bu mesajlar alıcı tarafın Link Yöneticisi tarafından filtrelenerek yorumlanır ve daha yüksek kademelere gönderilmezler.

LMP de hiçbir harici mesaj bilgisi sağlanmaz çünkü Link Yöneticisi bu tip bir bilginin sağlanma gereksinimini ortadan kaldıran güvenli bir link sağlar. Bununla birlikte LMP PDU taşıyan bir temelbant paketinin alınması ile geçerli bir cevap PDU su taşıyan bir temelbant paketinin gönderilmesi arasında geçen zaman LMP nin cevap zaman aşımı eşik değerinden daha az olmalıdır. Bu değer 30 sn.dir.

4.3.1 PDU Tipleri

Bluetooth spesifikasyonunda her biri bir fonksiyonu yerine getirmek üzere tanımlanmış 55 farklı PDU tipi bulunmaktadır. Her PDU, tipini tanımlamak için 7-bitli bir op kodu kullanır. PDU nun hedef adresi paket başlığındaki AM_ADDR ile belirlenir.

PDU lar zorunlu veya seçime bağlı olmak üzere iki türdür. LM seçime bağlı olan PDU ları iletmek zorunda değildir fakat tüm seçime bağlı PDU ları ayırtederek alır; ve eğer bir cevap istenmişse geçerli bir cevap gönderir. Eğer alınan seçime bağlı PDU cevap verilmesini gerektirmiyorsa, cevap gönderilmez.

Bazı LMP PDU ları gelecekte olması muhtemel kullanımlar için rezerve edilirler. Gücün azaltılması (LMP_decr_power_req) veya artırılması (LMP_incr_power_req) nı istemek için kullanılan PDU lar rezerve PDU lara örnek olarak verilebilir.

4.3.2 Genel Cevap Mesajları

LMP_accepted ve LMP_not_accepted PDU ları Link Yöneticileri arasında diğer PDU lara cevap vermek için kullanılan iki tip genel cevap mesajıdır. LMP_accepted PDU su kabul edilen mesajın op kodunu da içerir. LMP_not_accepted PDU su da kabul edilmeyen mesajın op kodunu ve kabul edilmeme nedenini içerir.

4.3.3 Doğrulama

Güvenlik için bir rasgele sayı (challenge)-cevap şemasına dayalı olan bir doğrulama prosedürü kullanılır. Yönetici de köle de doğrulamayı yapan taraf olabilir.

Doğrulamayı yapan taraf rasgele bir sayı (challenge) içeren LMP_au_rand PDU sunu talep eden tarafa gönderir. Bu mesajı alan taraf bir cevap hesaplar. Hesaplanan cevap rasgele sayının (challenge), talep sahibi tarafın “Bluetooth Cihaz Adresi” (BD_ADDR) nin ve bir gizli anahtarın fonksiyonudur. Bu cevap doğrulamayı yapan tarafa cevabın doğru olup olmadığının kontrolü için gönderilir. Doğrulama cevabının uygun bir şekilde hesaplanabilmesi için doğrulamayı yapan ve talepte bulunan tarafların gizli bir anahtar paylaşmaları gerekir.

Eğer talepte bulunan tarafın doğrulamayı yapan tarafla ilişkili bir link anahtarı varsa, cevabı hesaplar ve doğrulamayı yapan tarafa LMP_sres ile gönderir. Doğrulamayı yapan taraf bu cevabı kontrol eder. Gelen cevap doğru değilse doğrulamayı yapan taraf “kod doğrulama hatası” sebebiyle LMP_detach göndererek bağlantıyı sonlandırabilir. Talepte bulunan tarafın ilişkili bir link anahtarı yoksa “anahtar kayıp” sebep kodu ile LMP_not_accepted gönderir.

Bir doğrulama süreci başarısız sonuçlandığında, herhangi bir davetsiz atak sebebiyle defalarca birçok anahtar denenmesini de engellemek için, yeni bir doğrulama sürecinin başlaması için belirli bir bekleme aralığı uygulanır. Aynı Bluetooth adresi için alınan her başarısız sonuçta, bekleme aralığı üstel olarak artırılır. Maksimum bekleme aralığı uygulamaya bağlı olarak değişir. Bekleme süresi belirli bir zaman aralığında hiç hata alınmazsa bir minimuma düşürülür. [10]

4.3.4 Çiftleme (Pairing)

İki cihazın ortak bir link anahtarı yoksa, bir PIN ve rasgele bir numaraya dayalı olan bir başlangıç anahtarı yaratılmalıdır. 128-bitlik başlangıç anahtarı gönderen taraf talepte bulunan tarafa LMP_in_rand mesajı gönderdiğinde oluşturulur. Bu aşamadan sonra doğrulama yapılmalıdır; doğrulama cevabının hesaplaması başlangıç anahtarına dayanır. Başarılı bir doğrulamadan sonra ise link anahtarı oluşturulur.

Gönderen taraf talepte bulunan tarafa LMP_in_rand mesajı gönderdikten sonra, cevap LMP_accepted mesajı ile olur. Her iki cihaz da başlangıç anahtarını hesaplar ve bu anahtara bağlı olarak bir doğrulama gerçekleşir. Gönderen taraf doğrulama cevabını alır ve alınan cevap doğru ise link anahtarı oluşturulur. Doğrulama cevabı yanlışsa gönderen taraf “doğrulama başarısız” sebep kodu ile LMP_detach komutunu göndererek bağlantıyı sona erdirebilir.

Eğer talepte bulunan tarafın belirli bir PIN i varsa yeni bir rasgele numara yaratıp LMP_in_rand da geri göndererek talep eden-gönderen rollerinin değişmesini isteyebilir. Eğer çiftleme prosedürünü başlatan tarafın değişken PIN i varsa bu talebi kabul eder ve LMP_accepted ile cevap verir. Böylece roller başarıyla değişmiş olur ve çiftleme prosedürü devam eder.

Eğer çiftleme prosedürünü başlatan tarafın sabit PIN i varsa ve diğer cihaz bir rol değişimi talep ediyorsa, “çiftleme izni yok” sebep kodu ile LMP_not_accepted gönderilerek rol değişim işlemi reddedilir. Bu noktada çiftleme prosedürü durur. Talebi alan taraf çiftlemeyi kabul etmezse LMP_in_rand aldıktan sonra “çiftleme izni yok” sebep kodu ile LMP_not_accepted gönderir.

Doğrulama sona erdiğinde link anahtarı oluşturulmalıdır. Bu anahtar değişmediği sürece iki ünite arasındaki takip eden tüm bağlantılarda doğrulama yaparken kullanılacaktır. Çiftleme prosedürü sırasında oluşturulan link anahtarı bir kombinasyonun sonucu ya da iki üniteden birinin ünite anahtarı olabilir. Eğer bir ünite LMP_unit key gönderir ve diğer ünite de LMP_comb_key gönderirse link anahtarı ünite anahtarı olur. Eğer her iki ünite de LMP_unit_key gönderirse yöneticinin ünite anahtarı link anahtarı olur. Eğer her iki ünite de LMP_comb_key gönderirse link anahtarı hesaplanarak bulunur.

Çiftleme sırasında alınan hatalı bir doğrulama cevabı sonucu doğrulama süreci başarısız sonuçlanırsa yeni bir doğrulama sürecinin yaşanması için belirli bir süre geçmesi gerekir. Aynı Bluetooth adresi için alınan her başarısız sonuçta, bekleme aralığı üstel olarak artırılır. Böylelikle herhangi bir davetsiz atak sebebiyle kısa sürede birçok PIN denenmesi engellenir.

4.3.5 Link Anahtarının Değişmesi

İki cihaz çiftlenmiş ve link anahtarı da kombinasyon anahtarlarından elde edilmişse, link anahtarı değişebilir. Eğer link anahtarı aynı zamanda bir ünite anahtarıysa, link anahtarının değişmesi için ünitelerin tekrar çiftleme prosedüründen geçmesi gerekir. PDU ların içeriği mevcut link anahtarı ile korunur.

Link anahtarının değişimi başarılı olursa, yeni anahtar geçici olmayan bellekte tutulur ve eski anahtar kullanımdan kaldırılır. Yeni link anahtarı tekrar değişinceye veya geçici başka bir link anahtarı yaratılıncaya kadar iki cihaz arasındaki tüm bağlantılarda kullanılır.

Eğer link üzerinde şifreleme yapılıyorsa ve mevcut link anahtarı geçici bir anahtarsa, şifreleme işlemi acil olarak durdurulup link anahtarı değişim prosedürü uygulanmalıdır. Link anahtarı değiştikten sonra şifrelemeye devam edilebilir. Böylelikle yarı-kalıcı link anahtarının mevcut olduğu durumda pikonetteki cihazlar tarafından bilinen şifreleme kodlarının kullanılmaması sağlanmış olur.

4.3.6 Mevcut Link Anahtarının Değişmesi

Mevcut link anahtarı yarı kalıcı veya geçici olabilir. Zaman zaman değiştirilebilir fakat bu değişim sadece değişimin olduğu oturum için geçerlidir. Geçici bir link anahtarını değiştirmek pikonet şifrelenmiş yayını desteklediği durumda gereklidir.

Geçici bir link anahtarını değiştirmek için yönetici, yönetici anahtarını oluşturarak işe başlar. Daha sonra yönetici rasgele bir sayı üreterek LMP_temp_rand ile köleye gönderir. Her iki taraf da bir ara değer hesaplar. Yönetici köleye LMP_temp_key ile yönetici anahtarını gönderir. Ara değeri bilen köle de yönetici anahtarını hesaplar. Bunun sonucunda yönetici anahtarı mevcut link anahtarı haline gelir.

4.3.7 Şifreleme

Şifreleme mecburi olarak yapılmaz, seçime bağlı olarak yapılır. En az bir doğrulama yapılması gerekiyorsa şifreleme kullanılabilir. Eğer yönetici pikonetteki tüm kölelerin aynı şifreleme parametrelerini kullanmasını istiyorsa; öncelikle geçici bir link anahtarı oluşturur ve şifreleme başlamadan önce bu anahtarı tüm köleler için kalıcı anahtar haline getirir. Yayınlanan paketlerin şifreli olması isteniyorsa bu işlemin yapılması gereklidir.

Yönetici ve köle öncelikle şifreleme kullanılıp kullanılmayacağına; sonrasında ise şifrelemenin sadece noktadan noktaya paketlere ya da hem noktadan noktaya olan hem de yayınlanan paketlere uygulanmasına karar vermelidir. Şifrelemeye karar verilirse yönetici şifreleme ile ilgili detaylı bilgi vermeye başlar.

Sonraki aşama da şifreleme anahtarının boyutuna karar vermektir. Yönetici istenen boyut bilgisini içerecek şekilde LMP_encryption_key_size_req mesajını gönderir. Yönetici ve köle arasında boyut üzerine karar verilmesi için bir mesaj trafiği yaşanır. Bir karara varıldığında ise son LMP_encryption_key_size_req mesajındaki boyut kullanılır.

Boyut belirlendikten sonra şifreleme işlemi başlar. Yönetici rasgele bir sayı üretir ve şifreleme anahtarını hesaplar. Pikonet şifrelenmiş yayını destekliyorsa üretilen rasgele sayı tüm köleler için aynı olur. Yönetici rasgele sayıyı içeren LMP_start_encryption_req mesajını gönderir. Bu mesajı alan köle mevcut link anahtarını hesaplar ve LMP_accepted ACK mesajını gönderir. Her iki tarafta da hem mevcut link anahtarı hem de rasgele sayı şifreleme algoritmasını oluşturmak için kullanılır.

Şifrelemeye başlanmadan önce üst seviyelerdeki veri trafiği bozulma olasılığını ortadan kaldırmak için geçici olarak durdurulur. Şifrelemenin başlaması üç adımlı bir süreçtir:

1. Yönetici şifrelenmemiş paketleri göndermek ve şifrelenmiş paketleri almak üzere konfigüre edilir.
2. Köle şifrelenmiş paketleri almak ve göndermek üzere konfigüre edilir.
3. Yönetici şifrelenmiş paketleri almak ve göndermek üzere konfigüre edilir.

1. ve 2. adımlar arasında yöneticiden köleye iletim olabilir. 2. adım köle LMP_start_encryption_req mesajını aldığı anda başlar. 2. ve 3. adımlar arasında köleden yöneticiye iletim mümkündür. 3. adım yönetici LMP_accepted mesajını aldığı anda başlar.

Şifreleme sona ermeden önce de yine üst seviyelerdeki veri trafiği bozulma olasılığını ortadan kaldırmak için geçici olarak durdurulur. Şifrelemenin bitmesi de başlaması gibi üç adımlı bir süreçtir:

1. Yönetici şifrelenmiş paketleri göndermek ve şifrelenmemiş paketleri almak üzere konfigüre edilir.
2. Köle şifrelenmemiş paketleri almak ve göndermek üzere konfigüre edilir.
3. Yönetici şifrelenmemiş paketleri almak ve göndermek üzere konfigüre edilir.

1. ve 2. adımlar arasında yöneticiden köleye iletim olabilir. 2. adım köle LMP_stop_encryption_req mesajını aldığı anda başlar. 2. ve 3. adımlar arasında köleden yöneticiye iletim mümkündür. 3. adım yönetici LMP_accepted mesajını aldığı anda başlar.

Eğer şifreleme modu, anahtarı ya da rasgele sayısı değiştirilmek istenirse önce şifreleme işlemi durdurulur sonra yeni parametrelerle tekrar başlar.

4.3.8 Saat Ofset Talebi

Saat ofseti yönetici saati ile köle saati arasındaki farktır. Saat ofset değeri FHS taşınan bilgisinde (payload) bulunur. Bu paketi alan bir köle kendi saati ile yönetici saati arasındaki farkı hesaplayarak FHS paketinin taşınan bilgisine (payload) ekler. Saat ofseti yöneticiden alınan her paket için güncellenir. Yönetici, bağlantı sırasında herhangi bir zamanda bu saat ofset değerini isteyebilir. Böylelikle çağrı (paging) zamanı hızlandırılabilir ya da yönetici hangi RF kanalda hangi kölenin çağrı taraması (page scan) için uyandığı bilgilerini alabilir.

4.3.9 Zaman Aralığı (Slot) Ofset Bilgisi

Slot ofseti farklı pikonetlerdeki slot sınırları arasındaki farktır. LMP_Slot_Offset PDU su slot ofset değeri ve BD_ADDR olmak üzere iki parametre taşır. Slot ofseti mikrosaniyeler mertebesinde ve PDU nun aktarıldığı pikonetteki yöneticinin transmit slotu (TX) başlangıcı ile, BD_ADDR nin iletildiği pikonetteki yöneticinin TX slotu başlangıcı arasındaki zaman farkına eşittir. Bir yönetici-köle bağlaşması yapılmadan önce bu PDU bağlaşma prosedüründe yönetici rolünü alan cihaz tarafından gönderilir. Bağlaşma prosedürünü yönetici başlatmışsa köle LMP_accepted göndermeden önce LMP_slot_offset i gönderir. Bağlaşma prosedürünü köle başlatmışsa köle LMP_switch_req. göndermeden önce LMP_slot_offset i gönderir.

4.3.10 Zamanlama Doğruluk Bilgisi Talebi

Zamanlama bilgisi, durağan moddan çıkış esnasında belirli durağan mod süresi ve maksimum durağan mod süresini uzatmak için tarama penceresini minimize etmekte kullanılabilir. Bu bilgi aynı zamanda koklama modu slotları veya park modu işaret (beacon) paketleri için tarama yapılırken tarama penceresini minimize etmekte kullanılır. Bundan dolayı, LMP zamanlama için talepte bulunma konusunu destekler. Dönen zamanlama doğruluk parametreleri uzun dönemli drift (parts per million:ppm olarak ölçülür) ve uzun dönemli jitter (durağan, koklama ve park modları sırasında kullanılan saat değerinin milisaniyeleri mertebesinde ölçülür) parametreleridir.

Zamanlama doğruluk parametreleri belirli bir cihaz için sabit olmalı ve birden fazla defa istendiğinde birbirinin aynı olmalıdır. Eğer cihaz, zamanlama doğruluk bilgisini desteklemiyorsa talep geldiğinde PDU ya “unsupported LMP feature” (desteklenmeyen LMP hatası) sebep kodu ile LMP_not_accepted gönderir. Bu durumda talebi gönderen cihaz en kötü durum değerlerinin olduğunu varsayar (250 ppm drift ve 1 msn. jitter).

4.3.11 LMP Versiyonu

LMP LM protokolünün versiyonu için gelen istekleri destekler. Cevap veren cihaz versiyon numarası (VersNr), şirket Id si (CompId) ve alt-versiyon numarası (Sub-VersNr) parametrelerini gönderir. VersNr cihazın desteklediği Bluetooth LMP spesifikasyonunun versiyonunu belirler. CompId, alçak kademedeki Bluetooth katmanları ile olabilecek muhtemel problemleri takip etmek için kullanılır. Link Yöneticisinin eşi olmayan bir uygulamasını yapan her şirketin kendisine ait bir CompId si vardır. (Tablo 4.6)

Tablo 4.6 LMP_CompId parametre kodları

Kod	Şirket
0	Ericsson Mobile Communications
1	Nokia Mobile Phones
2	Intel Corp.
3	IBM Corp.
4	Toshiba Corp.
5-65534	Rezerve
65535	Atanmamış. Bir CompId verilmeden önce yapılan uygunluk testlerinde kullanılır, ürünlerde kullanılmaz.

Her şirket aynı zamanda SubVersNr nin de yönetim ve bakımını yapmakla yükümlüdür. Ayrıca her şirket her radyo frekansı, Bluetooth temelbant ve Link Yöneticisi uygulaması için tek olan bir SubVersNr ye sahip olmak zorundadır. Belirli bir VersNr ve CompId için SubVersNr değerleri her yeni uygulama piyasaya sunulduğunda artmalıdır. LMP versiyonu üzerinde sadece parametreleri alıp vererek karara varmak mümkün değildir.

4.3.12 Desteklenen Özellikler

Bluetooth Radyo ve Link kontrolörü belirli bir paket tipini ve özelliklerini desteklediği için, cihazların diğer cihazların hangi tipleri desteklediği bilgisini anlamaları gerekmektedir. Bu bilgi LMP_features_req ve LMP_features-res PDU ları ile alınıp gönderilir. Talep özellikleri sağlandıktan sonra paket tipleri de alınıp gönderilir.

Bir talep alındığında, bu talep diğer cihazın desteklediği özelliklerle uyumlu olmalıdır. Örneğin, bir SCO linki kurulurken, haberleşmeyi başlatan cihaz diğer cihazın desteklemediği türden bir paket tipini kullanmayı önermemelidir. Bu kural için sadece LMP_slot_offset ve seçime bağlı olan LMP_switch_req PDU ları istisnadır. Her iki PDU da iki Bluetooth cihazı bağlanıp, bağlantıyı talep eden taraf diğer tarafın özellikleri üzerinde bilgi sahibi değilken gönderilen ilk LMP mesajlarıdır.

4.3.13 Yönetici-Köle Rollerini Değişimi

Çağrı yapan (paging) cihaz her zaman pikonetin yöneticisi olduğu için, yönetici-köle rol değişimi bazen gerekli olmaktadır. Örneğin A cihazı köle, B cihazı da yönetici ise rol değişimini başlatan cihaz mevcut L2CAP mesajının transferini tamamlar ve rol değişimini isteyen LMP_switch_req PDU sunu gönderir. Rol değişimi kabul edilirse, diğer cihaz mevcut L2CAP mesajının transferini tamamlar ve LMP_accepted ile cevap verir. Rol değişimi kabul edilmezse LMP_not_accepted ile cevap verilir ve değişim gerçekleşmez. [10]

4.3.14 İsim İsteği

LMP başka bir Bluetooth cihazından isim istemini destekler. İsim bilgisi en fazla 248 byte olabilir ve bir veya birkaç pakete ayrıştırılabilir. LMP_name_req gönderildiğinde bir isim ofseti hangi paketin beklendiği bilgisini içerir. Buna tekabül

eden LMP_name_res aynı isim ofsetini taşır, isim uzunluğu Bluetooth cihazının ismindeki toplam byte sayısını ve ayrıştırılan paket bilgisini içerir.

4.3.15 Bağlantı Bitişi

Bluetooth cihazları arasındaki haberleşmeyi herhangi bir zamanda yönetici ya da köle bitirebilir. Bu özellik için kullanılan PDU LMP_detach dir. Karşı tarafı bilgilendirmek amaçlı bir sebep parametresi de mesajın içine dahil edilmiştir.

4.3.16 Durağan Mod

İki Bluetooth cihazı arasındaki ACL linki belirli bir zaman süresince durağan modda kalabilir. Durağan mod talebi için kullanılan PDU LMP_hold_req dir. Bu süre boyunca yöneticiden herhangi bir paket alışverişi olmaz.

Genellikle uzunca bir süre veri gönderilmeyecekse durağan moda girilir. Bu süre boyunca alıcı-verici güç korunumu yapmak için kapanır. Bunun yanısıra başka bir pikonete girmek isteyen bir cihaz ya da başka bir Bluetooth cihazı ile haberleşmeye geçmek isteyen bir cihaz tarafından da kullanılabilir.

Daha önceden kabul edilen bir durağan moda giriş talebi olmuşsa yönetici durağan moda girilmesini isteyebilir. Durağan mod süresindeki tek kısıtlama yönetici durağan moda girilmesini istediğinde PDU da bulunan durağan mod süresinin, kölenin daha önce kabul ettiği durağan mod sürelerinden daha uzun olamamasıdır. Aynı şekilde eğer daha önceden kabul edilen bir durağan mod talebi varsa köle de durağan moda girilmesini isteyebilir. Ve durağan mod süresi de yöneticinin daha önce kabul ettiği sürelerden daha uzun olamaz.

Hem yönetici hem de köle durağan moda geçmek isteyebilir. Durağan moda geçiş talebinin alınmasıyla, aynı talep değiştirilmiş parametrelerle geri gönderilebilir ya da bu görüşme sona erdirilir. Görüşme sonucunda anlaşmaya varılırsa LMP_accepted ile görüşme sona erdirilir ve ACL linki durağan moda alınır. Anlaşmaya varılamazsa “desteklenmeyen parametre değeri” sebep kodu ile LMP_not_accepted PDU su görüşmeyi sona erdirir ve durağan moda geçiş olmaz.

4.3.17 Koklama Modu

Bluetooth cihazları için başka bir güç korunumu modu da koklama modudur. Koklama moduna geçmek için yönetici ve köle bir koklama aralığı ve ofset değerine

karar verirler. Ofset değeri ilk koklama slotunun zamanlamasını belirler. Daha sonra koklama slotları koklama aralıkları ile periyodik olarak takip ederler. Koklama modundaki bir linkte sadece koklama slotunda yönetici bir iletim sağlayabilir.

Köledeki dinleme aktivitesini iki parametre kontrol eder. Birincisi kölenin kendi aktif üye adresini içeren bir paket gelmesi bile kaç slot dinlemek durumunda olduğu bilgisini içeren “koklama girişi” parametresidir. İkincisi ise köle kendi aktif üye adresi ile gelen paketleri almaya devam ederse kaç tane daha ek paket alacağını belirleyen “koklama zaman aşımı” parametresidir.

Yönetici kölenin koklama moduna girmesini isteyebilir, fakat hem yönetici hem de köle koklama moduna girilmesini talep edebilir. Talebin alınmasıyla, aynı talep değiştirilmiş parametrelerle geri gönderilebilir ya da bu görüşme sona erdirilir. Görüşme sonucunda anlaşmaya varılırsa LMP_accepted ile görüşme sona erdirilir ve ACL linki koklama moduna alınır. Anlaşmaya varılamazsa “desteklenmeyen parametre değeri” sebep kodu ile LMP_not_accepted PDU su görüşmeyi sona erdirir ve koklama moduna geçiş olmaz.

Koklama modu LMP_unsniff_req PDU su gönderilerek sona erdirilir. Sona erdirmeye talebini alan cihaz LMP_accepted ile cevap vermelidir. Talebi gönderen köle ise LMP_accepted cevabını aldıktan sonra aktif moda geçer. Talebi gönderen yönetici ise, köle LMP_unsniff_req i aldıktan sonra aktif moda geçer.

4.3.18 Park Modu

Eğer bir köle kanala dahil olmak durumunda değil, fakat hala FHS konumunda kalmak durumunda ise park moduna girebilir. Bu modda cihaz kendi AM_ADDR sinden vazgeçer. Bir köle park modunda ise eşsiz bir Park Üye Adresi (Parked Member Address-PM_ADDR) alır. Yönetici bu adresi kullanarak köleyi park durumundan çıkarabilir. Cihaz, AM_ADDR si olmadan dahi daha önceden belirlenmiş aralıklarda oluşan işaretlere (beacon) cevap olarak uyandığında kanal ile senkronize olabilir. Bir işaretle (beacon) park halindeki köle, yönetici tarafından tekrar aktif hale getirilebilir. Yönetici aynı zamanda park modu parametrelerini değiştirebilir, yayın (broadcast) bilgisini gönderebilir veya park modundaki kölenin kanala erişme talebinde bulunmasına izin verir.

Yöneticiden park halindeki kölelere gönderilen tüm PDU lar yayın (broadcast) ır. LMP_set_broadcast_scan_window, LMP_modify_beacon,

MP_unpark_BD_addr_req ve LMP_unpark_PM_addr_req PDU ları park modundaki bir köleye gönderilebilen yegane PDU lardır ve sadece yayınlanabilirler. Yayın güvenliğini artırabilmek için paketler mümkün olduğu kadar kısa tutulurlar.

Yönetici park modunu isteyebilir. Bu prosedürde yönetici mevcut L2CAP mesajının gönderimini bitirir ve LMP_park ı gönderir. Bu PDU yu alan köle, mevcut L2CAP mesajının iletimini sonlandırır ve LMP_accepted ı gönderir.

Yönetici ayrıca kölenin park moduna girmesini de isteyebilir. Bu prosedürde yönetici mevcut L2CAP mesajının gönderimini bitirir ve LMP_park_req ı gönderir. Eğer köle park moduna giriş talebini kabul ederse; mevcut L2CAP mesajının iletimini sonlandırır ve LMP_accepted ı gönderir. En son olarak da yönetici LMP_park ı gönderir. Eğer köle park moduna giriş talebini kabul etmezse LMP_not_accepted ı gönderir.

Köle de park modunda olma talebinde bulunabilir. Bu durumda da köle mevcut L2CAP mesajının gönderimini bitirir ve yöneticiye LMP_park_req ı gönderir. Eğer yönetici park moduna giriş talebini kabul ederse; mevcut L2CAP mesajının iletimini sonlandırır ve LMP_park ı geri gönderir. Eğer yönetici park moduna giriş talebini kabul etmezse LMP_not_accepted ı gönderir.

4.3.19 Güç Kontrolü

Güç kontrolü Bluetooth cihazının güç tüketimini ve gürültü seviyesini optimize etmek için iletim gücünü sınırlandırmak için kullanılır. Bir Bluetooth cihazı alınan işaretin gücünü ölçtüğünde, gücün artırılması ya da azaltılması gerektiği yönünde bir rapor verir. Eğer RSSI istenilen değerden çok çok farklıysa, Bluetooth cihazı diğer cihazın iletim gücünü artırmasını ya da azaltmasını isteyebilir.

Güç kontrolü yapabilen cihazlar bir linkteki çıkış gücünü LMP komutları ile optimize ederler. Yönetici tarafında iletim gücü farklı köleler için farklılık gösterir. Bir köleden gelen talep, yöneticinin iletim gücünü sadece o köle için etkiler.

LMP_incr_power_req alıcısı zaten maksimum güçte transferde bulunuyorsa, LMP_max_power geri döndürülür. Cihaz en az bir kere azaltım talebi almışsa, daha sonra tekrar bir artış isteyebilir. Benzer şekilde LMP_decr_power_req alıcısı zaten minimum güçte transferde bulunuyorsa, LMP_min_power geri döndürülür. Cihaz en az bir kere artım talebi almışsa, daha sonra tekrar bir azaltım isteyebilir.

LMP_incr/decr_power_req teki 1 byte gelecekteki kullanımlar için rezerve edilmiştir. Bu byte örneğin istenilen ve ölçülen RSSI değerleri arasındaki farklılığı ifade edebilir. LMP_incr/decr_power_req alıcısı bu byte ı kullanarak doğru güç ayarını yapabilir. Bu parametreye, tanımlanmadığı durumlarda LMP nin tüm versiyonları için belirli bir değer atanır.

4.3.20 Kanal Kalitesi Temelli Veri Hızı Değişimi

Bluetooth cihazları DM veya DH paketlerini kullanmak veya kanal kalitesine göre paket tipini otomatik olarak ayarlamak üzere konfigüre edilmişlerdir. DM ve DH arasındaki fark DM paketindeki taşınan bilginin (payload) Forward Error Correction (FEC) ile korunması, DH paketindeki taşınan bilginin (payload) ise korunmamasıdır. Eğer bir cihaz DM ve DH arasında otomatik olarak bir ayarlama yapmak istiyorsa, diğer cihaza LMP_auto_rate gönderir. Cihaz paket tipini değiştirmek suretiyle net çıkış verimi (throughput) artırılıp artırılmayacağına karar verir. Eğer gerekiyorsa diğer cihaza LMP_preferred_rate gönderir.

4.3.21 Servis Kalitesi (Quality of Service-QoS)

Link Yöneticisi bir yoklama (poll) aralığı boyunca (yöneticiden belirli bir köleye yapılan ve birbirini takip eden iletimler arasındaki maksimum zaman aralığı) belirlenmiş QoS özellikleri sağlar. Tarama aralığı, bant genişliği tahsisi ve gecikme süresi kontrolü için de kullanılır. Tarama aralığı çağrı (page) çakışmaları, çağrı taraması (page scan), sorgulama ve sorgulama taraması dışında garanti edilmiştir. Ek olarak, yönetici ve köle yayın paketlerinin tekrarlama sayısını (N_{BC}) görüşürler.

Bir yönetici bir köleyi yeni bir QoS hakkında bilgilendirebilir. Bu durumda yönetici yeni tarama aralığı ve N_{BC} uyarılarını köleye göndermelidir. Köle uyarıları reddedemez. Alternatif olarak yönetici ve köle dinamik olarak QoS değerini görüşmek için teşebbüste bulunabilirler. Bu durumda her bir cihaz yeni QoS değerini kabul ya da reddedebilir.

4.3.22 SCO Linkleri

İki Bluetooth cihazı arasındaki başlangıç linki bir ACL linkidir. ACL linki bir kez kurulduktan sonra bir veya birden fazla SCO linki kurulabilir. SCO linki SCO aralığı ile ayrılmış olan slotları rezerve eder. SCO linki için ayrılan ilk slot SCO aralığı ve SCO gecikmesi tarafından tanımlanır. Daha sonra SCO slotları SCO aralığını

koruyarak birbirlerini takip ederler. SCO linki kurulması sırasında, yöneticiden gelen mesajda ilk SCO slotunun nasıl hesaplanması gerektiği bilgisini içeren bir bayrak bulunur. Her SCO linki diğer SCO linklerinden SCO tanıtıcısı (handle) yardımıyla ayrılır.

Bir SCO linki kurmak için, yönetici SCO linkinde kullanılacak zamanlama, paket tipi ve kodlama bilgilerini belirten parametreleri içeren bir talep gönderir. Her bir SCO paketi için Bluetooth spesifikasyonu hava arayüzünde kullanılan μ -law PCM, A-law PCM ve CVSD olmak üzere üç farklı ses-kodlama formatı destekler. SCO linkleri için kullanılan slotlar yönetici tarafından kontrol edilen üç parametre ile belirlenir: SCO aralığı, SCO gecikmesi ve ilk SCO slotunun nasıl hesaplanacağına ilişkin bir bayrak. İlk slottan sonra, SCO slotları SCO aralığını koruyarak birbirlerini takip ederler.

Eğer Köle SCO linkini kabul etmez, fakat başka bir muhtemel SCO parametresi setini dikkate almak isterse, LMP_not_accepted in hata sebep alanında neyi kabul etmediğini belirtir. Bunun üzerine yönetici değiştirilmiş parametrelerle yeni bir talepte bulunabilir. Mesajdaki SCO tanıtıcısı (handle) mevcut herhangi bir SCO linkinden farklı olmalıdır.

Köle aynı zamanda LMP_SCO_link_req ile bir SCO linki kurulumunu başlatabilir fakat zamanlama kontrol bayrakları, SCO gecikmesi ve SCO tanıtıcısı (handle) bilgileri geçersiz olur. Eğer yönetici bir SCO linkini kurmaya muktedir değilse, LMP_not_accepted ile cevap verir. Aksi durumda LMP_SCO_link_req mesajını gönderir. Bu mesaj atanan SCO tanıtıcısı (handle), SCO gecikmesi ve zamanlama kontrol bayraklarını içerir. Diğer parametreler için, yönetici, kölenin talebindeki parametreleri kullanmaya çalışır, eğer kullanamazsa başka değerler kullanır. Bunun sonrasında köle LMP_accepted veya LMP_not_accepted ile cevap vermek zorundadır.

Yönetici de köle de bir SCO parametresinin değişmesini talep edebilir. Bu talebi isteyen tarafa bağlı olmaksızın, LMP_SCO_link_req ile başlatılır, SCO tanıtıcısı (handle) da parametreleri değiştirmek isteyen cihazın SCO tanıtıcısıdır (handle). Cihaz yeni parametreleri kabul ederse LMP_accepted ile cevap verir ve SCO linki parametreleri değişir. Cihaz yeni parametreleri kabul etmezse LMP_not_accepted ile cevap verir ve SCO linki parametreleri değişmez. Cihaz LMP_not_accepted ile

cevap verdiğinde hata sebep parametresinde kabul edilmeyen şeyin ne olduğu bilgisi gösterilir. Cihaz daha sonra değiştirilmiş parametrelerle SCO linkini tekrar değiştirmeyi deneyebilir.

Yönetici ya da köle SCO linkini, SCO linkinin SCO tanıtıcısının (handle) kaldırıldığı bilgisini ve kaldırılma sebebini de içeren bir istek göndererek sona erdirebilir. Bu durumda talebi alan cihaz LMP_accepted ile cevap vermek zorundadır.

4.3.23 Çok Slotlu Paketlerin Kontrolü

Bir kölenin geri dönüş paketinde kullanılan slot sayısı sınırlandırılabilir. Yönetici maksimum slot sayısını parametre olarak verdiği LMP_max_slot PDU sunu göndererek kölenin maksimum slot sayısını kullanmasını sağlayabilir. Aynı şekilde her bir köle de slot sayısını parametre olarak verdiği LMP_max_slot_req PDU sunu göndererek maksimum slot sayısını kullanmayı talep edebilir. İlk değer tek slottur. Eğer köle slot sayısı hakkında bilgilendirilmemişse, sadece bir slotlu paketleri kullanacaktır. Çok slotlu paketlerin kontrolünde iki PDU kullanılır.

4.3.24 Çağrı Yapma (Paging) Planı

Tüm Bluetooth cihazları tarafından desteklenen zorunlu çağrı yapma (paging) planına ek olarak Bluetooth spesifikasyonu seçime bağlı olan çağrı yapma (paging) planlarına da izin vermektedir. LMP, bir sonraki sefere çağrılacak (paged) Bluetooth cihazında kullanılacak çağrı (paging) planının görüşülmesini (negotiate) sağlar. Zorunlu ve seçime bağlı çağrı (page) planları arasındaki ana farklılık çağrıyı yapan ünite (pager) tarafından gönderilen çağrı dizisinin (page train) yapısıdır. Çift numaralı yönetici slotlarındaki iletimlere ek olarak, yönetici tek numaralı yönetici slotlarında da iletim yapmaktadır. Seçime bağlı olan yapıda, gönderim yapılırken kullanılan frekans setinin aynısı alım için de kullanılır. Bu durum kölenin tarama penceresini azaltmasına izin verir.

Çağrı (page) modu prosedürü A cihazı tarafından başlatılmıştır. A cihazı, B cihazı A cihazına çağrı (page) yaparken kullandığı çağrı (page) yapısını görüşür (negotiate). A cihazı, yapı için gereken parametreleri de içeren bir çağrı (page) yapısı talep eder. B cihazı bu talebi kabul veya reddedebilir. Talebin reddi durumunda, eski ayarlar değişmez. Zorunlu yapıya geri dönmeyi talep eden talep de reddedilir.

Çağrı tarama (page scan) prosedürü A cihazı tarafından başlatılmıştır. A cihazı B cihazına çağrı (page) yaparken kullandığı çağrı (page) yapısını görüşür (negotiate). A cihazı, yapı için gereken parametreleri de içeren bir çağrı (page) yapısı talep eder. B cihazı bu talebi kabul veya reddedebilir. Talebin reddi durumunda, eski ayarlar değişmez. Fakat zorunlu yapıya geri dönmeyi talep eden talep mutlaka kabul edilmelidir.

4.3.25 Link Denetimi

Her Bluetooth cihazı link denetimi için bir zamanlayıcı kullanmaktadır. Bu zorunlu özellik cihazların kapsam dışına çıkmaları, güçlerinin sonlanması ve başka sebepli hatalardan dolayı linkin kaybolmasını anlamak için kullanılmaktadır. Bir LMP prosedürü denetim zaman aşımı süresini ayarlamak için kullanılır. Bu iş için kullanılan PDU LMP_supervision_timeout dur.

4.3.26 Bağlantı Kurulumu

Çağrı (page) prosedüründen sonra, yönetici mutlaka maksimum tarama aralığı ile birlikte POLL veya NULL paketlerini göndererek köleyi taramalıdır. Böylelikle çağrı yapılan (paged) tarafta LM ile sunucu arasında herhangi bir etkileşime gerek duymayan LMP prosedürleri yerine getirilebilir.

Çağrı yapan cihaz Link Kontrolörü (LM) nün üzerindeki katmanları içeren bir bağlantı kurmak istiyorsa, LMP_host_connection_req PDU sunu gönderir. Diğer taraf mesajı aldığı anda, sunucu gelen bağlantıdan haberdar edilir. Uzak noktadaki cihaz LMP_accepted veya LMP_not_accepted göndererek bu talebi kabul veya reddedebilir. Bir cihaz daha fazla link kurulum prosedürü istemezse LMP_setup_complete mesajını gönderir. Bu durumda diğer cihazdan gelen taleplere halen cevap verebilir. Diğer cihaz da link kurulumu ile hazır olduğunda LMP_setup_complete gönderir. Bu aşamadan sonra kanalda LMP den farklı olan ilk paket gönderilebilir.

4.3.27 Test Modları

Daha önce açıklanan 55 PDU ya ek olarak, Bluetooth radyo ve temelbant cihazlarının sertifikasyon ve uygunluk testleri gibi farklı Bluetooth test modlarını desteklemek için LMP nin kullandığı PDU lar vardır. Bu fonksiyonlar Bluetooth cihazlarını kullanan son kullanıcılar tarafından görülmezler. Test modları gönderici

(transmitter) testlerini (sabit bit paternli paketler) ve loop back testlerini içerir. Test modundayken, cihaz normal çalışma şeklini korumaz. Bluetooth cihazı test modunda değilken, test için kullanılan kontrol ve konfigürasyon komutları reddedilir. LMP_not_accepted geri döndürülür.

Test modu test edilecek cihaza (her zaman köledir) LMP_test_activate gönderilerek aktif edilir. Link Yöneticisi bu mesajı her zaman alabilmelidir. Eğer cihazın test moduna girmesi lokal olarak mümkün kılınmışsa, LMP_accepted ile cevap verilir ve test moduna girilmiş olunur. Aksi takdirde LMP_not_accepted ile cevap verilir ve normal çalışma şekli devam eder. Bu durumda LMP_not_accepted da gönderilen sebep kodu “PDU izni yok” dur.

Test modu iki şekilde pasifize edilebilir. Birinci yöntemde “test modundan çıkış” test senaryosu ile LMP_test_control gönderilerek test modu sonlandırılır, köle normal çalışma şekline geri döner fakat halen yöneticiye bağlıdır. İkinci yöntemde ise test modundaki cihaza LMP_detach gönderilerek hem test modu hem de yönetici ile olan bağlantı bitirilmiş olur.

Bir cihaz test moduna girdiğinde, LMP_test_control gönderilerek daha spesifik bir teste başlaması sağlanabilir. Bu PDU nun alındığı bilgisi LMP_accepted ile alınır. Test modunda olmayan bir cihaz bu mesajı alırsa sebep kodu “PDU izni yok” olan bir LMP_not_accepted gönderir.

4.3.28 Hatanın İşlenişi

Link Yöneticisi tanınmayan operasyon kodlu bir PDU alması durumunda, “bilinmeyen LMP PDU” sebep kodlu bir LMP_not_accepted gönderir. Tekrarlanan op kodu parametresi tanınmayan op kodudur. Eğer Link Yöneticisi geçersiz parametreleri içeren bir PDU alırsa, “geçersiz LMP parametreleri” sebep kodlu bir LMP_not_accepted gönderir. Eğer maksimum cevap süresi aşılmış ya da linkin kaybolduğu belirlenmişse; cevap bekleyen taraf, prosedürün başarısız olup sonlandığına karar verir.

Hatalı LMP mesajları kanaldaki hatalardan ya da gönderen taraftaki sistematik hatalardan kaynaklanır. İkinci durumu belirleyebilmek için, LM hatalı mesajların sayısını monitör eder ve bu sayı bir eşik değerini aşmışsa bağlantıyı keser. LMP PDU ları gerçek zamanlı olarak işlenmedikleri için çakışma durumları iki LM de aynı prosedürü başlattığında ve her ikisi de tamamlanamadığında meydana gelebilir.

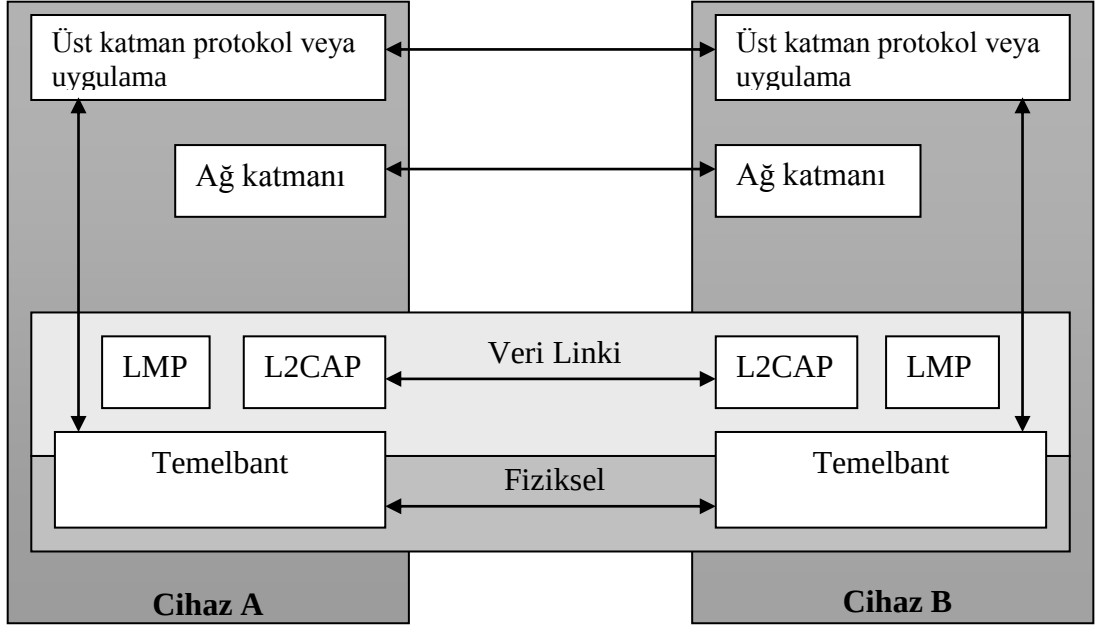
Bu durumda, yönetici, kölenin başlattığı prosedürü “LMP Hatası Hareket (Transaction) Çakışması” sebep kodlu bir LMP_not_accepted göndererek reddeder. Yöneticinin başlattığı prosedür daha sonra tamamlanır.

4.3.29 Özet

Link Yönetim Protokolü iki Bluetooth cihazı birbirlerinin etki alanına girdiklerinde Link Yöneticileri arasında noktadan noktaya haberleşme sağlanmasını sağlar. Diğer cihazın varlığını keşfeden kısım cihazdaki Link Yöneticisi dir. Link Yöneticileri arasındaki gerçek haberleşme Link Yönetim Protokolü üzerinden alınıp gönderilen değişik mesajlarla (PDU) sağlanır. Link kurulumu, doğrulama ve şifreleme gibi güvenlik mekanizmaları, temelbant paket boyutlarının kontrol ve görüşmeleri gibi değişik fonksiyonlar için kullanılan 55 tip PDU (ek 2 adet de Bluetooth radyo ve temelbant sertifikasyon ve uygunluk testleri için vardır) bulunmaktadır. LMP, bu mesaj iletimleri ile güç modlarını, Bluetooth radyo cihazlarının görev devrini ve bir pikonetteki Bluetooth birimlerinin bağlantı durumlarını kontrol eder. Bu mesajlara cevap olarak hangi fonksiyonun yerine getirildiğine bağlı olmaksızın, alıcı taraftaki Link Yöneticisi tarafından filtrelenerek yorumlanır ve daha üst katmanlara gönderilmez

4.4 Lojik Link Kontrolü ve Adaptasyon Protokolü (L2CAP)

Bluetooth spesifikasyonu, üst seviye protokol çoğullama, paket ayrıştırılması ve tekrar birleştirilmesi (SAR) özelliklerini sağlayan L2CAP protokolünü içerir. L2CAP ayrıca Bluetooth uç noktaları arasında QoS bilgisini de iletir. Bir önceki bölümde açıklanan Link Yönetim Protokolüne benzer şekilde L2CAP, temelbant protokolünün üzerinde yer almakta ve OSI referans modelinin veri link katmanı ile aynı yerde bulunmaktadır.

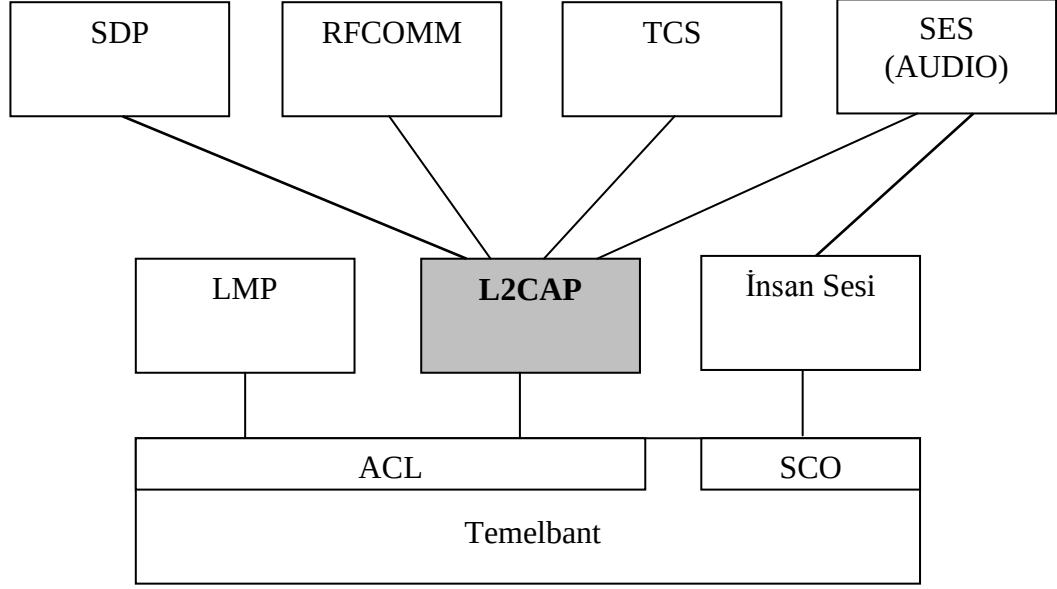


Şekil 4.25 L2CAP in Bluetooth protokol mimarisindeki yeri

L2CAP daha üst seviyedeki protokol ve uygulamaların maksimum 64 kilobyte uzunluğundaki L2CAP veri paketlerini alıp göndermelerine izin verir. Bluetooth'un temelbant spesifikasyonu SCO ve ACL olmak üzere iki çeşit link tipini tanımlarken, L2CAP spesifikasyonu sadece ACL linkleri için tanımlanmıştır. İki Bluetooth cihazı arasında birden fazla ACL linki bulunamaz. L2CAP, ACL linki üzerinden iletilen bilgiyi korumak için temelbant katmanındaki doğruluk kontrolüne itimat eder. SCO linkleri için herhangi bir destek planlanmamaktadır.

L2CAP, SDP, RFCOMM ve Telefon Kontrol Spesifikasyonu gibi diğer protokoller ile haberleşir (Şekil 4.26). Ses ve telefon uygulamalarında kullanılan ses-kalite kanalları genellikle temelbant SCO linkleri üzerinde çalışırken IP telefonu gibi paketlenmiş ses verileri de L2CAP üzerinde koşan haberleşme protokolleri kullanılarak gönderilir.

L2CAP in basitlik ve düşük ek yük (overhead) gibi karakteristikleri avuç içi bilgisayarlar, PDA'ler, mobil telefonlar, kablosuz kulaklık-mikrofon setleri ve Bluetooth teknolojisini destekleyen diğer cihazlar gibi düşük işlemcili ve hafızalı cihazlar üzerinde yazılım geliştirmeye imkan tanır. Protokolün düşük ek yük (overhead) özelliği ile çok fazla güç tüketmeden yüksek bant genişlik verimi sağlanmış olur.



Şekil 4.26 L2CAP in Bluetooth protokol mimarisindeki diğer protokollerle ilişkisi

4.4.1 L2CAP Fonksiyonları

L2CAP katmanında gerçekleşen fonksiyonlardan birisi protokol çoğullamadır. L2CAP bu özelliği desteklemek zorundadır çünkü temelbant protokolü üst katmanlarda çoğullanacak protokolleri tanımlayacak bir “tıp” alanını desteklemez. Bu sebeple L2CAP SDP, RFCOMM ve TCS gibi üst katman protokollerini ayırt etmek zorundadır.

L2CAP katmanında gerçekleştirilen diğer bir fonksiyon da ayrıştırma ve tekrar birleştirmedir. Bu işlemler temelbant tarafından desteklenen paketlerden daha büyüklerini kullanan protokolleri desteklemek için gereklidir. Kablolu dünyadaki fiziksel medya ile karşılaştırılacak olursa Bluetooth temelbant protokolü ile birleşmede kullanılan veri paketleri boyut açısından sınırlandırılmıştır. En büyük temelbant taşınan bilgisi (payload) (yüksek hızlı veri paketleri için 341 byte) ile ilişkili olan bir maksimum transfer ünitesi (MTU) göndermek, daha büyük paketleri kullanmak üzere tasarlanmış üst katman protokolleri için bant genişliğini kullanım verimliliğini sınırlar. Büyük L2CAP paketleri kablosuz olarak iletilmeden önce birçok küçük temelbant paketine ayrıştırılmalıdır. Alıcı tarafta da alınan küçük temelbant paketleri basit bir doğruluk testinden sonra tekrar tek ve büyük bir L2CAP paketine dönüştürülmelidir.

L2CAP bağlantısı kurulum süreci iki Bluetooth cihazı arasında beklenen QoS ile ilgili bilginin iletimine de izin verir. Her uçtaki L2CAP uygulamaları protokol

tarafından kullanılan kaynakları monitör ederek QoS gereksinimlerinin yerine getirilip getirilmediğini kontrol eder.

Birçok protokol, adres grupları kavramı içerir. Temelbant protokolü aynı saate göre birlikte çalışan maksimum sekiz cihazdan oluşan bir pikonetin adresini destekler. L2CAP grup kavramı pikonetler üzerine protokol gruplarının eşleşmesini (mapping) verimli yapmayı sağlayacak uygulamalara izin verir.

4.4.2 Temel Çalışma

İki Bluetooth cihazı arasındaki ACL linki, Link Yönetim Protokolü (LMP) kullanılarak kurulur. Temelbant, veri paketlerini ara sıra meydana gelen çakışma ve duplike olma sorunlarına rağmen düzenli olarak dağıtır. Temelbant ayrıca tam dupleks haberleşme kanalları sağlar. L2CAP haberleşmelerinin tamamı iki yönlü olmak zorunda değildir. Örneğin video gibi tek yönlü bir haberleşmede dupleks değil tek yönlü kanallara ihtiyaç duyulur.

L2CAP, temelbant katmanında bulunan mekanizmaları kullanarak güvenli bir kanal sağlar. Güvenlik, talep edildiği zaman yapılan veri doğruluk testleri ve başarılı olarak transfer edildiği bilgisi alınana kadar ya da zaman aşımı oluştuğunda tekrar transfer edilerek sağlanır. Alındı bilgileri de kaybolabilir, zaman aşımaları da veri başarılı olarak iletilmiş olsa bile oluşabilir. Temelbant protokolü duplike paketleri ortadan kaldıran 1-bitli bir sıra numarası kullanır. Güvenlik isteniyorsa yayın (broadcast) paketlere izin verilmez çünkü tüm yayın paketleri L2CAP paketinin ilk segmenti ile ve aynı sıra numarası ile başlar.

L2CAP in fonksiyonları dışında kalan bazı durumlar da söz konusudur:

- SCO linkleri için tasarlanmış ses verisi taşımaz.
- Güvenli bir kanal veya veri doğruluğunun sağlanması gibi fonksiyonları yoktur. L2CAP tekrar iletim veya checksum hesaplaması yapmaz.
- Güvenli çoklu (multicast) bir kanal sağlamaz.
- Global grup adı kavramını desteklemez.

4.4.2.1 Kanal Tanımlayıcıları

L2CAP kanal kavramı üzerine kurulmuştur. Bir L2CAP kanalının her bir sonlanma ucunun bir kanal tanımlayıcısı (CID) vardır. Bazı tanımlayıcılar işaretleşme ve bağlantısız veri trafiği gibi özel bazı L2CAP fonksiyonları için rezerve edilmiştir.

Rezerve edilen kanallar dışında, aynı CID lokal ve uzak cihazlar arasındaki çoklu L2CAP kanalları için lokal bir L2CAP kanalının sonlanma noktalarından biri olarak kullanılamaz prensibine dayanan bir yönetim mekanizması kullanılır.

Şekil 4.27 de değişik cihazlardaki L2CAP ler arasında CID lerin kullanımı gösterilmiştir. Bağlantı yönelimli veri kanalları CID lerin kanalın her bir sonlanma noktasını tanımladığı iki cihaz arasındaki bağlantıyı temsil eder. Bağlantısız kanallar veri akışını tek yönde sınırlar. Bu kanallar kaynak CID inin bir veya birden fazla cihazı temsil ettiği bir kanal grubunu desteklemek için kullanılır.

Bir L2CAP içinde işaretleşme kanalı desteği mutlaka olmalıdır. Diğer bir CID bütün gelen bağlantısız veri trafiği için rezerve edilmiştir. Şekilde bir CID C ve D cihazlarından oluşan grubu temsil etmek üzere kullanılmaktadır. Bu kanal ID sinden gönderilen trafik bağlantısız veri trafiği için rezerve edilmiş olan uzak kanala yönlendirilir.

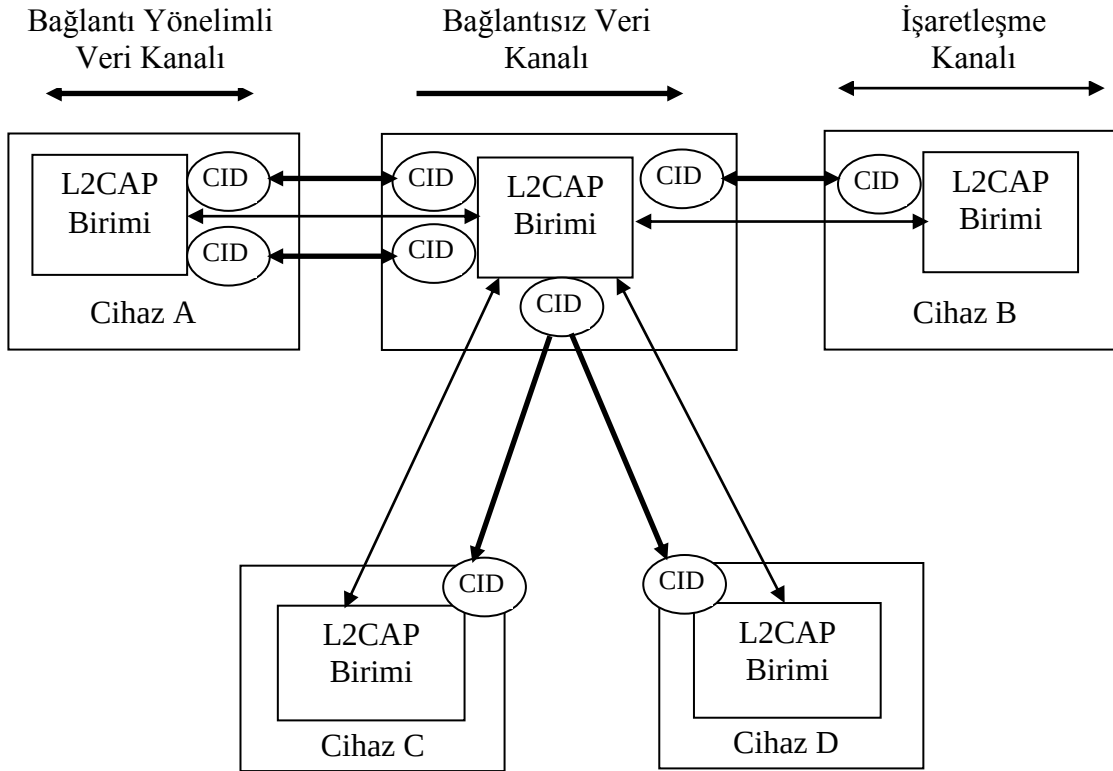
4.4.2.2 Ayırıştırma ve Tekrar Birleştirme

Ayırıştırma ve tekrar birleştirme (SAR) en büyük temelbant paketinden daha büyük boyuttaki MTU desteği sağlamak ve böylelikle verimliliği arttırmak için kullanılır. Tüm L2CAP paketleri temelbant paketleri üzerinde iletilmek üzere ayrıştırılırlar. Protokol herhangi bir ayırıştırma ve tekrar birleştirme işlemi yapmaz fakat paket formatı daha küçük fiziksel çerçeve boyutuna adaptasyonu destekler. Bir L2CAP uygulaması giden MTU yu gösterir (expose) ve üst katman paketlerini HCI üzerinden Link Yöneticisine aktaracak şekilde daha küçük parçalara ayırır. Alıcı tarafta, L2CAP uygulaması HCI'dan ayrıştırılmış paketleri alır ve HCI ile paket başlığından aldığı bilgiyi kullanarak paketleri tekrar birleştirir.

Ayırıştırma

L2CAP MTU uygulama-özel bir servis arayüzü ile gönderilir. L2CAP katmanına gönderilen paketlerin boyutunu MTU limitinin altında olan bir boyutta sınırlandırmak üst katman protokolünün sorumluluğundadır. Bir L2CAP uygulaması

paketi PDU lara böler ve alt katmana gönderir. Eğer L2CAP direk olarak temelbant ın üzerinde çalışıyorsa, bir uygulama paketi kablosuz haberleşme için paketi ayrıştırır. Eğer L2CAP tipik olarak HCI nın üzerinde çalışıyorsa bir uygulama boyutları sınırlandırılmış paketleri temelbant paketlerine dönüştürülecekleri host kontrolörüne gönderir. Bir L2CAP paketi ile ilişkilendirilen tüm L2CAP paket parçaları, aynı Bluetooth cihazını hedefleyen başka L2CAP paketleri gönderilmeden önce mutlaka temelbanttan geçirilmelidir.



Şekil 4.27 Cihazlar arasında L2CAP tarafından belirlenen kanallar

Tekrar Birleştirme

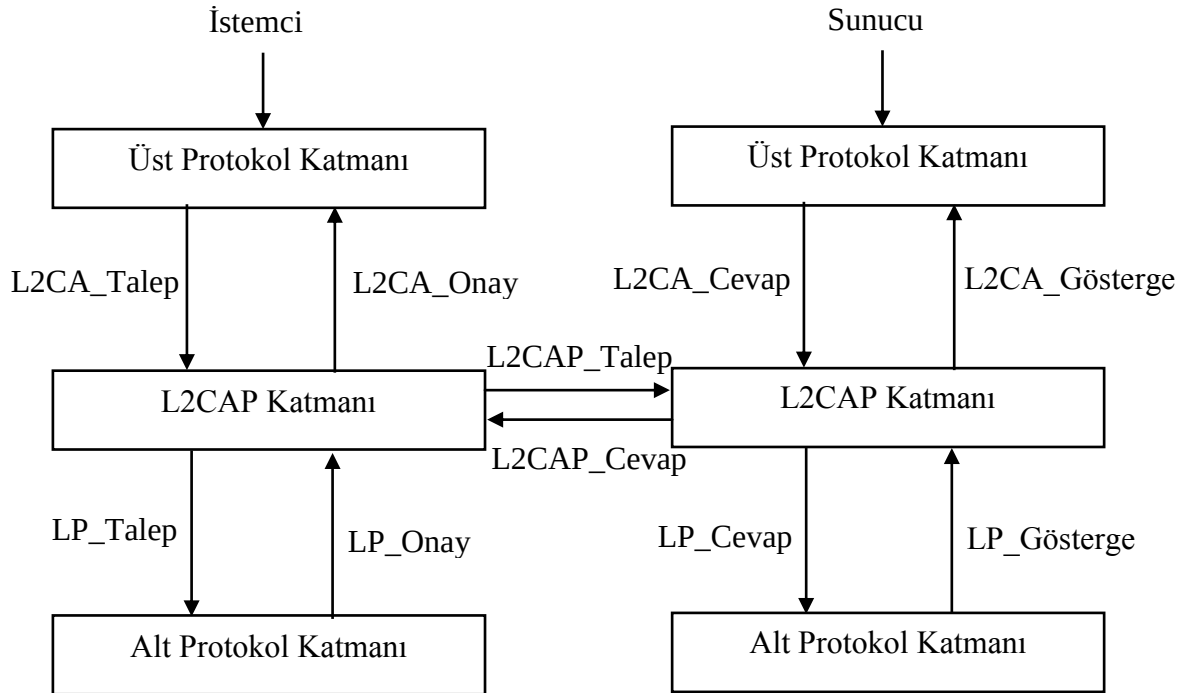
Temelbant protokolleri ACL paketlerini sıralı olarak dağıtır ve 16-bitli CRC kullanarak veri bütünlüğünü korur. Temelbant ayrıca bir ARQ kullanarak da güvenli bağlantı sağlar. Temelbant kontrolörü ACL paketlerini alırken, ya her temelbant paketi gelişinde L2CAP katmanına işaret verir ya da L2CAP katmanına işaret vermeden önce alıcı ara belleği dolmadan veya belirli bir zaman dolmadan bir miktar paket biriktirir.

L2CAP uygulamaları tutarlık kontrolü için L2CAP paketlerinin başlık bilgisindeki uzunluk alanını kullanırlar ve uzunluk alanı birbirini tutmayan paketleri atarlar. Eğer

kanal güvenliği istenmiyorsa uygun olmayan uzunluktaki paketler atılırlar. Eğer kanal güvenliği isteniyorsa L2CAP uygulamaları kanalın güvensiz olduğu konusunda üst katmanı uyarmalıdır. Güvenli kanallar düzgün bir zaman aşım değeri olan kanallar olarak tanımlanırlar.

4.4.3 Durum Makinesi

L2CAP bağlantı yönelimli kanalı farklı katmanlar arasındaki etkileşimler esnasında farklı durumlar olduğunu varsayar. Bluetooth spesifikasyonuna göre bu “durum makinesi” sadece iki yönlü CID lere uygulanabilir ve işaretleme kanalı ya da tek yönlü kanallar için kullanılmaz. Şekil 4.28 de bir L2CAP katmanı uygulaması tarafından gerçekleştirilen konu ve olaylar gösterilmektedir.



Şekil 4.28 L2CAP etkileşimleri

İstemciler talebi başlatırken, sunucular talepleri kabul ederler. Bir uygulama katmanı istemcisi talepleri hem başlatır, hem de kabul eder. Bu süreç, iki katman (dikey arayüz) arasında örneğin L2CA gibi üst katmana servis teklifinde bulunan bir alt katmanın prefix ini kullanan bir arayüz gerektirir. Aynı seviyedeki iki birim arasındaki arayüz (yatay arayüz) protokol prefix ini kullanır, “P” harfini katman

kimliğine ekler ve böylelikle L2CA L2CAP olur. Yukarıdan gelen olaylar Talep (Request=Req), bunlara karşılık gelen cevaplar ise Konfirmasyon (Cfm) olarak; aşağıdan gelen olaylar Gösterge (Ind), bunlara karşılık gelen cevaplar ise Cevap (Rsp) olarak adlandırılırlar.

Ek bir işlem gerektiren Cevap lara Askıda (Pnd) adı verilir. Konfirmasyon ve Cevaplar için olan notasyonlar pozitif olarak kabul edilirler. Negatif cevaplar L2CAP_ConnectCfmNeg de olduğu gibi “Neg” son ekini içerirler. Bir eylem için olan Talep ler her zaman buna karşılık gelen bir Konfirmasyon ile sonuçlanırken Gösterge ler her zaman Cevap alamazlar. Bu durum özellikle Gösterge ler yerel olarak tetiklenmiş olaylar hakkında bilgi taşıyorlarsa geçerlidir.

Şekil 4.29 daki mesaj sıralaması olayların normal sıralamasını betimlemektedir. Dış taraftaki iki dikey çizgi başlangıcı yapan ve başlangıcı yapan cihaza cevap veren cihazların L2CA arayüzlerini temsil etmektedir. L2CA arayüzündeki talep komutları, protokol tarafından tanımlanan Talep lerde sonuçlanır. Protokol, cevap veren tarafa talebi ilettiği zaman; uzak L2CA cihazı üst protokolü bir Gösterge ile sunar. Cevap veren tarafın üst protokolü cevap verdiğinde, cevap protokol tarafından paketlenir ve başlangıcı yapan tarafa geri gönderilir. Sonuç ise bir Konfirmasyon mesajı ile başlangıcı yapan tarafın üst protokolüne gönderilir.

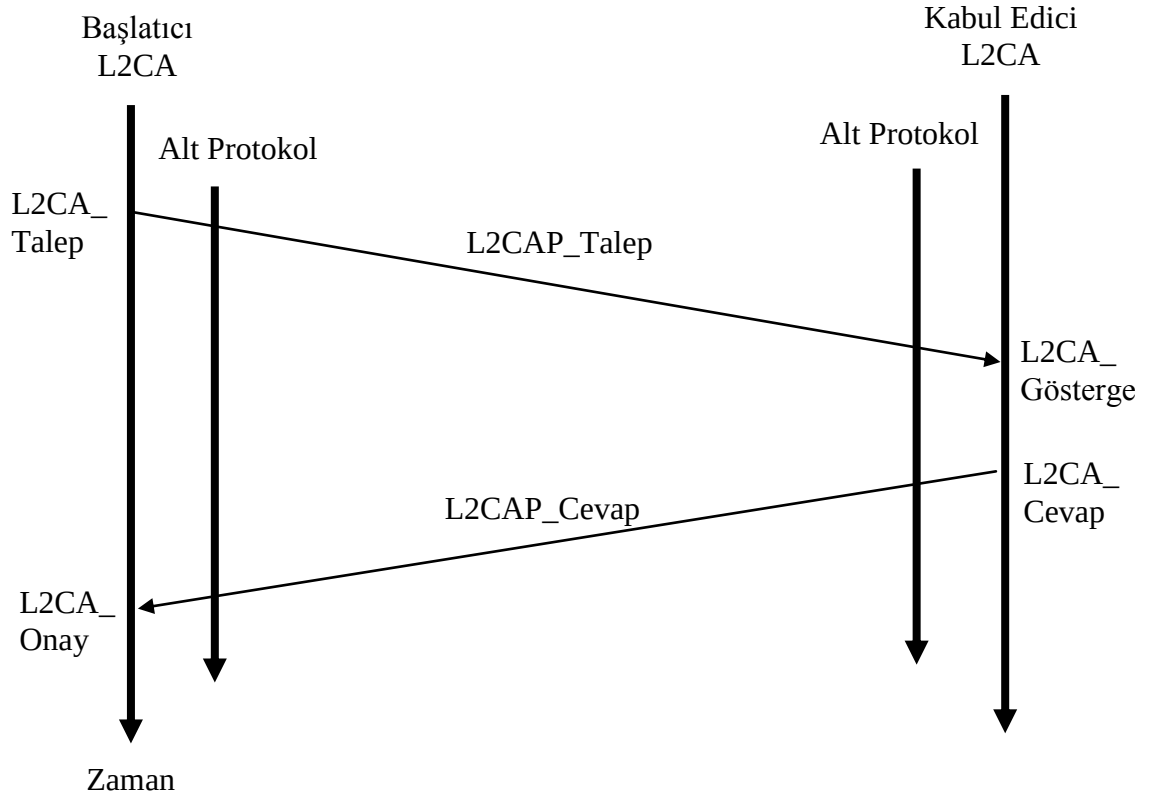
4.4.3.1 Olaylar

Olaylar, L2CA katmanına herhangi bir zaman aşımı ile birlikte gelen mesajlardır. Olaylar alt katmanlardan Gösterge ve Konfirmasyon, üst katmanlardan Talep ve Cevap, eşdeğer katmanlardan veri, işaret Talep ve Cevap ları ve zaman aşımları sebebiyle oluşan olaylar şeklinde kategorize edilmişlerdir.

Alt Katman’dan L2CAP’e Olaylar

Aşağıda Bluetooth spesifikasyonu tarafından tanımlanan ve alt katman protokolleri (örneğin temelbant) ile L2CAP arasında bağlantı kurulum aşamasında iletilen mesajlar sıralanmıştır:

LP_ConnectCfm: Alt katman bağlantısı kurma talebini konfirme eder. Fiziksel link kurulması için doğrulama istenmişse bu prosesin geçilmesini de içerir.



Şekil 4.29 Farklı katmanların etkileşimini gösteren mesaj dizisi planı

LP_ConnectCfmNeg: Alt katman bağlantısı kurma talebinin başarısız oluşunu konfirme eder. Bu durum cihaz ile bağlantı kurulamıyorsa, talep reddedilmişse ya da LMP doğrulaması başarısız olmuşsa görülür.

LMP_ConnectInd: Alt katman protokolünün bağlantıyı başarılı olarak yaptığını işaret eder. Temelbant durumunda kurulan bağlantı bir ACL linkidir. Bir L2CAP varlığı bu bilgiyi fiziksel linklerin takibini korumak için kullanır.

LP_DisconnectInd: Alt katman protokolünün LMP komutları ya da bir zaman aşımı olayı ile kapatıldığını gösterir.

LP_QoSfm: Bir servis kalitesi için talebi konfirme eder.

LP_QoSfmNeg: Bir servis kalitesi için talebin başarısız olduğunu konfirme eder.

LP_QoSViolationInd: Alt katman protokolünün bir önceki LP_QosReq de belirtilen QoS anlaşmasının ihlal edildiğini gösterir.

L2CAP'ten L2CAP'e İşaretleşme Olayları

L2CAP'ten L2CAP'e işaretleşme olayları uygun L2CAP işaretleşme PDU larının iletimini takiben her bir L2CAP varlığı tarafından meydana getirilirler. L2CAP işaretleşme PDU ları da diğer L2CAP PDU ları gibi bir alt katmandan bir alt protokol gösterge olayı üzerinden alınırlar. Bluetooth spesifikasyonuna göre aşağıdaki mesajlar L2CAP birimleri arasında iletilmektedir:

L2CAP_ConnectReq: Bir bağlantı talebi paketi alınmıştır.

L2CAP_ConnectRsp: Bağlantının kurulduğuna işaret eden olumlu sonuç içeren bir bağlantı cevap paketi alınmıştır.

L2CAP_ConnectRspPnd: Uzak uç noktanın talebi aldığını ve proses etmekte olduğuna işaret eden bir bağlantı cevap paketi alınmıştır.

L2CAP_ConnectRspNeg: Bağlantının kurulamayacağını gösteren bir bağlantı cevap paketi alınmıştır.

L2CAP_ConfigReq: Uzak uç noktanın kanal parametreleri üzerinde anlaşmaya varmak istediğini gösteren bir konfigürasyon cevap paketi alınmıştır.

L2CAP_ConfigRsp: Uzak uç noktanın görüşülen tüm kanal parametrelerini kabul ettiğini gösteren bir konfigürasyon cevap paketi alınmıştır.

L2CAP_ConfigRspNeg: Uzak uç noktanın alınan cevap paketindeki parametreleri kabul etmediğini gösteren bir konfigürasyon cevap paketi alınmıştır.

L2CAP_DisconnectReq: Kanalin bağlantıyı sona erdirmeye prosesini başlatması gerektiğini gösteren bir bağlantıyı sona erdirmeye talep paketi alınmıştır. L2CAP kanal bağlantısının sona erdirilmesinin ardından, L2CAP varlığı lokal CID ini atanmamış CID havuzuna geri gönderir.

L2CAP_DisconnectRsp: Bir bağlantıyı sona erdirmeye cevap paketi alınmıştır. Bu işaretin alınmasından sonra, cevabı alan L2CAP varlığı lokal CID ini atanmamış CID havuzuna geri gönderir. Uygun gelen bir negatif cevap yoktur çünkü bağlantıyı sona erdirmeye prosesi mutlaka gerçekleştirilmelidir.

L2CAP'ten L2CAP'e Veri Olayları

L2CAP birimleri arasında iletilen ve bir veri paketinin alındığını gösteren tek bir mesaj vardır ve bu mesaj L2CAP_Data dır.

Üst Katman'dan L2CAP'e Olaylar

Aşağıda Bluetooth spesifikasyonu tarafından tanımlanan ve üst katman protokolleri ile L2CAP arasında bağlantı kurulum aşamasında iletilen mesajlar sıralanmıştır:

L2CA_ConnectReq: Uzak bir cihaza kanal oluşturulması için üst katmandan gelen bir taleptir.

L2CA_ConnectRsp: Bir üst katmandan uzak bir cihazdan gelen bağlantı talebini gösteren bir cevap alınmıştır.

L2CA_ConnectRspNeg: Bir üst katmandan uzak bir cihazdan gelen bağlantı talebinin reddedildiğini gösteren bir cevap alınmıştır.

L2CA_ConfigReq: Bir üst katmandan kanalı tekrar konfigüre etme talebi gelmiştir.

L2CA_ConfigRsp: Bir üst katmandan kanalı tekrar konfigüre etme talebine istinaden cevap gelmiştir.

L2CA_ConfigRspNeg: Bir üst katmandan kanalı tekrar konfigüre etme talebine istinaden olumsuz cevap gelmiştir.

L2CA_DisconnectReq: Bir üst katmandan kanal bağlantısının acilen sonlanmasına ilişkin bir talep gelmiştir.

L2CA_DisconnectRsp: Bir üst katmandan bağlantının sonlanmasına ilişkin cevap gelmiştir. Uygun gelen bir negatif cevap yoktur çünkü bağlantıyı sona erdirme talebi her zaman kabul edilmelidir.

L2CA_DataRead: Bir üst katmandan L2CAP varlığından alınan verinin üst katmana iletimi isteği gelmiştir.

L2CA_DataWrite: Bir üst katmandan açık olan bir kanal üzerinden iletim yapmak üzere üst katmandan L2CAP varlığına veri iletimi isteği gelmiştir.

Zamanlayıcı Olayları

Aşağıda Bluetooth spesifikasyonu tarafından tanımlanan ve kanal sona erdiriliş prosesi aşamasında sonlanma noktaları arasında iletilen zamanlayıcı mesajları sıralanmıştır:

Response Timeout eXpired (RTX): Uzak sonlanma noktasının işaretleşme taleplerine tepki vermediği durumda kanalı sona erdirmekte kullanılır. Bu zamanlayıcı uzak cihaza bir işaretleşme talebi gönderildiğinde başlar ve cevap

alındığında sona erer. Eğer ilk zamanlayıcı zaman aşımına uğrarsa, ikinci bir talep mesajı gönderilir ya da talepte belirtilen kanaldan kopulur. İkinci bir talep mesajı gönderilirse, RTX zaman aşımı değeri bir öncekinin en az iki katı olacak şekilde yeni bir değere ayarlanır. Uygulamalar kanalı sona erdirmeden önce L2CAP katmanında gösterilecek maksimum talep tekrarı adedini belirlemek durumundadır. Bu karar işaretleşme linkinin temizleme (flush) zaman aşımına bağlıdır. Temizleme (flush) zaman aşımı değeri uzadıkça fiziksel katmanda daha fazla tekrar iletim yapılarak kanal güvenliği artırılmış olur. Böylelikle L2CAP katmanında daha az tekrar iletime gerek olur.

Extended Response Timeout eXpired (ERTX): Uzak sonlanma noktasının başka bir talep işaretini proses ettiğinden şüphe duyulduğunda RTX zamanlayıcısının yerine kullanılır. Bu zamanlayıcı uzak sonlanma noktası bir talebi beklettiğine dair cevap döndüğünde (L2CAP_ConnectRspPnd olayı alındığında) başlar, resmi cevap alındığında veya fiziksel link sonlandığında sona erer. Eğer ilk zamanlayıcı zaman aşımına uğrarsa, ikinci bir talep mesajı gönderilir ya da talepte belirtilen kanaldan kopulur. İkinci bir talep mesajı gönderilirse, özel ERTX zamanlayıcısı kaybolarak yeni bir RTX zamanlayıcı atanır. Tüm zamanlama prosedürü yukarıda RTX zamanlayıcısında anlatıldığı gibi tekrar başlar.

4.4.3.2 Hareketler

Hareketler, üst katmanlara Gösterge ve Konfirmasyon, alt katmanlara Talep ve Cevap, eşdeğer katmanlara Talep, Cevap ve veri iletimi ile zamanlayıcı ayarlamaları şeklinde kategorize edilmişlerdir.

L2CAP'ten Alt Katmana Hareketler:

Aşağıda Bluetooth spesifikasyonu tarafından tanımlanan ve alt katman protokolleri (örneğin temelbant gibi) ile L2CAP arasında bağlantı kurulum aşamasında iletilen mesajlar sıralanmıştır:

LP_ConnectReq: L2CAP, alt protokolün bir bağlantı yapmasını istemektedir. Eğer uzak cihaz ile fiziksel bir link kurulmamışsa, bu mesaj alt protokole fiziksel linki kurması için gönderilir. İki cihaz arasında birden fazla ACL linki kurulamayacağı için, bu iki cihaz arasındaki diğer L2CAP kanalları aynı temelbant ACL linkini paylaşmak durumundadır. Talebin proses edilmesinden sonra, alt katman LP_ConnectCfm ya da LP_ConnectCfmNeg cevabını verir.

LP_QoSReq: L2CAP, alt protokolün belirli bir QoS parametresi sağlamasını talep eder. Talep proses edildikten sonra alt katman LP_QoSReq ya da LP_QoSReqNeg cevabını verir.

LP_ConnectRsp: Bir önceki bağlantı gösterge talebinin kabul edildiğine ilişkin olumlu cevaptır.

LP_ConnectRspNeg: Bir önceki bağlantı gösterge talebinin reddedildiğine ilişkin olumsuz cevaptır.

L2CAP’ten L2CAP’e İşaretleşme Hareketleri

Bu hareketler mesajların alımı yerine gönderimi yapıldığı kabulü ile yukarıda “L2CAP’ten Alt Katman’a Hareketler” bölümünde incelenen hareketler ile aynıdır.

L2CAP’ten L2CAP’e Veri Hareketleri

Bu hareket “L2CAP’ten L2CAP’e Veri Olayları”nın karşısıdır. Yalnız hareket kavramı veri alımı yerine veri gönderimi anlamındadır.

L2CAP’ten Üst Katman’a Hareketler

Aşağıda Bluetooth spesifikasyonu tarafından tanımlanan ve üst katman protokolü ile L2CAP arasında bağlantı kurulum aşamasında iletilen mesajlar sıralanmıştır:

L2CA_ConnectInd: Uzak bir cihazdan alınan bağlantı talebini gösterir.

L2CA_ConnectCfm: Uzak bir cihazdan alınan bağlantı talebinden sonra bu talebin kabul edildiğini gösterir.

L2CA_ConnectCfmNeg: Bir bağlantı talebinin negatif konfirmasyonu (başarısızlığı) dır. (Önceden kalan bir bağlantı talebi için olan bir RTX zamanlayıcısının zaman aşımı da bu harekete neden olabilir.)

L2CA_ConnectPnd: Uzak cihazdan alınan bekleyen bir bağlantı cevabını gösterir.

L2CA_ConfigInd: Uzak bir cihazdan alınan konfigürasyon talebini gösterir.

L2CA_ConfigCfm: Uzak bir cihazdan alınan konfigürasyon talebinden sonra bu talebin kabul edildiğini gösterir.

L2CA_ConfigCfmNeg: Bir konfigürasyon talebinin negatif konfirmasyonu (başarısızlığı) dır. (Önceden kalan bir bağlantı talebi için olan bir RTX zamanlayıcısının zaman aşımı da bu harekete neden olabilir.)

L2CA_DisconnectInd: Uzak bir cihazdan alınan bağlantı sonlanma talebini ya da uzak cihaz bir işaretleşme talebine cevap veremediği için bağlantının sonlandığını gösterir.

L2CA_DisconnectCfm: Uzak bir cihazdan bağlantı sonlanma cevabı alınmasından sonra diğer uzak cihazın bu talebi proses ettiğini gösterir. Önceden kalan bir bağlantı sonlanma talebi için olan bir RTX zamanlayıcısının zaman aşımı da bu harekete neden olabilir. Bu hareketin alınması üzerine, üst katman L2CAP kanalının sonlandığını bilir. Dolayısıyla negatif bir konfirmasyon yoktur.

L2CA_TimeOutInd: Bir RTX ya da ERTX zamanlayıcısının zaman aşımına uğradığını gösterir. Bu gösterge, L2CAP uygulaması vazgeçip L2CA_DisconnectInd mesajını göndermeden önce uygulamaya bağlı zamanlarda görülür.

L2CA_QoSViolationInd: QoS anlaşmasının sona erdiğini gösterir.

4.4.3.3 Kanal Çalışma Durumları

Kanal kurulduğunda, Bluetooth spesifikasyonunda belirtilen birçok çalışma durumunun içine girer. Örneğin, iki cihaz arasında başlangıcı yapan cihaz ilk L2CAP kanalını oluşturduğunda, iki taraf da CLOSED durumundadır. Üst katmandan talep alındıktan sonra, cihaz alt katmandan fiziksel bir link kurmasını ister. Eğer mevcut bir fiziksel link yok ise, LMP komutları bu linki kurmak için kullanılırlar. Fiziksel link kurulduğunda, L2CAP işaretleri onun üzerinden iletilir. Başlangıç konfigürasyon durumunda veri alınmaz fakat bir tekrar konfigürasyon süreci sebebiyle konfigürasyon durumuna girildiğinde alınabilir. Başka durumlarda veri alımı söz konusu değildir.

CLOSED: Bu durumda, CID ile ilişkilendirilmiş herhangi bir kanal yoktur. Bu durum link derecesinde bir bağlantı (örneğin temelbant) bulunmadığında ortaya çıkar. Link bağlantısının sona ermesi tüm diğer durumları da CLOSED durumuna geçmeye zorlar.

W4_L2CAP_CONNECT_RSP: Bu durumda, CID lokal bir sonlanma noktasını temsil eder ve bu noktayı referans alan bir L2CAP_ConnectReq mesajının gönderildiğini, tekabül eden L2CAP_ConnectRsp mesajının beklendiğini anlatır.

W4_L2CA_CONNECT_RSP: Bu durumda uzak sonlanma noktası mevcuttur ve lokal L2CAP varlığı tarafından bir L2CAP_ConnectReq alınmıştır. Bir

L2CA_ConnectIndmesajı üst katmana gönderilmiştir ve lokal L2CAP varlığı da alınan fakat tekabül eden cevabı bekleyen L2CAP_ConnectReq mesajını proses etmektedir. Gelecek tekabül eden cevap mutlaka güvenlik kontrolünden geçirilmelidir.

CONFIG: Bu durumda bağlantı kurulmuş fakat her iki taraf da kanal parametreleri üzerinde görüşmektedir. Kanal parametrelerinin tekrar görüşülmesi durumunda da bu duruma girilebilir. CONFIG durumuna girilmeden önce, tüm giden veri trafiği; trafik parametreleri tekrar görüşüldüğü (negotiate) için bir süreliğine durdurulur. Gelen veri trafiği ise uzak kanal sonlanma noktası CONFIG durumuna girene kadar kabul edilmelidir. CONFIG durumunda, her iki taraf da L2CAP_ConfigReq mesajlarını işleme koymalıdır. Eğer parametrelerin büyük bir kısmı görüşülecekse (negotiate) proses herhangi bir MTU kısıtlamasına uğramamak için gönderilen çoklu mesajlarla artarak devam eder. CONFIG durumundan OPEN durumuna geçiş için her iki taraf da hazır olmalıdır. Bir L2CAP varlığı son talebine pozitif bir cevap almışsa ve uzak cihazdan gelen son talebe olumlu cevap vermiş ise hazır olur.

OPEN: Bu durumda, bağlantı kurulmuş ve konfigüre edilmiş; veri akışı başlamıştır.

W4_L2CAP_DISCONNECT_RSP: Bu durumda, bağlantı sonlanmış ve bir L2CAP_DisconnectReq mesajı gönderilmiştir. Durum tekabül eden cevabı beklemektedir.

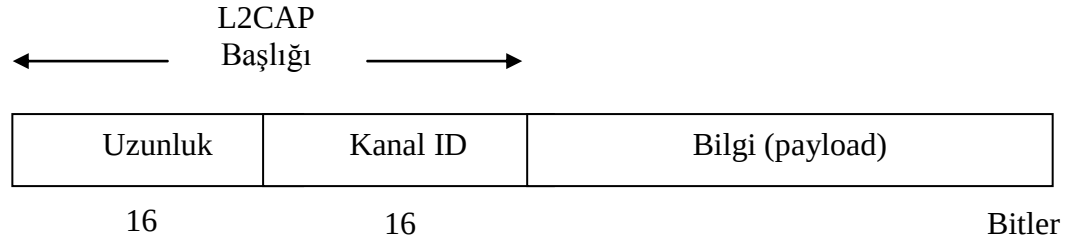
W4_L2CA_DISCONNECT_RSP: Bu durumda, uzak sonlanma noktasındaki bağlantı sonlanır ve bir L2CAP_DisconnectReq mesajı alınır. Bir L2CA_DisconnectInd mesajı CID in sahibini uzak sonlanma noktasındaki bağlantının sona erdiği konusunda uyarmak üzere gönderilir. Durum uzak sonlanma noktasına cevap vermeden önce üst katmandan gelecek tekabül eden cevabı beklemektedir.[9, 11]

4.4.4 Veri Paket Formatı

L2CAP paket tabanlıdır fakat uzak noktadaki L2CAP birimleri arasında veri akışını karakterize eden kanal yapısına dayalı olan bir haberleşme modeli içerir. Kanallar bağlantı yönelimli ya da bağlantısız olurlar.

4.4.4.1 Bağlantı Yönelimli Kanallar

Şekil 4.30 L2CAP paket formatını göstermekte ve bağlantı yönelimli bir kanal içindeki L2CAP PDU sunu betimlemektedir.



Şekil 4.30 L2CAP paket formatı

Şekilde gösterilen alanlar şu şekilde açıklanmaktadır:

Length (2 byte veya 16 bit): Taşınan bilginin (payload) boyutunu göstermektedir. L2CAP başlık bilgisi uzunluğu hariçtir. Bu alan, alıcı tarafta tekrar birleştirilen L2CAP paketinin doğruluk testlerinin yapılmasını sağlar.

Channel ID (2 byte veya 16 bit): Paketin hedef kanalının uç noktasını tanımlar.

Information (65,535 byte a kadar veya 524,280 bit): Üst katman protokolünden alınan (outgoing=çıkan paket) ya da üst katman protokolüne gönderilen (incoming=gelen paket) taşınan bilgiyi (payload) içerir.

4.4.4.2 Bağlantısız Veri Kanalı

Bağlantı yönelimli kanallara ek olarak L2CAP, verinin tüm grup üyelerine gönderildiği grup yönelimli kanal kavramını da destekler. Bu tip bir kanalda hiçbir QoS olmadığı için güvenliksizdir. Dolayısıyla, L2CAP gönderilen verinin tüm grup üyelerine ulaşacağını garanti etmez. Eğer güvenlik isteniyorsa, grup transmisyonu daha üst bir katmanda gerçekleştirilmelidir. Grup transmisyonları gruba dahil olmayanlar tarafından da alınabileceği için daha üst katmanda (ya da link katmanında) bir şifreleme, güvenliğin gözetildiği durumda mutlaka kullanılmalıdır. Şekil 4.31 de bağlantısız bir veri paketinin bölümleri gösterilmektedir.

Byte 0	Byte 1	Byte 2	Byte 3
Uzunluk		Kanal ID	
PSM		Bilgi (payload)	
Bilgi (devam)			

Şekil 4.31 Grup yönelimli veri haberleşmesi için kullanılan bağlantısız paketler

Şekilde gösterilen alanlar şu şekilde açıklanmaktadır:

Length (2 byte veya 16 bit): Taşınan bilginin (payload) boyutunu ve ek olarak PSM alanını göstermektedir. L2CAP başlık bilgisi uzunluğu hariçtir.

Channel ID (2 byte veya 16 bit): Paketin hedef kanalının uç noktasını tanımlar.

Protocol/Service Multiplexer (PSM) (minimum 2 byte veya 16 bit): PSM değerleri iki kademelidir. İlk kademedeki değerler Bluetooth SIG tarafından atanmışlardır ve protokolleri göstermektedirler. İkinci kademedeki değerler ise dinamik olarak tahsis edilir ve SDP ile birleşmede kullanılır.

Information (65,533 byte a kadar veya 524,264 bit): Tüm grup üyelerine dağıtılan taşınan bilgi (payload) bilgisini içerir.

L2CAP grup servis arayüzü tarafından sağlanan temel grup yönetim araçları; grup oluşturma, bir gruba üye ekleme ve bir gruptan üye çıkarma şeklindedir. Bununla birlikte, tüm ünitelerin etki alanı içinde olduğu bir grup önceden tanımlı bulunmamaktadır. [9]

4.4.5 İşaretleşme

Bluetooth kablosuz haberleşme teknolojisi uzak cihazlardaki iki L2CAP varlığı arasında iletilen işaretleşme komutlarını kullanır. L2CAP uygulaması komutları gönderen cihazın BD_ADDR sini belirler. Şekil 4.32 de bütün işaretleşme komutlarının genel formatı gösterilmektedir.

Byte 0	Byte 1	Byte 2	Byte 3
Kod	Tanımlayıcı	Uzunluk	
Veri			

Şekil 4.32 Uzak cihazlardaki iki L2CAP varlığı arasında iletilen işaretleşme komutları formatı

4.4.5.1 Paket Yapısı

Bluetooth spesifikasyonuna göre işaretleşme komutlarında kullanılan paket alanları şunlardır:

Code (1 byte veya 8 bit): Komutun tipini belirler. Bilinmeyen “Code” alanlı bir paket alındığında, cevap olarak “Command Reject” geri döndürülür.

Identifier (1 byte veya 8 bit): Talebi cevap ile eşleştirmek için kullanılır. Talepte bulunan cihaz bu alanı belirler ve cevap veren cihaz da cevabında aynı değeri kullanır.

Length (2 byte veya 16 bit): İşaretleşme komutundaki veri alanının boyutunu byte olarak gösterir. “Code”, “Identifier” ve “Length” alanlarındaki byte ları içermez.

Data (0 veya daha fazla byte): Bu alan uzunluğu belirsizdir ve “Length” alanı kullanılarak bulunur. “Code” alanı da “Data” alanının formatını belirler.

4.4.5.2 İşaretleşme Komutları

Bluetooth spesifikasyonu uzak Bluetooth cihazları arasında kullanılan 11 işaretleşme komutu içerir.

Command Reject

Bu paket bilinmeyen bir komut kodu ya da geçersiz bir kanal içeren komut paketine cevap olarak gönderilir. Örneğin geçersiz bir kanal ile ilgili bir komut alınırsa (tipik olarak bu problem kanal varolmadığı için görülür) cevap olarak Command Reject döndürülür. Aynı şekilde L2CAP paketinde çoklu komutlar var ise ve alıcının MTU su aşılmışsa yine Command Reject döndürülür.

Connection Request

Bu paket iki Bluetooth cihazı arasında bir kanal kurmak için kullanılır. Kanal bağlantısı konfigürasyon başlamadan önce kurulmalıdır.

Connection Response

Bir Bluetooth ünitesi bu paketi aldığı anda, Connection Response paketini göndermelidir. Başarılı bir cevap alındıktan sonra lojik kanal kurulabilir.

Configuration Request

Bu paket iki L2CAP varlığı arasında başlangıç lojik linkini kurmak için gönderilir ve istendiği zaman bu anlaşmayı tekrar görüşmek (negotiate) için de gönderilebilir. Bir tekrar görüşme (negotiate) sırasında, kanaldaki tüm veri trafiği sonucu beklediği için geçici olarak durdurulur. Görüşme esnasında kanal parametreleri üzerinde karar vermek için kullanılan mesajlar ya da harcanacak süre tamamen uygulamaya bağlıdır fakat hiçbir zaman 120 saniyeden fazla olamaz.

Configuration Response

Bu paket Configuration Request paketine cevap olarak gönderilir. Configuration Response daki her konfigürasyon parametresi, tekabül eden Configuration Request ile gönderilmiş olan konfigürasyon parametrelerine etki eder. Eğer Configuration Request teki bir konfigürasyon parametresi A cihazından B cihazına olan trafik ile ilgiliyse örneğin, Configuration Response u gönderen taraf sadece bu değeri ayarlayacaktır.

Disconnection Request

Bir L2CAP kanalını sonlandırmak için Disconnection Request paketi gönderilmeli ve cevap olarak Disconnection Response alınmalıdır. Hedef kanala gönderilen tüm diğer L2CAP paketleri otomatik olarak bir sonraki protokol katmanına geçmekte olduğu için bağlantı sonlanması talebi işaretleşme kanalı kullanılarak yapılır. Alıcı taraf bağlantı sonlanma işlemini başlatmadan önce kaynak ve hedef CID lerinin eşleştiğinden emin olmak zorundadır. Bir bağlantı sonlanma talebi yerine getirilir getirilmez, L2CAP kanalındaki gelen tüm veri atılır ve yeni bir veri gönderilmesine de izin verilmez. Bir bağlantı sonlanma talebi alınır alınmaz da o kanalda gönderilmek üzere sıraya konmuş tüm veri atılır.

Disconnection Response

Bu paket her Disconnection Request e cevap olarak gönderilir.

Echo Request

Bu paketler uzak bir L2CAP varlığından cevap istemek için kullanılır. Echo Request paketleri linki test etmek veya seçime bağlı veri alanını kullanarak üreticiye özel bilgileri göndermek için kullanılırlar. L2CAP birimleri Echo Request paketlerine mutlaka Echo Response paketleri göndermek zorundadırlar. Veri alanı seçime bağlıdır ve uygulamaya bağlıdır. L2CAP birimleri bu alanın içeriğini dikkate almazlar.

Echo Response

Echo Response paketleri Echo Request paketleri alındıktan sonra gönderilir. Cevaptaki kimlik tanımlayıcı talepte gönderilen kimlik tanımlayıcı ile eşleşmelidir. Seçime bağlı ve uygulamaya bağlı olan veri alanı talepteki veri alanını, başka bir veriyi içerebilir. Ya da hiç veri içermez.

Information Request

Bu paketler uzak bir L2CAP varlığından gelen uygulamaya özel bilgiyi istemek için kullanılır. L2CAP birimleri bu paketlere Information Response paketleri ile cevap vermek zorundadır.

Information Response

Bilgi cevap paketleri, bilgi talep paketleri alındıktan sonra gönderilir. Cevaptaki kimlik tanımlayıcı talepte gönderilen kimlik tanımlayıcı ile eşleşmelidir. Seçime bağlı ve uygulamaya bağlı olan veri alanı talepteki veri alanını, başka bir veriyi içerebilir. Ya da hiç veri içermez.

4.4.6 Konfigürasyon Parametre Opsiyonları

Bluetooth kablosuz teknolojisi farklı bağlantı gereksinimlerini görüşmek (negotiate) için opsiyon paketlerini kullanır. Bu tip bir paket opsiyon tipi, opsiyon uzunluğu ve bir veya daha fazla opsiyon veri alanlarından oluşur.

Byte 0	Byte 1	Byte 2	Byte 3
Type	Uzunluk	Seçimlik Veri	

Şekil 4.33 Konfigürasyon opsiyon paketi formatı

4.4.6.1 Paket Yapısı

Bluetooth spesifikasyonuna göre konfigürasyon opsiyon paketlerinde kullanılan alanlar şunlardır:

Type (1 byte veya 8 bit): Konfigüre edilecek parametreleri tanımlar.

Length (1 byte veya 8 bit): Opsiyon taşınan bilgisindeki (payload) byte sayısını gösterir. Taşınan bilgisi (payload) olmayan bir opsiyon tipinin uzunluğu sıfırdır.

Option Data (2 byte veya 16 bit) Bu alanın içeriği opsiyon tipine bağlıdır.

4.4.6.2 Opsiyonlar

Bluetooth spesifikasyonu L2CAP birimleri arasında görüşülebilecek dört opsiyon tanımlamaktadır.

Maksimum Transmisyon Ünitesi

Bu opsiyon gönderen tarafın o kanal için kabul edebileceği taşınan bilgi (payload) boyutunu byte cinsinden verir. L2CAP uygulamaları minimum 48 byte lık MTU boyutunu destekler. İlk (default) değer 672 byte dır.

Temizleme (Flush) Zaman Aşımı

Bu opsiyon alıcıyı transferi başlatan tarafın link kontrolörü/link yöneticisi bir L2CAP segmentini göndermekten vazgeçip, paketi temizlemeden (flush) önce kaç kere başarılı olarak göndermeyi denediği konusunda bilgilendirir. Bu değer mili saniyeler mertebesinde bir değer olur.

Servis Kalitesi (QoS)

L2CAP uygulamalarından en iyi servisi vermeleri beklenmektedir. En iyi servis herhangi bir garanti talep etmez, bu sebeple eğer konfigürasyon talebinde herhangi bir QoS opsiyonu yer almıyorsa, en iyi servisin verildiği farzedilir. Eğer herhangi bir

QoS garantisi isteniyorsa, aşağıdaki parametreleri içeren bir QoS konfigürasyon talebi gönderilmelidir:

- **Sembol Hızı (Token Rate):** Bu oran saniyede byte olarak gerçekleştirilen trafik değerini gösterir. Bir uygulama sürekli olarak bu oranda veri gönderir. Patlamalı (burst) veri en fazla sembolün (token) boyutu kadar gönderilebilir. Bir veri patlaması (burst) bitene kadar, uygulama sembol (token) oranına göre sınırlanma getirmelidir. En iyi servis için, uygulama mümkün olduğu kadar çok bant genişliği almalıdır. Garantili bir servis için ise uygulama talep anında olabilecek maksimum bant genişliğini alır.
- **Sembol Alan Boyutu (Token Bucket Size):** Sembol alanının (token bucket) (örneğin ara bellek (buffer)) boyutunu byte cinsinden verir. Eğer alan (bucket) dolu ise, uygulamalar ya beklemek ya da veriyi atmak zorundadır. En iyi servis için, uygulama mümkün olduğu kadar büyük bir alan (bucket) almalıdır. Garantili bir servis için ise uygulamaya talep anında maksimum ara bellek (buffer) alanı sağlanır.
- **Tepe Bant Genişliği:** Saniye başına byte olarak açıklanır. Bu değer, paketlerin uygulamalardan uygulamalara ne kadar hızlı gideceğini sınırlar. Orta dereceli bazı sistemler daha verimli kaynak tahsisi için bu bilginin avantajını kullanabilirler.
- **Gecikme Süresi:** Göndericiden gelen bir bitin transmisyonu ile onun hava üzerinden yaptığı ilk transmisyon arasındaki maksimum kabul edilebilir gecikmedir. Mikro saniyeler mertebesinde ölçülür.
- **Gecikme Değişimi:** Bir paketin kanal üzerinden gönderilirken uğrayabileceği maksimum ve minimum gecikmeler arasındaki farktır ve mikro saniyeler mertebesinde ölçülür. Bu değer, uygulamalar tarafından orijinal veri paternini yenilemek için alıcı tarafta ne kadar ara bellek (buffer) alanına ihtiyaç duyulduğunu anlamak için kullanılır.

4.4.6.3 Konfigürasyon Prosesi

Bluetooth spesifikasyonu kanal parametre görüşme sürecini üç adımda tanımlamıştır:

1. Uzak cihaz, lokal cihazın kabul ettiği, ilk (default) olmayan parametreler hakkında bilgilendirilir.

2. Uzak cihazın bu değerleri kabul edip etmediği bilgisi alınır.
3. Adım 1 ve 2 (önceki) uzak cihazdan (önceki) lokal cihaza ters yön için tekrarlanır.

Bu proses Talep görüşme yolu ve Cevap görüşme yolu olmak üzere iki bölümde incelenebilir.

Talep Yolu: Gelen MTU, temizleme (flush) zaman aşımı ve giden akış özelliklerini görüşür (negotiate).

Cevap Yolu: Giden MTU (uzak cihaz için gelen MTU), uzak cihazın temizleme (flush) zaman aşımı ve gelen akış özelliklerini (uzak cihazın giden akış özellikleri) görüşür (negotiate).

CONFIG durumundan çıkıp, OPEN durumuna geçmeden önce, her iki yol da kapanışa ulaşmış olmalıdır. Talep yolu kapanışa ulaşmak için lokal cihazın pozitif bir cevap almasını, cevap yolu da lokal cihazın pozitif bir cevap göndermesini bekler.
[11]

4.4.7 Servis Primitifleri

Bluetooth Spesifikasyonuna göre L2CAP tarafından yürütülen servisler servis primitifleri ve parametreleri açısından tanımlanmıştır.

4.4.7.1 Olay Göstergesi

Seçilen gösterge olayı meydana geldiğinde bir geri arama talebinde bulunmak için kullanılır. Aşağıdaki geri arama fonksiyonları kullanılır:

L2CA_ConnectInd Geri Araması

Bağlantı talebini alan uzak cihazın adresi, talep edilen kanalı temsil eden CID, talepte yer alan Tanımlayıcı ve PSM değeri için parametreler içerir.

L2CA_ConfigInd Geri Araması

Talebin gönderildiği kanalın lokal CID i, giden MTU boyutu (kanal boyunca iletebilecek maksimum paket) ve gelen verinin karakteristiklerini tanımlayan akış özelliklerini belirten parametreler içerir.

L2CA_DisconnectInd Geri Araması

Talebin gönderildiği lokal CID i gösteren parametreler içerir.

L2CA_QoSViolationInd Geri Araması

QoS anlaşmasını sona erdiren uzak Bluetooth cihazının adresini gösteren parametreler içerir.

4.4.7.2 Bağlantı

Bağlantı primitifi bir L2CA_ConnectReq mesajı başlatır ve buna tekabül eden L2CA_ConnectCfm(Neg) ya da L2CA_TimeOutInd mesajı alınana kadar servisi bloke eder. Bu primitif fiziksel bir adrese lojik bir bağlantıyı temsil eden bir kanalın kurulmasını talep etmek için kullanılır.

4.4.7.3 Bağlantı Cevabı

Bu primitif L2CA_ConnectRsp yi temsil eder. Bağlantı talebi olay göstergesine verilen cevabı yerine getirmek için kullanılır ve geri çağırma göstergesini aldıktan sonra bir kereden fazla çağrılmaz. Bu primitif lokal L2CAP varlığı talebi onaylar onaylamaz geri döner. Başarılı bir dönüş cevabın hava arayüzü üzerinden gönderildiğini gösterir.

4.4.7.4 Konfigüre

Bu primitif L2CA_ConfigReq mesajını gönderme işlemini başlatır ve tekabül eden bir L2CA_ConfigCfm (Neg) veya L2CA_TimeOut_Ind mesajı alınana kadar servisi bloke eder. Bu primitif bir kanalın başlangıç konfigürasyonu ya da tekrar konfigürasyonunu talep etmek için kullanılır.

4.4.7.5 Konfigürasyon Cevabı

Bu primitif L2CAP_ConfigRsp yi temsil eder. Konfigürasyon talebi olay göstergesine verilen cevabı yerine getirmek için kullanılır.

4.4.7.6 Bağlantı Sonlanma

Bu primitif L2CAP_DisconnectReq yi temsil eder. Geri dönen çıkış parametrelerini de tekabül eden L2CAP_DisconnectRsp yi veya RTX zamanlayıcısının zaman aşımını temsil eder. Kanalın bağlantı sonlanmasını talep etmek için kullanılır. Talep yerine getirildikten sonra, hiçbir proses CID den başarılı olarak okuma ya da yazma yapamaz. Fakat o an proses edilmekte olan yazma işlemleri devam eder.

4.4.7.7 Yazma

Bu primitif kanal üzerinden veri transferi yapılmasını talep etmek için kullanılır. Hem bağlantı yönelimli hem de bağlantısız trafik için geçerlidir.

4.4.7.8 Okuma

Bu primitif verinin kabulünü talep etmek için kullanılır. Bu talep veri uygun olduğunda veya link sonlandığında geri döner. Dönen veri tek bir L2CAP taşınan bilgisini (payload) gösterir. Eğer yeterli miktarda uygun veri yoksa, veri ulaşana veya link sonlanana kadar servisi bloke eder. Eğer taşınan bilgi (payload) ara bellekten (buffer) dan daha büyükse; ara bellek (buffer) kadar olan miktarı geri döndürülür, fazla kalan miktar ise atılır. Yazma komutuna benzer şekilde, Okuma komutu da hem bağlantı yönelimli hem de bağlantısız trafik için kullanılır.

4.4.7.9 Grup Yaratılması

Bu primitif birden fazla cihaza lojik bağlantıyı temsil eden CID in oluşturulmasını talep etmek için kullanılır.

4.4.7.10 Grup Kapatılması

Bu primitif bir “Grup” u kapatmak için kullanılır.

4.4.7.11 Gruba Üye Ekleme

Bu primitif gruba üye eklenmesini talep etmek için kullanılır. Giriş parametresi, grubu temsil eden CID i ve eklenecek üyenin BD_ADDR sini içerir. Çıkış parametresi sonucu talebin başarılı ya da başarısız olup olmadığı bilgisini içerir.

4.4.7.12 Gruptan Üye Çıkarmak

Bu primitif gruptan üye çıkarılmasını talep etmek için kullanılır. Giriş parametresi, grubu temsil eden CID i ve eklenecek üyenin BD_ADDR sini içerir. Çıkış parametresi sonucu talebin başarılı ya da başarısız olup olmadığı bilgisini içerir.

4.4.7.13 Grup Üyeliği Alma

Bu primitif grup üyelerine ilişkin bir rapor almak için kullanılır. Giriş parametresi, sorgulanan grubu temsil eden CID i içerir. Çıkış parametresi sonucu talebin başarılı

ya da başarısız olup olmadığı bilgisini içerir. Eğer sonuç olumlu ise grup üyelerini gösteren bir Bluetooth adres listesi alınır.

4.4.7.14 Ping

Bu primitif L2CA_EchoReq komutunun başlatılmasını ve tekabül eden L2CA_EchoRsp komutunun alınmasını temsil eder.

4.4.7.15 Bilgi Alma

Bu primitif L2CA_InfoReq komutunun başlatılmasını ve tekabül eden L2CA_InfoRsp komutunun alınmasını temsil eder.

4.4.7.16 Bağlantısız Trafiğin Olanaksız Kılınması

Bu primitif bağlantısız paketlerin alımını olanaksız kılmayı talep etmek için kullanılır. Giriş parametresi servisin bloke olması gerektiğini gösteren PSM değeridir.

4.4.7.17 Bağlantısız Trafiğin Olanaklı Kılınması

Bu primitif bağlantısız paketlerin alımını olanaklı kılmayı talep etmek için kullanılır. Giriş parametresi servisin bloke olmaması gerektiğini gösteren PSM değeridir.

4.4.8 Özet

Link Yönetim Prorokolüne (LMP) benzer şekilde Lojik Link Kontrolü ve Adaptasyon Protokolü (L2CAP) de Bluetooth temelbant biriminin üzerinde koşan link seviyesi bir protokoldür. L2CAP üst seviye protokol çoğullama (multiplexing) dan sorumludur. Çoklu kanallarda aynı protokol olabilmesine rağmen, tek kanalda çoklu protokoller olamaz. Kanalda alınan her bir L2CAP paketi uygun üst katman protokolüne yönlendirilir.

L2CAP ayırıştırma ve tekrar birleştirme mekanizmalarını kullanarak 64 kilobyte a kadar olan büyük paket boyutlarını destekler. Grup yönetimi, gruplar ve pikonet üyeleri arasında daha efektif eşlemeye (mapping) izin veren bir cihazlar grubu temsili sağlar. Grup haberleşmesi bağlantısızdır ve güvenli değildir. Grupların sadece iki üiteden oluştuğu durumlarda L2CAP in bağlantı yönelimli kanalına alternatif olarak bağlantısız bir kanal sağlanır. L2CAP kanallar arasında QoS bilgisini taşır ve

mevcut QoS anlaşmasını bozan ek kanalları engellemek için kontrol mekanizması sağlar.

4.5 Servis Keşif Protokolü (SDP)

Servis Keşif, ağda hangi cihaz ve servislerin bulunabileceğine dair bilgi toplamak ve ağdaki diğer servislerin kullanımını sağlamak için kullanılan bir protostir. LAN lar gibi geleneksel ağlarda bu servisler fiziksel olarak konfigüre edilir ve bir ağ yöneticisi tarafından yönetilirler. Bu ağlarda, ağ yöneticisi veya başka bir kullanıcı ağdaki bir üyenin diğer bir üyenin servislerini kullanabilmesi için gereken ayarları konfigüre eder. Örneğin, bir PC kullanıcısı ağ e-posta servisine ilişkin bilgileri (posta sunucu ismi, kullanıcı ve hesap adları, e-posta tipi, kapasitesi, vs..) kendisi belirleyebilir. Bu bilgiler PC ye girildikten ve e-posta servisi ile ilişkilendirildikten sonra, bu servis kullanıcı için olanaklı hale gelir.

Bu tipteki ağ servisleri birçok sabit ağ için uygun olabilir fakat anlık (ad hoc) ağlar için uygun değildir. Bu tiğ ağlarda daha dinamik, esnek ve adaptif bir çözüme gerek duyulmaktadır.

Yeni tip bağlantılar ve bilgi cihazları yeni tipte ağ gereksinimleri meydana getirmektedir: yönetilmeyen, dinamik tüketici cihazları ağlara anlık olarak girip çıkabilmelidir. Son kullanıcılar bu anlık (ad hoc), noktadan noktaya ağları evde, küçük işlerde ve ağ donanımlı araçlarda kullanmak istemektedirler.

Basitlik, çok yönlülük ve kullanıcı memnuniyeti sağlamak için cihazlar ve ağlar arasındaki haberleşme hemen çalışmalıdır. Hemen çalışma ile ağ katılımcılarının kendi konfigürasyonlarını basit olarak kendilerinin yapmaları kastedilmiştir. Kendi konfigürasyonunu kendisinin yapması ise ağ cihazları ve servislerinin birbirlerini keşfetmeleri, yapmaları gereken şeyler hakkında anlaşmaları ve elle yapılacak herhangi bir müdahaleye gerek kalmadan haberleşmeye başlamaları demektir. [12]

Servis keşfi için kullanılan protokoller kendi kendine konfigürasyon konusunu olanaklı hale getirmeyi sağlar. Bluetooth kullanım senaryolarının birçoğu noktadan noktaya, anlık (ad hoc) şekilde olduğu için SIG bir servis keşif protokolünün gerekli olduğuna karar vermiştir. Böylece SDP neredeyse tüm profillerin ve kullanım modellerinin merkez bileşeni olmuştur.

Servis keşif kavramı yeni ya da Bluetooth'a özgü bir kavram değildir. Birçok servis keşif teknolojisi hali hazırda değişik konularda kullanılmaktadır. Bluetooth protokol yığınının diğer katmanlarında açıkça görüldüğü gibi, SIG eğer anlamlı ise mevcut protokolleri adapte etme yolunu seçmiştir. Servis keşif konusunda ise SIG tamamen Bluetooth'a özgü bir protokol geliştirmiştir.

4.5.1 SDP Gelişimi

Protokol yığınının bir servis keşif bileşenine ihtiyaç duyulduğu, Bluetooth spesifikasyonunun geliştirme sürecinin başlarında farkedilmiştir. 1998 yılı ortalarına kadar, SIG in birçok üyesi iletim protokolleri ve RFCOMM üzerinde yoğunlaşmıştı. SDP ile ilgili ön çalışmalar Ericsson ve Intel tarafından 1998 yılı yazında başlatılmıştır.

SDP, ilk çalışma versiyonlarında, L2CAP in bir parçası gibi incelenmişti. Önceleri L2CAP kanalları bir bilgisayar yolundan (bus) sonra modellenmiş, servis keşif ise bu sanal yol (bus) üzerinden Tak ve Çalıştır parametrelerinin taşınması ile ilgilenmişti. 1998 yılının Ekim ayında Atlanta'da yapılan SIG konferansında sadece Tak ve Çalıştır parametreleri için bir protokol oluşturmanın gereksiz olduğuna ve SDP için ayrı bir çalışma grubu kurulmasına karar verilmiştir.

Bluetooth SDP için tanımlanan hedefler şunlardır:

Basitlik: Servis keşif konusu neredeyse tüm Bluetooth kullanım alanlarının bir parçası olduğu için bu prosesin olabildiği kadar basit olması hedeflenmiştir. Bu sebeple diğer Bluetooth protokollerinin mümkün olduğu kadar çok tekrar kullanımı istenmiştir.

Özlük: İki cihaz arasında Bluetooth haberleşme linki kurulumu bazı durumlarda çok zaman alabilir. Servis keşfi, linkler kurulduktan sonra yürüyen bir proses olduğu için, SDP hava arayüz trafiği olabildiği kadar düşük düzeyde kalmalı ve haberleşme başlangıç süresini uzatmamalıdır.

Çok yönlülük: Bluetooth spesifikasyonu birçok profil içermektedir ve gelecekteki versiyonlarının daha fazla profil içereceği de aşikardır. Profillerin, kullanım alanlarının ve ilgili servislerin ayrıntılı tahminleri şimdiden mümkün olmadığı için, SDP nin kolaylıkla genişleyebilir ve Bluetooth cihazlarında yeni servislerin

bulunmasına imkan verecek ölçüde çok yönlü olması gerekmektedir. Bu gereksinimi yerine getirebilmek için “servis” tanımı olabildiğince geniş yapılmıştır.

Sınıf ve özellik açısından servis lokasyonu: Dinamik anlık (ad hoc) ağ cihazlarında istemci cihaz ve kullanıcılarının istedikleri servisi olanaklı hale getirmelerini sağlamak önemlidir. Genel bir servis sınıfını (cihazın yazıcı olduğunu söylemek gibi) ve o servisle ilgili özellikleri (yazıcının renkli IBM marka yazıcı olduğunu söylemek gibi) belirlemek temel olmalıdır.

Servis tarama (browsing): Servisleri sınıf veya özellikle aramaya ek olarak, uygun servisleri browse etmek de kullanışlı bir yöntemdir. Bu kullanım senaryosu, özel servisleri aramaktan farklı, hatta zıt bir senaryodur. Fakat SIG her iki kullanımından önemi olduğuna karar vermiş ve hem özel servis arama hem de genel servis arama için bir çözüm geliştirmiştir.

Bu hedefler doğrultusunda servis keşfi için basit, esnek bir protokol ve veri sunumu geliştirilmiştir. Endüstride kullanılan tüm servis keşif metodolojileri incelenmiş, fakat bu teknolojilerin çoğu çok geniş kapsamlı ve zor kullanımlı olduğu için SIG tarafından daha düşük seviyeli, basit, dar skoplu bir çözüme yönelmiştir. Bu noktada Motorola, SIG e Bluetooth teknolojisine uygun bir servis keşif protokolü teklifinde bulunmuştur. Sonrasında ise Motorola SIG içindeki SDP grubuna katılarak, kendi teknolojisini adapte etmiştir. 1999 yılının Temmuz ayında da protokol yığınındaki yerini resmi olarak almıştır.

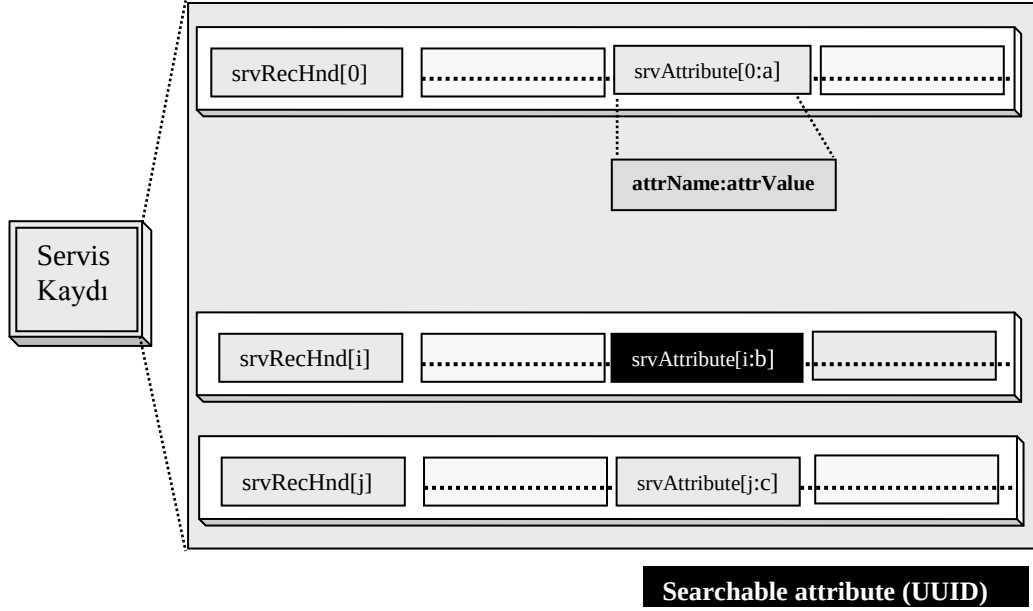
4.5.2 SDP Temel Özellikleri

SDP Bluetooth cihazlarının uygun servisleri kendileri için ayırmalarını amaçlar. Bluetooth ağları LAN veya WAN gibi geleneksel ağlardan niteliksel olarak çok farklıdır. Cihazlar ve servisler Bluetooth pikonetlerine sık sık girip çıkarlar. SDP de bu tarzda çalışan ağ gereksinimleri için geliştirilmiştir.

SDP istemcinin fikrini (servis arayan birim) ve bir sunucuyu (servisleri sağlayan birim) içerir. Cihazlar kimi zaman istemci kimi zaman da sunucu olarak davranabilir.

Servis sağlayıcı, sağladığı servisleri tanımlayan bir “servis kaydı” listesi tutmalıdır. Bu liste “servis kaydı” olarak adlandırılır. Bir servis kaydı spesifikasyon tarafından tanımlanan standart şekilde servisleri tanımlar. Servis kaydı servisin sınıfı ve özellikleri hakkında (yazma, faks gönderme, ses servisleri, bilgi servisleri gibi),

servis ile etkileşecek protokol katmanları hakkında ve servis hakkında kişilerin bilgi edinmesini sağlayacak ek bilgiler gibi bölümler içerir. Şekil 4.34 de bir servis kaydının genel yapısı gösterilmiştir. Her biri bir servis kayıt eki (srvRecHnd[0] dan srvRecHnd[j] ye kadar) ve servis özelliği (srvAttribute[0:a] dan srvAttribute[j:c] ye kadar) ile gösterilen bir servis seti gösterilmiştir.



Şekil 4.34 SDP servis kaydının genel yapısı

Servis kayıtları hem genel servis özelliklerini hem de servise özel özellikleri içerir. Genel servis özellikleri tüm servis tiplerine uygulanan servis sınıfı ve protokol yığın bilgisi gibi bilgilerdir. Servise özel özellikler ise özel bir sınıf ya da bir servis durumu ile ilgili bilgilerdir. Servise özel özellik örnekleri bir yazma servisine özgü özellikler (renkli, dublex ve bitirme kapasitesi gibi), bir ses servisine özgü özellikler (veri hızı veya kodlama yapısı gibi) veya bir çevirmeli ağ servisine özgü servisler (seri port konfigürasyonu veya modem kurulum bilgisi gibi) şeklinde verilebilir. Servislere özgü özellikler Bluetooth profilleri içerisinde tanımlanmıştır. Profiller kullanım senaryolarını ve protokol yığınının kullanımını tanımlarlar. Örneğin kulaklık-mikrofon seti profili servise özgü olan “uzak ses kontrolü” özelliğini tanımlar. Genel servis özellikleri her tipteki servise uygulanabilir olmakla birlikte zorunlu değildir. Her servisin kendi servis kaydı içinde her genel servis özelliğini içermesi şart değildir. Sadece iki genel servis özelliği zorunludur: sınıfı veya servis tipini belirleyen servis sınıfı özelliği ve servis kaydını gösteren servis kayıt tanıtıcısı

(handle). Servis kayıt tanıtıcısı (handle) istemci tarafından sunucunun servis kaydına ulaşmak için kullanılır.

Bir servis kaydındaki her servis özelliği bir özellik belirleyici (özellik ID, 16-bitli işaretli bir tamsayıdır) ve o özellik belirleyici ile ilişkili olan bir özellik değeri içerir. Her servis kayıt girdisi bu iki değeri içerir. Bu özellikler her türde bilgiyi tanımladıkları için, SDP özellik değeri için “veri elementi” kavramını kullanır. Veri elementi kendi kendine tanımlanan bir veri parçasıdır. Veri elementinin ilk kısmı verinin gerçek boyutu ve tipini belirten 1 byte lık başlık bilgisinden oluşur. Veri elementinin geriye kalan kısmı da özellik ve format için olan veri değerlerini ve veri elementi başlığı tarafından belirlenen boyut bilgisini içerir. SDP veri elementlerini kullanarak, özellik değerlerinin string, Boolean, işaretli ve işaretli tamsayı ve genel tek belirleyiciler (universal unique identifier - UUID) gibi farklı şekillerde olmasına izin verir. Böylelikle birçok veri tipi için esnek bir sunum imkanı sağlanmış olur.

Bluetooth kablosuz haberleşmesinde bir servisi keşfetmek basit bir işleme dönüşmüş olur: istemci ilgilendiği servisi ya da servisleri belirler, sunucu istemcinin talebine uygun olan servisleri belirterek cevap verir. Pratikte, istemci hangi servisleri aradığını belirten ve SDP protokolü veri ünitesi formatında (SDP_PDU) olan bir talep gönderir. Benzer şekilde sunucu da SDP_PDU formatında bir cevap gönderir. Bu süreci gerçekleştirmek için istemci ve sunucu talep ve cevaplarını belirtmek için standart bir metoda gereksinim duyarlar. Bu amaçla SDP UUID leri tanımlamıştır.

Bir UUID, International Organization for Standardization (ISO) dan alınarak benimsenen bir kavramdır. UUID ler algoritmik olarak üretilen ve tek olan 128-bitlik değerlerdir. Hiçbir UUID daha önce üretilen bir UUID ile aynı değeri alamaz. UUID kullanmanın bir avantajı SIG mevcut profiller ile ilgili servislere ilişkin “iyi bilinen” UUID lerin listesini yayınlamış olmasına karşın; yeni servisler için yeni tanımlayıcılar belirleme işleminin SIG tarafından sağlanan tanımlayıcılara merkezi bir kayıt işlemi gerektirmemesidir. Böylelikle bir servis arayan istemci servis arama talebinde sadece o servis sınıfı ya da özel servisle ilgili olan UUID yi belirtir; servis sağlayıcı da bu UUID yi uygun cevabı verecek şekilde eşleştirir.

İstemci ile sunucu arasında değiş tokuş edilen SDP_PDU ları basit iletimlerdir. SDP protokol akışı genel olarak iki iletim gerektirir; spesifikasyon üç farklı SDP iletimi

tanımlar fakat üçüncüsü sadece ilk ikisinin karşıtıdır. Tipik bir SDP iletimi aşağıdaki bölümlerden oluşur:

1. İstemci ilgilendiği servisleri aramak için bir talep gönderir; sunucu da bu talebe uygun gelen tanıtıcılar (handle) ile cevap verir.
2. İstemci ilgilendiği servislerle ilgili servis özellikleri hakkında ek bilgi almak için ilk adımda elde edilen tanıtıcıları (handle) kullanarak bir talep gönderir.

Yukarıdaki iletimi takiben, istemci 2.adımda elde ettiği bilgiyi kullanarak SDP den farklı bazı protokoller kullanarak servise erişir ve faydalanır. 1.adım “Servis Arama” iletimi olarak adlandırılır ve istemciden sunucuya gönderilen Servis Arama Talebi SDP_PDU su ile sunucudan istemciye gönderilen Servis Arama Cevabı SDP_PDU sundan oluşur. Servis Arama Cevabı SDP_PDU su talep ile eşleşen bir veya birden fazla tanıtıcı (handle) içerir. 2. adımda istemci bu tanıtıcıların (handle) bir veya birden fazlasını bir Servis Özellik Talebi SDP_PDU sunda kullanır, sunucu da bir Servis Özellik Cevabı SDP_PDU su oluşturur. Bu değiş tokuş Servis Özellik iletimi olarak adlandırılır. Servis Özellik Cevabı SDP_PDU sunda istemcinin Servis Özellik Talebi SDP_PDU sunda belirlediği özellik ID lerine karşılık gelen servislerle ilgili özellik değerleri bulunur. Bu özellikler genel servis özellikleri ile servislere özgü özelliklerin bir kombinasyonu şeklinde olabilir. Çoğu durumda istemciye servise sonradan bağlanmak için yeterli bilgi sağlar.

Bluetooth spesifikasyonu Servis Arama Özelliği adında üçüncü bir SDP iletimi tanımlar. Bu iletim Servis Arama Özellik Talebi SDP_PDU su ile Servis Arama Özellik Cevabı SDP_PDU sundan oluşur. Bu iletim yukarıda açıklanan diğer iki iletime göre daha az gereklidir fakat verimlilik için kullanılmaktadır. Servis Arama Özellik iletiminin sağladığı şey 1. ve 2. adımların kombinasyonudur. İstemci tek bir taleple sadece servis talebinde bulunmakla kalmaz, sunucunun cevabındaki uygun servislerle ilgili özellikleri de talep etmiş olur. Sunucu da uygun servislerle ilgili tanıtıcıları (handle) ve bu uygun servislerin istenen özellik değerlerini de cevaplamış olur. Bu sebeple uygulama geliştiricilerin SDP iletimleri için uygulanacak profile bağlı olmakla birlikte iki alternatifleri vardır. Daha önemlisi, Servis Arama Özellik iletimi bazı durumlarda hava arabirimi üzerinden iletilen byte miktarı gözönüne alındığında daha verimli sonuç verir. Konsolide olmuş iletimin kendisi tek tek yapılan iletimlere göre daha çok byte gerektirebilir fakat daha az sayıda toplam

iletim ile sonuç verir. Özellikle birçok servis kaydına erişilen bazı durumlarda, örneğin bir servis tarama (browsing) uygulamasında, Servis Arama Özellik iletimi daha verimli olabilir.

Bluetooth spesifikasyonu bir hata cevabı SDP_PDU su ve Devamlılık Durumu şeklinde adlandırılan bir mekanizma gibi özel durumlar için de protokol tanımlamaları içerir. Bu tanımlamalar tek bir SDP_PDU suna uymayan sunucu cevapları için kullanılır. İstemci kendi SDP_PDU suna karşılık gelecek cevabın maksimum boyutunu belirleyebilir. Sunucunun cevabının bu boyuttan daha büyük olması mümkündür. Bu durumda, sunucu kendi cevabının sonuna bazı devamlılık durum bilgileri de ekleyerek istemcinin istediği takdirde cevabın devamı için tekrar talepte bulunmasını sağlar. Bazı durumlarda iletimin kendisi basit olmasına rağmen bu iletimler için yaratılan byte dizileri kompleks olabilir. Bu kompleks olma durumu özellikle SDP_PDU ları içinde kompleks veri elementleri taşındığı zaman ortaya çıkar. SDP_PDU ları içinde bu tip kompleks veri tipleri bulunduğunda ya da devamlılık durum bilgisi kullanılarak SDP_PDU sunun bölünmesi gerektiğinde, SDP_PDU sunun her segmentindeki byte sayısını doğru olarak veren değişik “sayı” alanları oluşur.

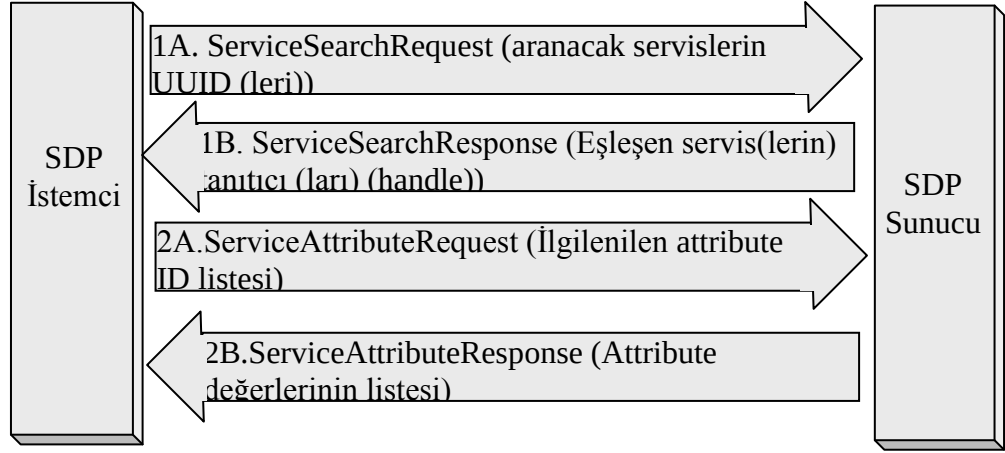
Şekil 4.35 SDP iletimlerini özetlemektedir. Şekilde gösterilen argüman ve parametreler SDP_PDU ları içinde geçen bazı argüman ve parametrelerdir. Şekil 4.34 ten de anlaşılabileceği gibi sadece UUID ler tarafından tanımlanan servisler ve servis özellikleri aranabilir (searchable) özelliktedir. UUID ler tarafından tanımlanmayan bir servisin özellikleri aranamaz (unsearchable) ve o servis ancak bir UUID özelliği kullanarak yerleştirildikten sonra alınabilir. [2,13]

4.5.3 SDP Kullanımı

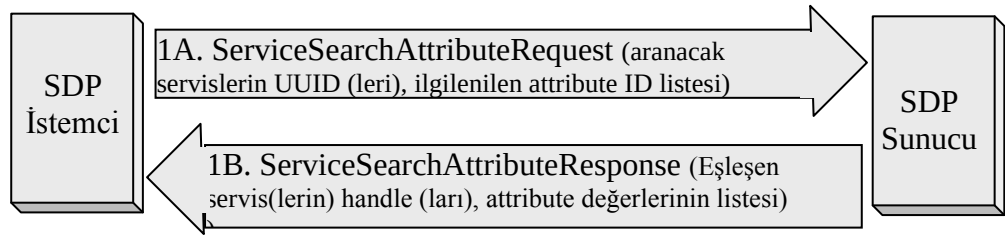
SDP öncelikle Bluetooth cihazlarındaki servisleri keşfetmek için geliştirildiğinden dolayı, SDP yi kullanan uygulamaların çoğu bilinen mevcut uygulamaların tersine Bluetooth kablosuz haberleşmesinden haberdardırlar. SDP kullanımına bir örnek olarak Bluetooth Pikonet Minder (BPM) verilebilir. Bir BPM uygulaması pikonetteki uygun cihaz ve servisleri kullanıcıya ve diğer uygulamalara gösterir. Bu tip bir uygulama bir kullanıcı arayüzü içerebilir ve böylelikle kullanıcıya diğer Bluetooth cihazları ile olan bağlantıyı kontrol etme imkanı sağlar. Bunun gibi fonksiyonlar içermesi için bir BPM uygulaması servis arama ve servis tarama (browsing)

özelliklerini kullanmalı bu yüzden de SDP iletimlerini kullanarak servis bilgilerini almalıdır.

Alternatif 1: Bireysel Hareket (Transaction)



Alternatif 2: Toplu Hareket (Transaction)



Şekil 4.35 SDP iletimleri

Bluetooth cihazlarında kullanılmak üzere tasarlanan diğer uygulamalar da SDP yi kullanabilirler. Her profil (ya da her jenerik olmayan ve somut kullanım senaryoları içeren her profil) bir SDP servis kaydı içerir. Uygulamalar diğer cihazla bir SDP iletimi oluşturarak, o cihazın istenen servisi verip vermediğini öğrenir, eğer veriyorsa ek SDP iletimleri ile o servise nasıl ulaşılacağı bilgisini servis kayıtlarından almaya gerek duyarlar.

Birden fazla uygulamanın SDP kullandığı durumda, tüm uygulamalara uygunluk gösteren bir merkez SDP istemcisi ve SDP sunucusu oluşturmak avantajlı olabilir. Bu SDP “yardımcı uygulamaları” genel SDP servislerine erişmek için platform API lerini kullanırlar.

Servis keşfini kullanan bilinen uygulamalar da mevcuttur fakat bunlar genellikle başka endüstri keşif protokollerini (Jini, Universal Plug and Play, Salutation, Service Location Protocol, IrDA servis keşif protokolü gibi..) kullanırlar. SDP Bluetooth uygulamaları için geliştirildiği için, bilinen mevcut uygulamaların bu protokolü kullanması beklenemez. Fakat SDP bu tip uygulamalar için bile bir uygunluk sağlar. SDP nin tasarım noktalarından bir tanesi de diğer popüler endüstri keşif protokolleri ile ortak bir noktada kullanılabilirliğini garanti eder. Bu sebeple SDP servisi keşfetmek için başlangıç servis keşif fazı olarak kullanılabilir, sonrasında ise SDP iletimleri servisin desteklediği diğer protokolleri keşfetmek için kullanılır. Örneğin Salutation kullanılıyorsa ve bu SDP tarafından keşfedilmişse servisle etkileşim için bu noktadan sonra kullanılabilir. SDP bu tipteki çalışma şeklini desteklemektedir. [2]

4.6 RFCOMM

Seri arabirimler bilgisayar ve haberleşme cihazlarının tamamında, özellikle Bluetooth teknolojisi ile ilgili olan cihazlarda mutlaka bulunurlar. Dizüstü bilgisayarların, cep bilgisayarlarının seri portları (özellikle cep bilgisayarını başka bir cihazla senkronize etmek için kullanılır) vardır, birçok mobil telefonda (genellikle kablolu bir mikrofön-kulaklık seti için kullanılır), birçok dijital kamerada (başka bir cihaza imaj verisi transferi için kullanılır), yazıcı ve diğer bilgisayar çevre birimlerinde de seri port bulunmaktadır. Kızıl ötesi haberleşme de kızıl ötesi (IR) alıcı-vericisi ile haberleşmek için seri port kullanır.

Bluetooth teknolojisi kabloların yerini almayı hedeflediği için, özellikle seri kabloların yerini almak için pek çok alternatif olduğu görülmektedir. Bunu efektif olarak yapmak ve uygulamaları benzer bir arabirimle sunabilmek için, Bluetooth protokol katman yapısı seri haberleşmeyi kablo ile yapıldığı şekliyle desteklemelidir. Bu durum Bluetooth teknolojisinden haberdar olmayan uygulamaların da Bluetooth linkleri üzerinden haberleşebilmelerini sağlar. Ayrıca seri port haberleşmesi ile ilgili yazılım geliştiren kişilerin, aynı şekilde çalışmalarına devam etmeleri ile, uygulamalarının Bluetooth linkleri üzerinden de çalışabilmesini sağlar. L2CAP ve hava arayüzleri seri port modellemesi içermemektedir. L2CAP paket veri yapısını destekler. Hava arayüzü de bit paternlerini seri şekilde iletir ancak bu çalışma şekli bilinen RS-232 tipinde bir çalışma şekli değildir.

Bu sebeple SIG protokol katmanında tipik seri arabirime benzer bir katman olan RFCOMM u tanımlamıştır. Seri arabirimler genellikle COM port olarak adlandırılmaktadır. RFCOMM ismi sanal bir COM portun RF uzantısı anlamında seçilmiştir. RFCOMM, mevcut uygulamalar için kabloyu ortadan kaldırmayı olanaklı hale getirmeyi amaç edinmiştir.

4.6.1 RFCOMM Protokol Gelişimi

Protokol katmanındaki seri port fonksiyonu SIG ilk kurulduğunda farkedilmişti. SIG resmi olarak kurulduktan bir ay sonra, RFCOMM katmanını geliştirmek üzere çalışmalar başladı. Aynı zamanda ETSI TS 07.10 standardı (ETSI99) Bluetooth seri haberleşmesine temel teşkil etmek üzere seçildi. Bluetooth seri haberleşme gereksinimleri şu şekildedir:

Çoklanmış seri haberleşme: Katmandaki seri arabirimde IrOBEX, telefon kontrolü ve ağ istemcileri gibi aynı anda birçok istemci bulunabilir. Bu sebeple seri port çoklanmış bağlantılar üzerinden paylaşılabılır olmalıdır.

RS-232 işaret uygunluğu: RS-232 kablolar için kullanılan seri arabirimdir ve bu sebeple Bluetooth teknolojisi RS-232 ile uyumlu olmalıdır. Birçok uygulama RS-232 arabirimi ve RS-232 ile ilgili olan kontrol işaretleri ile uyumlu çalışır. Bu kontrol işaretleri Request to Send/Clear to Send (RTS/CTS), Data Terminal Ready/Data Set Ready (DTR/DSR) gibi sıklıkla kullanılan işaretleri de içerir. RFCOMM bu işaretleri emüle ederek, seri kablo ile kullanılan seri portun aynısını sanal olarak sağlar.

Uzak durum ve konfigürasyon: Bir noktadan noktaya haberleşme platformunda, seri link üzerinden haberleşen iki taraf, diğer uçtaki seri arabirimin durum ve konfigürasyonunu belirlemek ve buna uygun şekilde kendi konfigürasyonunu yapmak durumundadır. Bir önceki bölümde ele alınan Servis Keşif Protokolü, bir seri haberleşme kanalı kurmak için gereken temel bilgiyi sağlamakta kullanılabilir. Seri bağlantı kurulduktan sonra, bağlantı için gereken uygun seri haberleşme ayarlarını görüşmeye (negotiate) ihtiyaç duyarlar.

Dahili ve harici seri port: Bluetooth uygulamalarında seri haberleşmenin değişik kullanımlarını desteklemek için, RFCOMM hem dahili emülasyonlu bir seri portu (seri port parametrelerinin sadece lokal olarak kullanıldığı, hava arabirimi üzerinden iletilmediği durumlarda), hem de harici bir seri portu (seri port parametrelerinin ve

durum bilgisinin RF linki üzerinden veri ile birlikte iletildiği ve alıcı taraf tarafından kullanıldığı durumlarda) desteklemelidir.

Bu gereksinimler sadece Bluetooth cihazları için gerekli değildir. SIG daha önce açıklanmış olan ETSI TS 07.10 standardının Bluetooth seri haberleşmesi gereksinimlerine uygunluk gösterdiğini farketmiş ve bu standardı adapte etmiştir. Fakat TS 07.10 tek başına Bluetooth protokol yığnında kullanılmak için mükemmel bir uygunluk göstermediğinden dolayı, SIG bu standarda birtakım modifikasyonlar adapte etmiştir. Bu eklemeler ve değişiklikler arasında şunlar bulunmaktadır:

Veri çerçeve adaptasyonları: Bluetooth haberleşmesi L2CAP kullanımı yüzünden bir paket yapısına dayandığı için, TS 07.10 tarafından belirlenen bazı veri çerçeve içerikleri RFCOMM için gerekli olmamaktadır. Örneğin TS 07.10 da belirtilen çerçeve kısıtlayıcı bayraklar, RFCOMM da yoktur.

Bağlantı kurulumu ve sonlanması: Bluetooth haberleşmesinin protokol yapısında kendi bağlantı yönetimi olduğu için, TS 07.10 nin bağlantı yönetim fonksiyonları RFCOMM için gereksizdir.

Çoğullama: RFCOMM TS 07.10 için belirlenmiş olan bir çoklu kanal alt takımını (subset) ve bazı TS 07.10 çoğullama kontrol komutlarını kullanmaktadır.

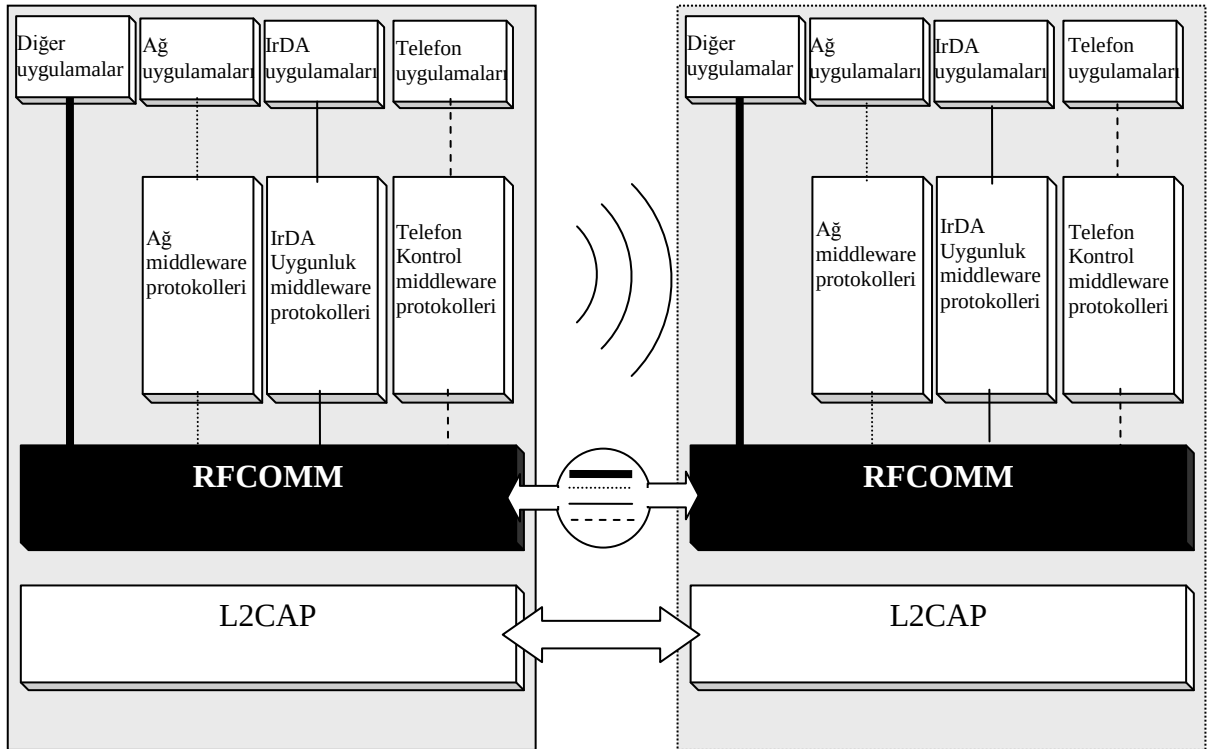
Uygulanabilirlik: RFCOMM spesifikasyonu TS 07.10 standardı için seçime bağlı olan bir çok özelliğin desteklenmesini zorunlu kılar. Bu özellikler, seri bağlantının durum ve konfigürasyon bilgisini değış tokuş etmek, seri port ile kanal ayarlarını görüşmek (negotiate) ve seri port durumunu almak gibi özellikleri içerir. Bluetooth uygulamaları için bu fonksiyonlar oldukça kullanışlıdır ve hava arabiriminin verimli kullanımı için gereklidir.

Akış kontrolü: Tipik seri port veri transferini XON/XOFF hız denetimi (pacing) veya DTR işaret hız denetimi (pacing) kullanarak denetler. RFCOMM için Bluetooth protokol yığnına özel akış kontrol mekanizmaları tanımlanmıştır. Çoğullanmış tüm RFCOMM kanallarına ve tek kanal başına hız denetimine (pacing) uygulanan akış kontrol mekanizmaları mevcuttur.

4.6.2 RFCOMM Protokol Özellikleri

RFCOMM iki cihaz arasında lojik seri bir link kurmak için bir L2CAP bağlantısı kullanır. Özellikle iki cihazdaki iki RFCOMM varlığı arasında bağlantı kurmak için

bir L2CAP bağlantı yönelimli kanal kurulur. İki cihaz arasında sadece bir tek RFCOMM bağlantısı kurulmasına izin verilmektedir, fakat bu bağlantı çoğullanarak cihazlar arasında çoklu lojik seri linkler kurulması sağlanabilir. Birinci RFCOMM istemcisi L2CAP üzerinden RFCOMM bağlantısı kurar, mevcut bağlantının diğer kullanıcıları mevcut link üzerinden yeni kanallar kurmak için RFCOMM un çoğullama özelliklerini kullanabilirler. Son RFCOMM seri linkini kullanacak son kullanıcı RFCOMM bağlantısını ve dolayısıyla L2CAP bağlantısını sona erdirmelidir. Her çoğullanmış link, bir “Veri Linki Bağlantı Tanıtıcısı” (DLCI) ile numaralandırılmıştır. Şekil 4.36 L2CAP üzerinde RFCOMM kullanan çoğullanmış seri haberleşme linklerini göstermektedir. RFCOMM un değişik istemcileri birbirlerinden DLCI değeri ile ayırdedilebilen sadece kendi emüle edilmiş seri portlarını görmektedir. (Farklı DLCI numaraları şekilde farklı çizgi tipleri ile gösterilmiştir.) Bu ayrı kanallar daha sonra RFCOMM linki üzerinden çoğullanmakta ve L2CAP bağlantısı üzerinden taşınmaktadır.



Şekil 4.36 L2CAP üzerinde RFCOMM kullanan çoğullanmış seri haberleşme linkleri

Bluetooth spesifikasyonu tek bir RFCOMM bağlantısı üzerinden 60 çoğullanmış lojik seri kanala kadar izin vermektedir fakat bu ölçüde bir çoğullamayı uygulamalar için zorunlu kılmaz. Birçok taşınabilir cihaz için çok sayıda eş zamanlı seri linkin

kullanılması gerekmez. Birçok cihaz belirli sayıda profili destekler, bu durum cihazlar için protokol yığınının nasıl uygulanacağını ve desteklenen RFCOMM seri link sayısı gibi tasarım parametrelerini belirleyici bir faktördür. Ağ erişim noktaları gibi cihazlar ise taşınabilir cihazların Bluetooth kablosuz haberleşmesini kullanarak internet gibi geniş ağlara erişmelerini sağlarlar. Örneğin LAN Erişim Profili, RFCOMM üzerinden PPP kullanmayı sağlar, bu sebeple bir LAN erişim noktası birçok cihaza aynı anda seri bağlantıya ihtiyaç duyabilir. RFCOMM spesifikasyonu bu tarz bir kullanımı birden fazla çoğullama oturumuna izin vererek sağlar. Bu işleyiş ise L2CAP in çoğullama özellikleri kullanılarak gerçekleştirilir.

RFCOMM spesifikasyonu RFCOMM un desteklediği iki farklı cihaz çeşidi ile ilgili bir tartışma içerir: haberleşme son noktası (bilgisayar ya da çevre birimi gibi cihazlar) ve haberleşme orta noktası (modem gibi cihazlar). Genel seri haberleşmede bu tip cihazlar sırasıyla veri terminal cihazı (DTE) ve veri haberleşme cihazı (DCE) olarak adlandırılırlar. RFCOMM bu tip cihazlar arasındaki farkı ayırtedemez. RFCOMM bu farkları ayırtetmeden, standart bir seri kabloda olduğu gibi direk seri bağlantı veya modem operasyonu için konfigüre edilebilir. RFCOMM DCE haberleşmeyi desteklemek için özelliklere sahiptir, bu özellikler DTE haberleşmeye uygulanamaz. RFCOMM her iki tipi de aralarındaki farkı ayırtetmeye gerek duymaksızın destekler.

Kablolu seri bağlantılar kabloda belli sayıda işarete sahiptirler (RS-232 için tüm uygulamalarda gerekmemesine rağmen genellikle 9 işaret kullanılır). Bluetooth kablosuz haberleşmesinde iletim ortamı kablo yerine hava olduğu için bu işaretlere gerek yoktur. TS 07.10 da tanımlandığı gibi çoğullanmış bir ortamda her bir seri kanalın kendi kontrol ve veri işaretleri ile farklı bir birim olarak görülmesi talep edilebilir. Bu yüzden kablolu ortamda bile seri işaretleri çoğullamak için bir plana ihtiyaç duyulur. TS 07.10 ve RFCOMM bu gereksinimi verinin iletildiği kanal boyunca bir kontrol kanalı tanımlayarak gerçekleştirirler. Standart bir RS-232 arabirimi ile yapıldığı gibi işaret seviyelerini ayarlamak ve görüntülemek yerine, RFCOMM çoğullanmış seri arabirimin durumu hakkında bilgi almak için komut ve cevaplar kullanır (böylece RS-232 işaretleri sanal hale getirilmiş olur).

RS-232 işaretler ile temsil edilmeyen başka durumlar da tanımlar. Bunlar arasında en önemlisi veri alıp göndermekte kullanılan bilgi akış hızı (baud rate) veya saat frekansıdır. Standart kablolu seri haberleşmede bir saat iletilecek işaret ile ilgili

zamanı ve 0/1 bit paternini tanımlayan alçak ve yüksek seviyeleri yönetir. Arabirimin her iki tarafı da veriyi doğru yorumlamak için aynı saat frekansını kullanmalıdır. Kablosuz ortamlar için kablo yoktur ve bu sebeple belli frekansta vurum yapacak (pulse) bir işaret kanalı da yoktur. Buna rağmen Bluetooth teknolojisi, temelbant seviyesinde hava arabirimi üzerinden haberleşme sağlamak için saat zamanlamaları kullanır. RFCOMM protokol katmanında iletim katmanlarının üzerinde yer aldığı için, alt katmanlar tarafından kullanılan iletim ortamı ve paket yapısını kullanır. Bluetooth kablosuz haberleşmesinde kullanılan bilgi akış hızı (baud rate) hava arabirimi üzerinden gönderilen paket tipleri ve yapıları tarafından belirlenir. Gerçek haberleşme RFCOMM katmanında belirlenen bilgi akış hızına (baud rate) bakılmaksızın temelbant protokolü tarafından belirlenen bilgi akış hızında (baud rate) gerçekleşir. Bir uygulama ya da RFCOMM un başka bir istemcisi bir bilgi akış hızı (baud rate) belirleyebilmesine rağmen bu değerler gerçek veri hızını belirlemez. Birçok durumda, Bluetooth kablosuz haberleşmesi kullanan bir veri iletim hızı, kablolu haberleşmeye göre daha hızlı olmaktadır. [2,14]

4.7 IrDA Uyumluluğu

4.7.1 Giriş

IrDA uyumluluğu sağlanmasının sebebi yazılacak uygulamaların hem RF hem de IR ortamlarında çalışmasını sağlamaktır. Bluetooth ve IrDA uygulamalarının kesişme noktası IrOBEX dir.

IrOBEX, IrDA tarafından tanımlanmış bir oturum protokolüdür. Bu protokol, uygulamaların hem Bluetooth RF teknolojisi hem de IrDA IR teknolojisini kullanabilmeleri için Bluetooth teknolojisi tarafından da kullanılmaktadır. Bluetooth ve IrDA kısa dalga kablosuz haberleşmesi için tasarlanmış olmalarına rağmen düşük seviye protokol yapıları ile ilgili olarak temel farklılıklara sahiptirler. IrOBEX (kısaca OBEX), Bluetooth tarafından benimsenen düşük seviye protokoller üzerine eşlenmiştir (mapping).

Bu bölümde IrOBEX in RFCOMM ve TCP/IP üzerine nasıl eşlendiği (mapping) anlatılmaktadır. OBEX (Object Exchange Protocol) IrDA protokol hiyerarşisi içinde yer alır ve kızıl ötesi bir link üzerinden veri objelerini değiş tokuş etmek için geliştirilmiştir. Fakat RFCOMM ve TCP/IP gibi başka iletim katmanları üzerinde de

yer alabilmektedir. TCP/IP üzerinden OBEX uygulaması OBEX protokolünü destekleyen Bluetooth cihazları için seçime bağlı bir özelliktir.

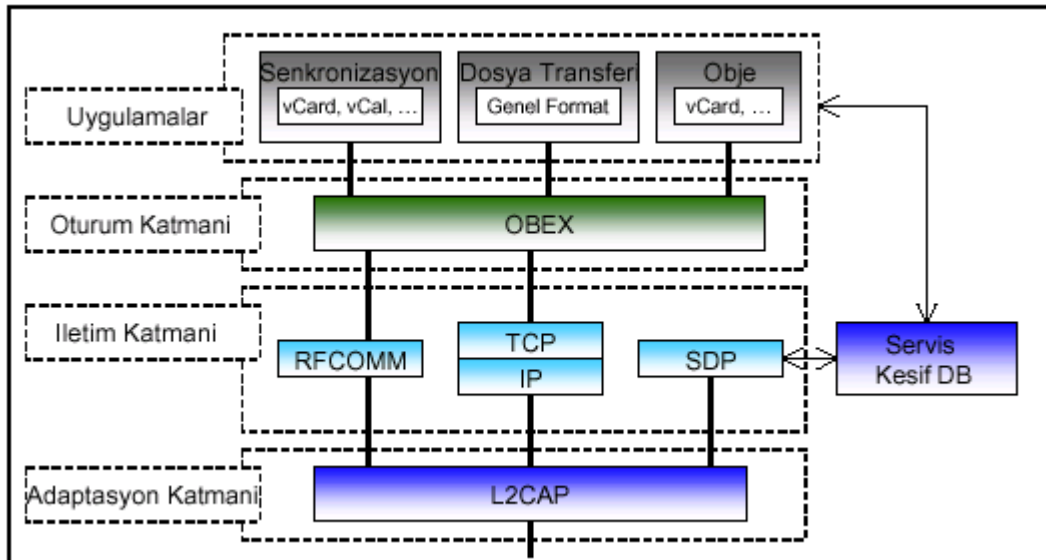
IrOBEX spesifikasyonu objeleri temsil etmek için bir model ve iki cihaz arasındaki diyalogun yapısını belirleyen bir oturum protokolü sağlar. IrOBEX protokolü çeviri formatı için bir sunucu/istemci talep-cevap örneği kullanır.

Bluetooth sadece bağlantı yönelimli OBEX i kullanırken, IrDA bağlantısız OBEX i de kullanır. Bağlantı yönelimli kullanım sebepleri şunlardır:

- OBEX, Bluetooth protokol yapısında bağlantı yönelimli protokoller üzerine eşlenmiştir (mapping).
- OBEX ve Bluetooth kullanan birçok uygulama profili bağlantı yönelimli yapıya ihtiyaç duyar.
- Bağlantı yönelimli OBEX ile birlikte kullanılacak bağlantısız OBEX istenmeyen uyumluluk sorunlarına yol açabilir.

4.7.1.1 OBEX ve Bluetooth Mimari Yapısı

Şekil 4.37 Bluetooth protokol yapısının bir kısmını, OBEX protokolünün yerini ve bu protokolü kullanan uygulama profillerini göstermektedir. Şekilde gösterilmemiş olmasına rağmen, protokoller servis keşif veri tabanı ile de haberleşebilirler.



Şekil 4.37 Bluetooth protokol yapısında OBEX protokolünün yeri

Bluetooth sisteminde OBEX protokolünün amacı veri objelerinin deęiř tokuřunu olanaklı kılmaktır. Tipik bir obje itme řeklinde gerekleřen rnek, iř kartı transferi olabilir. Biraz daha kompleks bir rnek olarak ise birden fazla cihaz zerindeki takvimleri OBEX kullanarak senkronize etmek verilebilir. Dosya transferi uygulamaları da OBEX kullanarak gerekleřtirilebilir. Objeye itme ve senkronizasyon uygulamalarında ierik formatları vCard, vCalender, vMessage ve vNotes olabilir. Bu formatlar sırası ile elektronik iř kartı, elektronik takvim ve programlama, elektronik mesaj ve e-posta ile elektronik not formatlarını belirler.

4.7.1.2 Bluetooth OBEX ile İliřkili Spesifikasyonlar

Bluetooth spesifikasyonu OBEX ve OBEX kullanan uygulamalar ile ilgili beř farklı spesifikasyon ierir:

1. Bluetooth IrDA Uyumluluk Spesifikasyonu (bu dokümanda anlatılan spesifikasyon)
 - a. Uygulamaların hem Bluetooth hem de IrDA zerinde nasıl alıřabileceğini tanımlar.
 - b. OBEX in RFCOMM ve TCP/IP zerine nasıl eřleneceğini (mapping) belirler.
 - c. Bluetooth zerinde OBEX kullanan uygulama profillerini tanımlar.
2. Bluetooth Genel Objeye Deęiř Tokuř Profili Spesifikasyonu
 - a. OBEX kullanan uygulama profilleri iin genel uyumluluk spesifikasyonudur.
 - b. Alt protokol katmanlarının (rneğin temelbant ve LMP) uygulama profilleri iin uyumluluk gereksinimlerini tanımlar.
3. Bluetooth Senkronizasyon Profili Spesifikasyonu
 - a. Senkronizasyon uygulamaları iin uygulama profilidir.
 - b. Senkronizasyon uygulama profili ile alıřacak uygulamaların uyumluluk gereksinimlerini tanımlar.
 - c. Temelbant, LMP, L2CAP ya da RFCOMM iin gereksinimleri tanımlamaz.

4. Bluetooth Dosya Transfer Profili Spesifikasyonu

- a. Dosya transferi uygulamaları için uygulama profilidir.
- b. Dosya transferi uygulama profili ile çalışacak uygulamaların uyumluluk gereksinimlerini tanımlar.
- c. Temelbant, LMP, L2CAP ya da RFCOMM için gereksinimleri tanımlamaz.

5. Bluetooth Obje İtme Profili Spesifikasyonu

- a. Obje itme uygulamaları için uygulama profilidir.
- b. Obje itme uygulama profili ile çalışacak uygulamaların uyumluluk gereksinimlerini tanımlar.
- c. Temelbant, LMP, L2CAP ya da RFCOMM için gereksinimleri tanımlamaz.

4.7.1.3 Diğer IrOBEX Uygulamaları

IR dışında IrCOMM ve TinyTP üzerinden de OBEX uygulanabilir. Bluetooth teknolojisi bu protokolleri OBEX için iletim protokolleri olarak tanımlamamıştır fakat istenirse bağımsız yazılım üreticileri tarafından desteklenebilirler.

4.7.2 OBEX Objesi ve Protokolü

4.7.2.1 Obje

OBEX obje modeli, OBEX objelerinin nasıl prezente edileceğini tanımlar. OBEX protokolü objeleri “Yerleştirme ve Alma” fonksiyonları ile transfer eder. Bir obje bir veya birden fazla Yerleştirme-talebi ve Alma-cevabı ile değiş tokuş edilebilir.

Bu model hem objenin kendisi hem de obje ile ilgili bilgiler (örneğin tip bilgisi) hakkında işlem yürütür. Bir başlık ID si ve değerinden oluşan başlıklardan meydana gelir. Başlık ID si başlık içeriğinin ne olduğu ve formatı hakkında bilgi verir. Başlık değeri ise Başlık ID si tarafından belirlenir ve bir veya daha çok byte uzunluğundadır. Kullanılan bazı özel başlıklar şunlardır: Sayı, İsim, Tip, Uzunluk, Zaman, Tanımlama, Hedef, HTTP, Body, Body sonu, Who, Bağlantı ID si, Uygulama Parametreleri, Doğrulama Cevabı, Obje Sınıfı ve kullanıcı tarafından tanımlanan başlıklar.

4.7.2.2 Oturum Protokolü

OBEX işlemleri cevap-talep çiftleri halinde şekil alır. Talepler istemci, cevaplar ise sunucu tarafından üretilir. İstemci bir talep gönderdikten sonra, sunucudan cevap gelmeden yeni bir talepte bulunamaz. Her bir talep paketi bir byte lık bir op kodu, iki byte lık uzunluk göstergesi ve operasyona göre talep edilen ya da opsiyonel olan veri den oluşur. Her bir cevap paketi de bir byte lık bir op kodu, iki byte lık uzunluk göstergesi ve operasyona göre talep edilen ya da opsiyonel olan veriden oluşur.

Aşağıdaki bölümlerde genel olarak OBEX operasyonları anlatılmıştır:

Bağlantı Operasyonu

Bir uygulama bir OBEX objesini ilk defa göndermek istediğinde OBEX oturumu başlamış olur. Bir OBEX istemcisi OBEX bağlantısının kurulmasını başlatır. Oturum bağlantı talebinin gönderilmesi ile başlar.

Tablo 4.7 OBEX oturumu bağlantı talep formatı

Byte 0	Byte 1 ve 2	Byte 3	Byte 4	Byte 5 ve 6	Byte 7 - n
0x80 (op kodu)	Bağlantı talebi paket uzunluğu	OBEX versiyon numarası	Bayraklar	Maksimum OBEX paket uzunluğu	Opsiyonel başlıklar

Bu spesifikasyonda PDU lar için Big Endian formatı kullanılır. En yüksek değerli bit (MSB) en solda ve en az değerli bit (LSB) de en sağdadır.

Uzak host da, bağlantı talebi OBEX sunucu üzerinden alınır. Sunucu başarılı cevabı istemciye göndererek bağlantıyı kabul eder. İstemciye gönderilen başka bir cevap (örneğin başarısız bir cevap) bağlantı kurulumunda bir hata olduğunu gösterir.

Tablo 4.8 OBEX oturumu bağlantı cevap formatı

Byte 0	Byte 1 ve 2	Byte 3	Byte 4	Byte 5 ve 6	Byte 7 - n
Cevap kodu	Bağlantı cevabi paket uzunluğu	OBEX versiyon numarası	Bayraklar	Maksimum OBEX paket uzunluğu	Opsiyonel başlıklar

5. ve 6. byte lar sunucu tarafından alınabilecek maksimum OBEX paket uzunluğunu tanımlar. Bu değer istemcinin alabileceği paket uzunluğu değerinden farklı olabilir. Bağlantı talebi ve cevap paketlerinin her biri tek bir paket şeklinde olmalıdır.

Bir bağlantı kurulduktan sonra, sonlanma talep ve cevapları olmadığı ya da bir hata (örneğin her OBEX objesi tamamen transfer edildikten sonra bağlantı otomatik olarak sonlanmamışsa) oluşmadığı sürece devam eder.

Bağlantı Sonu Operasyonu

Bir OBEX oturumunun sonlanması, bir uygulama sona erdiğinde veya uygulama hostu değiştirmek istediğinde gerçekleşir. İstemci bağlantı sonu operasyonunu sunucudan talep eder.

Tablo 4.9 OBEX oturumu bağlantı sonu talep formatı

Byte 0	Byte 1 ve 2	Byte 3
0x81	Paket uzunluğu	Opsiyonel başlıklar

Bu talep sunucu tarafından reddedilemez. Bu sebeple cevap göndermek zorundadır.

Tablo 4.10 OBEX oturumu bağlantı sonu cevap formatı

Byte 0	Byte 1 ve 2	Byte 3
0xA0	Cevap paket uzunluğu	Opsiyonel cevap başlıkları

Yerleştirme Operasyonu

İstemci ile sunucu arasında bağlantı kurulduğunda istemci sunucuya OBEX objelerini itebilir. Yerleştirme-talebi bir OBEX objesini itmek için kullanılır.

Tablo 4.11 OBEX oturumu yerleştirme talep formatı

Byte 0	Byte 1 ve 2	Byte 3
0x02 (0x82 Son bit düzeni durumunda)	Paket uzunluğu	Başlık dizisi

Bir Yerleştirme-talebi transfer edilecek objenin ve paket boyutunun büyüklüğüne bağlı olarak bir veya birden fazla paketten oluşabilir. Alınan her Yerleştirme-talebi için sunucunun bir cevap paketi göndermesi gereklidir. Bu sebeple tek bir cevabın bir OBEX objesine ait olmalarına rağmen birden fazla paket için gitmesine izin verilmez.

Tablo 4.12 OBEX oturumu yerleştirme cevap formatı

Byte 0	Byte 1 ve 2	Byte 3
Cevap kodu	Cevap paket uzunluğu	Opsiyonel cevap başlıkları

Alma Operasyonu

İstemci ile sunucu arasında bağlantı kurulduğunda istemci sunucudan OBEX objelerini çekebilir. Alma-talebi bir OBEX objesini çekmek için kullanılır.

Tablo 4.13 OBEX oturumu alma talep formatı

Byte 0	Byte 1 ve 2	Byte 3
0x03 (0x83 Son bit düzeni durumunda)	Paket uzunluğu	İsim ile başlayan başlık dizisi

Objeler bir başlıklar dizisi şeklinde alınır. İstemci her cevap paketi için bir talep paketi göndermek zorundadır.

Tablo 4.14 OBEX oturumu alma cevap formatı

Byte 0	Byte 1 ve 2	Byte 3
Cevap kodu	Cevap paket uzunluğu	Opsiyonel cevap başlıkları

Diğer Operasyonlar

Diğer OBEX operasyonları SetPath ve Abort operasyonları içerir. İstemci her cevaptan sonra bir talep/cevap sürecinin ortasında olursa bile bir Abort talebi gönderebilir. Bu sebeple bütün OBEX objesi bir Abort talebi göndermeden önce alınmak zorunda değildir. Bu operasyonlara ek olarak IrOBEX spesifikasyonu kullanıcı-tanımlı operasyonlara da yer verir ancak bu operasyonların Bluetooth'a adaptasyonlarına gerek yoktur.

4.7.3 RFCOMM Üzerinde OBEX

Bu bölümde OBEX in RFCOMM üzerinde nasıl eşlendiği (mapping) açıklanmıştır. OBEX protokolünü destekleyen Bluetooth cihazları şu gereksinimleri sağlamalıdır:

1. OBEX destekleyen cihaz istemci, sunucu olarak veya her ikisi yerine de çalışabilmelidir.
2. Bir cihaz üzerinde eş zamanlı olarak çalışan bütün sunucular yarı RFCOMM sunucu kanalları kullanmalıdır.
3. OBEX kullanan uygulamalar (servis/sunucu) servis keşif veri tabanına uygun bilgileri kayıt etmelidir. Değişik uygulama profillerine ait olan bu bilgiler profil spesifikasyonlarında belirlenmiştir.

4.7.3.1 RFCOMM Üzerinde OBEX Sunucu Başlangıcı

İstemci bir bağlantı talebi gönderdiğinde, sunucunun talepleri almaya hazır olduğunu varsaymaktadır. Fakat sunucunun alma konumuna hazır olmasından önce bazı ön şartlar yerine getirilmelidir:

1. Sunucu bir RFCOMM sunucu kanalı açmalıdır.
2. Sunucu servis keşif veri tabanına yeteneklerini kaydetmelidir.

Bu aşamadan sonra, diğer hostlar ihtiyaç duyulursa sunucuyu bulabilirler ve sunucu da istemcilerden gelen talepleri dinleyebilir.

4.7.3.2 Seri Porttan OBEX Paketlerini Almak

Bir obje bir veya birden fazla Yerleştirme-talebi veya Alma-cevabı üzerinden değiş tokuş edilebilir (obje bir veya daha çok paket halinde alınabilir). Fakat OBEX direkt olarak seri port üzerinde çalışıyorsa, RFCOMM dan gelen paketleri alamaz. Onun yerine RFCOMM tarafından emüle edilen bir seri port tan bir byte dizisi alınır.

Byte dizisindeki paketleri algılamak için, OBEX paketin talep veya cevap paketi olduğuna bağlı olarak op kodları veya cevap kodlarına bakar. Op kodları ve cevap kodu paketlerin başlangıç bayrakları olarak düşünülebilir. OBEX paketlerinde, paketin sonunu belirleyen bir “bitiş bayrağı” bulunmaz. Fakat op kodu veya cevap kodundan sonraki iki byte da paketin uzunluk bilgisi bulunur. Böylelikle paketin toplam uzunluğu bilinmiş olur.

Tanımlanmayan veriler atılmalıdır. Bu durum bir senkronizasyon problemine yol açabilir fakat OBEX protokolünün doğal yapısı göz önünde tutularak, RFCOMM üzerinden problem olmaz.

4.7.3.3 Bağlantının Kurulması

İstemci bağlantı kurulumunu başlatır. İlk veri talebini göndermeden önce aşağıdaki adımlar izlenmelidir:

1. SDP spesifikasyonunda belirtilen SD protokolü kullanılarak, istemci bağlantı kuracağı sunucu ile ilgili uygun bilgiyi (örneğin RFCOMM kanalını) keşfeder.
2. İstemci RFCOMM bağlantısı kurabilmek için RFCOMM kanalını keşfeder
3. İstemci OBEX oturumu kurmak için sunucuya Bağlantı-talebini gönderir. Sunucudan “başarılı” cevabı alınırsa oturum kurulur.

4.7.3.4 Bağlantının Çözülmesi

RFCOMM üzerinden OBEX oturumunun sonlanması işlemi Bağlantı sonu-talebi ile gerçekleştirilir. İstemci cevabı aldığı da OBEX istemcisine atanan RFCOMM kanalı kapatılır.

4.7.3.5 RFCOMM Üzerinden OBEX Paketlerini İtmek ve Çekmek

OBEX paketlerindeki veriler Yerleştirme-talebi kullanılarak RFCOMM üzerinden itilirler. Her talepten sonra, bir sonraki talebin itilebilmesi için cevap beklenir.

Uzak bir host dan veri çekmek ise Alma-talebi gönderilmesi ile mümkün olur. Çekilen veri OBEX cevap paketlerine ulaşır. Her cevaptan sonra daha çok veri çekmek için yeni bir talep gönderilmelidir.

4.7.4 TCP/IP Üzerinden OBEX

Bu bölümde OBEX in TCP/IP üzerinden nasıl eşlendiği (mapping) açıklanmıştır. TCP/IP üzerinden OBEX protokolünü destekleyen Bluetooth cihazları şu gereksinimleri sağlamalıdır:

1. OBEX destekleyen cihaz istemci, sunucu olarak veya her ikisi yerine de çalışabilmelidir.
2. Sunucu için IANA tarafından belirlenen TCP port numarası 650 tahsis edilmiştir. Eğer atanan bir numara istenmiyorsa, port numarası 1023 ten büyük bir değer alabilir. Fakat IANA tarafından tanımlanan TCP port

numarası (650) nin kullanılması tavsiye edilmektedir. 0-1023 arası numaralar IANA tarafından rezerve edilmiştir.

3. İstemci mutlaka kendi tarafında 0-1023 arasında olmayan bir port numarası kullanmalıdır.
4. OBEX kullanan uygulamalar (servis/sunucu) servis keşif veri tabanına uygun bilgileri kayıt etmelidir. Değişik uygulama profillerine ait olan bu bilgiler profil spesifikasyonlarında belirlenmiştir.

4.7.4.1 TCP/IP Üzerinde OBEX Sunucu Başlangıcı

İstemci bir Yerleştirme veya Alma talebi gönderdiğinde, sunucunun talepleri almaya hazır olduğunu varsaymaktadır. Fakat sunucunun alma konumuna hazır olmasından önce bazı ön şartlar yerine getirilmelidir:

1. Sunucu 650 numaralı veya 1023 ten büyük numaralı bir TCP portu açmalıdır.
2. Sunucu servis keşif veri tabanına yeteneklerini kaydetmelidir.

Bu aşamadan sonra, diğer cihazlar ihtiyaç duyulursa sunucuyu bulabilirler ve sunucu da istemcilerden gelen talepleri dinleyebilir.

4.7.4.2 Bağlantının Kurulması

İstemci bağlantı kurulumunu başlatır. İlk veri talebini göndermeden önce aşağıdaki adımlar izlenmelidir:

1. SDP spesifikasyonunda belirtilen SD protokolü kullanılarak, istemci bağlantı kuracağı sunucu ile ilgili uygun bilgiyi (örneğin TCP port numarası) keşfeder.
2. İstemci 1023 ten büyük numaralı bir TCP port ile ilişkilendirdiği bir soketi başlangıç durumuna getirir (initialize) ve sunucu host u ile bir TCP bağlantısı kurar.
3. İstemci OBEX oturumu kurmak için sunucuya Bağlantı-talebini gönderir. Sunucudan “başarılı” cevabı alınırsa oturum kurulur.

4.7.4.3 Bağlantının Çözülmesi

TCP üzerinden OBEX oturumunun sonlanması işlemi Bağlantı çözülmesi-talebi ile gerçekleştirilir. İstemci cevabı aldığı da OBEX istemcisine atanan TCP portu kapatılır.

4.7.4.4 TCP Üzerinden OBEX Paketlerini İtmek ve Çekmek

OBEX paketlerindeki veriler Yerleştirme-talebi kullanılarak TCP üzerinden itilirler. Her talepten sonra, bir sonraki talebin itilebilmesi için cevap beklenir.

Uzak bir host dan veri çekmek ise Alma-talebi gönderilmesi ile mümkün olur. Çekilen veri OBEX cevap paketlerine ulaşır. Her cevaptan sonra daha çok veri çekmek için yeni bir talep gönderilmelidir.

4.7.5 OBEX Kullanan Bluetooth Uygulama Profilleri

Bluetooth SIG, OBEX kullanan üç farklı uygulama profili tanımlamıştır:

4.7.5.1 Senkronizasyon

Senkronizasyon temel olarak iki obje deposunu karşılaştırmak, farklılıklarını belirlemek ve bu iki obje deposunu aynı duruma getirmektir. Senkronizasyon destekleyen Bluetooth cihazları PC ler, diz üstü bilgisayarlar, PDA ler, cep telefonları veya akıllı telefonlardır.

Bluetooth Senkronizasyon profili IrDA tarafından belirlenen IrMC senkronizasyonu ile uyumlu olan istemci ve sunucuları kullanır. Bu istemci ve sunucular IrMC spesifikasyonunda belirtilen 4. seviye senkronizasyon fonksiyonaltısını desteklemelidir.

İstemci cihazdaki senkronizasyon algoritmalarını proses eden senkronizasyon devrelerinin çalışma mantığı uygulamaya göre değişir. Bu sebeple yazılım üreticilerine bırakılmıştır.

Senkronizasyon bir tip uygulama ile sınırlandırılmamıştır. Dört değişik uygulama sınıfı olanaklı hale getirilmiştir:

1. Telefon Defteri: Kullanıcının kişisel kayıtlarını kolaylıkla yönetmesini sağlar.
2. Takvim: Kullanıcının takvim içeriğini ve görev listesini yönetmesini sağlar.
3. Mesajlaşma: Kullanıcının mesajlarını (örneğin e-postalarını) yönetmesini sağlar.
4. Notlar: Kullanıcının notlarını yönetmesini sağlar.

Bluetooth Senkronizasyon profilinin uyumluluk gereksinimleri Senkronizasyon Profili ve Genel Obje Değiş Tokuş Profili'nde açıklanmıştır.

4.7.5.2 Dosya Transferi

Dosya Transferi profili Bluetooth cihazından dosya almak ve göndermek için kullanılmaktadır. Dosya Transferi profili uzak Bluetooth cihazının dosya dizininde tarama yapmak (browse) için de kullanılır.

Bluetooth Dosya Transferi profilinin uyumluluk gereksinimleri Dosya Transfer Profili ve Genel Obje Değiş Tokuş Profili'nde açıklanmıştır.

4.7.5.3 Obje İtme

Obje İtme profili objeleri yaymak ve opsiyonel olarak çekmek için kullanılmaktadır ve Dosya Transfer Profili'nin özel bir şeklidir. En azından iş kartı değiş tokuş işlemini yerine getirmek için kullanılır fakat sadece bununla da sınırlı değildir.

Bluetooth Obje İtme profilinin uyumluluk gereksinimleri Obje İtme Profili ve Genel Obje Değiş Tokuş Profili'nde açıklanmıştır. [15]

4.7.6 IrDA ve Bluetooth

Bluetooth ve IrDA kendilerine özel zayıf ve kuvvetli tarafları olan benzer iki teknolojidir. Yapılan bu karşılaştırma ile verilen bir uygulama için hangi teknolojinin daha doğru bir seçim olduğuna karar verilmesi amaçlanmıştır. Her iki teknolojiye ilişkin kısa açıklamalar ve kullanım modeli örnekleri ile teknolojiler arasındaki farklar ve kesişim noktaları verilmiştir. Ayrıca uygulama geliştirme maliyetleri ve düzenleme gereksinimleri üzerinde de durulmuştur.

İlk bakışta, teknolojik olarak IrDA ve Bluetooth teknolojilerinin birbirleriyle rekabet içinde oldukları sanılabilir. Analistler de kısa-dalga kablosuz haberleşme sağlayan bu iki teknolojinin her ikisinin de yaşayıp yaşamayacağını merak etmişlerdir. Her iki teknolojinin de faydaları incelendiği zaman ikisinin ayrı ayrı önemli olduğu anlaşılmaktadır. İkisinin de avantaj ve dezavantajları mevcuttur. Bluetooth ve IrDA birlikte oldukça güçlü bir kablosuz haberleşme imkanı sağlarlar.

4.7.6.1 IrDA ye Genel Bakış

Infrared Data Association (IrDA) üç kızıl ötesi haberleşme standardı tanımlar: IrDA-Veri, IrDA-Kontrol ve yeni bir standart olan AIr. Burada IrDA-Veri ve onun Bluetooth ile olan ilişkisi üzerinde durulmaktadır. Bu sebeple IrDA terimi IrDA-Veri terimi yerine kullanılacaktır. IrDA genellikle haberleşme için kablo kullanan cihazlar

için kablosuz haberleşme imkanı sağlar. IrDA 0-1m. lik bir mesafede ve 9600 bit/sn.-16 Mbit/sn. bir hız dilimi çerçevesinde çalışan; noktadan noktaya, dar açılı (30° koni), anlık (ad hoc) bir veri iletim standardıdır.

Genel IrDA Karakteristikleri

- Dünya çapında kanıtlanmış genel kablosuz haberleşme standardı
- 50 milyondan fazla üniteye var olma
- Geniş bir donanım ve yazılım platformu desteği
- Noktadan-noktaya kablo haberleşmesinin yerine geçmek üzere yapılan tasarım
- Geriye dönük standartlarla uyumluluk
- Dar açılı (30°) koni, hedefle ve vur stili uygulamalar (Diğer elektronik cihazlarla girişimsiz ve sabit cihazlar için düşük seviyeli güvenlik)
- Yüksek veri hızları (şu anda 4 Mbit/sn. olup, 16 Mbit/sn. üzerinde çalışılmaktadır.)

IrDA Ne İçin Kullanılır?

IrDA aşağıdaki cihazlar arasında veri haberleşmesi sağlamak için kullanılır:

- Diz üstü bilgisayar, bilgisayar ve el bilgisayarları
- Yazıcılar
- Telefonlar ve çağrı cihazları
- Modemler
- Kameralar
- LAN erişim cihazları
- Medikal ve endüstriyel cihazlar
- Saatler

Dünya Çapında Kabul Görme

IrDA dünyada şu an 150 milyondan fazla çalışan ve yılda %40 artış gösteren cihaz sayısı ile, oldukça fazla sayıda kişisel bilgisayarda, çevre biriminde ve birçok değişik cihazda kullanılan kabul görmüş bir teknolojidir. Dünya çapında gördüğü kabul sayesinde IrDA donanımsal olarak cihazlarda standart hale gelmekte ve yazılımlarla da uyumluluk sağlamaktadır.

4.7.6.2 Bluetooth'a Genel Bakış

Bluetooth kısa-dalga, tek noktadan çok noktaya ses ve veri transferi için kullanılan bir RF teknolojisidir. Bluetooth katı, metal olmayan nesnelerden de iletilebilir. Nominal link kademesi 10 cm. den 10 m. ye kadardır fakat iletim gücü artırılarak bu uzaklık 100 m. ye kadar çıkarılabilir. Bluetooth düşük maliyetli bir kısa-dalga radyo linki temeline dayandırılmıştır. Sabit ve mobil haberleşme cihazları için anlık (ad hoc) bağlantıları kolaylaştırır.

Genel Bluetooth Karakteristikleri

- 2.4 GHz. ISM bandında çalışır.
- Saçılmış frekans atlama (Frequency Hop = FH) spektrumu kullanır. Bu spektrum frekans bandını atlama (hop) kanallarına ayırır. Bir bağlantı sırasında, Bluetooth alıcı-vericileri bir kanaldan diğerine atlarlar.
- Bir piconette (bir kanalı paylaşan iki veya daha çok Bluetooth cihazı) en fazla 8 cihaz bulunabilir.
- Güvenlik gereksinimlerini sağlar.
- Işık hizalamasına gerek duymaz. Duvar vs..gibi yapılardan etkilenmez.
- Çok yönlü haberleşme sağlar.
- Senkron ve asenkron haberleşmeyi destekler. TCP/IP ile kolay entegre olur.
- Dünya çapında hükümetler tarafından kabul edilmiştir.

Bluetooth Ne İçin Kullanılır?

Bluetooth kullanıcıların kablolarla gerek duymaksızın bilgi ve haberleşme cihazlarına erişmelerini sağlar. Hızlı, anlık (ad hoc) bağlantı sağlar ve gelecekte de muhtemelen cihazlar arasında otomatik, istemdişi bağlantı sağlayacak bir teknolojidir.

Bluetooth aşağıdaki cihazlar tarafından kullanılır (bu cihazların büyük kısmı IrDA de kullanmaktadır):

- Diz üstü bilgisayar, bilgisayar ve el bilgisayarları
- Telefonlar ve çağrı cihazları
- Modemler
- LAN erişim cihazları
- Kulaklık-mikrofon setleri

Üreticilerin Kabulü

Bluetooth taşınabilir elektronik cihazların kısa-dalga anlık (ad hoc) ağlar yardımıyla birbirlerine kablosuz olarak bağlanıp haberleşmelerini olanaklı kılar. 2.45 GHz. frekansındaki evrensel radyo arabirimi Ericsson, Nokia, IBM, Toshiba, Intel ve bunlardan başka 1700 den fazla üretici tarafından desteklenmektedir. Bluetooth lisanslanmayan bölgede ve her radyo ünitesine açık olan bir radyo frekansı gerektirmektedir. 2.45 GHz. ISM bandı bu gereksinimi karşılamakla birlikte aynı frekansı kullanan garaj kapısı açan düzenekler, telsiz telefonlar ve mikrodalga fırınlarla da olabilecek girişimle ilgili sorunları da beraberinde getirmektedir.

4.7.6.3 IrDA ve Bluetooth Uygulama Kesişmesi

IrDA için tanımlanan çoğu uygulama Bluetooth için de tanımlanmıştır. Bazı durumlarda IrDA, bazı durumlarda ise Bluetooth veri transferi için uygun olur.

Veri Alışverişi

Hem IrDA hem de Bluetooth veri alışverişi konusunu temel bir fonksiyon olarak ele almaktadır. Veri alışverişi bir mobil telefondan bir PDA ye iş kartı göndermek kadar basit bir işlem şeklinde olabildiği gibi, bir PDA ile PC arasında veri senkronizasyonu sağlamak kadar kompleks de olabilir. Bluetooth ve IrDA bu tip uygulamaları ve diğer veri alışverişi uygulamalarını destekler. Her iki teknoloji de bu uygulamaları

desteklemek için aynı üst katman protokolünü, OBEX'i, kullanırlar. Aynı protokolü kullandıkları için tek bir uygulamanın hem IrDA hem de Bluetooth üzerinde çalışması mümkün olmaktadır. İki teknolojinin de aynı uygulamaları desteklediği düşünülürse, neden ikisine de ihtiyaç olduğu sorusu akla gelebilir. Her iki teknolojinin de birbirlerine karşı avantaj ve dezavantajları bulunmaktadır.

Genel bir veri alışverişi uygulaması içinde birçok cihaz bulunan bir oda içinde gerçekleşir. Buna örnek olarak elektronik kart değiş tokuşu verilebilir. Büyük bir konferans odasında iki kişinin kartlarını değiştirmek üzere karşılaştığını düşünelim. Odada kablolu cihazı olan ve aynı şeyi gerçekleştirmeye çalışan başka insanlar da bulunmaktadır. Bu durum IrDA nin üstün olduğu durumlardan birisidir. Kısa-dalga, dar açılı IrDA “nokta hedefle ve vur” prensibi ile bu gereksinime daha iyi cevap verir. Bir kart değişme olayında kişilerin birbirlerine yakın bir mesafede olmaları ve karşılıklı durmaları kaçınılmazdır. IrDA in uzaklık ve açı limiti sayesinde diğer kişiler de girişim oluşturmaksızın haberleşebilirler. IrDA teknolojisinin doğası gereği basit bir güvenlik ve kullanım kolaylığı sağlanmış olur.

Bu durum Bluetooth'un zayıf olduğu durumlara bir örnektir. Çok-yönlü haberleşme karakteristiği sebebiyle alıcı cihazı belirlemekte güçlük çekilir. Kullanıcının basit olarak alıcı tarafı hedeflemesi mümkün olmaz. Bir Bluetooth cihazı mutlaka zaman gerektiren bir keşif süreci geçirir ve bu süreç sonunda odadaki diğer cihazların çoğunu da bulur. Hedef cihaza yakın mesafede bulunmanın çok fazla yararı olmaz. Kullanıcı keşfedilen birçok cihaz arasından bir seçim yapmak durumunda kalır. Doğru cihazı seçmek için 48-bit cihaz adresi veya isim gibi yardımcı bir bilgiye ihtiyaç duyulur. Bluetooth çok noktalı erişim kapasitesine sahip olduğu için yetkisiz erişimlere karşı bir güvenlik mekanizması kullanmak zorundadır.

Diğer veri alışverişi çözümlerinde Bluetooth daha çok tercih edilen bir çözümdür. Katı objelere penetre edebilmesi ve sağladığı maksimum mobilite özelliği sayesinde IrDA ile yapılması imkansız olan veri değişim işlemleri Bluetooth ile gerçekleştirilir. Örneğin, Bluetooth ile kişinin cep telefonu cebinde iken dahi PC ile senkronizasyon sağlanabilir (bu işlem IrDA ile mümkün değildir). Bluetooth un çok yönlülük özelliği sayesinde telefon PC nin etki alanına girdiğinde senkronizasyon başlar. Bluetooth ile yapılan senkronizasyon işleminde telefonun sabit bir lokasyonda kalması gerekmez. IrDA ile ise telefon mutlaka uygun bir pozisyonda sabit kalmalıdır.

LAN Eriřimi

Bluetooth ve IrDA in önemli ortak özelliklerinden birisi, bir cihazı kablosuz olarak, kablolu bir ağı bağlayabilmeleridir. Bluetooth'da bir ışık hizalama durumu söz konusu olmadığı için bu tip bir uygulamada kullanmak için idealdir. Bluetooth kullanıcıları özellikle bir LAN erişim noktasının konumlandırıldığı durumda IrDA'ya oranla çok daha esnek bir haberleşme olanağına sahip olurlar.

Bununla birlikte Bluetooth'un çok noktalı haberleşme altyapısı sunması da birden fazla cihazın ortamı paylaşmasına olanak sağlar. Bluetooth'un IrDA'ya oranla tek potansiyel zayıf noktası performansdır. Bluetooth'un toplam bant genişliği 1 Mbit/sn. ile sınırlıdır; IrDA ise 4 Mbit/sn. yi desteklemekte ve 16 Mbit/sn. için de geliştirilmektedir.

IrDA bir IrDA destekli cihazı kablolu bir ağı bağlarken IrLAN protokolünü kullanmaktadır. İki cihaz arasındaki mesafe ise maksimum 1 metre olmalıdır.

Çevirmeli Ağ

Taşınabilir bir bilgisayar ile bir cep telefonu arasında EIA/TIA 232 bağlantısını emüle ederek, internete çevirmeli ağ üzerinden bağlanmak; günümüzde IrDA in en çok kullanıldığı alanlardan birisidir. Aynı uygulamanın Bluetooth ile de gerçekleştirilmesi hedeflenmektedir. Bluetooth'un en büyük avantajı kullanıcı cep telefonu cebinde yürürken bile çevirmeli ağ bağlantısının devam etmesidir.

Ses Uygulamaları

Bluetooth spesifikasyonunun doğal özelliklerinden birisi senkron ses kanallarıdır. Bluetooth sayısal ses verisini taşımak için bant genişliği ayırabilir. Bir piconette en fazla üç adet simültane ve tam dubleks ses transferine imkan tanınabilir. Infrared for Mobile Communications (IrMC) spesifikasyonu, bir IrDA linki üzerinden tam dubleks ses verisini taşımak için "Gerçek Zamanlı Transfer Kontrol Protokolü" (RTCON) nı tanımlamıştır. RTCON 115.2 kbit/sn. lik IrDA linkinin tamamını bu iş için harcar ve başka bir verinin taşınmasına izin vermez. Eğer linkin uçlarındaki her iki taraf da birbirlerine göre sabit pozisyonlarda ise IrDA bu tip bir uygulamada iyi sonuç verir. En yaygın olan kullanım alanı bir araba kitinde çalışan cep telefonu örneğidir.

Güvenlik

IR ın yön ile ilgili özelliği ve gönderici ile alıcı arasındaki ışık hizalama gereksinimi sebebiyle düşük serecede bir güvenlik ile sorun yaşanmaz. Buna rağmen yansıyan ışığı dedekte edip, çevredeki gürültüyü de filtreleyerek müdahalede bulunmak mümkündür. IrDA, Bluetooth gibi güvenlik özelliklerini link katmanında sağlamaz. Bunun yerine doğrulama ve/veya şifreleme için daha yüksek katman protokollerine ve uygulamalarına dayanır.

Bluetooth çok yönlü bir teknoloji olduğu için herhangi bir yöndeki hatta görünmeyen yerlerdeki casus bir cihaz tarafından monitör edilebilir. Bluetooth temelbant protokolünde doğrulama ve şifreleme sağlayarak güvenlik sağlar. Doğrulama bir gizlilik anahtarı (şifre veya PIN) kullanan rasgele bir sayı (challenge)-cevap protokolüne sayarır. Her iki cihaz da aynı gizlilik anahtarına sahip olmalıdır. Protokol her bir cihazın diğerini doğrulamasını sağlar. Cihazlar birbirini doğruladıktan sonra transferi şifrelemek de ek bir güvenlik sağlar.

RF ve IrDA Uygulama Maliyetleri

IrDA yi son kullanıcıya yönelik cihazlarda kullanmak çok basittir. Bazı üreticiler tamamen entegre IR paketlerine sahiptirler. IrDA kontrolörleri de basittir. Cihaz üreticileri bütün bir çözümü 1\$ lar mertebesinde bir maliyetle elde edebilmektedirler. Bir cihaza IR entegrasyonu yapmak da 2\$ gibi düşük rakamlarda bir maliyet getirir.

Bluetooth cihazları halen çok yaygın olmadıkları için bir cihaza Bluetooth entegrasyonu yapmanın maliyeti değişiklik göstermekte; bununla birlikte 20\$ gibi bir rakam referans alınabilmektedir. Birkaç yıl içinde ise bu rakamın 5\$ mertebesine inmesi beklenmektedir.

IR ve RF Teknoloji Regülasyonu

IR teknolojisi genellikle regüle değildir, fakat IEC-825-1 göz güvenlik standardının bütün led tabanlı alıcı-vericilerde yer alması kesinleşmiştir. Günümüzde mevcut olan IrDA spesifikasyonları IEC kuralları çerçevesinde düzenlenmektedir. Fakat daha geniş kapsamlı ve bant genişlikli IrDA çözümleri üzerinde çalışıldığına dikkat edilmelidir.

RF tabanlı bir teknoloji olan Bluetooth ise dünya genelindeki regülasyon gruplarına tabidir. Dünya genelinde lisanslanmamış 2.45 GHz. ISM bandının Bluetooth için

kullanılmasına karar verilmiş olmasına karşılık istisnalar mevcuttur. Fransa, İspanya ve Japonya istisna uygulayan ülkeler arasındadır.

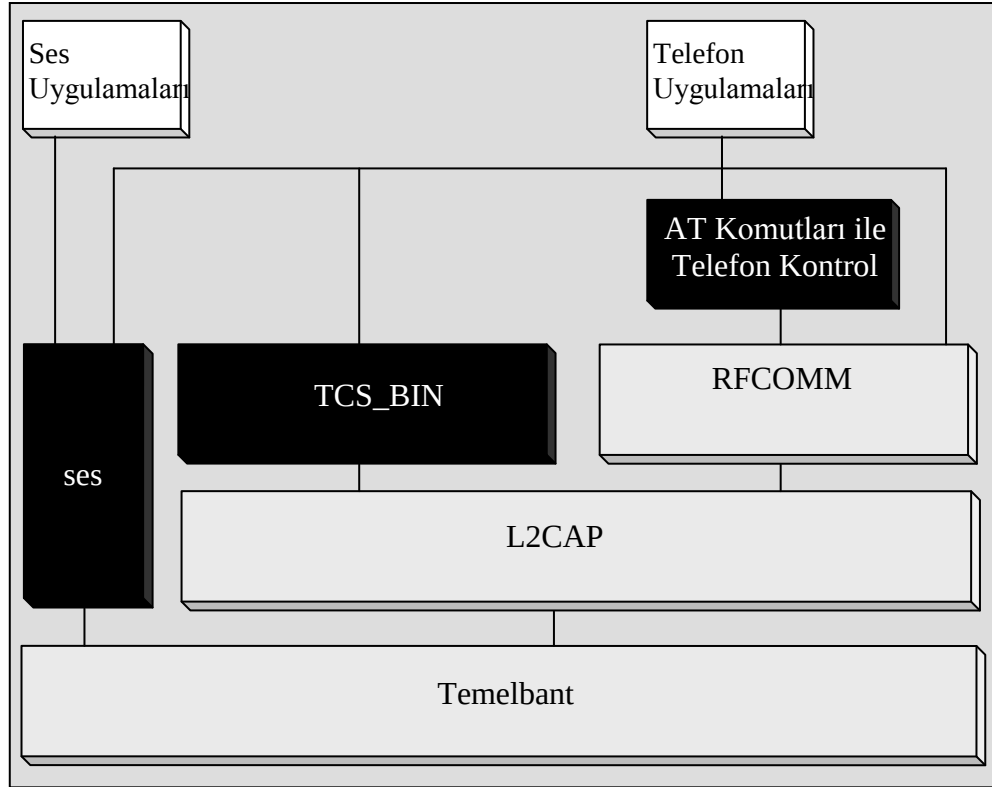
Özet

IrDA ve Bluetooth teknolojileri veri alış verişi ve ses uygulamaları için birbirini tamamlayıcı özelliklere sahiptir. Bazı cihazlar için, hem Bluetooth, hem de IrDA özelliklerine sahip olmak en mükemmel kısa-dalga kablosuz çözümü sunar. Diğer cihazlar için ise hedeflenen kullanım modeli ve uygulamalara göre karar verilmelidir. Kısa-dalga kablosuz haberleşme teknolojisi için çalışmalar devam etmektedir ve IrDA ile Bluetooth bu alandaki en önemli teknolojilerdir. [16]

4.8 Ses ve Telefon Kontrolü

Ses iletimini desteklemesi Bluetooth kablosuz haberleşmesinin ayırdedici bir özelliğidir. Hem ses hem de veri desteği ile Bluetooth teknolojisi bilgisayar ve haberleşme teknolojileri arasında avantajlı bir köprü görevi görür. Bu bölümde telefon ve ses haberleşmesini olanaklı kılan protokol katmanı incelenmiştir. Telefon kontrol protokolü TCS-BIN (kısaca TCS) ile hayata geçmekte; ses ise temelbant üzerinden taşınmaktadır. TCS mevcut ITU-T Q.931 protokolü üzerine kurulmuştur. TCS, paket tabanlı telefon kontrolü için kullanılan binary bir şifrelemedir ve L2CAP katmanının üzerinde yer almaktadır. Ses, protokol yığınının bir katmanı değildir; temelbant katmanının üzerinden direkt olarak transfer edilen özel bir paket formatıdır. Ses sıklıkla telefon uygulamaları ile ilgili olduğu için, TCS ile birlikte ele alınmaktadır.

Şekil 4.38 protokol yığınındaki ses ve TCS-BIN katmanları ile AT Komut Telefon Kontrol bileşenini göstermektedir. Bu bileşen TCS-AT olarak adlandırılır. Genel olarak sadece TCS denildiğinde protokol yığınının TCS-BIN katmanı anlaşılır. TCS-BIN L2CAP in üzerinde yer alır, ses direkt olarak temelbant ile temas halindedir ve AT komut telefon kontrolü de RFCOMM un üzerinde çalışır. Telefon kontrol uygulamaları direkt olarak TCS-BIN ile haberleşebilir ve AT komut telefon kontrolünü de kullanabilirler.



Şekil 4.38 Protokol yığınınındaki ses ve TCS-BIN katmanları ile AT Komut Telefon Kontrol bileşeni

4.8.1 Ses ve Telefon Kontrol İşleyişi

TCS-BIN telefon bağlantılarının arama kontrollerini yapmak, bağlantıları kurmak ve sona erdirmek fonksiyonları için kullanılır. TCS hem ses, hem de veri çağrılarını kontrol edebilir. TCS-BIN aralarında gerçek bir çağrı bağlantısı olmayan cihazlar arasında çağrı işaretleşme bilgisinin değiş tokuş edilmesi için bir yöntem tanımlar. Bu yöntem bağlantısız TCS adını alır. TCS-BIN in diğer bir işlevi de grup yönetimi fonksiyonlarıdır. TCS-BIN protokolünü destekleyen bir cihaz grubu olduğunda, grup üyeleri TCS tarafından tanımlanan bazı özel fonksiyonları (grup üyelik yönetimi, telefon servisi paylaşımı, iki grup üyesi arasında hızlı ve direkt bir bağlantı kurulumu gibi) kullanabilirler.

Çağrı kontrolünün ikinci şekli olan AT komut telefon kontrolü, ayrı bir protokol olarak tanımlanmamasına rağmen, birçok profil tarafından kullanılmakta ve çağrı kontrolünde başarı sağlayan bir yöntem olarak bilinmektedir. AT komutları modem kontrol komutlarıdır bir seri port üzerinden bir modemle haberleşmek üzere konfigüre edilmiş uygulamalar tarafından kullanılırlar. Bu uygulamalar RFCOMM

kullanarak da aynı işlevi yerine getirebilirler. TCS-BIN spesifikasyon içinde tanımlanan tek telefon kontrol protokolüdür ve birçok telefon profili bu protokol üzerine inşa edilmiştir. AT komut tabanlı telefon kontrolü de mikrofon-kulaklık seti, faks ve çevirmeli ağ profillerinde kullanılmaktadır.

Ses ise daha önce de belirtildiği gibi, protokol yığınının bir katmanı değildir. Sesi, iletim katmanının özel bir çeşidi şeklinde kabul edebiliriz. Ses, temelbant protokolünü kullanarak direkt hava arayüzü üzerinden alınıp gönderilebilen özel bir paket formatıdır. [17]

4.8.1.1 TCS Protokol Gelişimi

Telefon kontrolü, ses fonksiyonları ile içiçe geçmiştir. Telefon kontrolüne ihtiyaç duyulmasının en büyük sebebi ses fonksiyonlarıdır. TCS çalışma grubu kurulmadan önce, Bluetooth protokol yığınının ses desteği olmasına; böylelikle hem ses hem de veri trafiğinin olanaklı hale getirilmesine karar verilmişti. İlk ses gereksinimleri olarak ultimate headset, konuşan laptop ve three-in-one telefon kullanım modelleri ile arama yapma, gelen çağrıya cevap verme, ses ayarlama gibi basit bazı fonksiyonlar düşünülmüştür. Telefon profillerinin daha fazla geliştirilmesini takiben, telefon kontrol fonksiyonlarının da gelişmesi gerektiğine karar verilmiştir.

Ses kontrol fonksiyonlarına olan ihtiyaç ilk farkedildiğinde, bu basit fonksiyonların RFCOMM kullanılarak AT komutları ile yapılabileceği farzedilmiş ve TCS-AT spesifikasyonu oluşturulmuştur. Bu spesifikasyonda standart AT komutlarının Bluetooth protokol yığını üzerinde nasıl kullanılacağı ve Bluetooth için gereken yeni AT komutlarının tanımlanması üzerinde durulmuştur. TCS-AT bir seri port üzerinden AT komutlarını alan ve gönderen bilinen mevcut uygulamaları desteklemek için tasarlanmıştır. TCS-AT, seri port yerine RFCOMM kullanmak üzere geliştirilmiştir. Spesifikasyon ilerledikçe yeni AT komutlarına çok fazla gerek olmadığı görülmüş (sadece iki yeni komut geliştirilmiştir); bu sebeple AT komutlarını kullanan profiller (mikrofon-kulaklık seti, faks ve çevirmeli-ağ profilleri) içinde tanımlanmakla yetinilmiştir.

Bu süre içinde binary ve paket tabanlı bir telefon kontrol protokolü Bluetooth protokol yığını içinde tanımlanmıştır. Yapılan araştırmalar sonucu da varolan ITU-T Q.931 spesifikasyonunun Bluetooth uygulamaları için yeterli olacağına karar verilmiştir. TCS-BIN in tüm telefon tabanlı profiller için gerekli olan fonksiyonları

sağladığı görülmüştür. Zamanla SIG, TCS-AT yi -fonksiyonları kullanılmaya devam edilmesine rağmen- ayrı bir spesifikasyon olarak kullanılmaktan vazgeçmiştir. Bu sebeple versiyon 1.0 da sadece TCS-BIN açıklanmıştır.

4.8.2 TCS Protokolü

TCS üç ana konuyu tanımlar:

- Çağrı kontrolü
- Grup Yönetimi
- Bağlantısız TCS

4.8.2.1 TCS Çağırma (Call) Kontrolü

TCS çağırma kontrolü fonksiyonları ses veya veri trafiği taşıyacak olan çağrıları kurmaya yarar. TCS bir durum makinesi gibi çalışır, bir çağrıyı bir durumdan diğerine iletirmek için gerekli olan işlevleri yerine getirerek sonuç durumunu izler. Bir çağrı yapıldığında, çağrıyı başlatma (arama bilgisi dahil olmak üzere), bağlantıyı kurma ve onaylama, çağrı tamamlandığında bağlantıyı sonlandırma gibi fonksiyonlar yerine getirilir. Alınan çağrılardaki durumlar ve geçişler, çağrı varlığı (çalma), çağrı kabulü, bağlantı kurulumu ve sonlandırma fonksiyonlarını içerirler.

Telefon kontrol fonksiyonları hem tek noktadan tek noktaya hem de tek noktadan çok noktaya olan ağ topolojilerini desteklerler. Çok noktalı durum, birçok telefonun gelen arama işaretini ve kontrol bilgisini almaya ihtiyaçları olduğu durum ile ilgilidir. Bu durumda TCS bütün telefonları gelen çağrı konusunda uyarmak için çok noktalı işaretleşme kullanır. Sonrasında aramaya cevap veren telefon ile ise ses veya veri trafiğinin akacağı tek bir içerik kanalı kurar. TCS kanalda akan içerik ile ilgilenmez, kontrol kanalında oluşan arama kontrolü fonksiyonları ile ilgilenir.

RFCOMM dan farklı olarak, birden çok çağrıyı kontrol etmek için çoklu TCS örneği oluşturulabilir (Bluetooth kablosuz haberleşmesi temebant üzerinde aynı anda üç ses kanalına izin vermektedir). Çoklu TCS örnekleri de çoklu L2CAP kanalları kullanır.

4.8.2.2 TCS Grup Yönetimi

Grup yönetim fonksiyonları “kablosuz kullanıcı grubu (wireless user group-WUG)” kavramını kullanır. Bu tip bir grup TCS in olanaklı hale getirdiği bazı özel

fonksiyonların avantajlarından yararlanmak için TCS grup yönetimi fonksiyonlarını kullanabilirler. Bu fonksiyonlar bir cihazın gruptaki diğer bir cihazın telefon servislerini kullanabilmesi yöntemini, grup üyeliğinin yönetimini (konfigürasyon dağıtımı olarak adlandırılır), ve iki köle üyenin TCS protokolünü kullanarak direkt bir bağlantı sağlamasını (hızlı içüye erişimi olarak adlandırılır) mümkün hale getirir.

Grup yönetimi; çoğu kullanıcının beklediği birçok telefon fonksiyonunu (birden fazla telefon numarası uzantısı, çağrı yönlendirme ve grup çağrıları) olanaklı hale getirmek için elverişli bir yoldur. Grup yönetimi ile three-in-one telefon profili için telefonların bir WUG'a katılmalarına izin verilir (böylece bir mobil telefonun telsiz telefon olarak kullanılması sağlanır) ve diğer TCS cihazları ile direkt haberleşmeleri (böylece intercom veya walkie-talkie fonksiyonu sağlanır) sağlanır.

WUG, tamamı TCS i destekleyen bir cihazlar grubudur. WUG yöneticisi, yönetici ile köleler arasındaki haberleşme dahil olmak üzere WUG içindeki haberleşmelerde ve WUG üyeleri ile başka bir WUG'un üyeleri arasındaki haberleşmede kullanılmak üzere anahtarlar dağıtır.

WUG daki bir cihaz, aynı WUG da bulunan başka bir cihazın telefon servislerini kullanmak için talepte bulunabilir. TCS bu talebe "erişim hakkı talebi" adını verir. Örneğin bir el terminali (handset), çağrı yapmak için bir baz istasyonunun telefon servislerini kullanmayı talep edebilir. Bir çağrıyı bir TCS cihazından (el terminali (handset) veya mikrofön-kulaklık seti) diğerine iletme için de aynı talep kullanılabilir.

Konfigürasyon dağıtımı WUG üyeliğini yönetmek için kullanılan bir TCS-BIN yöntemidir. WUG Yöneticisinin WUG ile ilgili bütün bilgiyi sağlaması kavramı kullanılarak, TCS-BIN WUG yöneticisinin en son WUG konfigürasyon bilgisi her değiştiğinde bu bilgiyi tüm üyelere göndermesini sağlayan bir protokol tanımlar. Örneğin, WUG a yeni bir üye katıldığında veya WUG dan bir üye çıktığında tüm üyeler bilgilendirilebilir. WUG üyelerini (örneğin evdeki sabit el terminalleri (handset) ve baz istasyonlar) WUG a yeni aktılan üye (örneğin eve giren bir mobil telefon) hakkında bilgilendirerek three-in-one telefon profili desteklenmiş olur. Böylece mobil telefonun varlığı bilinmiş olur ve baz istasyonuna bağlanır (telsiz telefon gibi davranır) veya WUG da bulunan diğer telefonlar ile direkt olarak haberleşir (intercom gibi davranır).

Hızlı içüye erişimi herhangi iki WUG üyesinin birbirleri ile hızlı bağlantı kurmasını sağlar. Bu özellik, iki üyenin bir WUG a ait oldukları ve WUG yöneticisi ile kurulu bağlantıları olduğu gerçekleri ışığında kullanılabilir. Bu gerçekler doğrultusunda tüm WUG üyeleri aynı pikonet içindedir ve WUG yöneticisinin saati ile sağlanan aynı atlama dizisini kullanırlar. Yukarıda anlatılan konfigürasyon dağıtımı sayesinde bütün WUG üyeleri diğer tüm üyeler hakkında bütün özellikleri bilmektedirler. Bu bilgiler bilindiği için üyeler arasında bağlantı kurmak çok hızlı gerçekleşir. Hızlı içüye erişimi ile, bir WUG üyesi haberleşeceği diğer üyeyi belirlemek için konfigürasyon bilgisini kullanır. Elde ettiği bilgiyi yöneticiye gönderir, yönetici de hedef WUG üyesi ile temasa geçer. Hedef üye yöneticiye kendi saat ofset değerini içeren bir cevap verir ve kendisini bir çağrı tarama (page scan) durumuna geçirir. Yönetici, bu saat ofset değerini bağlantı talep eden üyeye gönderir. Bu değeri alan üye, bu değeri kullanarak hedef üyeye çağrı yapar (paging) ve hızla bağlantı kurabilir. Sonuçta iki cihazdan meydana gelen yeni bir pikonet oluşur.

4.8.2.3 Bağlantısız TCS

TCS-BIN, cihazların gerçek bir arama yapmadan veya bir TCS arama bağlantısı kurmadan çağrı işaretleme bilgisini değiş tokuş etmelerini sağlar. Bu durum bağlantısız TCS olarak adlandırılır. Bağlantısız TCS, bir WUG içindeki cihazların aralarında bir TCS bağlantısı bulunmaksızın birbirlerine mesaj göndermelerini sağlayan bir çeşit “yan kanal” oluşturur. Bağlantısız TCS için tek bir mesaj formatı tanımlanmıştır: CL Info. CL_Info mesajları sadece iki tip bilgi içerebilir: mikrofon kazancı ve hoparlör ses ayarları için kullanılan ses kontrolü ve standardize olmuş TCS formatında belirtilmeyen bir bilginin verilmesi için kullanılan şirket bilgisi. Bu bilgilerden de anlaşılabilir gibi, bağlantısız TCS WUG daki tüm üyelerin ses ayarlamalarını ve aynı üretici tarafından üretilen ürünler arasında ürüne-özel özelliklerin bildirilmesini yönetmek için kullanılabilir. Bağlantısız TCS in bu şekilde kullanımı ile, örneğin aynı üreticiye ait baz istasyonu ve el terminali (handset) arasında kullanılan ileri telefon özelliklerinin diğer üreticiler tarafından üretilen el terminallerine (handset) olanaklı kılınmaması sağlanabilir.

4.8.3 Bluetooth Ses Özellikleri Gelişimi

Ses, Bluetooth kablosuz haberleşmesinin gelişiminin en başından itibaren protokol yığınının temel tasarımı içine entegre edilmiştir ve temelbant katmanında SCO

linkleri üzerinden taşınır. Ses, protokol yığınının ayrı bir katmanı değildir fakat Bluetooth teknolojisinin temel bir bölümüdür. Temelbanda entegre edilmiştir.

4.8.3.1 Bluetooth Ses İncelemesi

Bluetooth kablosuz haberleşmesinde ses (audio) sadece ses (voice) için kullanılmak zorunda olmamakla birlikte, tasarım açısından tamamen ses (voice) içeriğine göre optimize edilmiştir. Ses zaman içerisinde sürekli olma eğiliminde olduğu için isonkron veya zaman kısıtlamalıdır. Bluetooth ses trafiğinde, normal sesli konuşmalar için yeterli olmak üzere seçilen iletim hızı 64 kbit/sn. ile sınırlandırılmıştır. Müzik gibi diğer farklı ses medyalarının iletimi spesifikasyonun dışında bırakılmamakla birlikte daha çok ses trafiği üzerine yoğunlaşmıştır.

Bluetooth ses için iki tip kodlama planı geliştirilmiştir. Bu planlardan ilki kendi içinde iki tip logaritmik sıkıştırma tekniği kullanan (A-law ve μ -law) darbe kod modülasyonu (PCM) tekniğidir. PCM ses çok iyi bilinen ve çok sık kullanılan bir modülasyon türüdür. İkinci kodlama planı ise CVSD modülasyonudur. Tipik ses konuşmalarının karakteristiklerinin genel sese (örneğin müziğe) göre daha tahmin edilebilir bir sürekliliği vardır ve bir delta-slope yaklaşımını anlamlı kılar. CVSD haberleşme hatalarına karşı da daha toleranslıdır. Bu sebeple Bluetooth ses haberleşmesi için daha çok tercih edilen bir yöntemdir.

Bluetooth ses direkt hava arayüzü üzerinde, temelbant protokollerini kullanarak çalışan sayısal isonkron (etkili olarak akan) bir ses trafiğidir. Ses bilgisi yerel kayıt özellikleri kullanılarak sayısal paket tabanlı bir formatta kodlanmış olabilir. Bu tip bir ses bilgisi L2CAP katmanı kullanılarak Bluetooth linkleri üzerinden transfer edilebilir fakat bu transfer Bluetooth ses olarak tanımlanan veriden çok farklıdır.

4.8.3.2 Ses ve Telefon Kontrol Kullanımı

Telefon uygulamalarının birçok çeşidini gerçekleştirmek mümkündür. TCS-BIN telsiz telefon ve intercom profillerini desteklemek üzere tasarlanmıştır. Sadece bu iki profil teknik olarak telefon profili şeklinde sınıflandırılabilir.

Çevirmeli-ağ, faks ve mikrofon-kulaklık seti profil uygulamaları da bazı açılardan telefon profili sayılabilirler. Fakat bu profiller RFCOMM üzerinden AT komutlarını kullanarak çalıştıkları için daha çok bir seri port profil ailesi içinde yer almaktadırlar.

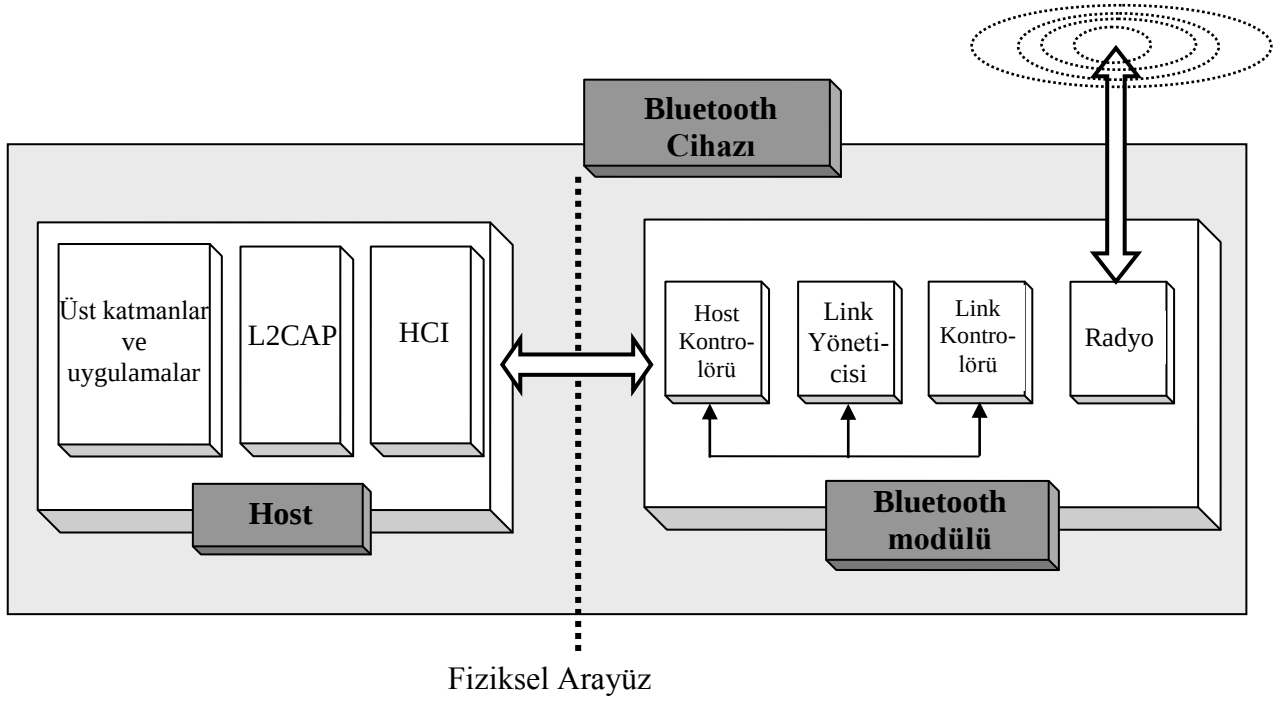
Bu uygulamalar TCS-BIN tabanlı olmamakla birlikte telefon uygulaması olarak kabul edilebilirler. Şekil 4.38 de de bu durum gösterilmektedir.

Seri kabloların kullanıldığı durumlarda genel programlama yöntemi olarak AT komut telefon kontrolleri kullanıldığı için bilinen mevcut uygulamalar da büyük çoğunlukla AT komutlarını kullanır. Bluetooth kablosuz linkleri için geliştirilen yeni uygulamalarda TCS-BIN protokolü kullanılarak daha güçlü telefon kontrol fonksiyonlarına imkan tanınmaktadır.

Telefon ve ses, özellikle insan sesi, Bluetooth protokol yığnında çok önemli bir rol oynamaktadır. Hem bilgisayar hem de haberleşme cihazlarını içeren bazı profillerde ve kullanım modellerinde Bluetooth'un ayırdedici bir özelliği olarak karşımıza çıkmaktadır. [2]

4.9 Host Kontrolör Arayüzü (Host Controller Interface (HCI))

Bluetooth iletim protokolleri, iletim protokollerini kullanan uygulamaları çalıştıran host (anakart veya işlemci) üzerinde entegre edilerek uygulanabilir. Veya hosttan bağımsız olarak ayrı bir Bluetooth modülünde uygulanarak, sonrasında host'a bir ek aksesuar ya da plug-in kart olarak (hosttaki USB portu veya RS-232 seri portu gibi fiziksel bir arayüz üzerinden) bağlanır. Ayrı olarak uygulandığında, modül bir host kontrolör ünitesi içerir. Bu ünite hosttan alınan bilgiyi yorumlar ve link yöneticisi ya da link kontrolörü gibi modülün uygun bileşenlerine gönderir. Ayrıca host kontrolörü modülden veri ve donanım/firma yazılımı durumlarını alarak gerek duyulduğu durumda hosta iletebilir. SIG tarafından ele alınan Bluetooth referans modelinde Bluetooth modülü radyo, link kontrolörü, link yöneticisi ve modülü bir hosta bağlamak için gereken bir host kontrolör arayüzü içerir (Şekil 4.39). Bu referans uygulaması diğer uygulamaların değişik yığın bileşenlerinden oluşmasını engellemez.



Şekil 4.39 Bluetooth referans modeli

Farklı üreticilerin entegre olmayan modüllerini birbirleri ile uyumlu olarak kullanabilmek için, SIG tarafından modülün host kontrolörü ile haberleşmek için standart bir arayüz tanımlanmıştır. Bu haberleşme host ile host kontrolörü arasında kullanılan iletim mekanizmasından ve fiziksel arayüzden bağımsız şekilde gerçekleşir. SIG ayrıca host ile host kontrolörü arasında bilgi taşıyacak bir hareket (transaction) tabanlı haberleşme protokolü de tanımlamıştır. Host ile host kontrolörü arasındaki bu standart arayüz ve aralarındaki uygun haberleşme protokolü beraberce Host Kontrolör Arayüzü (HCI) olarak adlandırılır.

HCI Bluetooth hostu ve hostta çalışan uygulamalar tarafından erişilebilen Bluetooth modülü fonksiyonlarını tanımladığı için, modülün fonksiyonlitesini sınırlandırmaktadır.

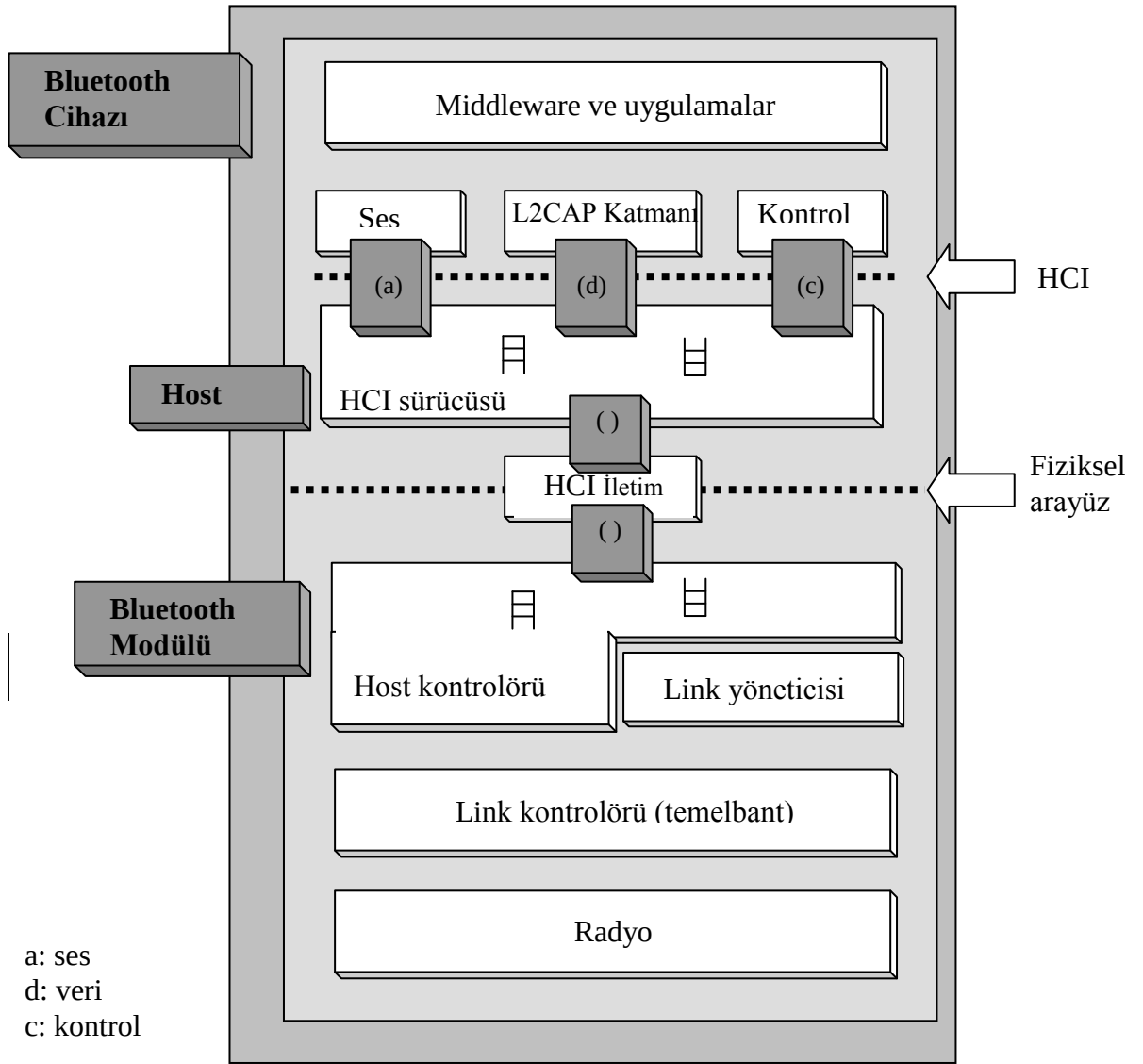
Şekil 4.40 HCI içeren bir protokol yığını göstermektedir. HCI bölümü üst katmanlar için bir arayüzler takımı (HCI_PDU ları ile tanımlanmıştır) içermektedir. HCI sürücüsü, host kontrolörü ile HCI_PDU larını değiş tokuş etmek için kullanılan haberleşme protokolünü oluşturur. Fiziksel arayüz üzerinden HCI_PDU larını taşıyan iletim protokolü HCI iletim dir. HCI iletim için SIG tarafından yeni bir geliştirme yapılmamış, USB, RS-232 ve UART protokolleri kullanılmıştır. HCI iletim, hem host hem de modül tarafında kendi tamamlayıcı sürücü bileşenlerine sahiptir.

HCI uygulaması zorunlu değildir ve tamamen entegre olan sistemlerde gerekli de olmaz. Fakat üretici şirketler kendi ürünlerini düşük seviye iletim protokol test şartnamelerine göre test etmek zorunda oldukları için HCI ya benzer bir arayüz sunmak zorundadırlar.

4.9.1 HCI_PDU Paket Sınıfları

Hosttaki HCI katmanı ile modüldeki host kontrolörü arasında bilgi değiş tokuşu yapmak için üç tip HCI_PDU su kullanılır (Şekil 4.41). Komut-sınıfı HCI_PDU ları, HCI katmanından host kontrolörüne gönderilirler ve kontrol ve yönetim bilgisi taşırlar. Olay-sınıfı HCI_PDU ları host kontrolöründen HCI katmanına gönderilirler ve kontrol ve yönetim bilgisi taşırlar. Veri-sınıfı HCI_PDU ları L2CAP_PDU parçaları ve SCO verisi taşırlar. HCI spesifikasyonu veri-sınıfı HCI_PDU larını birisi asenkron L2CAP verisi, birisi de senkron veri için olmak üzere iki kategoriye ayırmıştır. Fakat pratikte bütün veri-sınıfı HCI_PDU ları aynı sayıda alana ve eş alan şekillerine sahiptir. Bu sebeple iki veri-sınıfı HCI_PDU kategorisi, aynı HCI_PDU sınıfının iki farklı modu gibi yorumlanırsa daha doğru bir yaklaşım olur. HCI_PDU larındaki bilgi little-endian formatında kodlanmıştır. Şekil 4.41 host ve modül arasındaki fiziksel arayüzü de göstermektedir.

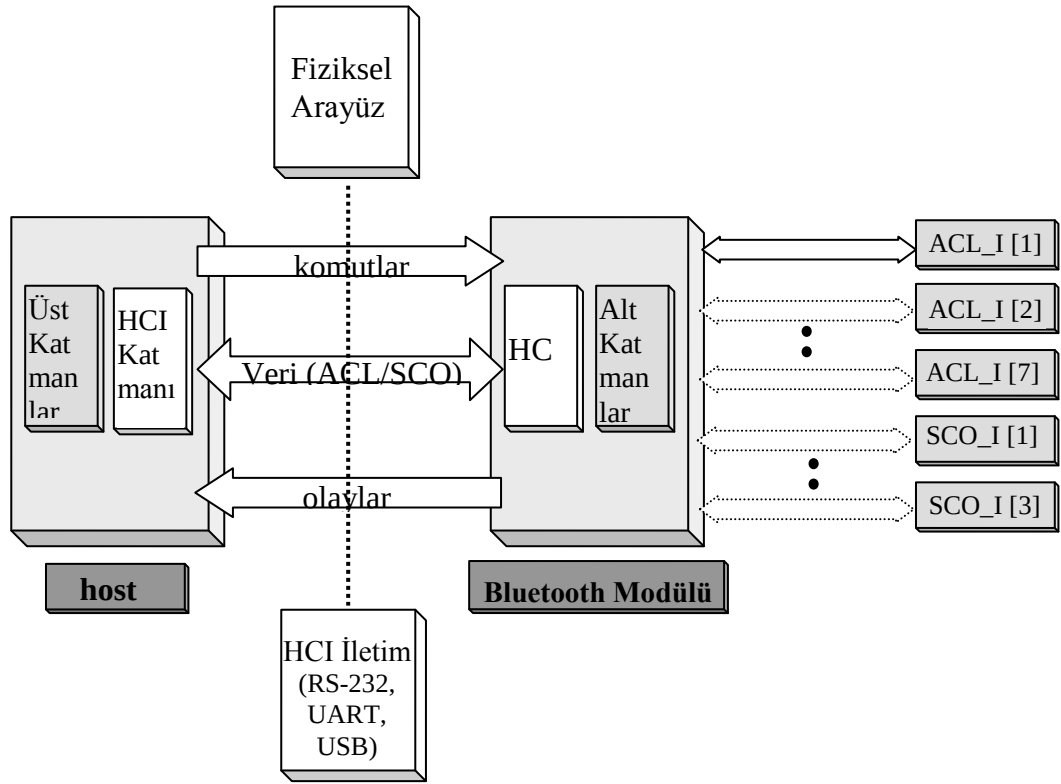
Şekil 4.41 bir cihazın sahip olabileceği muhtemel aktif linkleri de göstermektedir. İki cihaz arasında en fazla bir ACL linki olabilir. Bir yönetici köleleri ile arasında en fazla yedi aktif ACL linkine sahip olabilir (her aktif köle için bir tane). Yönetici ile pikonetteki bütün köleleri arasında en fazla üç SCO linki bulunabilir. İki cihaz arasındaki ACL linki SCO linki kurulmadan önce kurulmalıdır.



Şekil 4.40 HCI içeren bir protokol yığını

Bir host, komut HCI_PDU larını aşağıdaki gibi durumlarda kullanır:

- Doğrulama için bir link anahtarı sağlamak gibi modülün operasyonel parametrelerini ayarlamak için,
- Modülün operasyonel durumu ve ilgili parametrelerini konfigüre etmek için (örneğin modülü aktive etmek ve parametrelerini düşük güç moduna almak gibi),
- Yayın (broadcast) paketlerinin tekrarlama sayısı (N_{BC}) gibi kayıt girişlerini okumak ve yazmak için.



Şekil 4.41 HCI_PDU sınıfları

Komuta bağlı olarak, modül kayıtları okunur veya ayarlanır (set edilir), link yöneticisi bir LMP hareketi (transaction) oluşturur, link kontrolörü durumu değiştirir ve bir çağrı (page) yaratır. Host kontrolörü, hosta bir olay HCI_PDU su göndererek komutun sonucu hakkında bilgilendirir. Bu gönderme işlemi komut hosttan gönderilir gönderilmez ya da daha sonra yapılabilir. Hosta gönderilen host kontrolör HCI_PDU larının cevap değil de olay olarak tanımlanmasının sebebi, host kontrolörünün kendi talebini kendisinin başlatabilmesi (örneğin hosttan kayıp bir link anahtarını istemesi) veya hostun ilk hareketi olmaksızın hosta bir iletim göndermesidir. Hosttan gönderilen bazı komut HCI_PDU ları, host kontrolörü tarafından oluşturulan olay HCI_PDU larına olan cevaplardır. Örneğin HCI_Accept_Connection_Request komutu hosttan host kontrolörüne, uzak bir cihazdan gelen bir bağlantı talebini kabul etmesi için gönderilir. Host HCI_Accept_Connection_Request komutunu iletmeden önce, host kontrolörü hosta gelen bağlantı talebi hakkında Connection_Request olayı göndererek uyarır.

Veri HCI_PDU larının fiziksel arayüz üzerinden iletimi, PDU yu alan tarafın ara bellek (buffer) büyüklüğü ile düzenlenir. Host ve host kontrolörü karşı tarafın ara bellek (buffer) büyüklüklerini sorgular ve iletimlerini bu bilgiye göre ayarlarlar. Bu sebeple büyük bir L2CAP_PDU su HCI katmanı içinde bölünerek host kontrolörüne gönderilmelidir. Alıcı tarafta HCI katmanı, alınan veri HCI_PDU sundaki paket sınır bayrak bilgisine dayanarak L2CAP_PDU larını tekrar inşa eder. Fiziksel arayüz üzerinden HCI_PDU larının iletimi ilk-giren-ilk-çıkart prensibine göre yapılır. Komutlar host kontrolöründe geliş sıralarına göre proses edilirler fakat her birinin uygulanması farklı zaman alacağı için paketler düzensiz olarak alınmış olabilirler. Kısaca, olaylar sunucuda geliş sıralarına göre proses edilirler fakat işlem süreleri sırayı bozar.

HCI_PDU larının hiçbirinde HCI_PDU nun sınıfını (olay veya veri) tanımlayacak bir alan bulunmamaktadır. Sınıf tanımlaması PDU ları host ile host kontrolörü arasında taşıyan HCI iletim protokolüne bırakılmıştır. Bu durum protokol katmanlama işlemine aykırıdır. Buna rağmen, HCI ın altta yatan iletim protokolünün yeteneklerini almasına izin verilerek minimum problem ile üç farklı sınıfın ayırtedilmesi sağlanır.

4.9.2 HCI_PDU ları

Komut HCI_PDU sunun başlığındaki “Op Kodu Grup Alanı” (OGF) ile tanımlanan birkaç gruba ayrılmış komut HCI_PDU ları bulunmaktadır. Komut HCI_PDU larının birçoğu için tekabül eden olay HCI_PDU ları bulunur. Bu olay HCI_PDU ları komut ile ilgili sonuç ve geri dönüş parametrelerini taşırlar. Birçok komut için, durumları ve uygulama sonuçları ile ilgili bilgi iki özel olay ile taşınır: Command_Status_Event ve Command_Complete_Event. Command_Status_Event, host kontrolörü tarafından komutun durumunu (bekleme durumu, komutun anlaşılmaması vs..) göstermek üzere bir komut alınır alınmaz gönderilir. Böylelikle komut ve komutun proses durumu ile ilgili bilgi edinilmiş olur. Command_Complete_Event bir komutun oluşum sürecinin tamamlandığını belirtmek ve ilgili parametreleri (istenen komutun başarı ile yerine getirilip getirilmediği bilgisi dahil olmak üzere) geri döndürmek için kullanılır. Bir tek komuta cevap olarak birden fazla olay meydana getirilebilir.

Link kontrolör hareketleri, ilke (policy) ayarlama komutları, host kontrolörünün kendisi ve bunun gibi birçok konu ile ilgili komut HCI_PDU ları vardır. Komut ve olay HCI_PDU larının sayısı 100'ü geçmiştir.

4.9.2.1 Link Kontrol HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000001” değeri ile belirlenirler ve çevredeki cihazları keşfetmek için gönderilecek sorgulamalara imkan verirler. ACL ve SCO bağlantılarını kurup sonlandırmak ve gelen bağlantı taleplerini kabul etmek veya reddetmek için komutlar vardır. Doğrulama ve şifreleme prosedürlerini başlatmak için ve sunucudan link yöneticisine doğrulama anahtarları ile PIN leri iletmek için de komutlar bulunur. Bu grupta uzak cihazın ismini, desteklediği link yönetim seçeneklerini ve kayıtlı olan saat ofset değerini sorgulamak için de bilgi komutları kullanılır.

HCI_Inquiry komut PDU su, verilen bir sorgulama erişim kodunu kullanarak modülün sorgulama moduna girmesini ve belirlenen bir süre boyunca veya belirlenen sayıda cevap gelene kadar bu modda kalmasını sağlar.

Bu komutla başlatılan sorgulama modu, Inquiry_Length alanında belirtilen zaman aşılar veya cevap veren cihazların sayısı Num_Responses da belirtilen sayıya erişirse sona erer.

Sunucu kontrolörü sorgulardan elde edilen sonuçları toplayarak Inquiry_Result_Event i ile sunucuya gönderir.

HCI_Create_Connection komut PDU su modülün belirlenmiş bir cihazla bir ACL linki için verilen BB_PDU larını kullanarak bağlantı oluşturmasını sağlar. Bu komut, bağlantı prosesi lokal cihazın uzak cihazı çağırması (page) gerektirdiği için; çağrı (paging) prosesini hızlandıracak bilgi de sağlar. Çağrı (paging) bilgisi lokal cihazın sunucusuna Inquiry_Result_Event PDU su ile gönderilir.

Bağlantının başarılı olarak kurulmasını takiben, bir Connection_Complete_Event i bağlantının her iki ucundaki sunuculara gönderilir. Olaylar bağlantıyı tanımlamak için Connection_Handles içerirler. Connection_Handles her bir sunucu kontrolör tarafından bağımsız olarak belirlenir ve kapsamaları da sadece lokal cihaza bağlıdır.

4.9.2.2 Link İlke (Policy) HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000010” değeri ile belirlenirler. Bir cihazın güç yönetim ilkesini (policy) durağan, koklama ve park temelbant modları ile belirlemesini ve bu modlar için parametreleri tanımlamasını sağlarlar. Ayrıca, L2CAP katmanından link yöneticisine QoS parametrelerini gönderen, cihazın bağlantıdaki rolünü (yönetici ya da köle) öğrenen ve eğer gerekiyorsa rol değişimi için talepte bulunulmasını sağlayan komutlar da mevcuttur.

4.9.2.3 Host Kontrolör ve Temelbant HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000011” değeri ile belirlenirler ve sunucunun operasyonel parametreleri sağlayan çeşitli donanım kaydedicilerine (register) ulaşmasını ve konfigüre etmesini sağlarlar. Yerine getirilebilecek operasyonlar arasında host kontrolörünün oluşturabileceği olay tiplerinin belirlenmesi; saklanan anahtarları okuma, yazma ve silme; cihaz adını okuyup yazma; sorgulama ve/veya çağrı tarama (page scan) fonksiyonlarını aktif/pasif hale getirme; bir link için doğrulama ve/veya şifreleme aktivitesi bayrağını okuma ve yazma; sorgu taramaları sırasında dinleme yapmak için kullanılan sorgulama erişim kodlarını okuma ve yazma; bir bağlantı için ACL paketlerini zorlama; ses kodlama-kod çözme (codec) parametrelerini okuma ve yazma bulunmaktadır.

Host kontrolör ilgili kayıtları (register) güncellemeyi bitirdikten sonra sunucuya Command_Complete_Event i gönderir.

4.9.2.4 Bilgi Parametreleri HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000100” değeri ile belirlenirler ve cihazlar üzerine üretim zamanında “işlenen” donanım ve yazılım ile ilgili statik bilgileri istemek için kullanılırlar. Modülün desteklediği çeşitli protokollerin (LMP, HCI vs..) versiyonlarını sorgulamak; link yöneticisi tarafından desteklenen özelliklerin bir listesini almak; modülün çalıştığı ülkeyi öğrenmek; modülün BD_ADDR sni öğrenmek; sunucuda verimli akış kontrolü sağlamak için kullanılan ACL ve SCO paketleri için host kontrolörünün ara bellek (buffer) bilgisini öğrenmek için komutlar mevcuttur. Talep edilen bilgi Command_Complete_Event içinde geri döner.

4.9.2.5 Durum Parametreleri HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000101” değeri ile belirlenirler ve dinamik olarak güncellenen bilgileri talep etmek için kullanılırlar. Uzak cihaz lokal iletimlere cevap vermez iken başarılı olunan anların sayısını ölçen sayıcı değeri için kullanılan bir komut bu gruptadır. Linkin kalitesi ve RSSI değeri de bu gruptaki HCI_PDU lar ile öğrenilir. Talep edilen bilgi Command_Complete_Event içinde geri döner.

4.9.2.6 Test amaçlı HCI_PDU ları

Bu gruptaki komutlar OGF alanındaki “b000110” değeri ile belirlenirler ve Bluetooth modülünü test etmek için kullanılırlar. Bu komutların tamamı Command_Complete_Event olayları içinde sonuçlanır. [2]

5. BLUETOOTH GÜVENLİK MİMARİSİ

5.1 Giriş

Bluetooth link katmanında güvenlik özelliklerini içerir. Doğrulama (tek veya çift yönlü) ve şifrelemeyi destekler. Bu özellikler bir çift cihaz tarafından paylaşılan gizli bağlantı anahtarı temeline dayanır. Bu anahtarı üretmek için iki cihaz ilk defa haberleştiğinde bir çiftleme (pairing) prosedürü kullanılır.

Bluetooth güvenlik gereksinimleri le ilgili kısım “Genel Erişim Profili” nde açıklanır. Bu profil bir Bluetooth cihazı için geçerli olan üç güvenlik modunu açıklar:

- Güvenlik modu 1 (güvenli olmayan): Cihaz hiçbir güvenlik prosedürünü başlatmaz.
- Güvenlik modu 2 (servis kademesinde gerçekleşen güvenlik): Cihaz L2CAP katmanında kanal oluşturulmadan önce hiçbir güvenlik prosedürünü başlatmaz. Bu mod özellikle güvenlik gereksinimleri farklı olup, paralel çalışması gereken uygulamalar için değişik ve esnek erişim politikalarına imkan verir.
- Güvenlik modu 3 (bağlantı kademesinde gerçekleşen güvenlik): Cihaz LMP katmanındaki başlangıç bağlantısı tamamlanmadan önce güvenlik prosedürlerini başlatır.

Pratikte daha çok Güvenlik modu 2 kullanılmaktadır. 2.mod esnek güvenlik mekanizmalarının nasıl kurulması gerektiğine rehberlik eder. [18]

5.2 Fonksiyonlar ve Sınırlamalar

5.2.1 Güvenlik Kademeleri

- Cihaz ve servisler için farklı güvenlik kademeleri tanımlamak mümkündür.
- Cihazlar için iki güvenlik kademesi düşünülür:

- Güvenilen cihaz: Bağlantının kurulduğu (anahtar çiftinin oluşturulduğu) ve servislere erişimine izin verilen cihazdır.
- Güvenilmeyen cihaz: Kalıcı bir bağlantı şeklinin kurulmadığı (geçici bir bağlantı kurulmuş olabilir) veya kalıcı bir bağlantı kurulduğu halde güvenilen kabul edilmeyen cihazdır. Servislere erişime izin verilmez.
- Servislere erişim için doğrulama, yetkilendirme ve şifreleme gereksinimleri birbirlerinden bağımsız olarak değerlendirilirler. Erişim gereksinimleri üç güvenlik kademesinin tanımlanmasını sağlar:
 - Doğrulama ve yetkilendirme gereksinimi olan servisler: Otomatik erişim hakkı sadece güvenilen cihazlara verilir. Diğer cihazlar manuel yetkilendirmeye ihtiyaç duyarlar.
 - Sadece doğrulama gereksinimi olan servisler: Yetkilendirme gerekli değildir.
 - Tüm cihazlara açık olan servisler: Doğrulama gerekmez, servis erişimi sağlanmadan önce erişim onayına ihtiyaç yoktur.

5.2.2 Esneklik ve Kullanılabilirlik

- Servislere erişimi ayırarak, bazılarında erişim verip, bazılarında vermemek mümkündür. Örneğin bir cep telefonunda servis keşif kayıtlarına erişim mümkün olurken, çevirmeli ağ sadece belirli cihazlar için erişilebilir olur.
- Güvenlik mimarisi, değişik uzak cihazlarla haberleşmek için gerekli olan bazı servislerin güvenlik politikalarını destekler (örneğin dosya transferi ya da kartvizit değişimi uygulamaları). Bu şekilde yapılan erişim:
 - Cihazdaki diğer servislere açık değildir.
 - Cihazdaki servislere gelecekte yapılacak erişim için yetkili değildir.
- Servislere erişim için kullanıcı müdahaleleri mümkün olduğu kadar engellenmiştir.
- Mimari yapı uygulama seviyesindeki güvenlikle ilgilenmez.

5.2.3 Gerçekleştirme ve Bluetooth’a Özel Sorunlar

Bluetooth çoğullama protokolleri için kullanılan güvenlik mimarisi L2CAP katmanında veya daha üst katmandadır. Günümüzde sadece RFCOMM dikkate alınmakta, diğer protokoller Bluetooth’a özel olmadıkları ve kendilerine özel güvenlik prosedürleri olduğu için üzerlerinde durulmamaktadır.

Güvenlik mimarisi güvenlik politikalarını uygulamak için değişik protokollerin kullanımına olanak tanır. Örneğin L2CAP telsiz telefon haberleşmesi için, RFCOMM çevirmeli ağ bağlantısı için Bluetooth güvenlik politikalarını uygularlar. OBEX ise dosya transferi ve senkronizasyon için kendi güvenlik politikalarını kullanır.

Mimari “Genel Erişim Profili”nin 2. güvenlik modunu kullanarak çalışabilir. Özellikle temelbantta ve LMP fonksiyonlarında doğrulama ve şifreleme için herhangi bir değişiklik yoksa sorun yaşanmaz.

Doğrulama ve şifreleme fiziksel bağlantı için düşünülmüştür (örneğin temelbant katmanında).

Daha düşük katmanlarda servis/uygulama katmanı güvenliği ile ilgilenilmez.

Doğrulama, yetkilendirme ve şifreleme için geçerli olan uygulama politikaları istemci ve sunucu rolleri için farklılıklar içerir. [19]

5.2.4 Riskler ve Kısıtlamalar

Aşağıdaki senaryolar kısıtlamaları belirlemek için ele alınmıştır:

- Senaryo 1: 2 adet Bluetooth cihazımız var (örneğin PDA ler). Her cihazın kendisine özel bir uygulama seti var: takvim, dosya senkronizasyonu vs..gibi. Bu iki cihaz bir Bluetooth linki üzerinden haberleşecek ve dosya senkronizasyonu gibi bir belirli bir görev yerine getirecekler.
- Senaryo 2: Senaryo 1’de yer alan cihazlardan 2’den fazla adette var. Bütün cihazlar Bluetooth linkleri üzerinden kartvizit değişimi yapmak gibi güvenlik gereksinimi olmayan bazı işlemler yapacaklar.
- Senaryo 3: PDA gibi bir cihaz, bir Bluetooth linki üzerinden internet, bir e-ticaret uygulaması, kurumsal veri tabanı gibi bir altyapı servisine ulaşacak. Cihaz Bluetooth linki üzerinden bir LAN Erişim Noktası’na bağlanacak.

LAN Eriřim Noktası da yukarıdaki altyapı servislerine kablolu ya da kablosuz ađ üzerinden bađlanacak. Bu bađlantı 3 katmanlı bir bađlantı olacaktır. 1. katman PDA cihazı, 2.katman LAN Eriřim Noktası, 3. katman ise altyapı servisleridir.

Bluetooth gvenlik mimarisi ařađıdaki kısıtlamaları ierir:

1. Bilinen mevcut uygulamalar iin destek: Hibir senaryoda, mevcut uygulama gvenlik yneticisi ile haberleřmemektedir. Mevcut uygulama yerine Bluetooth uyumlu bir adaptasyon uygulaması Bluetooth gvenlik yneticisi ile gvenlikle ilgili olarak haberleřir.
2. Kullanıcı dođrulanmamakta, sadece cihaz dođrulanmaktadır. Kullanıcı dođrulamasının gerektiđi durumlarda (uygulama katmanı gvenlik zellikleri gibi) bařka fonksiyonlar da kullanılmalıdır.
3. Senaryo 1 ile ilgili olarak: Her servis iin gerekli yetkilendirmeyi nceden belirleyecek bir mekanizma bulunmamaktadır. Fakat bu mimari ile Bluetooth protokol yıđınını deđiřtirmeksizin olduka esnek bir gvenlik politikası uygulanabilir. Gvenlik yneticisinin ve kayıt proseslerinin modifikasyonu gerekecektir.
4. Yaklařım sadece bađlantı bařlangıcındaki eriřim kontrolne izin vermektedir. Eriřim kontrol asimetrik olabilir fakat bađlantı bir kere kurulduđunda veri akıřı prensip olarak iki ynl olacaktır. Bu yapının genel erevesi iinde tek ynl trafik mmkn olmayacaktır.
5. Senaryo 3 teki 3 katmanlı konfigrasyon desteđi: Gvenlik mimarisi Bluetooth link gvenliđi ve linkin sonlarındaki tm cihazlar iin karřılıklı dođrulamaya dayanan Bluetooth temelbant gvenliđi prosedrleri zerine kurulmuřtur. Senaryo 3 teki gibi utan ua gvenlik iin daha “st katman” gvenlik zmlerinin kullanıldıđı varsayılmaktadır.

5.3 Gereksinimleri Karřılayacak Gvenlik Mimarisi

Bu blmde Bluetooth’un link katmanı zellikleri zerine kurulu olan esnek gvenlik mimarisi incelenmiřtir.

5.3.1 Genel Bakış

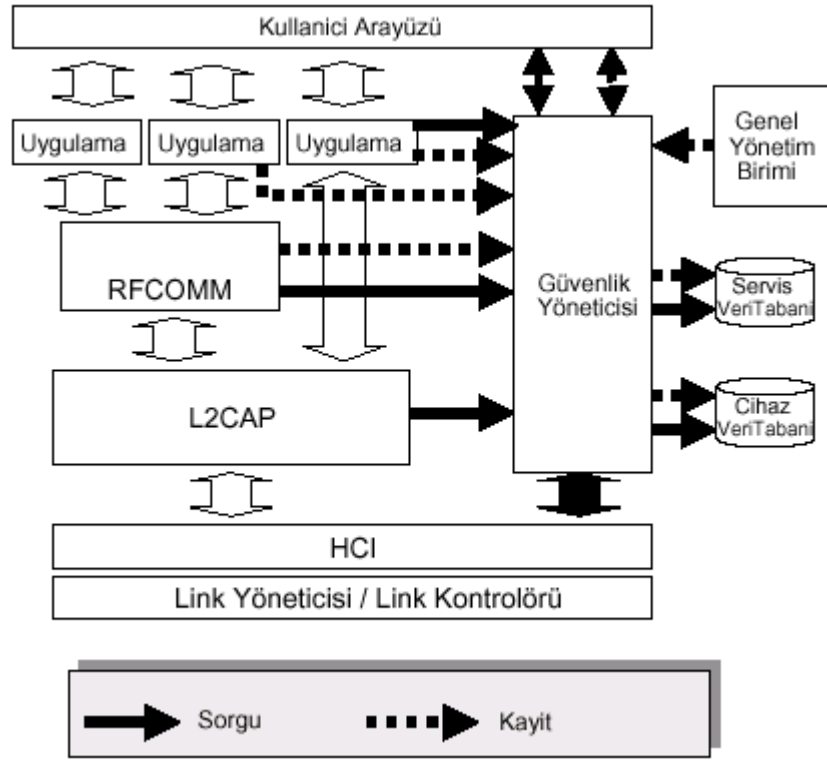
Güvenlik mimari yapısı Şekil 5.1 de gösterilmiştir. Mimarinin ana bileşeni aşağıdaki görevleri yerine getiren güvenlik yöneticisidir:

- Servisler üzerinde güvenlikle ilgili bilgileri saklar.
- Cihazlar üzerinde güvenlikle ilgili bilgileri saklar.
- Erişim isteklerine cevap verir (red veya onay).
- Uygulamaya başlanmadan önce doğrulama ve/veya şifreleme işlevlerini yerine getirir.
- Cihaz katmanında güvenli bir bağlantı başlatmak için Harici Güvenlik Kontrol Birimi (ESCE) (örneğin cihaz kullanıcısı) girişini başlatır veya proses eder.
- Çiftlemeyi ve kullanıcı tarafından girilen sorgulama PIN ini başlatır. PIN girişi uygulama tarafından da yapılabilir.

Güvenlik mimarisi çok esnek bir güvenlik çalışma yöntemi (framework) sunmaktadır. Bu çalışma yöntemi (framework) ile kullanıcının ne zaman sürece dahil olacağı (PIN gireceği) ve istenen güvenlik kontrolleri için Bluetooth protokol katmanlarının nasıl bir yol izleyeceği anlatılmaktadır.

Merkezi güvenlik yöneticisi ile modellenen yapı ile esnek erişim politikaları uygulanabilmektedir. Protokol ve diğer birimler için varolan arayüzler basit tutulmuş ve sorgu/sonuç ve kayıt prosesleri ile kısıtlandırılmıştır. Erişim kontrolü için gerekli olan politikalar güvenlik yöneticisi içinde düşünülmektedir. Böylelikle, daha kompleks politikaların uygulanması diğer birimleri etkilemez.

Uygulamalar, kayıt görevini kimin yapacağına (örneğin uygulamanın kendisi veya bir genel yönetim birimi) karar verir, protokol yığnında izlenecek yolu (path) tanımlar ve/veya servis keşif kısmında servisleri kaydeder.



Şekil 5.1 Bluetooth güvenlik mimarisi

5.3.2 Güvenlik Kademeleri

5.3.2.1 Doğrulama ve Yetkilendirme

Doğrulama bağlantı linkinin diğer ucundaki kişinin kim olduğunun doğrulanması prosesidir. Cihazlar (BD_ADDR) için uygulanır. Bluetooth da saklı link anahtarı veya çiftleme (PIN girerek) üzerine kurulmuş doğrulama prosedürü ile gerçekleştirilir.

Yetkilendirme cihaz X in servis Y ye erişim izni olup olmadığına karar verilmesi sürecidir. Bu süreç “güvenilirlik” kavramı ile iç içe geçmiştir. Güvenilen cihazlara (doğrulanmış ve güvenilen olarak tanımlanmış) servislere erişim için izin verilir. Güvenilen olmayan veya bilinmeyen cihazlardan servislere erişim öncesinde kullanıcı etkileşimine dayalı olarak yetkilendirme istenir. Yetkilendirme bazen otomatik olarak bir uygulama tarafından da yapılabilir. Yetkilendirme her zaman doğrulamayı içerir.

5.3.2.2 Cihaz Güvenlik Derecesi

Üç farklı cihaz güvenlik derecesi vardır:

- **Güvenilen cihaz:** Daha önceden doğrulanmış, bir bağlantı anahtarı saklanmış ve cihaz veri tabanında “güvenilen” olarak belirlenmiş cihazdır.
- **Güvenilmeyen cihaz:** Daha önceden doğrulanmış, bir bağlantı anahtarı saklanmış fakat cihaz veri tabanında “güvenilen” olarak belirlenmemiş cihazdır.
- **Bilinmeyen cihaz:** Hakkında hiçbir güvenlik bilgisi olmayan cihazdır. Bu tip bir cihaz aynı zamanda güvenilmeyen bir cihazdır.

Güvenlik yöneticisinde tutulan bir veri tabanı tablosu bulunmaktadır. Bu veri tabanı tüm servisler için birlikte tutulabileceği gibi, her servis için ya da bir grup servis için ayrı ayrı tutulabilir.

Güvenilen cihazların doğrulanması

LMP ve temelbant özelliklerinde tanımlanan doğrulama prosedürü kullanılarak doğrulama yapılır. Pozitif bir doğrulama cevabı alınırsa ve güvenilen bayrağı işaretlenirse (set edilirse) cihaz “güvenilen” olarak doğrulanır.

Güvenilir bağlantının kurulması

Güvenli bir bağlantı çiftlee prosedürü esnasında kurulur. Genellikle bağlanma prosedürü kısmında gerçekleştirilir.

Güvenilmeyen bir cihaz bir servisi kullanmak üzere yetkilendirildiğinde cihazı aynı prosedür esnasında güvenilen cihazlar arasına dahil etmek de mümkündür. Bu işlemin yapılabilmesi için kullanıcının aktif seçimi gerekmektedir.

Güvenilmeyen cihazın doğrulanması

Güvenilmeyen cihazların doğrulanması güvenilen cihazlarda olduğu gibi yapılır. Yalnız cihaz veri tabanına güvenilen olarak işlenmez.

5.3.2.3 Servislerin Güvenlik Dereceleri

Bir servisin güvenlik derecesini karakterize eden 3 unsur vardır:

- **Yetkilendirme İstemi:** Erişim sadece güvenilen cihazlara veya yetkilendirme sonrasında güvenilmeyen cihazlara sağlanır.

Uzak cihazın doğru cihaz olup olmadığının anlaşılması için yetkilendirme daima doğrulama ister.

- **Doğrulama İstemi:** Uygulamaya başlanmadan önce uzak cihaz mutlaka doğrulanmalıdır.
- **Şifreleme İstemi:** Servise erişim başlamadan önce bağlantı linki şifrelenmiş moda çevrilmelidir.

Bilgi; güvenlik yöneticisinin servis veri tabanında tutulur.

Herhangi bir kayıt mekanizması yoksa, varsayılan bir güvenlik derecesi kullanılır. Şöyle ki:

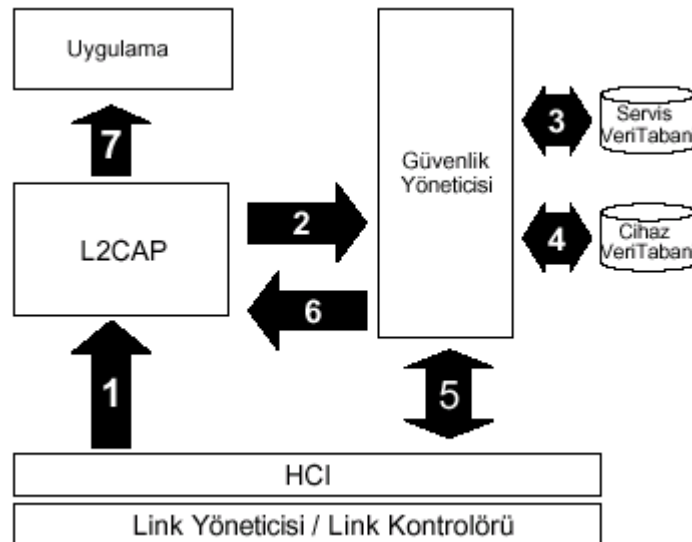
- Gelen bağlantı isteği: Yetkilendirme ve doğrulama istenir.
- Giden bağlantı isteği: Doğrulama istenir.

5.3.3 Bağlantı Kurulum Prosedürü

5.3.3.1 Genel Kavramlar

Kullanıcı müdahalesi olmadan servislerin değişik isteklerini karşılamak için, önce istenen servisin güvenlik derecesi belirlenmeli sonrasında ise doğrulama sağlanmalıdır. Bu sebeple ACL linki kurulduğunda doğrulama sağlanamaz. Doğrulama bir servise bağlantı talebi alındığında gerçekleşir.

Şekil 5.2 güvenilir bir servise erişim için olması gereken bilgi akışını göstermektedir.



Şekil 5.2 Güvenilir servise erişim için gerekli bilgi akışı

Güvenilir servise erişim için şu prosedürler gerçekleştirilir:

1. L2CAP a bağlantı isteği gelir.
2. L2CAP güvenlik yöneticisinden erişim talep eder.
3. Güvenlik yöneticisi servis veri tabanını kontrol eder.
4. Güvenlik yöneticisi cihaz veri tabanını kontrol eder.
5. Eğer gerekli görülürse güvenlik yöneticisi doğrulama ve şifreleme yapılmasını ister.
6. Güvenlik yöneticisi erişime izin verir.
7. L2CAP bağlantıyı kurmaya devam eder.

Doğrulama iki yönde de olabilir, istemci sunucuyu ya da sunucu istemciyi doğrulayabilir.

5.3.3.2 Temelbant Bağlantı Linki Kurulumunda Doğrulama

Güvenlik modu 3 hedeflenmemesine rağmen, bu yapı 3. modu da destekler. Güvenlik yöneticisi HCI kullanarak bir temelbant erişiminin sağlanmasından önce bağlantı yöneticisinin doğrulama istemesini sağlayabilir. Farklı modlar paralel olarak yürütülebilir:

- Temelbant bağlantısında doğrulama
- Uygulamalara bağlanırken doğrulama

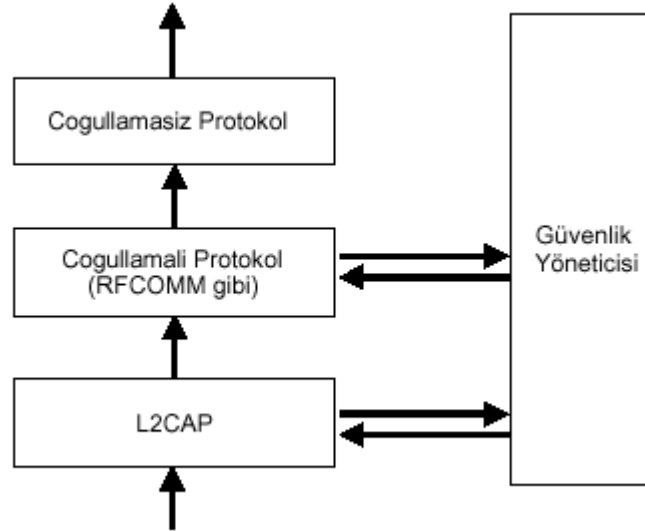
Bu iki proses aynı anda yürüyemeyeceği için, eğer her ikisi de uygulanacaksa hangisine öncelik verileceğine karar verilmelidir. Mod2 den Mod3 e geçiş sağlanmadan önce güvenilemeyen cihazların istenmeyen erişimler yapmayacağından emin olunmalıdır. Bunu yapabilmek için, güvenlik yöneticisi radyo modülünde güvenilemeyen cihazlar için tutulan bağlantı anahtarlarını kaldırır. Güvenlik yöneticisi HCI da kullanabilir.

5.3.3.3 Protokol Yığını İşlenmesi

Gelen bağlantılar için Şekil 5.3 de açıklanan erişim kontrol prosedürü uygulanır. Erişim kontrolü L2CAP da ve bazı durumlarda da buna ek olarak L2CAP'ın üzerindeki çoğullama (multiplexing) protokollerinde (örneğin RFCOMM gibi) istenir. Bağlantı talebi geldiğinde protokol, güvenlik yöneticisini sorgular ve bağlantı

istemiyle birlikte herhangi bir çoğullama (multiplexing) bilgisi alıp almadığını da bildirir. Güvenlik yöneticisi erişim talebine “tamam” veya “red” cevabı verir ve protokole bilgi verir. Erişim hakkı tanınmışsa, bağlantı prosedürleri izlenir. Erişim reddedilmişse bağlantı sonlandırılır.

Eğer protokol katmanında erişim kontrolü yapılmazsa, güvenlik yöneticisi ile veya diğer birimlerle herhangi bir etkileşim olmaz.

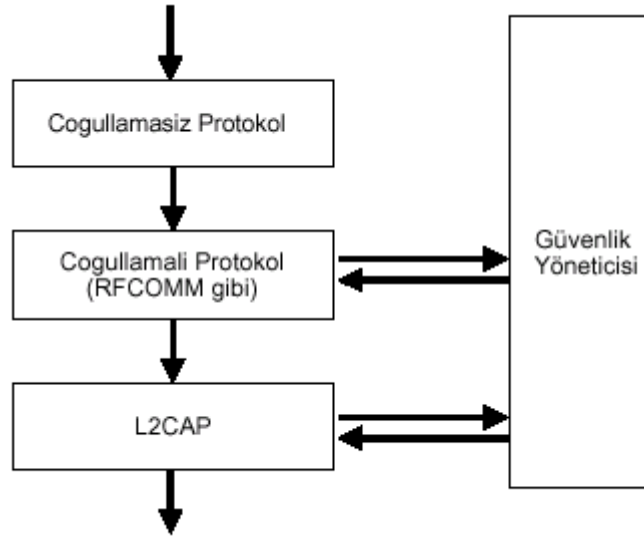


Şekil 5.3 Gelen bağlantılar için protokollerin davranışı

Bu modelde güvenlik yöneticisine iki sorgulama (fonksiyon çağırımı) yapılmaktadır. Güvenlik yöneticisi mevcut doğrulamalara ilişkin bilgiyi de tutabilir. Böylelikle LMP katmanı (örneğin hava) üzerinde aynı oturumda birden fazla doğrulama prosedürü yürütülmez.

RFCOMM güvenlik yöneticisine bir ilke (policy) kontrol çağrısında bulunur. Bu fazladan bir fonksiyon gerektirir fakat fazladan bir doğrulama gerektirmez.

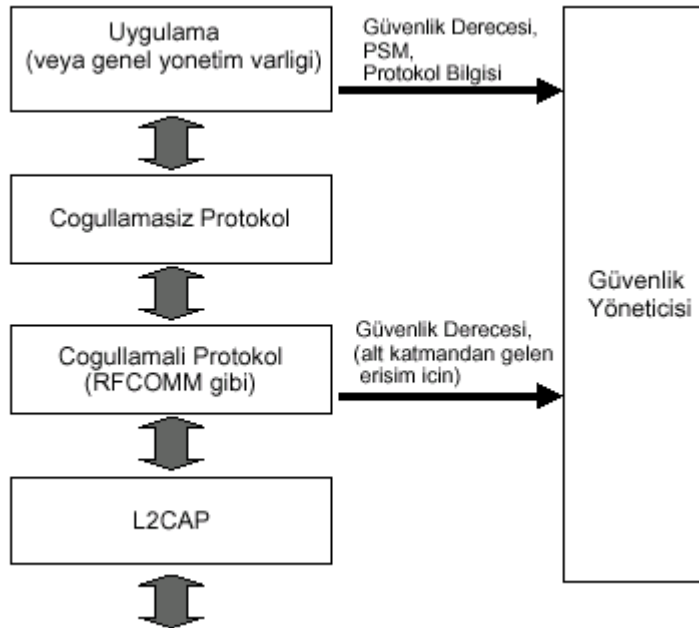
Giden bağlantılarda karşılıklı doğrulama (yetkilendirme çoğu durumda yararlı olmaz) yapılması için bir güvenlik kontrolü istenebilir. Giden bağlantılarda da gelenlere benzer bir prosedür uygulanır. En doğru yol hiç şüphesiz ki, uygulamanın güvenlik yöneticisi ile direkt temasa geçip talepleri göndermesidir. Bunun mümkün olmadığı durumlarda (örneğin bilinen mevcut uygulamalar) güvenlik yöneticisine yapılan sorgulamalar baştan sona çoğullama (multiplexing) protokolleri ile gönderilir (Şekil 5.4).



Şekil 5.4 Giden bağlantılar için protokollerin davranışı

5.3.3.4 Kayıt Prosedürleri

Bölüm 5.3.1 de belirtildiği gibi güvenlik yöneticisi güvenlik veri tabanlarındaki servisler için gereken güvenlik bilgisini sağlar. Uygulamalar erişilebilir olmadan önce güvenlik yöneticisine kayıt olmalıdır (Şekil 5.5).



Şekil 5.5 Kayıt prosesleri

Uygulamalar ya da uygulamaların güvenlik birimleri güvenlik kademelerini ve çoğullama (multiplexing) bilgilerini hazır bulundurmak durumundadırlar. (Bu konu güvenlik yöneticisinin bir protokol birimi tarafından bildirilen bir talep üzerine karar verebilmesi için gereklidir. İstekte bulunan protokol birimi çoğu durumda sonuç uygulama hakkında bilgi sahibi olmaz.)

Çoğullama (multiplexing) protokol işlemleri güvenlik yöneticisine sorgulama yaparlar.

İki kayıt da Bluetooth protokol yığnında izlenecek yok (path) tanımlamasından sorumlu olan birim tarafından yapılabilir. Hangi birimin kayıt işlemini yaptığı, yürütmeden bağımsızdır.

Hiçbir kayıt yapılmamışsa, güvenlik yöneticisi bölüm 5.3.2.3 de incelendiği gibi karar vermek için varsayılan güvenlik derecesini dikkate alır.

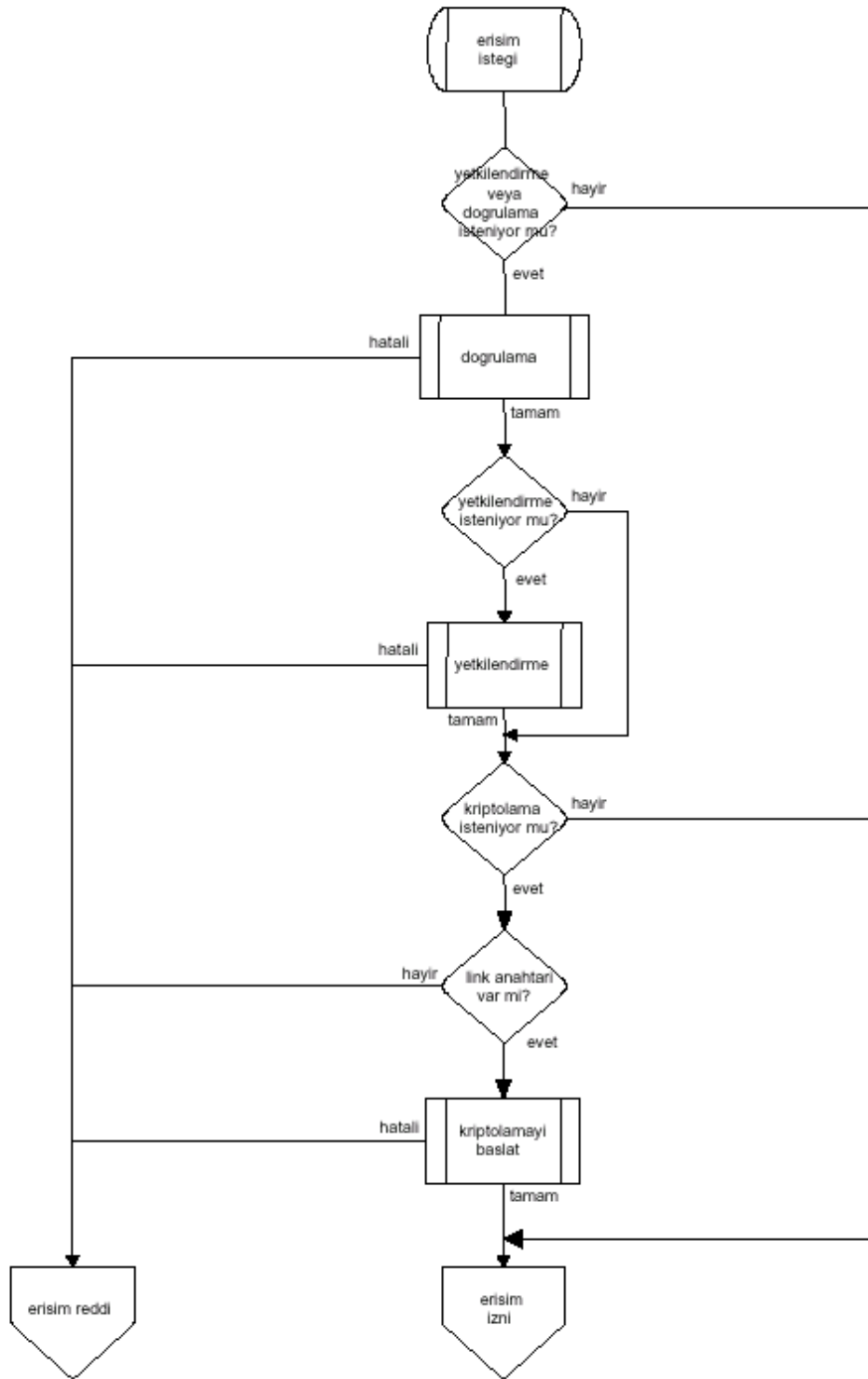
L2CAP burada kayıt istemez. L2CAP Bluetooth yığnındaki ilk çoğullama (multiplexing) protokolüdür ve her bağlantı talebi için bir sorgulama olacaktır.

5.3.3.5 Harici Anahtar Yönetimi

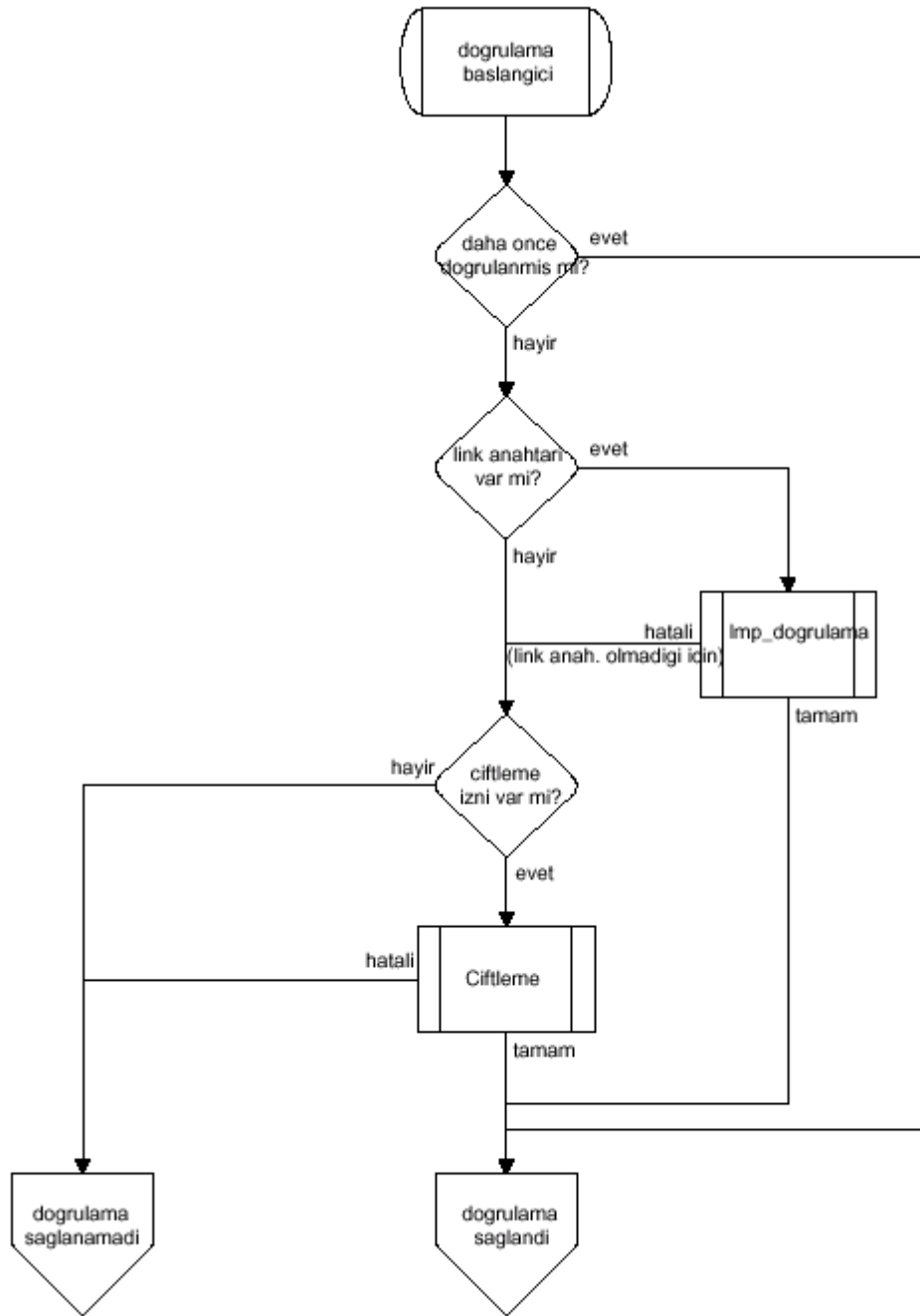
Bu yapı harici anahtar yönetim prosedürlerini hariç tutmaz. Anahtar yönetim uygulamaları PIN leri veya bağlantı linki anahtarlarını direkt olarak dağıtabilirler. Bu durumda Bluetooth uyumlu cihazların uygun etkileşimlerini sağlamak üzere ilerlenmelidir.

5.3.4 Erişim Kontrol Prosedürleri

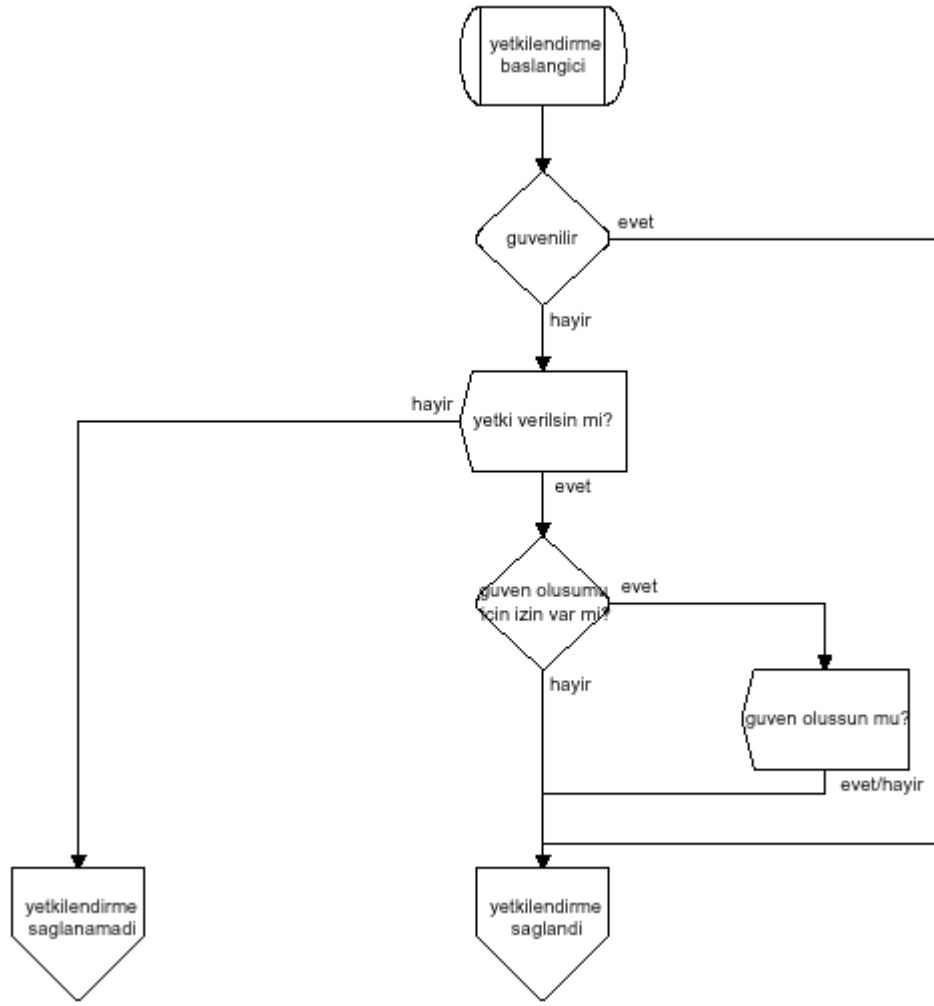
Bu bölümde güvenlik yöneticisinde erişim kontrolünün nasıl sağlandığı anlatılacaktır.



Şekil 5.6 Link Yöneticisi tarafından yapılan erişim kontrolü için örnek akış diyagramı



Şekil 5.7 Doğrulama prosedürü için örnek akış diyagramı



Şekil 5.8 Yetkilendirme prosedürü için örnek akış diyagramı

5.3.5 Bağlantısız L2CAP

Bir üstteki protokol veya uygulamaya bağlantı kurulması için L2CAP e güvenlik kontrolü amaçlı bir bağlantı isteği geldiği için, bağlantısız veri paketlerinin güvenlik kontrolü bu şekilde yapılamaz. Her bir bağlantısız veri paketi üzerinde güvenlik kontrolü yapmak pratik bir çözüm değildir. Bu sebeple L2CAP katmanında bağlantısız paketleri idare etmek üzere genel bir politika kullanılır.

L2CAP bağlantısız trafiği blok haline getirebilir. Bu blok L2CAP'in en üstündeki tek bir protokol (PSM) için yapılabileceği gibi, bir kısım ya da bütün protokoller için de yapılabilir. Her durumda bağlantısız trafik mümkün hale gelir.

Güvenlik yöneticisi, servis veri tabanında bağlantısız veri paketlerine izin vermeyen herhangi bir servis olup olmadığını kontrol etmelidir. Kontrol sonucuna göre de izin verir ya da vermez.

Eğer bağlantısız paketler geçmişse, herhangi bir güvenlik kontrolü yapılmaz. Bu durumda L2CAP'ın üzerindeki protokol herhangi bir güvenlik problemi olup olmadığını kontrol etmelidir. Veri bağlantılı veya bağlantısız modda olabilir fakat bağlantısız paketlerin kaynağı bilinmemekte ya da doğrulanamamaktadır.

5.4 Güvenlik Yöneticisinin Arayüzü ve Fonksiyonları

5.4.1 Veri tabanları

Güvenlik yapısını yöneten güvenlik yöneticisi birçok veri tabanını (ya da bilgi listesini) de korumak zorundadır.

Veri tabanı tabloları için şu kısaltmalar kullanılır:

Zorunlu destek için “M”

Opsiyonel destek için “O”

Koşula bağlı destek için “C”

Zorunlu, opsiyonel ve koşula bağlı durumları gerçekleyen güvenlik mimarisine bağlıdır. Basit veya karışık güvenlik uygulamaları farklı durumlar da gerektirebilir.

5.4.1.1 Servis veri tabanı

Servis veri tabanı her servis için aşağıda belirtilen güvenlikle ilgili girişleri yürütür. Bu bilgiler geçici olmayan bir hafızada tutulur veya servisler başlangıçta kayıt edilir.

Tablo 5.1 Servis veri tabanı güvenlik ile ilgili girişleri

Yetkilendirme İsteniyor	M	Boolean
Doğrulama İsteniyor	M	Boolean
Şifreleme İsteniyor	M	Boolean
PSM Değeri	M	Uint16
Yayın (broadcast) mümkün	O	Boolean
Diğer routing bilgisi	C	Structure TBD (sadece gerek görüldüğü duruma)

5.4.1.2 Cihaz veri tabanı

Güvenilirlik bilgisi geçici olmayan bir hafızada tutulmalıdır. Eğer girişler herhangi bir sebeple silinirse cihaz bilinmeyen bir cihazmış gibi işlem görür. Örneğin bölüm 5.3.2.3 de belirtildiği gibi varsayılan erişim kademesine atanır.

Tablo 5.2 Cihaz veri tabanı

BD_ADDR	M	48 Bit IEEE adresi
Güven derecesi	M	Güvenilir/Güvenilmez
Link Anahtarı	M	Bit alanı (uzunluğu en fazla 128 bit)
Cihaz İsmi	O	String (isim talebini önlemek için kullanılabilir)

5.4.1.3 Geçici depolama

Hava arayüzündeki fazla yükü azaltmak için bazı veriler depolanmalıdır. Her bir temelbant linki için aşağıdaki veriler geçici olarak depolanır:

- Doğrulama durumu
- Şifreleme durumu

5.4.2 L2CAP Arayüzü

L2CAP bir servise gelen veya giden bağlantı taleplerine ilişkin erişim haklarını güvenlik yöneticisinden kontrol eder. L2CAP Bluetooth protokol yığığında kullanılması zorunlu bir katman olduğu için herhangi bir kayıt prosedürü yoktur.

erişim :=SEC_erişimTalebi(

ProtokolTesbiti,

KanalTesbiti,

BD_ADDR,

BağlantıBaşlangıcı

GelenBağlantı

);

5.4.3 Diğer çoğullama (multiplexing) protokolleri arayüzü

Diğer çoğullama (multiplexing) protokolleri (RFCOMM gibi) servislere erişime karar vermek için L2CAP tekine benzer şekilde güvenlik yöneticisine danışırlar. Ek olarak çoğullama (multiplexing) protokolünün kendisine bağlantı için erişim politikası düzenleyen bir kayıt prosedürü bulunur

Erişim :=SEC_erişimTalep Çoğullama (Multiplexing)protokol (

ProtokolTesbiti,

KanalTesbiti,

BD_ADDR,

BağlantıBaşlangıcı

GelenBağlantı

);

5.4.4 ESCE Arayüzü

Güvenlik mimarisi yetkilendirme amaçları için kullanıcı etkileşimini de içermektedir. Bu durum servislere erişim hakkı verme ve uzak bir cihazla güvenli bir ilişki başlatmayı içermektedir.

Erişim = SEC_yetkilendirmeTalebi (

ServisAdı

CihazAdı,

&GelecektekiGüvenliİlişki = yanlış

);

Güvenlik yöneticisi ESCE yi (örneğin kullanıcı arayüzünü) çağırır; gelen parametreler taleple bildirilen bilgileri, giden parametreler ise cevabı taşır.

Eğer güvenlik yöneticisi tarafından PIN istenirse, ESCE ye yapılacak bir çağrı kullanılabilir. PIN girişi direkt link yöneticisinden de istenebilir (sonrasında güvenlik yöneticisi doğrulama ister, link yöneticisi de geçerli bir link mevcut değilse gerekli işlemleri yapar)

SEC_PinTalebi (

BD_ADDR,

İsim,

PIN

);

ESCE'nin güvenlik yöneticisinden diğer prosedürler dışında güvenli bir ilişki yaratmasını istemesi durumunda, basit bir komut seti kullanılır:

SEC_GüvenliİlişkiYarat (

BD_ADDR

);

ESCE güvenlik yöneticisini çağırır.

5.4.5 Kayıt Prosedürleri

Kullanılması gerekli olan bazı kayıt prosedürleri bulunmaktadır:

- Servislerin güvenlik dereceleri ve protokol yığın bilgileri
- L2CAP ın üzerindeki çoğullama (multiplexing) protokolleri

Bu kayıt işlemi Bluetooth protokol yığınınındaki izlenen yolu (path) düzenlemekle sorumlu olan birim tarafından yapılabilir. Kayıdı hangi birimin yaptığı yürütme bağımsızdır. Kayıt yapılmazsa varsayılan ayarlar uygulanır.

SEC_kayıtUygulama (

İsim,

GüvenlikDerecesi,

PSM,

ProtokolTesbiti,

KanalTesbiti,

);

SEC_kayıt Çoğullama (Multiplexing)Protokol (

ProtokolTesbiti,

AltProtokol,

AltKanal,

GüvenlikDerecesi,

);

5.4.6 HCI / Link Yöneticisi Arayüzü

5.4.6.1 Doğrulama Talebi

Uzak bir cihazın doğrulamasını istemek için HCI_Dogrulama_Istemi komutu ve cevap olarak da Doğrulama Tamamlandı olayları kullanılır.

5.4.6.2 Şifreleme Kontrolü

Şifreleme kontrolü için HCI_Bağlantı_Şifreleme_Ayarı komutu ve cevap olarak da Şifreleme Değişim olayları kullanılır.

5.4.6.3 Uzak cihazdan isim isteme

Uzak cihazdan isim isteme için HCI_Uzak_İsim_Talebi komutu ve cevap olarak da Uzak İsim Talebi Tamamlandı olayları kullanılır.

5.4.6.4 Link katmanında şifreleme politikası ayarı

Genel olarak link katmanında şifreleme politikası ayarı için HCI_Yaz_Şifreleme_Mod komutu ve cevap olarak da Komut Tamamlandı olayları kullanılır. Şifreleme modu parametresi Bluetooth ünitesinin diğer Bluetooth üniteleri ile her bağlantısında link katmanında şifreleme istemesi durumunu kontrol eder.

5.4.6.5 Link katmanında doğrulama politikası belirleme

Genel olarak link katmanında doğrulama politikası belirlemek için HCI_Yaz_Doğrulama_Yetki komutu kullanılır. Doğrulama_Yetki parametresi Bluetooth ünitesinin diğer Bluetooth üniteleri ile her bağlantısında link katmanında şifreleme istemesi durumunu kontrol eder. Cevap olarak Komut tamamlandı olayı kullanılır. [18,19]

6. BLUETOOTH PROFİLLERİ

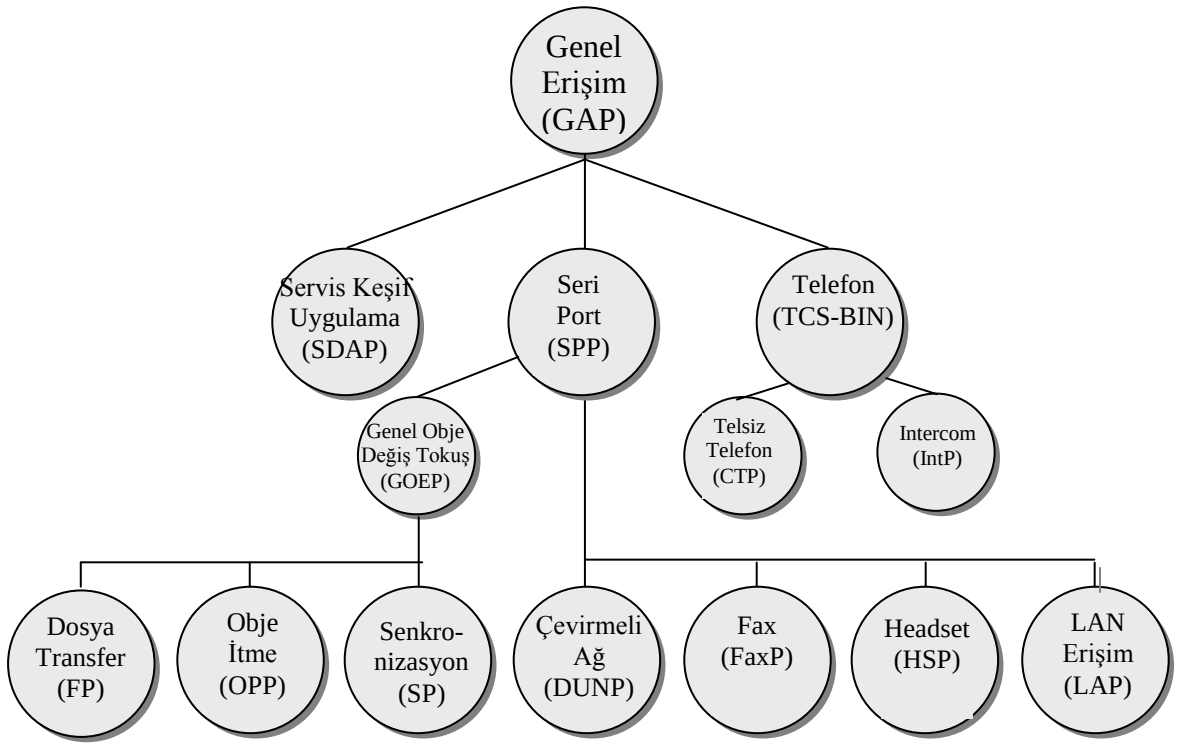
Bluetooth spesifikasyonunun 2. bölümü profilleri içermektedir. Profiller protokol yığınının birçok uygulaması arasında uyumluluk (interoperability) sağlamak için oluşturulmuşlardır. Bu bölümde profillerin genel yapıları, ortaya çıkış nedenleri, geçmişleri ve evrimleri ile aralarındaki iç ilişkileri incelenmiştir.

Versiyon 1.0 Profilleri

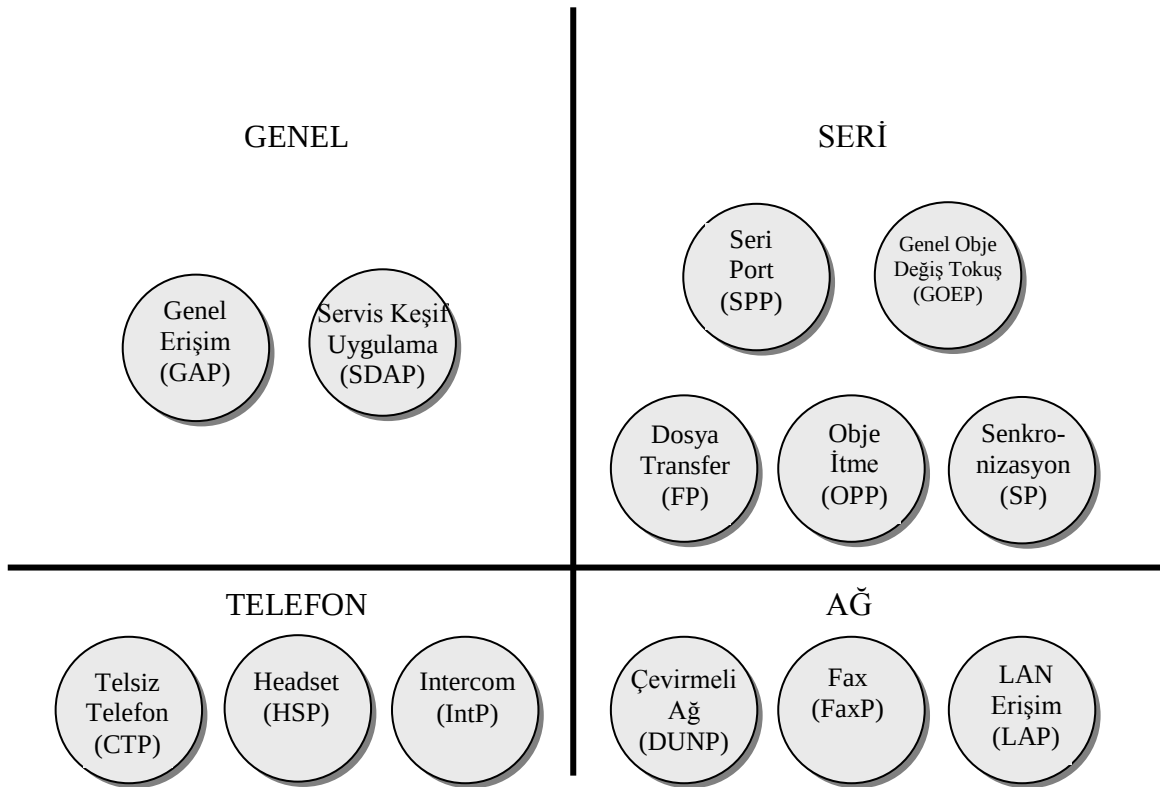
Profiller kullanım ihtiyaçlarından doğmuşlardır. Profillerin çoğu kullanım senaryolarının paylaşılan elementlerine dayanılarak birlikte gruplandırılabilir, bu bölümde de bu şekilde gruplandırılmışlardır. Profiller ayrıca teknik temellerine dayanarak da sınıflandırılabilirler. Versiyon 1.0 spesifikasyonu kullanım durumlarını kapsamayan ek profiller (genel erişim profili, servis keşif uygulama profili, genel nesne değiş-tokuş profili ve seri port profili) de içerir. Bu profillerden her biri; diğer uygulama profillerinin oluşturabildiği paylaşılan karakteristiklerden oluşan bir temel tanımlayan iletim profilleri olarak düşünülebilir.

Şekil 6.1, versiyon 1.0 profil ailelerini, teknik ilişkilerine dayanarak betimlemektedir. Şekil 6.1 bir nesne hiyerarşi gösterimi kullanmaktadır. Şekildeki parantez içindeki kısaltmalar spesifikasyonda kullanılan terminolojiyi belirtmektedir.

Bu bölümde her bir profil, Şekil 6.1 de gösterilen ilişkiye dayalı olarak anlatılmaktadır. Profilleri gruplamanın birçok yolu bulunmaktadır. Şekil 6.2 de lojik, servis tabanlı bir gruplama şekli görülmektedir. Bu çok yönlü görüş noktalarına bir örnek olarak mikrofon-kulaklık seti profili verilebilir. Şekil 6.1 de gösterildiği gibi, profil hiyerarşisinde mikrofon-kulaklık seti profili seri port profilinin bir türevidir. Bununla birlikte, Şekil 6.2 de gösterildiği gibi; işlevsel veya servisler ile ilgili bakış açısından mikrofon-kulaklık seti profili, telefon profil grubunun parçası olarak düşünülebilir. Başka bir örnek ise teknik bakış açısına göre bir seri port profili türevi olan faks profilidir. Faks profilinin işleniş şekli çevirmeli ağ şebekesinin ve LAN erişim profilleri ile birlikte, spesifikasyonun belirtmediği bir “ağ” kategorisi içinde ele alınabilir.



řekil 6.1 Protokol yıęını iliřkilerine gre sınıflandırılmıř Bluetooth profilleri



řekil 6.2 Servis tabanlı sınıflandırılmıř Bluetooth profilleri

Bu tartışma ve şekiller; versiyon 1.0 profillerinin bir çok şekilde kategorize edilebileceğini göstermek için tasarlanmıştır. Hangi metodun kullanılacağını seçimi ise genelde amaca dayalı olarak ve profillerin nasıl gruplanması gerektiğine bağlı olarak yapılır. Bununla birlikte, profillerin sayısının zamanla artması beklendiği için, profiller karışık olmayan yollardan gruplanmalı ve gruplama avantajlı olacak şekilde yapılmalıdır. [2]

6.1 Bluetooth Genel Profilleri

Bluetooth SIG, her biri bir “profil” ile ilişkilendirilmiş çeşitli kullanım modelleri tanımlamıştır. Profiller belirli bir kullanım modelini destekleyen protokolleri ve özellikleri tanımlar. Değişik üreticilerin ürettiği cihazlar aynı Bluetooth SIG profil özelliklerine uyuyor ise, o özel servis ve kullanım durumu için kullanıldıklarında birbirleri ile etkileşime girmeleri beklenir.

Bir profil bir özelliği uygulayabilmek için kullanılan özel mesajları ve prosedürleri tanımlar. Bazı özellikler zorunlu, bazıları seçime bağlı, bazıları ise koşulludur. Tanımlanmış tüm özelliklerin belirli bir şekilde uygulanmaları gerekmektedir. Bu durum sayesinde sağlanan özelliklerin üreticiden bağımsız olarak cihazlar için aynı şekilde çalışması sağlanır.

Çeşitli kullanım modellerinde gört genel profil kullanılır: Genel Erişim Profili (General Access Profile-GAP), Seri Port Profili (Serial Port Profile-SPP), Servis Keşif Uygulama Profili (Service Discovery Application Profile-SDAP) ve Genel Obje Değiş-Tokuş Profili (Generic Object Exchange Profile-GOEP).

6.1.1 Genel Erişim Profili

Genel Erişim Profili, Bluetooth cihazlarını keşfetmek ve aralarında haberleşme sağlamak için kullanılan link yönetim prosedürleri için genel prosedürleri tanımlar. Bu profilin temel amacı Bluetooth protokol yığınının alt katmanları olan Link Kontrol (Link Control-LC) ve Link Yönetim Protokolü (Link Management Protocol-LMP) nün kullanımını açıklamaktır. Daha üst katmanların -L2CAP, RFCOMM ve OBEX- dahil olduğu durumlarda güvenlik ile ilgili prosedürler de bu profile tanımlanmıştır.

Bu profil ayrıca kullanıcı arayüzünden erişilebilen parametreler için genel format gereksinimlerini de karşılar. Başka bir deyişle, cihazların bekleme (standby) ve bağlantı durumlarında nasıl davranmaları gerektiğini açıklar. Böylelikle Bluetooth cihazları arasında bekleme (standby) durumunda linklerin ve bağlantı durumunda kanalların kurulması garantilenir. Eğer cihazlar aynı anda birden fazla profile göre çalışıyorsa, GAP bunların tamamını idare etme için bir çalışma mekanizması tanımlar.

GAP, “keşfedilebilir modda” bulunan Bluetooth cihazlarının kimlikleri, adları ve temel yetenekleri gibi özelliklerini keşfetmek için kullanılan genel prosedürleri tanımlar. Keşfedilebilir modda olan bir cihaz diğer cihazlardan gelen servis ve bağlantı taleplerini kabul etmeye hazırdır. İki Bluetooth cihazının aynı uygulamayı paylaşmadığı durumda dahi, bu durumu belirlemek için birbirleriyle haberleşmelidirler. İki cihazın aynı uygulamayı paylaştığı fakat farklı üreticilere ait oldukları durumda, üreticilerin temel Bluetooth fonksiyonlarını kullanıcı arayüzü katmanında farklı adlarla çağırması veya temel prosedürleri değişik sırada uygulaması sayesinde bağlantı kurulması engellenmez.

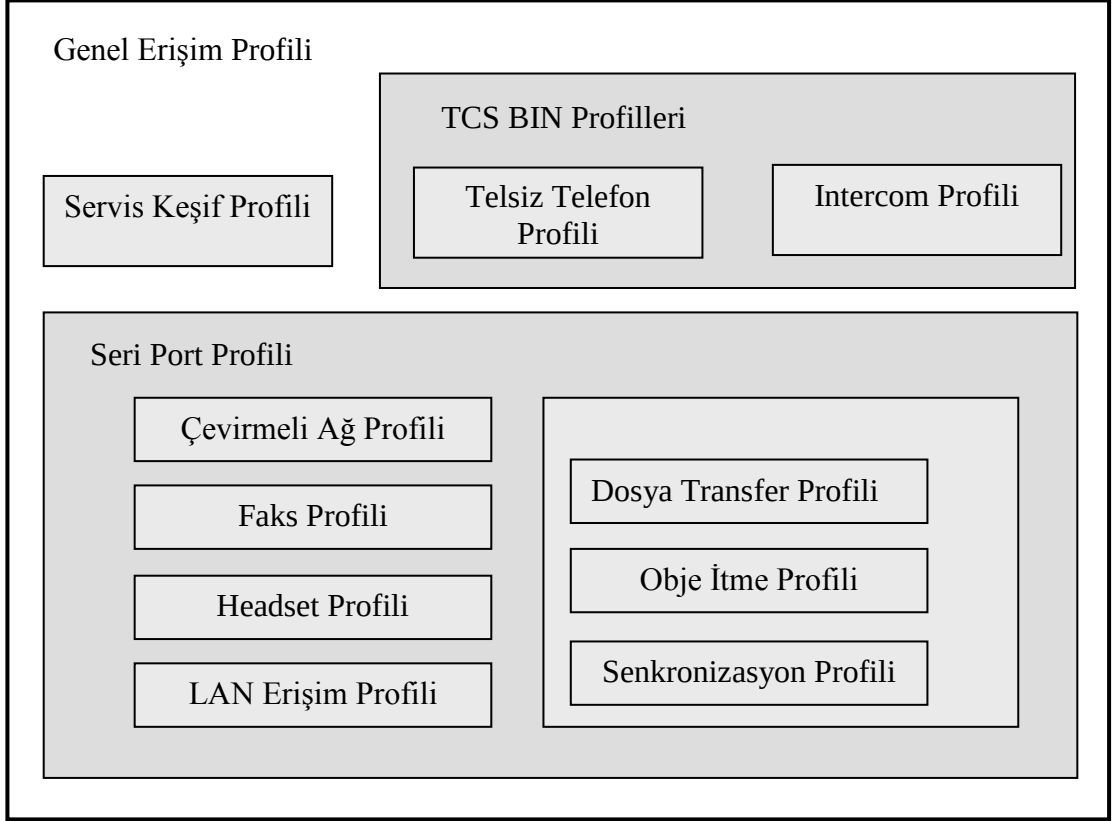
Bluetooth cihazları başka hiçbir profile uygunluk göstermeseler dahi, GAP a uygunluk göstermek zorundadır. Böylelikle cihazların desteklediği uygulamalardan bağımsız olarak temel uyumluluk ve bir arada çalışma fonksiyonları gerçekleşir. Başka bir profile uygunluk gösteren cihazlar hem o profil tarafından belirlenen temel prosedür adaptasyonlarını kullanmak hem de GAP ile uyumlu olmak durumundadır (Şekil 6.3).

6.1.1.1 Genel Parametreler

Üreticisi tarafından GAP a uygunluk gösterdiği söylenen bir ürün, profilin tüm zorunlu özelliklerini Bluetooth spesifikasyonunda belirtildiği şekilde desteklemelidir. Yine üretici tarafından sağlanan özelliklere göre profilin seçime bağlı ve koşula bağlı özellikleri de desteklenmelidir. Üretici tarafından sağlanan tüm özellikler Bluetooth sertifikasyon programı gereğince test edilir ve doğrulanır. Bluetooth cihazlarının genel prosedür seviyesinde çalışabilmeleri için desteklemek zorunda oldukları genel parametreler şunlardır:

Cihaz Adları

GAP, Bluetooth cihazlarının kullanışlı (user friendly) adlarının maksimum 248 byte uzunluğunda olmasına izin vermektedir. Buna rağmen, bir uzak cihazın ilk Bluetooth cihaz adının ilk 40 karakterinden daha fazlasını algılayacağı varsayılmaz. Uzak cihazın kısıtlı gösterge kapasitesi var ise, örneğin genellikle mobil telefonlarda olduğu gibi, sadece ilk 20 karakter kullanılacaktır.



Şekil 6.3 Genel Erişim Profili'nin diğer Bluetooth profilleri ve kullanım modelleri ile ilişkisi

Bluetooth PIN

Bluetooth PIN (personel identification number) daha önce güvenilir bir ilişkiye girmemiş ve link anahtarlarını değiş tokuş etmemiş olan iki Bluetooth cihazının doğrulama yapmasında ilk adım olarak kullanılır. PIN, çiftleme (pairing) prosedüründe doğrulama işleminin devamı için ilk link anahtarını oluşturmak için kullanılır. PIN kullanıcı arayüzü seviyesinde girilebilir, fakat giriş yapmaya uygun bir kullanıcı arayüzü yoksa cihazda depolanabilir.

Cihaz Sınıfı

Cihaz keşif prosedürü sırasında, uzak cihazdan kendi sınıfını ve desteklediği servis tiplerinin bilgisini içeren ve “Cihaz Sınıfı” olarak adlandırılan bir parametre iletilir. Kullanıcı PIN i girerek bağ kurma (bonding) prosedürünü başlatabilir veya kullanıcıdan bağlantı prosedürü sırasında daha önce genel bir link anahtarı paylaşılmadığı için PIN i girmesi istenir. Kullanıcı ilk durumda “bağ kurma (bonding)” işlemini, ikinci durumda ise “doğrulama” işlemini gerçekleştirmiş olur.

Keşif Modları

Bluetooth cihazları keşfedilebilir ya da keşfedilemez modda bulunabilirler. Kısıtlı ve genel olmak üzere iki keşfedilebilir mod vardır. Bir cihaz kısıtlı keşfedilebilir modda bulunduğu, kendisini sadece belli bir periyot için, geçici koşullar esnasında veya özel bir olay için uygun durumda tutar. Cihaz periyodik olarak “çağrı tarama durumu (page scan)” na girip belirli tipteki sorgulama kodlarını kontrol ederek kendisini uygun duruma getirir. Bu gibi durumlarda cihaz, Sınırlı Sorgulama Erişimi (Limited Inquiry Access-LIAC) olarak adlandırılan özel bir kod kullanarak kısıtlı sorgulama yapan başka bir Bluetooth cihazına cevap verebilir.

Bir cihaz genel keşfedilebilir modda bulunduğu, kendisini sürekli uygun durumda tutabilir. Bu gibi durumlarda cihaz, GIAC kullanarak genel sorgulama yapan başka bir Bluetooth cihazına cevap verebilir. Bir cihaz sadece bir keşfedilebilir modda (kısıtlı ya da genel) bulunabilir. Cihaz, keşfedilebilir olduğu durumda dahi başka bir temebant aktivitesi sebebiyle bir sorgulamaya cevap veremeyebilir. Bir Bluetooth cihazı keşfedilemez modda ise hiçbir tipte sorgulamaya cevap vermez.

Bağlantı Modları

Çağrı yapma (paging) prosedürüne göre, bir Bluetooth cihazı bağlanılabilir ya da bağlanılamaz modda bulunmalıdır. Çağrı yapma (paging), etki alanı içerisinde aktif olarak bulunan bir üniteye, o üniteyle bir haberleşme linki kurmak amacıyla bir mesaj dizisi gönderilmesini içeren bir prosedürdür. Bir Bluetooth cihazı bağlanılabilir modda ise kendisini “çağrı tarama (page scan)” durumuna getirir. Bir çağrı (page) alınması üzerine cevap verebilir. Bir Bluetooth cihazı bağlanılamaz modda ise kendisini “çağrı tarama (page scan)” durumuna getirmez. Bu durumda çağrı (page) alamayacağı için cevap da vermez.

Çiftleme (Pairing) Modları

Çiftleme (pairing), ilk defa haberleşen iki cihazın sonraki doğrulama işlemlerinde kullanmak üzere genel bir link anahtarı oluşturma süreçlerini başlatma prosedürüdür. İlk defa haberleşmede, çiftleme (pairing) prosedürü kullanıcının bir Bluetooth güvenlik kodu veya PIN girmesini gerektirir. Bluetooth cihazları çiftlenebilir (pairable) ya da çiftlenemez (non-pairable) modda bulunabilirler. Çiftlenebilir (pairable) modda bulunan bir Bluetooth cihazı uzak cihaz tarafından başlatılan çiftlemeyi (pairing) (örneğin bağların (bond) oluşturulmasını) kabul eder, çiftlenemez (non-pairable) modda ise etmez.

Güvenlik Modları

Bluetooth cihazları için üç güvenlik modu vardır. Bir cihaz güvenlik modu 1 de ise hiçbir zaman bir güvenlik prosedürü başlatmaz. Güvenlik modu 2 de ise bir kanal kurulum talebi alınmasından veya kendisi bir kanal kurulum talebinde bulunmadan önce bir güvenlik prosedürü başlatmaz.

Bir güvenlik prosedürünün başlatılması ya da başlatılmaması istenen kanalın ya da servisin güvenlik gereksinimlerine bağlıdır. En azından güvenlik modu 2 de bulunan bir Bluetooth cihazı servislerinin güvenlik gereksinimlerini doğrulama, yetki verme ve şifreleme açılarından sınıflandırmalıdır.

Bir Bluetooth cihazı güvenlik modu 3 de ise link kurulumunun tamamlandığını gösteren bir mesaj göndermeden önce güvenlik prosedürlerini başlatır. Güvenlik modu 3 te bulunan bir Bluetooth cihazı iç ayarlara dayalı olan bağlantı taleplerini reddedebilir.

6.1.1.2 Boş Mod Prosedürleri

Bir Bluetooth cihazı tarafından başlatılabilen ve uzak bir Bluetooth cihazına yöneltilen birkaç boş mod prosedürü vardır.

Genel Sorgulama

Genel sorgulama prosedürü, sorguyu başlatan cihaza Bluetooth cihaz adresi, saati, cihaz sınıfı ve genel keşfedilebilir cihazların çağrı tarama (page scan) modlarını sağlar. Başlatan cihazın etki alanı içinde bulunan GIAC ile sorgulama mesajları için taramaya ayarlanabilirler. Kısıtlı keşfedilebilir modda bulunan bütün cihazlar genel sorgulama prosedürü kullanılarak keşfedilir.

Kısıtlı Sorgulama

Kısıtlı sorgulama prosedürü, sorguyu başlatan cihaza Bluetooth cihaz adresi, saati, cihaz sınıfı ve kısıtlı keşfedilebilir cihazların çağrı tarama (page scan) modlarını sağlar. Başlatan cihazın etki alanı içinde bulunan cihazlar GIAC a ek olarak LIAC ile sorgulama mesajları için de taramaya ayarlanabilirler. Keşfedilebilir cihazın LIAC için taranacağı garanti edilmediği için, başlatan cihaz genel veya kısıtlı sorgulama prosedürünü seçebilir.

İsim Keşfi

İsim keşfinin amacı, başlatan cihaza diğer bağlanılabilir cihazların –özellikle etki alanı içinde ve çağrıya (paging) cevap verecek olan cihazların- cihaz isimlerini sağlamaktır. İsim keşfi bağlanılabilir cihazlardan cihaz ismi bilgisini alma prosedürüdür. Bu prosedür talebin cihaz adresleri uygun olan ve bilinen Bluetooth cihazlarına iletilmesi ile gerçekleşir.

İsim keşfi ile ilgili olan bir başka prosedür de “isim talebi” dir. İsim talebi de bağlanılabilir cihazlardan cihaz isimlerini almak için kullanılır. Cihazın sadece ismini öğrenmek için tam bir link kurulmasına gerek yoktur. İsim talebi prosedüründe, başlatan cihaz uzak cihazın sorgulama prosedürü başlamadan önce alınan cihaz erişim kodunu kullanır.

Cihaz Keşfi

Cihaz keşfinin amacı, sorguyu başlatan cihaza keşfedilebilir Bluetooth cihazlarının adres, saat, cihaz sınıfı, çağrı tarama (page scan) modu ve cihaz ismi bilgilerini sağlamaktır. Cihaz keşif prosedürü sırasında, genel veya kısıtlı bir sorgulama yapılarak, sorgulamaya cevap veren bazı veya tüm cihazlar için isim keşfine başlanır.

6.1.1.3 Bağ Kurma (Bonding)

Bağ kurmanın (bonding) amacı iki Bluetooth cihazı arasında genel bir link anahtarına (bir bağ (bond)) dayalı olarak ilişki kurmaktır. Link anahtarı bağ kurma (bonding) prosedürü sırasında oluşturulur, değiş tokuş edilir (çiftlenir) ve tipik olarak her iki cihazda da gelecekteki doğrulamalarda kullanılmak üzere depolanır. Bağ kurma (bonding) prosedürü çiftlemeye (pairing) ek olarak üst katman başlangıç prosedürlerini de içerebilir.

Adanmış ve genel olmak üzere iki tip bağ kurma (bonding) bulunmaktadır. Adanmış bağ kurma (bonding) cihazlar sadece bir genel link anahtarı oluşturup değiş tokuş ederlerse meydana gelir. Genel bağ kurma (bonding) ise normal kanal ve bağlantı kurulum prosedürlerinin bir parçasıdır. Bağ kurma (bonding) link kurulumu ile aynı prensiptedir. Eğer hedef cihaz normal bağlanılabilirlik ve güvenlik modlarındayken bir cihaz bağ kurma (bonding) başlatmışsa, çiftleme (pairing) başarı ile gerçekleşir.

Bağ kurma (bonding) başlamadan önce, başlatan cihaz eşleşeceği cihazın cihaz erişim kodunu bilmelidir. Bu normal olarak ilk önce cihaz keşfinin yapılması ile sağlanır. Bağ kurma (bonding) başlatan bir Bluetooth cihazı kısıtlı sorgulama kullanır, bağ kurmayı (bonding) kabul eden Bluetooth cihazı da kısıtlı keşfedilebilir modu destekler.

6.1.1.4 Kuruluş Prosedürleri

Bluetooth spesifikasyonunda tanımlanmış üç kuruluş prosedürü bulunmaktadır: link, kanal ve bağlantı. Herhangi bir kuruluş prosedürü başlatılmadan önce, cihaz keşfi sırasında sağlanan belirli bilgiler başlatan tarafa olanaklı hale getirilmelidir:

- Cihaz erişim kodunun oluşturulduğu cihaz adresi
- Uzak cihazın sistem saati
- Uzak cihaz tarafından kullanılan çağrı tarama (page scan) modu

Cihaz keşfi sırasında elde edilen bu bilgiler dışında elde edilebilecek cihaz sınıfı ve cihaz ismi bilgileri de kuruluş prosedürü başlatma kararı vermek için faydalı olacaktır.

Link Kurulumu

Link kurulum prosedürü, Bluetooth IrDA Uygunluk Spesifikasyonu ve Genel Obje Değiş Tokuş Profili prosedürlerini kullanan iki Bluetooth cihazı arasında fiziksel bir link kurmak –özellikle bir ACL linki- için kullanılır.

Bluetooth da kullanılan çağrı (paging) prosedürü Bluetooth IrDA Uygunluk Spesifikasyonu'na uygunluk gösterir. Çağrıyı yapan (paging) ünite önceki bir sorgulamadan elde edilen cihaz erişim kodu ve çağrı (page) modunu kullanır. Çağrı (paging) tamamlandıktan sonra, iki Bluetooth cihazı arasında fiziksel bir link kurulur. Eğer yönetici-köle rollerinin değişmesi isteniyorsa -genellikle rol değişimini

isteyen cihaz çağrı yapılan (paged) cihazdır- bu değişim fiziksel link kurulduktan sonra yapılır. Eğer çağrıyı yapan (paging) cihaz bu rol değişimini kabul etmezse, çağrı yapılan (paged) cihaz fiziksel linkin kurulup kurulmamasına karar verir. İki cihaz da link kurulumunu uzak taraftaki host ile etkileşime girmeksizin Link Yönetim Protokolü (LMP) prosedürlerini kullanarak gerçekleştirirler. Seçime bağlı olan LMP özellikleri diğer cihazın istenen özelliği desteklediği onayı ile kullanılabilir.

Çağrıyı yapan (paging) cihaz link kurulum aşamasından sonra, ihtiyaç duyarsa uzak cihazın sunucusuna bağlanmayı talep edebilir. Çağrı yapılan (paged) cihaz güvenlik modu 3 te ise, bu talep doğrulama başlangıcını tetikler. Daha sonra çağrıyı yapan (paging) cihaz link kurulumu sırasında fakat kanal kurulumundan önce bir host bağlantı talebi gönderir ve doğrulama sürecini başlatır. Doğrulama gerçekleşikten sonra, cihazlardan herhangi biri şifrelemeyi başlatabilir.

Bu işlemler sonrasında link konfigürasyonu sunucu bağlantı talebinden sonra gerçekleşir. İki cihazın da gereksinimleri sağlandığında, her iki taraf da birbirine kurulumun tamamlandığına dair bir mesaj gönderir.

Kanal Kurulumu

Kanal kurulum prosedürü Bluetooth Dosya Transferi Profili ni kullanan iki Bluetooth cihazı arasında bir kanal (lojik bir link) kurmak için kullanılır. Kanal kurulumu, link kurulumu tamamlandıktan sonra başlar. Bu noktada, başlatan cihaz bir kanal kurulum talebi gönderir. Kanal kurulum işlemi başladıktan sonra güvenlik prosedürleri uygulanır. Uzak cihazın kanal kurulum talebine vereceği pozitif cevap ile kanal kurulumu tamamlanmış olur.

Bağlantı Kurulumu

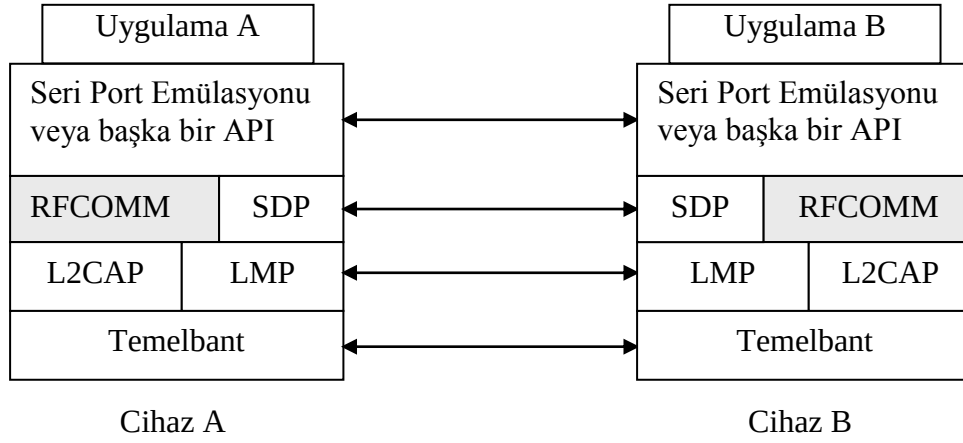
Bağlantı kurulum prosedürü, iki Bluetooth cihazındaki uygulamalar arasında bağlantı kurmak için kullanılır. Bağlantı kurulumu, kanal kurulumu tamamlandıktan sonra başlar. Bu noktada, başlatan cihaz bir bağlantı kurulum talebi gönderir. Gönderilen özel talepler uygulamaya bağlı olarak değişir. Bir Bluetooth telefon uygulamasında TCS SETUP mesajı gönderilirken, seri port tabanlı bir uygulamada RFCOMM başlangıcı ve veri-linki bağlantısının kurulması talep edilebilir. Uygulama her ne olursa olsun, uzak cihaz bağlantı kurulum talebini kabul ettiğinde bağlantı kurulumu tamamlanmış olur.

Bir Bluetooth cihazı bir başka Bluetooth cihazı ile bağlantı kurduğunda, aynı kanal üzerinde ikinci bir bağlantı, aynı link üzerinde ikinci bir kanal veya ikinci bir fiziksel link kurmak ya da bunların herhangi bir kombinasyonunu uygulamak mümkündür. Aynı cihaz ile yapılacak yeni kurulum prosedüründe, kurulumun güvenlik kısmı kullanılmakta olan güvenlik modlarına bağlıdır. Eğer farklı bir uzak cihaz ile yeni bir bağlantı prosedürü başlatılmak isteniyorsa, başlatan cihaz kurulu olan fiziksel link gerçeği göz önünde bulundurulmaksızın aktif modlara göre davranır. [9]

6.1.2 Seri Port Profili

Seri port profili Genel Erişim Profili üzerine inşa edilmiştir ve Bluetooth cihazlarının RFCOMM kullanarak seri kablo emülasyonu gerçekleştirmeleri işlemini tanımlar. RFCOMM iki cihaz arasında RS-232 seri port haberleşmesini emüle eden temel bir iletim protokolüdür (Şekil 6.4). RFCOMM kullanıcı verisi, modem kontrol işaretleri ve konfigürasyon komutlarını iletmek için kullanılır. RFCOMM oturumu bir L2CAP kanalı üzerinde çalışır. Her iki cihazdaki uygulamalar da seri bir kablo üzerinden haberleşerek çalışan uygulamalardır.

Cihazlarda çalışan uygulamalar, sanal seri portu fiziksel bir seri kablo olarak kullanırlar. Bu uygulamalar seri kablo emülasyonu için kullanılan Bluetooth prosedürlerinin farkında olmadıkları için, linkin her iki tarafında Bluetooth spesifikasyonunu kullanan yardımcı bir uygulamaya ihtiyaç duyulur. Bluetooth spesifikasyonu yardımcı uygulamalar için gereksinimleri tanımlamaz, çünkü Bluetooth SIG in üzerinde en önemle durduğu konu uyumluluktur. Bu sebeple iki cihazı birleştirecek bir uygulamanın çözüm üreten firma tarafından önerileceği varsayılmaktadır.



Şekil 6.4 Emüle edilmiş bir seri kablo bağlantısı için protokol modeli

İki bilgisayarın bir seri kablo ile birbirlerine bağlı oldukları temel bir seri port konfigürasyonunda, bir cihaz diğer bir cihazla bağlantıyı başlatma görevini üstlenir. Bu cihaz “başlatıcı”, bağlantı için hedeflenen cihaz ise “kabul edici” olarak adlandırılır. Başlatıcı cihaz link kurulumuna başladığında, seri kablo emülasyon bağlantısını kurmak için servis keşif prosedürleri uygulanır.

Seri port profilinde veri hızı 128 kbit/sn. ye kadar desteklenmektedir. Bluetooth spesifikasyonu tarafından iki cihaz arasında noktadan noktaya tek bir seri port emülasyon bağlantısı tanımlanmakla birlikte, aynı cihaz üzerinde aynı anda çoklu bağlantı kurulması da mümkündür. Bu gibi durumlarda, cihazlar aynı anda hem başlatıcı, hem de kabul edici rollerini üstlenebilirler. Cihazların eş olduğu kabul edildiği için bu profile belirlenmiş kesin bir yönetici-köle rol tanımı yoktur.

Doğrulama, yetkilendirme ve şifreleme gibi güvenlik özellikleri desteği seçime bağlıdır. Bununla birlikte bir cihaz, eş olan bir cihaz tarafından talep edildiği durumda, uygun güvenlik prosedürlerini desteklemelidir. Bir güvenlik özelliğinin kullanılması isteniyorsa, iki cihaz bağlantı kurulum aşamasında eşleştirilir. Bağ kurma (bonding) desteği de güvenlik özellikleri gibi seçime bağlıdır.

6.1.2.1 Uygulama Seviyesi Prosedürleri

Bluetooth spesifikasyonunda üç adet uygulama seviyesi prosedür tanımlanmıştır ve bu prosedürler iki cihaz arasında bir seri kablo bağlantı emülasyonu kurmak için gereklidir.

Link Kurma/Sanal Seri Bağlantı Kurma

Bu prosedür uzak cihazın emüle edilmiş seri portuna bağlantı kurmak için gereken adımları tanımlar:

1. Uzak cihazdaki uygulamanın RFCOMM sunucu kanal numarasını belirlemek için SDP kullanarak bir sorgulama yapılır. Eğer tarama (browsing) yeteneği varsa, kullanıcı diğer cihazdaki uygun portlar (veya servisler) arasından seçim yapabilir. Kullanıcı bağlanacağı servisi kesin olarak biliyorsa, o servis ile ilgili olan Servis Sınıfı ID sini kullanarak parametreleri araması yeterlidir.
2. Bir opsiyon olarak, uzak cihazın kendisini doğrulaması istenebilir; başka bir opsiyon olarak da şifreleme olanaklı hale getirilebilir.
3. Uzak RFCOMM birimine yeni bir L2CAP kanalı istenir.
4. L2CAP kanalında bir RFCOMM oturumu başlatılır.
5. RFCOMM oturumunda 1. adımda belirtilen sunucu kanal numarası kullanılarak yeni bir veri linki bağlantısı başlatılır.

Bu prosedür tamamlandığında, her iki cihazda da uygulamalar tarafından kullanılmak üzere sanal seri kablo bağlantısı hazır hale gelmiş olur. Eğer yeni bir veri linki bağlantısı kurulduğunda cihazlar arasında bir RFCOMM oturumu hali hazırda mevcut ise, yeni bağlantı mevcut RFCOMM oturumu üzerinde kurulur ve 3. ile 4. adımlara gerek kalmaz.

Link Kabulü/ Sanal Seri Bağlantı Kurma

Bu prosedür kabul edicinin aşağıdaki adımları sağlamasını gerektirir:

1. Doğrulama istenmişse sağlanır ve akabindeki taleplerle şifreleme başlatılır.
2. L2CAP ten gelen başlatma talebi ile yeni bir kanal kurulumu kabul edilir.
3. Kurulan kanal üzerinde bir RFCOMM oturumu sağlanması kabul edilir.
4. RFCOMM oturumu üzerinde yeni bir veri linki bağlantısı kabul edilir.

Eğer kullanıcı seri port emülasyonunun güvenlik gereksinimlerini yerine getirmesini istiyorsa, son madde uzak cihazın doğrulanması ve şifrelemeye başlanması için lokal bir talebi tetikler.

Servis Kaydının Lokal SDP Veri Tabanına Kaydedilmesi

RFCOMM üzerinden erişilebilen bütün servisler/uygulamalar, ilgili servise/uygulamaya erişmek için gereken parametreleri içeren bir SDP servis kaydına sahip olmalıdır. Bu kayıt bir servis veri tabanına ve SDP sorgularına cevap vermeye gereksinim doğurur. Sanal seri portlar üzerinde çalışan uygulamaları desteklemek için, servis kaydı kullanıcıya portu ayarlarken yardımcı olan bir uygulama tarafından yapılır.

6.1.2.2 Güç Korunumu ve Kayıp Link Durumu

Birbirlerine emüle edilmiş seri portlarla bağlı olan cihazların güç gereksinimleri birbirlerinden oldukça farklı olabilir. Bu sebeple Seri Port Profili dahilinde herhangi bir güç korunum modu kullanımına gerek duyulmaz. Ancak, düşük-güç modu kullanmak için gelen talepler geri çevrilmez. Eğer koklama, park veya durağan mod kullanılıyorsa, ne RFCOMM veri-linki bağlantısı ne de L2CAP kanalı kurulur. Eğer bir ünite linkin kaybolduğunu teşhis ederse, RFCOMM kapatılmış varsayılır. Üst katmanlardaki haberleşme kaldığı yerden devam etmeden önce, RFCOMM oturumu başlangıç prosedürü uygulanmak zorundadır.

6.1.2.3 RS-232 Kontrol İşaretleri

Kablo tabanlı seri port bağlantılarında cihazlar arasındaki akış kontrolü Transmitter On/Trasmitter Off (XON/XOFF) karakterleri kullanarak yazılım kontrolü ile ya da Request to Send/Clear to Send (RTS/CTS) veya Data Terminal Ready/Data Set Ready (DTR/DSR) gibi işaretler kullanarak sağlanır. Bu yöntemler kablonun iki ucundaki cihazlar tarafından veya sadece bir yönde kullanılabilir.

RFCOMM protokolü iki akış kontrol mekanizması sağlamaktadır. Bunlardan biri RS-232 işaretlerini taşıyan Modem Durum Komutu (Modem Status Command-MSC) dur. Bu akış kontrol mekanizması tekil veri linki bağlantılarında çalışır. RFCOMM protokolü iki cihaz arasındaki toplam veri akışı üzerinde çalışan kendi akış kontrol komutlarını –Flow Control On/Flow Control Off(FCON/FCOFF)- da kullanır.

Eğer lokal cihaz fazla çalışma (overrun), parite veya çerçeveleme hatalarının oluşabileceği bir fiziksel seri porttan bilgi aktarıyorsa, uzak cihaz Uzak Hat Durum Göstergesi (Remote Line Status Indication) komutu ile RS-232 hattındaki herhangi bir değişiklikten haberdar edilmelidir.

RS-232 port ayarları cihazlar arasında veri linki kurulumundan önce “Remote Port Negotiation” komutu ile aktarılır.

6.1.2.4 L2CAP Uygunluk Gereksinimleri

Yukarıda belirtildiği gibi Seri Port Profili sadece bağlantı yönelimli kanallar için kullanılır. Bağlantısız kanallar bu profil içine dahil edilmemiş olmasına rağmen, iki tip kanalın da başka profiller ve uygulamalar tarafından kullanılmasına izin verilmiştir.

İşaretleşme

Bu profil dahilinde yalnızca başlatıcı bir L2CAP bağlantı talebinde bulunabilir. Bunun dışında Seri Port Profili nin L2CAP işaretleşmesi için getirdiği başka bir kısıtlama yoktur.

Konfigürasyon Seçenekleri

Seri Port Profiline L2CAP için üç konfigürasyon seçeneği mevcuttur. Birincisi veri linki üzerinden mümkün olan en yüksek miktarda verinin gönderilmesine izin veren MTU nun boyutudur. L2CAP uygulamaları minimum 48 byte lık bir MTU boyutunu desteklemelidir. Varsayılan değer 672 byte dır. Haberleşmeye dahil olan cihazların fiziksel kısıtlamalarının gözönünde bulundurulması ve cihazlar arasında daha önce kararlaştırılmış olan QoS değerlerinin yerine getirilmesi, başka bir deyişle haberleşme kaynaklarının verimli kullanılması için MTU mümkün olduğu kadar büyük tutulmalıdır.

Diğer bir konfigürasyon seçeneği de Temizleme (Flush) Zaman Aşımı dır. Bu seçenek alıcıyı başlatıcının link kontrolörü/link yöneticisinin bir L2CAP segmentinden vazgeçip, paketi “temizlemeden (flush)” önce başarılı olarak iletmeyi denemek için kullandığı zaman miktarı hakkında bilgilendirmek için kullanılır.

Üçüncü opsiyon QoS opsiyonudur. L2CAP uygulamalarının sadece “en iyi çaba” servisi desteği olması istendiği için diğer servis destekleri seçime bağlıdır. “En iyi çaba” servisi performans garantisi içermez. Eğer bir QoS garantisi talep ediliyorsa, gecikme değişimi (mikro saniyeler), tepe bant genişliği (byte/saniye) ve gecikme süresi (mikro saniyeler) gibi performans parametrelerini içeren bir QoS konfigürasyon talebi gönderilmelidir. Eğer talepte herhangi bir QoS seçeneği yoksa “en iyi çaba” servisi olduğu varsayılır.

6.1.2.5 SDP Uygunluk Gereksinimleri

Lokal cihazda Seri Port Profili ile ilgili hiçbir SDP Servis Kaydı yoktur. Bununla birlikte, uzak cihazın SDP veri tabanında Seri Port ile ilgili girişler bulunur. Bu girişler ServiceClassIDList, ProtocolDescriptorList ve ServiceName gibi özellikler içerir. Bu servis kayıtlarını profili destekleyerek almak için, lokal cihazdaki SDP istemci varlığı, SDP ve L2CAP prosedürlerini kullanarak uzak cihazdaki SDP sunucu varlığına bağlanmalı ve etkileşime girmelidir.

6.1.2.6 Link Yöneticisi Uygunluk Gereksinimleri

Link Yöneticisi spesifikasyonunda belirtilen gereksinimlere ek olarak; Seri Port Profili haberleşen iki cihazda da şifreleme desteğine gereksinim duyar.

Hata Davranışı

Bir Bluetooth ünitesi zorunlu bir özelliği kullanmak ister ve diğer ünite bu özelliği desteklemediği şeklinde bir cevap verirse, bağlantıyı başlatan cihaz “desteklenmeyen LMP özelliği” sebepli bir bağlantı sonu mesajı gönderir. Seçime bağlı olan bir özellik talebi için gelebilecek olası bir red cevabı her zaman işlem görebilir olmalıdır.

Link İlkesi (Policy)

Seri Port Profiline kesinleşmiş yönetici-köle rolleri yoktur. Ayrıca hangi düşük-güç modlarının kullanılacağı ve ne zaman kullanılacağına ilişkin de bir zorlama yoktur. Herbir cihazın Link Yöneticisi bu konulara kendisi karar vererek, uygun olduğunda talep oluşturabilir.

Link Yöneticisi Uygunluğu

Link Kontrol (Link Control-LC) katmanı sorgulama, sorgulama tarama, çağrı yapma (paging) ve hata davranışı gibi bir çok prosesi tanımlar

Sorgulama

Lokal cihazda bir sorgulama olduğunda, GAP'ta açıklanan Genel Sorgulama Prosedürünü kullanır. Sadece lokal cihaz Seri Port Profilini oluşturmak suretiyle sorgulama prosedürünü başlatabilir.

Sorgulama Tarama

Sorgulama tarama için, eğer uzak cihazda çalışan uygulama için de uygunsa GAP ta tanımlanan kısıtlı keşfedilebilir moda göre GIAC kullanılır. Uzak cihaz sorgulama taramaya sorgulama cevap mesajları ile cevap verir.

Çağrı Yapma (Paging)

Seri Port Profili uygulamasında sadece lokal cihaz çağrı (page) yapabilir. Eğer lokal ve uzak cihazlar arasında zaten bir temelbant bağlantısı kurulmuşsa, çağrı (paging) aşaması yapılmadan atlanır. Bu durumda bağlantı bir önceki çağrının (page) bir sonucu olarak kurulur.

Hata Davranışı

LC katmanındaki özelliklerin çoğu LMP prosedürleri tarafından aktive edilmek zorunda olduğu için, hatalar da bu katmanda yakalanır. Sorgulama ve çağrı (paging) gibi bazı LC prosedürleri ise LMP katmanından bağımsızdır. Bu sebeple bu özelliklerin yanlış kullanımının farkına varmak çok zordur ve SPP içinde bu gibi durumlar için herhangi bir dedeksiyon mekanizması tanımlanmamıştır. [2,9]

6.1.3 Servis Keşif Uygulama Profili

Servis Keşif Uygulama Profili (Service Discovery Application Profile-SDAP), diğer Bluetooth cihazlarında kayıtlı olan servisleri keşfetmek ve bu servislerle ilgili bilgi almak için kullanılan özellik ve prosedürleri tanımlar.

Bu profilde, daha önce Seri Port Profili'nde de belirtildiği gibi, sadece bağlantı yönelimli kanallar kullanılır. Ve hiçbir L2CAP yayını (broadcast) kullanılmaz. İki Bluetooth cihazı birbirleriyle haberleşmeden önce güçleri açılmış (power on) ve başlatılmış olmalıdırlar. Başlatma işlemi cihaz doğrulaması ve veri şifrelemede kullanılacak bir link anahtarının oluşturulması için bir PIN sağlanmasını gerektirir. Sonrasında link oluşturulur; link oluşturma da diğer ünitenin Bluetooth cihaz adresini bir sorgulama prosesi ile keşfetmek ve diğer cihaza çağrı yapmak (page) ile mümkün olur.

Bluetooth protokol yığnında yer alan Servis Keşif Protokolü ile, bir Bluetooth cihazının etki alanındaki cihazlara/cihazlardan uygun servislerin yerleşimi sağlanır. Link kurulduğunda, servisler yerleştirilebilir ve bir veya birden fazlası kullanıcı arayüzü üzerinden seçilebilir. SDP direkt olarak özel bir servise erişme ile ilgili

olmadığı halde, lokal Bluetooth yığınına yönlendirerek istenen cihaza erişmeyi sağlar. Diğer profillerden farklı olarak, servis keşif işlemleri RFCOMM gibi bir iletim servisini olanaklı hale getirmek için gerekli olduğundan veya dosya transferi gibi bir kullanım şekli için, bu profil kullanıcı tarafından başlatılmayı gerektirir.

SDP aşağıdaki servis sorgulamalarını destekler:

- Servis sınıfına göre arama
- Servis özelliklerini arama
- Servis tarama (browsing)

Sorgulamalardan ilk ikisi özel servisler için arama yapıldığında kullanılır. “Servis X uygun mu” ya da “Servis X, 1 ve 2 nolu karakteristikleri ile uygun mu” gibi kullanıcı sorularının cevabını sağlar. Servis tarama (browsing) ise genel servis arama için kullanılır. “Hangi servisler uygun” veya “X tipinde hangi servisler uygun” gibi kullanıcı sorularının cevabını sağlar. Bu servis sorgulamalarının herhangi birini uygulayabilmek için cihazlar keşfedilmiş ve aralarında bir link kurulmuş olmalıdır.

6.1.3.1 İstemci ve Sunucu Roller

Servis Keşif Protokolü, Bluetooth cihazlarının rollerini lokal cihaz (LocDev) ve uzak cihaz (RemDev) olarak tanımlar. LocDev servis keşif prosedürünü başlatan cihazdır. Bunu başarabilmek için en azından Bluetooth SDP yapısının istemci kısmını içermelidir. Bir LocDev, kullanıcının keşif işlemini başlatabilmesi ve bu keşiflerin sonuçlarını gösterebilmesi için bir servis keşif uygulaması (SrvDscApp) içermelidir.

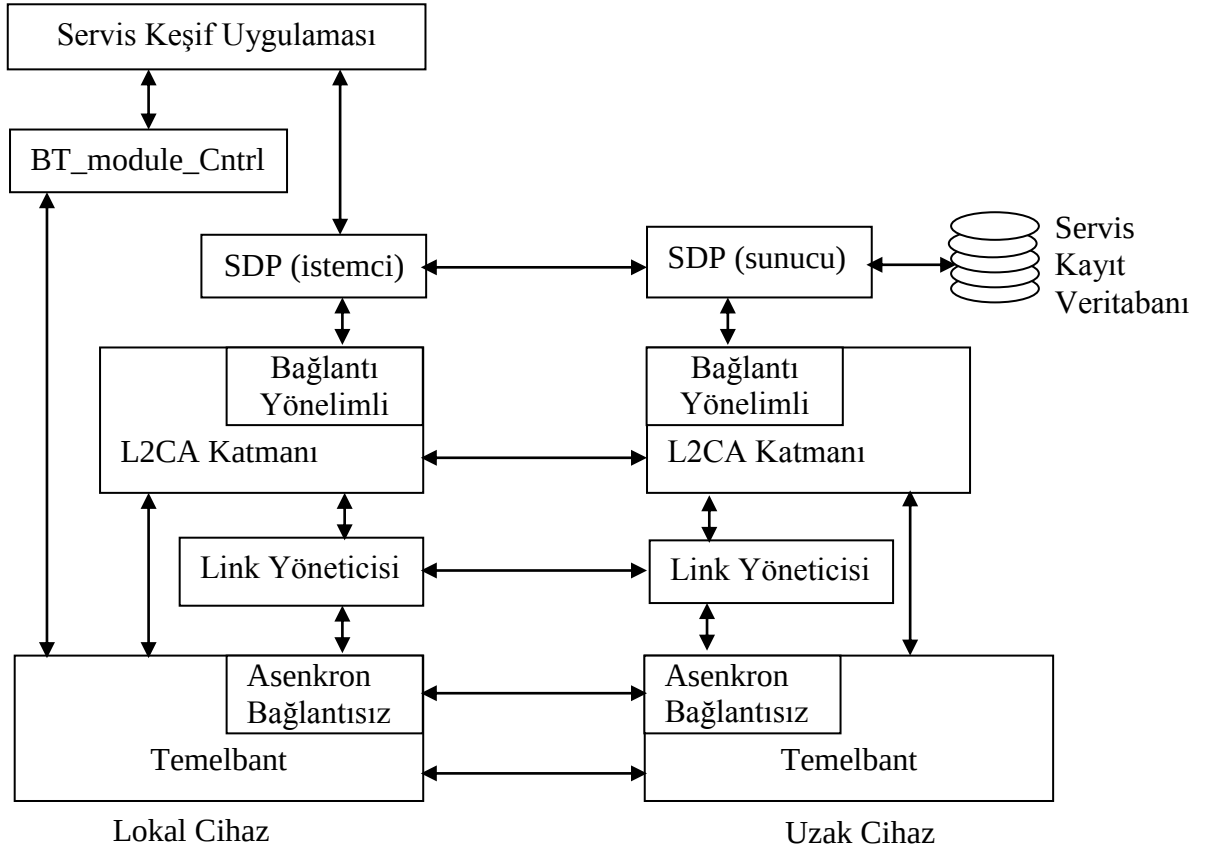
RemDev, bir lokal cihaz tarafından oluşturulan servis sorgulamalarına cevap vererek servis keşif prosesine katılan herhangi bir cihazdır. Bunu başarabilmek için en azından Bluetooth SDP yapısının sunucu kısmını içermelidir. Bir RemDev, servis keşif taleplerine cevap verebilmek için bir servis kayıt veri tabanı içermelidir.

LocDev ve RemDev rolleri kalıcı ve özel olarak herhangi bir cihaza verilmez. Örneğin bir RemDev, SDP istemcisi gibi SrvDscApp içerebilir ve bir LocDev de bir SDP sunucuya sahip olabilir. Böylelikle bir cihaz belirli bir SDP hareketi (transaction) için LocDev olurken, başka biri için RemDev olarak görev yapabilir.

Servis keşif profiline katılan cihazlarda yönetici-köle ilişkisi aranmaz. Başka bir deyişle, bir lokal cihaz yönetici, uzak cihaz da köle olarak ele alınmaz. Servis keşfi

aynı pikonetin üyesi olan bir yönetici ya da köle tarafından başlatılabilir. Ayrıca bir pikonetteki bir köle, aynı pikonetteki yöneticiyi uygun olmayacağına dair bilgilendirip, büyük olasılıkla durağan moda girerek yeni bir pikonette bir servis keşfi başlatabilir.

Şekil 6.5 servis keşif profilinin içerdiği Bluetooth protokollerini ve desteklenen birimleri göstermektedir.



Şekil 6.5 Servis Keşif Profilinin içerdiği Bluetooth protokol yığını

Servis keşif uygulaması temelbant ile Bluetooth modülü kontrol fonksiyonu üzerinden haberleşir. Bu fonksiyon Bluetooth modülünün değişik arama modlarına ne zaman gireceğini belirler. Bir lokal cihazdaki servis keşif kullanıcı uygulamasının Bluetooth SDP istemcisi ile arayüzü bulunur. Bu arayüz sayesinde bir veya birden fazla uzak cihazın SDP sunucusuna servis sorgulamalarını gönderir ve servis sorgulama cevaplarını alır. SDP, L2CAP teki bağlantı yönelimli (connection-oriented-CO) iletim servisini kullanır.

Servis keşif profili SDP hareketi (transaction) için doğrulama ve/veya şifreleme gerektirmez.

6.1.3.2 Çiftleme (Pairing)

Servis keşif profili tarafından çiftleme (pairing) ile ilgili bir gereksinim tanımlanmamıştır. Çiftleme (pairing) işlemi yapılabilir, yapılmayabilir. Çiftleme (pairing) ilk defa haberleşecek iki cihazın sonraki doğrulamalarda kullanılmak üzere ortak bir link anahtarı yaratması olarak tanımlanan bir başlangıç prosedürüdür. Bir lokal cihaz, bağlanılmamış uzak cihazlara servis keşfi uygulamak istediğinde, bağlantıdan önce çiftlemeye (pairing) izin vermek ya da çiftlemeyi (pairing) ilk olarak talep edebilecek cihaza geçirmek servis keşif uygulamasının sorumluluğundadır. Servis dağıtım konusu sadece lokal cihazın bir veya birden çok uzak cihazla temelbant linki kurmasını takiben servis keşif işlemi yerine getirebilme ile ilgilidir.

6.1.3.3 Servis Keşif Uygulaması

SrvDscApp ile lokal cihazın sorgulama ve/veya çağrı (page) durumlarına girebileceği farzedilir. Ayrıca uzak cihazın da sahip olduğu servisleri diğer cihazlara (yazıcı, LAN erişim noktası vs..) olanaklı hale getirmek için sorgulama tarama ve/veya çağrı tarama (page scan) durumlarına girebileceği farzedilir.

SrvDscApp bağlı olan uzak cihazlara karşı servis sorgulamalarını da yerine getirir. Uzak cihazla olan bir bağlantıda lokal cihazın her zaman yönetici olması gerekli değildir, benzer olarak, uzak cihazın da her zaman köle olması şartı aranmaz.

Servis keşfinin uygulanması için birkaç alternatif bulunmaktadır. Örneğin, lokal cihazın kullanıcısı istenen servis için servis keşif uygulaması üzerinde arama yaparak gerekli bilgiyi sağlayabilir. Sonrasında SrvDscApp Bluetooth sorgulama prosedürünü kullanarak cihazlar için arama yapar. Lokal cihaz bulunan her cihaza bağlanır, gerekli link ayarlarını yapar ve istenen servisleri arar. Alternatif olarak, cihaz sorgulaması servis araması için kullanıcı girişlerinin toplanmasından önce yapılabilir.

Başka bir durumda çağrı (page), link oluşturulması ve servis keşfinin tamamı uzak cihaz üzerinde bir kerede yapılır; lokal cihaz önceki uzak cihazla servis araması bitmeden başka bir uzak cihaza çağrı (page) yapmaz ve gerekirse önceki cihazla

bağlantıyı keser. Servis keşfi aynı anda maksimum yedi cihaz arasında uygulanabilir. Bu durumda, SrvDscApp kontrolündeki lokal cihaz bütün uzak cihazlara çağrı (page) yapar, hepsi ile link kurar ve istenen servisler için aynı anda sorgulama yapar.

Servis keşif uygulamasının özellikleri şu şekilde özetlenebilir:

- Bluetooth sorgulamaları, bir kullanıcının bir servis arama talebini takiben aktif olur.
- Bir sorgulamayı takiben bulunan herhangi bir uzak cihaz için, SrvDscApp servis keşfini bitirir ve bir sonraki uzak cihazla bağlantıya geçmeden önce, ilk cihazla bağlantısını sona erdirir.
- Bağlı bulunan herhangi bir uzak cihaz için, lokal cihaz servis keşfini takiben bağlantıyı sonlandırmaz

Servis keşif uygulamasının başka bir özelliği de kullanıcının güvenli veya güvenli olmayan bir çalışma modu seçebilmesidir. Kullanıcı SrvDscApp nin sadece güvenli cihazlar ile veya sadece çiftleme (pairing) gerektiren yeni keşfedilmiş uzak cihazlarla bağlantıya geçmesine izin verir.

Bir lokal cihaz bir servis keşif aramasını üç tip uzak cihaz için gerçekleştirebilir:

- Güvenilir cihazlar: Lokal cihazla bağlantı halinde olmayan fakat güvenli bir ilişki kurmuş olan cihazlardır.
- Bilinmeyen (yeni) cihazlar: Lokal cihazla bağlantı halinde olmayan ve güvenilir olmayan cihazlardır.
- Bağlı cihazlar: Lokal cihazla bağlantı halinde olan cihazlardır.

Güvenilir veya bilinmeyen cihazları keşfetmek için, SrvDscApp Bluetooth sorgulaması ve/veya çağrı (page) proseslerini aktif eder. Bağlı olan uzak cihazlar için, sadece çağrı yapılmasına (paging) ihtiyaç vardır. SrvDscApp görevini yerine getirebilmek için lokal cihazın çevresindeki cihazların Bluetooth cihaz adreslerine erişim sağlamalıdır. Bir lokal cihazdaki Bluetooth modül kontrolörü çevrede bulunan cihazların listesini oluşturarak SrvDscApp ye verir.

6.1.3.4 Mesaj Dizisi

Servis Keşif profili üç Bluetooth prosedürünü adresler: cihaz keşfi, cihaz ismi keşfi ve servis keşfi. İlk iki prosedür host ile bir ilişki gerektirmezken, üçüncü prosedür

gerektirir. Şekil 6.6 bu profilin oluşması esnasında gerçekleşen mesaj değiş tokuş fazlarını göstermektedir. Bütün prosedürler her zaman gerçekleşmek ve bütün cihazlar bütün fazlardan geçmek durumunda değildir. Örneğin doğrulama istenmiyorsa, doğrulama fazı gerçekleşmez. Eğer SrvDscApp lokal cihazın bağlı olduğu belirli bir uzak cihazdaki servisleri sorgulamaya gereksinim duyuyorsa, sorgulama ve çağrılar (page) gerçekleşmez.

6.1.3.5 Servis Keşfi

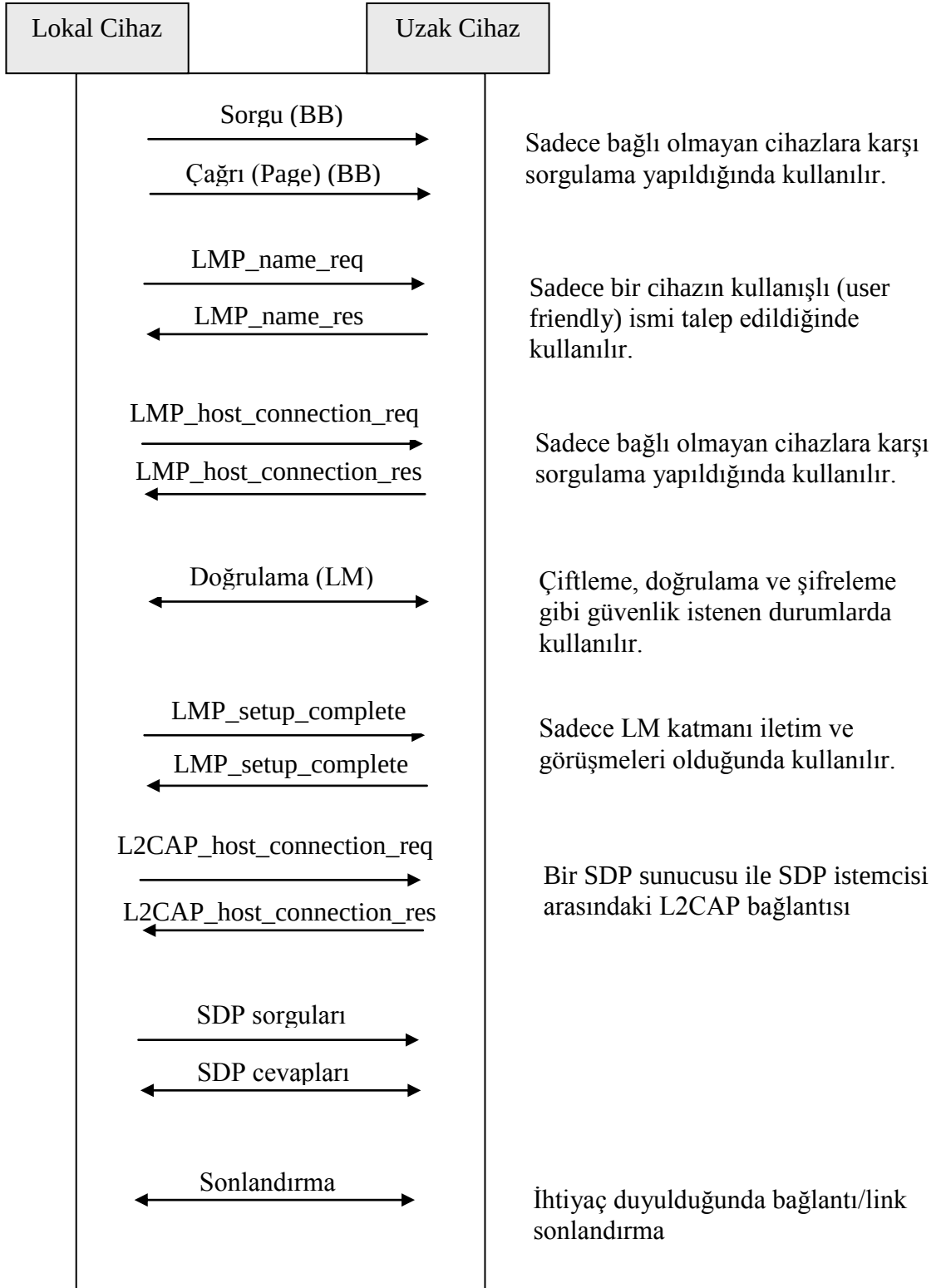
Servis keşif uygulaması SDP yi bir servise erişmek için kullanmaz. SDP lokal cihazın kullanıcılarını uygun servisler hakkında bilgilendirmek için kullanılır. Lokal cihazda çalışan Bluetooth uygulamaları uzak cihazdaki istenen bir servise erişmeyi kolaylaştırmak için geçerli bilgileri de alabilirler.

6.1.3.6 İşaretleşme

SDP ile ilgili bilgilerin alınması için sadece lokal cihaz bir L2CAP bağlantısını başlatabilir. SDAP L2CAP işaretleşmesi üzerinde herhangi bir ek kısıtlama ya da gereksinim oluşturmaz.

6.1.3.7 Konfigürasyon Seçenekleri

Servis Keşif Profili'nde Seri Port Profiline L2CAP için geçerli olan üç konfigürasyon opsiyonu geçerlidir.



Şekil 6.6 Servis Keşif Profili'ni destekleyen Bluetooth prosesleri

İki cihaz arasındaki SDP hareketleri (transaction) için kurulan L2CAP bağlantısının süresi boyunca (bu süre SDP oturumu olarak adlandırılabilir), cihazların birinin ya da

her ikisinin diğ er cihaz veya uygulamalarla bir L2CAP bağlantısı bulunabilir. Eğ er herhangi bir yeni bağlantı varsayılan QoS değ erlerine sahip değ ilse, orijinal SDP oturumu için kullanılan MTU değ eri yeni oturum devam ederken tekrar görü ş ülebilir (negotiate).

6.1.3.8 SDP Hareketleri (Transaction) ve L2CAP Bağlantıları

SDP hareketleri (transaction) PDU değ iş -tokuşlarının talep ve cevap dizilerinden oluş ur. SDP nin kendisi bağlantısız bir datagram servisidir. Bunun sebebi ise hiçbir SDP seviyesi bağlantının PDU ların değ iş tokuşundan önce gerçekleşmemesidir. SDP, bunun yerine bağlantıların oluşturulması ve sonlandırılması iş ini L2CAP katmanına delege eder.

Normal olarak gerçek bir bağlantısız serviste, bağlantı bir servis talep PDU su gönderildikten sonra sonlandırılır. SDP sunucuları “durumsuz” olarak varsayıldığı için, L2CAP in bir servis talep PDU su gönderildikten sonra bağlantıyı sona erdirmesi, SDP hareketlerinin (transaction) aksamasına yol açabilir. Ayrıca birbirini izleyen her bir SDP PDU su için yeni bir L2CAP bağlantısı kurulması gerekirse ciddi bir performans problemi doğ ar. Bu problemlerin önüne geçmek için, SDP hareketleri (transaction) için olan L2CAP bağlantıları, tek bir SDP PDU sunun iletiminden daha uzun süre kalır. Pratik uygulamalarda, bir SDP oturumu belirli bir cihazla etkileş im için ihtiyaç duyulan süre kadar (mümkün olduğ u kadar uzun süre) devam eder.

Bir SDP hareketi (transaction) bir SDP istemcisinden SDP sunucusuna olan PDU iletim talebi ile SDP sunucusundan SDP istemcisine gönderilen cevap PDU sunun değ iş tokuşunu içerir. Fakat, bir SDP oturumu bu süreç tamamlanmadan önce lokal ve uzak cihazda SDP nin altındaki katmanlarda oluş an hatalar, SDP katmanının kendisinde oluş an hatalar veya uzak cihazdaki servis kayıt veritabanında oluş an hatalar sebebiyle sona erebilir. Kullanıcı da SDP oturumunu hareket (transaction) tamamlanmadan önce sona erdirebilir.

SDP oturumu için minimum bir süre belirlemek SDP hareketlerinin (transaction) doğru şekilde gerçekleşmesine yardımcı olur. Geliş miş bir performans için, Bluetooth kablosuz teknolojisini uygulayan kişi ya da kurumlar SDP oturumlarının minimum süreden daha uzun bir sürede bitmelerine izin vermelidir. Genel bir kural olarak, bir SDP oturumu belirli bir cihazla interaktivite için gereken süre kadar uzun tutulmalıdır. Bu süre çok kolay tahmin edilemeyeceğ i için belirli bir SDP

oturumundan sonraki aktif olunmayan periyotları izleyen zamanlayıcılar kullanılabilir. Belirlenen süre aşıldığında, L2CAP bağlantısı sonlanır.

SDP uygulamaları üst bir katmandan alınan ve SDP oturumunu başlatıp bitirmek için SrvDscApp nin kendisi tarafından başlatılan giriş değerine dayanır. Bu girişler “open search” ve “close search” ü gösteren düşük katman parametrelerinin kullanılmasından gelir. Son olarak bir uygulama kullanıcıların “terminate” servis parametresini kullanarak SDP oturumunu herhangi bir zamanda sonlandırmalarına izin verir.

Genellikle uzak cihaz SDP oturumunu sonlandırmaz fakat sonlandırması mümkündür. Örneğin uzak cihaz L2CAP bağlantı sonlandırma PDU sunu kullanarak SDP oturumunu sonlandırabilir veya SDP taleplerine ve L2CAP işaretleşme komutlarına cevap vermeyerek de oturumu sonlandırabilir. İkinci durum uygulama ile ilgili bir probleme de işaret edebilir.

6.1.3.9 Link Yöneticisi

Link Yöneticisi link kurulumu, doğrulama, link konfigürasyonu ve diğer yönetim fonksiyonlarını yerine getirir. Şifreleme kontrolü, güç kontrolü ve QoS yetenekleri gibi servisleri de sağlar. Farklı modlardaki (park, durağan, koklama ve aktif) cihazları da yönetir.

Hata Davranışı

Bir Bluetooth ünitesi zorunlu bir özelliği kullanmak ister ve diğer ünite bu özelliği desteklemediği şeklinde bir cevap verirse, bağlantıyı başlatan cihaz “desteklenmeyen LMP özelliği” sebepli bir bağlantı sonu mesajı gönderir. Seçime bağlı olan bir özellik talebi için gelebilecek olası bir red cevabı her zaman işlem görebilir olmalıdır.

Link İlkesi (Policy)

Servis Keşif Profiline kesinleşmiş yönetici-köle rolleri yoktur. Ayrıca hangi düşük-güç modlarının kullanılacağı ve ne zaman kullanılacağına ilişkin de bir zorlama yoktur. Her bir cihazın Link Yöneticisi bu konulara kendisi karar vererek, uygun olduğunda talep oluşturabilir.

6.1.3.10 Link Kontrolü

Lokal cihaz bağlantısı olmayan bir uzak cihazla servis aramaya başladığında, bu servisleri sorgulamak veya çağrı yapmak (page) gerekir.

Sorgulama

SrvDscApp tarafından istendiğinde, lokal cihaz temel bandını sorgulama moduna sokar. Eğer QoS gereksinimlerinin karşılanmak zorunda olduğu mevcut bağlantılar var ise, bu duruma geçiş hemen olmayabilir. Bu olasılığı kompanze edebilmek için, SrvDscApp nin kullanıcısı sorgulamanın süresi için kriter belirleyebilir. Sorgulama lokal cihazdan başlarsa, GIAC prosedürü kullanılır.

Sorgulama Tarama

Sorgulama taramalar bu profilin kapsamı dışında kalan cihaza bağlı ilkelerdir (policy). Keşfedilebilir modda çalışan cihazlar diğer cihazlar tarafından gönderilen sorgulamalarla keşfedilebilir. SrvDscApp den gelen bir sorgulama ile keşfedilmek için, uzak cihaz mutlaka GIAC kullanarak sorgulamaları taramalıdır.

Çağrı Yapma (Paging)

SrvDscApp belirli bir uzak cihaza servis kayıtlarını sorgulamak için bağlandığında, lokal cihaz temel bandını çağrı (page) durumuna sokar, mevcut ve devam eden bağlantıların QoS gereksinimlerini bir kenara bırakır. Uzak cihaz tarafından belirlenen çağrı (paging) sınıfına (R0, R1, R2) bağlı olarak, lokal cihaz çağrıyı yapar (page). Çağrılar (page) için uzak cihazın 48 bitlik Bluetooth cihaz adresi kullanılır.

Çağrı Tarama (Page Scan)

Çağrı taramalar (page scan) sorgulama taramaya benzer şekilde bu profilin kapsamı dışında kalan cihaza bağlı ilkelerdir (policy). Bağlanabilir modda çalışan Bluetooth cihazları, Genel Erişim Profili nde açıklandığı şekilde, çağrı (page) yapan başka cihazlarla Bluetooth linkleri kurabilir. Uzak bir cihazla link kurmak için, lokal cihaz uzak cihazın 48-bitlik Bluetooth cihaz adresini kullanan bir SrvDscApp hareketinden elde edilen bir çağrı (page) gönderir.

Hata Davranışı

LC katmanındaki özelliklerin çoğu LMP prosedürleri tarafından aktive edilmek zorunda olduğu için, hatalar da bu katmanda yakalanır. Sorgulama ve çağrı (paging)

gibi bazı LC prosedürleri ise LMP katmanından bağımsızdır. Bu sebeple bu özelliklerin yanlış kullanımının farkına varmak çok zordur ve SDAP içinde bu gibi durumlar için herhangi bir dedeksiyon mekanizması tanımlanmamıştır. [2,3,9]

6.1.4 Genel Obje Değiş-Tokuş Profili (Generic Object Exchange Profile-GOEP)

GOEP, Bluetooth cihazlarının Dosya Transfer Profili, Obje İtme Profili ve Senkronizasyon Profili gibi obje değiş tokuş kullanım modellerini nasıl desteklediğini tanımlar. Bu kullanım modellerini en çok kullanan cihazlar diz üstü bilgisayarlar, PDA ler, akıllı telefonlar ve mobil telefonlardır.

GOEP spesifikasyonu Obje Değiş-Tokuş (Object Exchange-OBEX) kullanan uygulama profilleri için genel bir uyumluluk sağlar ve bu uygulama profillerine uyumluluk için daha alt protokol katmanlarının (temelbant ve LMP gibi) gereksinimlerini tanımlar.

OBEX world wide web de kullanılan HTTP ye benzer şekilde obje değiş tokuş servisleri sunar. HTTP den farklı olarak; bir HTTP sunucusunun gerektirdiği oldukça zengin kaynak gereksinimi olmaksızın bir çok cihaz için çalışabilir. OBEX in en çok kullanıldığı alan “itme (push)” ve “çekme (pull)” uygulamalarıdır. Taşınabilir cihazlar arasında hızlı haberleşme imkanı yaratır.

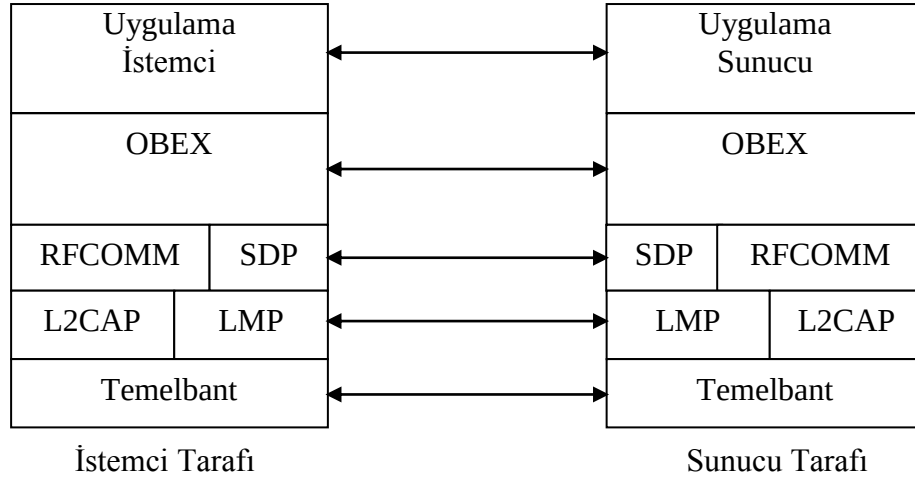
OBEX hızlı bağlan-ilet-bağlantıyı bitir senaryoları ile kısıtlı değildir. Belirli bir periyot boyunca iletimin devam ettiği ve bağlantı durumunun iletim olmadığında dahi korunduğu oturumlara imkan tanır. Bu sebeple veri tabanı transferleri ve senkronizasyon gibi kompleks görevleri de yerine getirebilir.

6.1.4.1 Profil Yığını

Şekil 6.7 de gösterildiği gibi, hem sunucu hem de istemcide GOEP profil yığını bulunur. GOEP profil yığını temelbant, LMP ve L2CAP ten oluşur. RFCOMM seri port emülasyonu için bir iletim protokolüdür ve GSM TS 07.10 un Bluetooth adaptasyonundan elde edilmiştir. SDP Bluetooth servis keşif protokolüdür. OBEX, IrOBEX in Bluetooth adaptasyonudur. Uygulama İstemci katmanı, OBEX operasyonlarını kullanarak Uygulama Sunucu ya veri objeleri gönderen ve veri alan birimdir. Uygulama Sunucu bir veri depolama birimidir, veri objeleri buradan itilip (push) çekilebilir (pull).

6.1.4.2 Sunucu ve İstemci

GOEP'te istemci veri objelerini sunucuya gönderir (push) veya sunucudan veri objelerini alır (pull).



Şekil 6.7 Genel Obje Değiş-Tokuş Profili için protokol modeli

GAP ın doğası gereği, istemcide sorgulama ve link kurulum prosedürleri oluşurken, kullanıcı da sunucu özelliği içeren cihazı keşfedilebilir ve bağlanılabilir duruma getirmelidir.

GOEP noktadan noktaya konfigürasyonlarda kullanılmak üzere prosedürleri tanımlar. Bu nedenle sunucunun belirli bir zamanda sadece bir istemciye servis sunabildiği varsayılmaktadır. Ayrı noktadan-noktaya linkler üzerinden aynı anda birden fazla istemciyi desteklemek de uygulamalar açısından mümkündür.

6.1.4.3 Profil Temelleri

Bir sunucu bir istemci ile ilk defa kullanılmadan önce, çiftleme (pairing) içeren bir bağ kurma (bonding) prosedürü gerçekleştirilebilir. Bağ kurma (bonding) prosedürü desteklenmek zorunda olduğu halde, kullanımı uygulama profillerine bağlıdır. Bağ kurma (bonding) genellikle kullanıcının manuel olarak prosesi aktive etmesini ve sunucu ve istemci cihazların klavyelerini kullanarak Bluetooth PIN kodunu girmesini gerektirir.

Link katmanındaki bağ kurmaya (bonding) ek olarak, bir OBEX başlangıç prosedürü de uygulanabilir. GOEP kullanan uygulama profilleri beklenen güvenlik derecesini sağlamak için bu prosedürün desteklenip desteklenmediğini belirtmelidir.

Link ve kanal kurulumları GAP da açıklanan prosedürlere göre yapılmalıdır. Güvenlik bağlantı kurulumundan sonra diğer tarafı doğrulayarak ve link katmanındaki tüm kullanıcı verisini şifreleyerek sağlanabilir. Cihazlar tarafından desteklenen doğrulama ve şifreleme GOEP kullanan uygulama profiline bağlıdır.

Kullanıcı arayüzü GOEP te tanımlanmamış, gerek duyulduğunda uygulama profillerinde tanımlanmıştır. Ayrıca GOEP belirli yönetici-köle rolleri de tanımlamaz.

6.1.4.4 Özellikler

GOEP üç özellik sağlar. Mevcut dizini düzenlemek gibi diğer özelliklerin kullanımı, bu özelliğe gereksinim duyan uygulama profilleri tarafından tanımlanmalıdır.

Bir Obje Değiş-Tokuş (OBEX) Oturumu Kurma

Bu özellik istemci ile sunucu arasında bir OBEX oturumu kurmak için kullanılır. Bir oturum kurulmadan önce, taşınan bilgi (payload) verisi istemci ile sunucu arasında değiş tokuş edilemez.

Bir Veri Objesini İtmek (push)

Bu özellik istemciden sunucuya veri transferi yapmanın gerektiği durumlarda kullanılır. Veri objesi sunucuya OBEX protokolünün PUT operasyonu kullanılarak gönderilir. Veri bir veya birden fazla OBEX paketi içinde gönderilebilir.

Bir Veri Objesini Çekmek (pull)

Bu özellik sunucudan istemciye veri transferi yapmanın gerektiği durumlarda kullanılır. Veri objesi sunucudan OBEX protokolünün GET operasyonu kullanılarak alınır. Veri bir veya birden fazla OBEX paketi içinde gönderilebilir.

6.1.4.5 OBEX Operasyonları

OBEX protokolü tarafından tanımlanan operasyonlar Bağlanma, Bağlantıyı Sonlandırma, Put, Get, Abort ve SetPath dir. GOEP kullanan uygulama profilleri hangi operasyonların kullanıldığını belirtmelidir.

IrOBEX spesifikasyonu bir istemcinin bir OBEX talebine karşılık olarak gelecek cevabı ne kadar beklemesi gerektiğini tanımlamaz. Ancak operasyonu otomatik olarak iptal etmeden önce; talep ve cevap arasında makul bir süre olması gerektiğini

belirtir. Bluetooth spesifikasyonu makul zaman periyodu olarak 30 sn. veya daha fazla önermektedir.

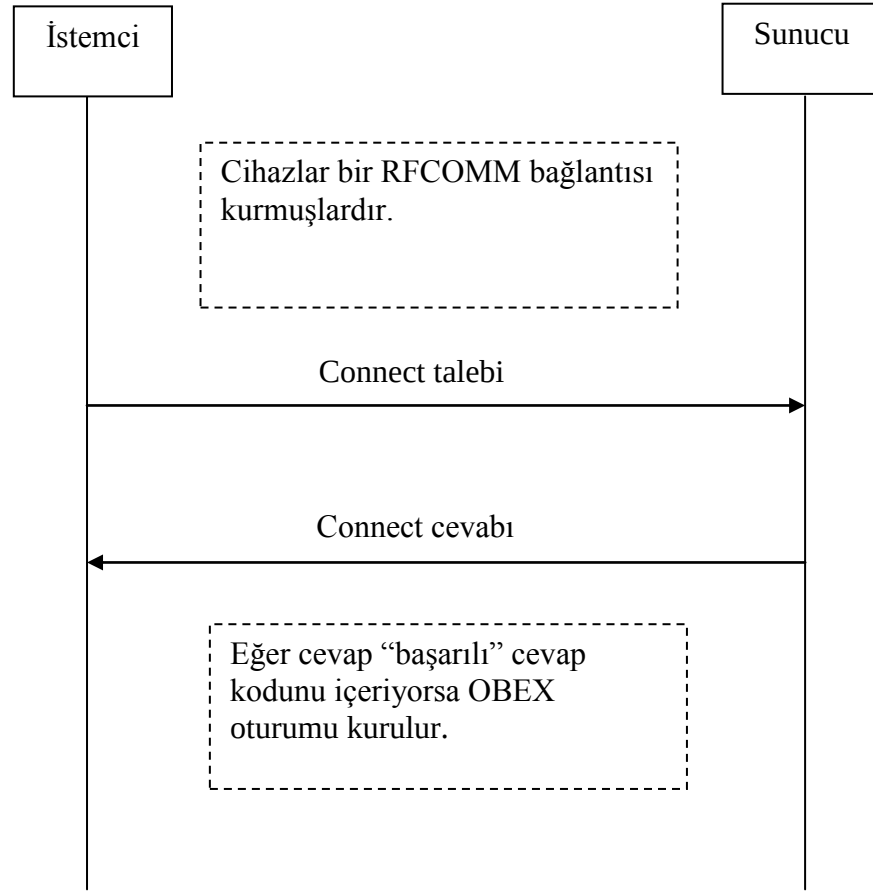
OBEX Başlangıcı

Eğer istemci ve sunucu tarafından doğrulama kullanılıyorsa, ilk OBEX bağlantısı kurulmadan önce doğrulama işlemi başlatılmış olmalıdır. Bu başlangıç ilk OBEX bağlantısı yapılmadan herhangi bir süre önce yapılabilir fakat hem istemci hem de sunucu tarafında kullanıcı müdahalesine gereksinim duyar.

Doğrulama bir OBEX şifresi kullanılarak yapılabilir. OBEX şifresi Bluetooth PIN kodunun aynısı olabilir. Kullanıcı hem link doğrulaması hem de OBEX doğrulaması için aynı kodu girmiş olsa bile bu kodlar ayrı ayrı girilmelidir. İstemci ve sunucu tarafında OBEX şifresi girildikten sonra, gelecek kullanımlar için her iki tarafta da saklanır.

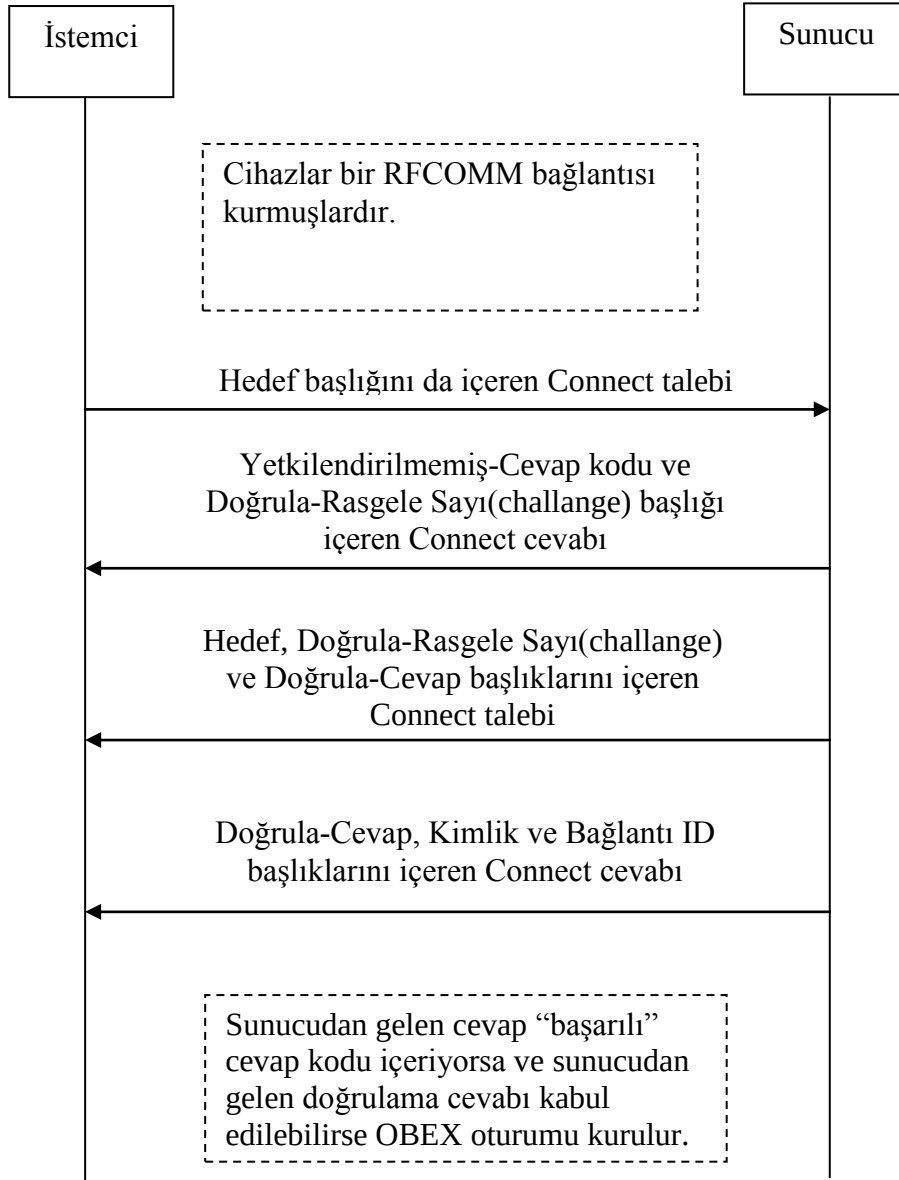
OBEX Oturum Kurulumu

OBEX bağlantısı doğrulama yapılarak ya da yapılmayarak sağlanabilir ancak en azından GOEP kullanan tüm uygulama profilleri doğrulama gerektirmeyen bir OBEX oturumunu desteklemelidir. Şekil 6.8 bir OBEX oturumunun CONNECT operasyonu kullanılarak nasıl gerçekleştirildiğini göstermektedir. CONNECT talebi bağlantıya gereksinim olduğunun göstergesidir ve hangi servisin kullanıldığına ilişkin bir gösterge de olabilir.



Şekil 6.8 Bir OBEX oturumunun doğrulama olmaksızın CONNECT operasyonu kullanılarak gerçekleştirilmesi

İstemcide ve sunucuda kullanılan OBEX doğrulama yapısı HTTP ye dayanmakla birlikte, HTTP nin tüm özelliklerini desteklemez. GOEP te OBEX doğrulaması istemciyi ve sunucuyu doğrulamak için kullanılır. Şekil 6.9 doğrulama yapılarak bir OBEX oturumunun kurulumunu göstermektedir.



Şekil 6.9 Bir OBEX oturumunun doğrulama yapılarak gerçekleştirilmesi

6.1.5 Özet

GOEP, Bluetooth cihazlarının OBEX kullanım modellerini desteklemeleri için gereksinimlerini tanımlar.

Bluetooth spesifikasyonu GOEP'e ek olarak OBEX ve OBEX kullanan uygulamalar için şu spesifikasyonları içerir:

- Bluetooth Senkronizasyon Profili Spesifikasyonu: Bu profil Senkronizasyon uygulama profili kullanan uygulamalar için uyumluluk gereksinimlerini tanımlar. Temelbant, LMP, L2CAP veya RFCOMM için gereksinimleri tanımlamaz.
- Bluetooth Dosya Transfer Profili Spesifikasyonu: Bu profil Dosya Transfer uygulama profili kullanan uygulamalar için uyumluluk gereksinimlerini tanımlar. Temelbant, LMP, L2CAP veya RFCOMM için gereksinimleri tanımlamaz.
- Bluetooth Obje İtme Profili Spesifikasyonu: Bu profil Obje İtme uygulama profili kullanan uygulamalar için uyumluluk gereksinimlerini tanımlar. Temelbant, LMP, L2CAP veya RFCOMM için gereksinimleri tanımlamaz.
- Bluetooth IrDA Uyumluluk Spesifikasyonu: Bu profil, uygulamaların hem Bluetooth hem de IrDA cihazları üzerinde nasıl çalışacağını, OBEX in RFCOMM ve TCP üzerinden nasıl eşlendiğini (mapping) ve OBEX kullanan Bluetooth uygulama profillerini tanımlar.

Bluetooth IrDA uyumluluk spesifikasyonu hem kızıl ötesi hem de Bluetooth cihazları için ilk ortak oturum katmanını temsil ettiği için dikkate değerdir. Genel kullanım modellerini benimseyip her iki teknolojinin de kendisine özgü avantajlarından faydalanılarak kullanıcı taleplerini karşılayan tek kısa-dalga kablosuz haberleşme imkanı ortaya çıkartılır. Böylelikle kablosuz ses iletiminden yüksek hızda (16 Mbit/sn.) veri iletimine kadar geniş bir yelpazede ideal çözüme kavuşulur.

[9]

7. BLUETOOTH KULLANIM MODELLERİ

Bu bölümde SIG tarafından yüksek önem derecesinde tanımlanan kullanım modelleri anlatılmıştır. Her kullanım modeli bir profil ile eşleşmektedir. Bluetooth SIG profilleri kullanım modelleri için belirlemiştir.

7.1 Kablosuz Bilgisayar

Bluetooth teknolojisinin amacı kablo kullanımına son vermektir. Masaüstü bilgisayar uygulamalarında çok fazla kablo bulunduğu için kullanım ve taşıma zorlukları yaşanmaktadır. Bilgisayar çevre birimlerinin kablolu olanları yerine kablosuz linkler kullanılabilir. Klavye, mouse, joystick, hoparlör, yazıcı, tarayıcı, PDA beşikleri (cradle), dijital kamera kabloları, ağ bağlantı kabloları gibi birimler kablosuz olarak kullanılabilir.

Kablosuz haberleşme ile bilgisayar kurarken ve çalıştırırken elde edilecek faydaların yanı sıra, kullanım yeri açısından da büyük bir rahatlama sağlanır. Kabloara bağlı kalınmadığı için daha rahat bir yerleşim düzeni kurulabilir.

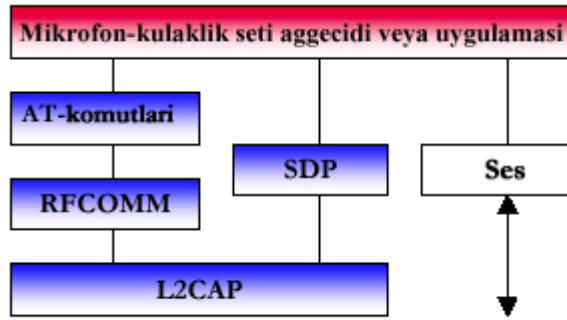
Cihazların çok amaçlı kullanımı da bu tip kullanım şekli sayesinde daha kolay olur. Örneğin bir joystick hem bilgisayarla, hem de bir video oyunu ile kullanılabilir. Özellikle yazıcı ve tarayıcı cihazları için bir ağ ortamına gerek kalmaksızın noktadan noktaya erişim ve paylaşım sağlanabilir. [2]

7.2 Mikrofon-Kulaklık Seti

Bu kullanım modeli Bluetooth teknolojisinin ses desteği sayesinde oluşmuştur. Telefon mikrofon-kulaklık setleri hem normal şebeke, hem de mobil telefonlar ile birlikte kullanılmaya başlanmıştır. Çağrı merkezi, yardım masası gibi yerlerde bu tip setler normal şebeke ile kullanılarak kullanıcının hareket serbestisi kazanmasını sağlarlar. Bu tip setler mobil telefonlarla da kullanılarak, araba kullanırken veya yürürken rahatlık sağlarlar. Bluetooth kablosuz haberleşmesi mikrofon-kulaklık setleri ile telefon arasındaki kabloları kaldırır.

Mikrofon-kulaklık setinin bir avantajı da mobiliteye imkan vermesidir. Seti kullanan kişi ses cihazına bağlı kalmaksızın hareket edebilir. Başka bir avantaj ise aynı setin birden fazla cihaz ile kullanılabilmesidir. Bluetooth spesifikasyonu standart bir arayüz sağladığı için aynı set mobil telefon, sabit telefon, telsiz telefon baz istasyonu gibi bir ses erişim noktası, bilgisayar ses çıkışı ya da portatif bir CD çalar ile kullanılabilir.

Bu kullanım modelinin protokol yığını Şekil 7.1 de gösterilmektedir. Ses dizisi direkt olarak temebant protokolüne bağlıdır. (Şekilde L2CAP ile Ses arasında bir bağlantı bulunmadığı, L2CAP katmanı ile bağlantı yapılmadan geçildiği gösterilmektedir.) Mikrofon-kulaklık seti AT-komutlarını gönderebilir ve sonuç kodlarını alabilir. Bu sayede gelen çağrılara cevap verilebilir ve seti elle hareket ettirmeksizin çağrı sonlandırılabilir.



Şekil 7.1 Mikrofon-kulaklık seti protokol yığını

7.3 Bir Telefonda Üç Kullanım (Three-in-One Telefon)

Bugün birçok kişi birden fazla telefon kullanmaktadır: ofiste bir telefon, evde birden fazla telefon (kablolu, telsiz), mobil telefon vs.. Bluetooth teknolojisini kullanan tek bir telefon, tüm bu telefonların yerine kullanılabilir. Three-in-One telefon kullanım modeli üç farklı kullanım şeklini destekler. Birincisi PSTN’e bağlı bir kablosuz telefon olarak çalışma şeklidir. Bu çalışma şekli bir telsiz telefon baz istasyonu yardımıyla telefon görüşmesi yapmayı, baz istasyonu yardımıyla iki telefon arasında görüşme yapmayı ve harici bir ağ tarafından sağlanan ek servislere erişmeyi sağlar. Sabit şebeke ücretlendirmesi yapılır. İkinci çalışma şeklinde, “walkie-talkie” gibi telefondan telefona haberleşme mümkün olur (intercom). Bu bağlantı şeklinde bir ücretlendirme yapılmaz. Üçüncüsü mobil telefon şebekesine bağlı olarak çalışan bir mobil telefon olarak kullanım şeklidir. Bu kullanım şeklinde mobil görüşme

ücretlendirmesi yapılır. Telsiz ve intercom senaryoları aynı protokol katmanını kullanır (Şekil 7.2). Ses dizisi direkt olarak temelbant protokolüne bağlıdır. (Şekilde L2CAP ile Ses arasında bir bağlantı bulunmadığı, L2CAP katmanı ile bağlantı yapılmadan geçildiği gösterilmektedir.)

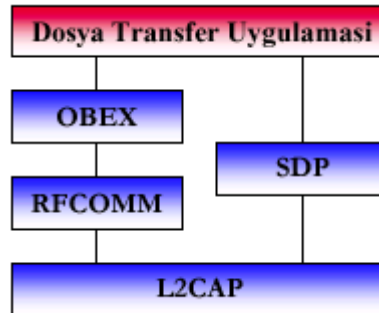


Şekil 7.2 Telsiz telefon ve intercom kullanım modelleri protokol yığını

7.4 Dosya Transferi

Her türlü veri ağı için en önemli kullanım alanlarından biri dosya ve diğer veri objelerini değiş tokuş etmektir. Disketler, cd ler veya kablolar yardımıyla veri transferi yapmak çok kullanılan yöntemlerdir, kablosuz haberleşme ile tüm bunlara olan ihtiyaç ortadan kalkar. Örneğin bir interaktif konferans odası senaryosunda katılımcılar arasında iş kartları ve çeşitli dosyalar değiş tokuş edilir. Bu yöntem ile .xls, .ppt, .wav, .jpg, .doc gibi birçok dosya çeşidi transfer edilebilir. Bu yöntem ile uzak cihazdaki dosyaların içerikleri üzerinde tarama yapmak da mümkündür.

Şekil 7.3 te bu kullanım modeli için geçerli olan protokol yığını gösterilmektedir. Şekil üzerinde LMP, temelbant ve radyo katmanları pratikte kullanılmalarına rağmen gösterilmemiştir.



Şekil 7.3 Dosya transferi kullanım modeli protokol yığını

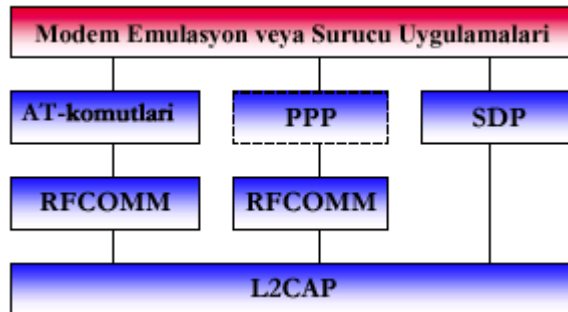
7.5 İnternet Köprüsü

Bluetooth haberleşmesini internet ya da kampüs/şirket içi intranetlerde olduğu gibi kurulu ağlar için kablosuz köprü olarak kullanan iki farklı yöntem bulunmaktadır. İlk yöntem bir telefonu kablosuz modem olarak kullanan çevirmeli ağ, ikinci yöntem ise bir veri erişim noktası kullanan LAN lardır.

7.5.1 Çevirmeli Ağlar

İnternet köprüsünün bu şekli bugün çoğu kişinin internete bağlanmak için kullandığı yöntemden farklı değildir. Bilgisayardaki modem ve bu modeme bağlı telefon hattı yardımıyla bir servis sağlayıcısının numarası aranarak internete bağlanılır. Bluetooth teknolojisinin bu senaryoya olan katkısı kabloları ortadan kaldırmak şeklinde olmaktadır. Bugün internete bağlanılırken bir mobil telefon kullanılıyor olsa dahi, bilgisayar ve telefon arasında haberleşmeyi sağlayacak bir kabloya ihtiyaç duyulmaktadır. Çevirmeli Ağ profilini destekleyen bir bilgisayar ve telefon yardımıyla bağlantı tamamen kablosuz olarak sağlanır.

Bu kullanım modelinde bir mobil telefon ya da kablosuz modem bir modem gibi görev yapmakta ve bilgisayar ile fiziksel bağlantı gerekmeksizin çevirmeli ağ ile faks işlevlerini yerine getirmektedir. Çevirmeli Ağ senaryosu SDP ye ek olarak iki protokol katmanına ihtiyaç duyar (Şekil 7.4). AT-komutları mobil telefonu veya modemi ve diğer katmanları (örneğin RFCOMM üzerinden PPP) kontrol ederek taşınan bilgi (payload) verisini aktarmak için kullanılır. Faks senaryosu da benzer protokol katman yapısını kullanır. Fakat PPP ve PPP nin üzerindeki ağ protokolleri kullanılmaz ve uygulama yazılımı direkt RFCOMM üzerinden faks gönderir.



Şekil 7.4 Çevirmeli ağ kullanım modeli protokol yığını

7.5.2 Direkt Ağ Erişimi

Direkt ağ erişimi, kurumlar, üniversite kampüsleri gibi oluşumlarda kullanılmakta olan bir yöntemdir. Direkt erişimli LAN lar internete bir arageçit sağlayarak, çevirmeli ağ bağlantısı kullanmadan LAN dan internete erişim sağlarlar.

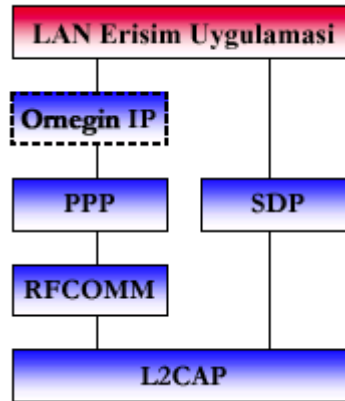
Bluetooth kablosuz haberleşmesi ile sağlanan direkt ağ erişimi, veri erişim noktaları kullanılarak mümkün olur. Bir veri erişim noktası, cihazların kendisine kablosuz olarak bağlanmalarını sağlar ve sonra internete bağlanır. Kablolu ağlarda (örneğin bir ethernet ağında) bu fonksiyonun aynısı kablolar yardımıyla yerine getirilmektedir.

Veri erişim noktaları, mevcut kablolu ağlar ile entegre edilerek de kablosuz erişim sağlayabilir.

7.5.3 LAN Erişimi

Bu kullanım modelinde birden fazla veri terminali bir LAN erişim noktası kullanarak LAN'a kablosuz olarak bağlanır. Bağlantı gerçekleştiğinde veri terminali LAN'a çevirmeli ağ ile bağlanmış gibi çalışır. Veri terminalleri LAN tarafından sağlanan bütün servislere bağlanır.

LAN erişim protokol yığını AT-komutlarının kullanılmaması dışında internet köprüsü kullanım modeline benzer (Şekil 7.5).



Şekil 7.5 LAN erişimi kullanım modeli protokol yığını

7.6 Konuşan Laptop

Konuşan Laptop kullanım modeli mikrofon-kulaklık seti uygulama modelinin bir uzantısı olarak algılandığı için Bluetooth spesifikasyonunun 1.0 versiyonunda ayrıca tanımlanmamıştır. Bu modelin temelinde bir laptop ya da diz üstü bilgisayarın

mikrofon ve hoparlörünün bir mobil telefondaki ses çağrısı için ses giriş ve çıkışı olarak kullanılabilmesi yatar. Örneğin bir toplantı sırasında katılımcılardan birinin cep telefonuna gelen çağrının, diğer katılımcılar tarafından da dinlenmesi gerektiğini düşünecek olursak; Bluetooth kablosuz haberleşmesi kullanılarak bu çağrı odada bulunan bir diz üstü bilgisayara aktarılarak bir hoparlörden dinlenirmiş gibi dinlenebilir.

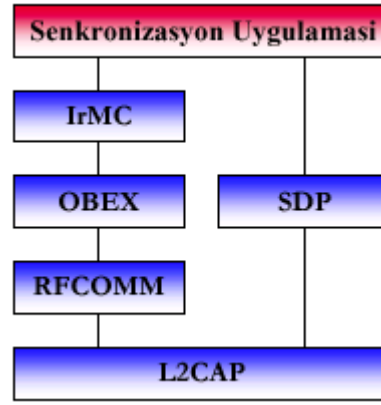
Konuşan laptop kullanım modeli bir cihazın, başka bir cihazın yeteneklerini ödünç alarak fonksiyonlarını genişletmesine bir örnektir.

7.7 Otomatik Senkronizasyon

Senkronizasyon, iki farklı kaynaktan gelen verinin bir kurallar bütünü dahilinde birleştirilmesi prosesidir. Genel bir örnek olarak bir PDA ile bir masa üstü veya diz üstü bilgisayarın senkronizasyonu düşünülebilir. Günümüzde bu işlem daha çok özel seri kablolar ve cihaza özgü yazılımlar kullanılarak gerçekleştirilir. Bluetooth spesifikasyonundaki standart protokoller ve nesne formatları sayesinde bir cihazdaki veri başka herhangi bir cihaz (PDA, diz üstü bilgisayar, akıllı telefon veya hatta bir veri erişim noktasından erişilen ağ verisi) ile senkronize edilebilir.

Kullanım modelinin “otomatik” olan kısmı yakınlık (proximity) ağ kavramı ile olanaklı hale gelmektedir. Günümüzde senkronizasyon işlemi bir seri kablo bağlayarak bir düğmeye basmak veya iki kızıl ötesi haberleşebilen cihazı birbirlerini görecektir şekilde uygun mesafede yerleştirerek bir uygulama çalıştırmak suretiyle gerçekleştirilir. Bluetooth kablosuz haberleşmesinde ise iki cihaz birbirlerinin etki alanına girdiklerinde senkronizasyon otomatik olarak yapılabilir. Örneğin hareket halinde bulunan bir kişinin cebinde bulunan bir PDA ile masasındaki bilgisayarı senkronize olabilir. Cihazların ne zaman otomatik senkronizasyona geçecekleri ve hangi cihaz ile senkronize olacakları konusunda konfigüre etmek gerekir.

Senkronizasyon kullanım modeli için protokol yığını Şekil 7.6 da gösterilmiştir. Şekildeki senkronizasyon uygulama bölümü bir IrMC istemci ya da IrMS sunucu yazılımı olabilir.



Şekil 7.6 Senkronizasyon kullanım modeli protokol yığını

7.8 Kartpostal

Kartpostal kullanım modeli versiyon 1.0 profilleri arasında resmi olarak yer almamaktadır. Temel olarak bir fotoğraf imajını kablosuz olarak başka bir cihaza transfer edebilen bir dijital kamera ve imajı alan cihazın da bu imajı e-posta ile göndermesi prensibine dayanır. Günümüzde çoğu sayısal kamera bilgisayara fotoğraf transferi için bir seri kablo kullanmaktadır.

Bu kullanım modeli ticari açıdan da faydalı olarak (emlak ofisleri, sigorta şirketleri tarafından vs..) kullanılabilir.

7.9 Anlık (Ad Hoc) Ağlar

Bu kullanım modeli dosya transfer senaryosunun bir uzantısı olarak düşünülebilir. Bluetooth kablosuz haberleşmesi 1.0 versiyonunda özellikle tanımlanmış fakat gelecekte mümkün olabilecek kullanım modelleri arasında gösterilmiştir. Anlık (ad hoc) ağlar, spontane olarak şekil alan ağlardır ve Bluetooth da bu tip uygulamaları olanaklı kılan bir teknolojidir. Dosya transferi bölümünde verilen toplantı örneğinde, katılımcılar arasında anlık (ad hoc) ağlar kurulabilirse iş kartı transferi dışında kesintisiz mesajlaşma ve bir prezantasyon üzerinde beraber değişiklik yapma gibi başka uygulamalar da mümkün hale gelir.

7.10 Gizli Hesaplama

Gizli hesaplama Bluetooth teknolojisinin en heyecan verici gelecek uygulamalarından biridir. Gizli hesaplama için gerekli olan bazı temel elementler mevcut Bluetooth spesifikasyonunda tanımlanmıştır.

Gizli hesaplama konusuna bir örnek olarak otomatik senkronizasyon verilebilir. Otomatik senkronizasyonda PDA cihazı kullanıcının cebinde “gizli” olabilir. Farklı örnekler ise şu şekilde verilebilir:

- Bir çantada “gizli” bulunan ve “uyku” modunda olan bir dizüstü bilgisayar periyodik olarak “uyanmaya” ve yeni e-postalar almaya ve bir mobil telefona e-posta uyarıları göndermeye programlanabilir. Daha sonra kullanıcı da gelen e-postayı mobil telefonu ya da bilgisayarını üzerinden okumaya karar verebilir.
- Kullanıcının cebinde ya da çantasında “gizli” bulunan mobil telefon, başka bir çantada “gizli” bulunan ve uygun şekilde konfigüre edilmiş olan bir dizüstü bilgisayar tarafından ağa bağlanmak için kullanılabilir. Bilgisayar bu yolla ağa bağlandıktan sonra, ağ senkronizasyonu veya e-posta alıp göndermek gibi fonksiyonları kullanıcı müdahalesi olmadan yerine getirebilir.

Gelecekte olması planlanan diğer uygulamalar arasında klima, ışık, müzik, arabada sürücü koltuğu ve ayna kontrolünü “gizli” bir cihaz ile yapmak gibi birçok çevre birim uygulaması bulunmaktadır. [2,7,20]

8. BLUETOOTH'UN GLOBAL 3G SİSTEMİ İÇİNDEKİ YERİ

Günümüzdeki mobil telefon sistemleri için kullanılan hücrel radyo sistemlerinin gelecek jenerasyonu Üçüncü Jenerasyon (Third Generation-3G) olarak adlandırılır. 3G, sesin yanında geniş bantlı veri haberleşmesine de izin veren ilk hücrel radyo teknolojisidir. 3G nin teknik çalışma çerçevesi ITU'nun International Mobile Telecommunications 2000 (IMT-2000) programı tarafından tanımlanmıştır. IMT-2000 in en önemli özelliklerinden birisi tek ve düşük maliyetli bir cihazla global dolaşıma olanak verme yeteneğidir. Bluetooth spesifikasyonu geniş bir yelpazede bulunan servislerin lokalize edilmiş cihazlardan da (avuç içi bilgisayarlar, PDA ler gibi) kullanılmasını sağlayarak 3G sistemleri destekler.

8.1 Global 3G Girişimi

IMT-2000 global telekomünikasyon altyapısına hem uydu hem de karasal sistemler üzerinden kablosuz olarak erişerek, sabit ve mobil kullanıcılara hizmet vermek amacıyla ortaya çıkmıştır. Bu teşebbüs, bugünkü 2G sistemlerden 3G sistemlere geçişi kolaylaştırmak amacıyla şekillenmiştir. ITU'nun bu noktadaki rolü de geliştirilen birçok teknoloji arasındaki koordinasyonu sağlayarak gelişmelere yön verilmesini sağlamaktır.

8.1.1 Standartların Geliştirilmesi

1992 yılında Dünya Radyo Konferansı (World Radio Conference-WRC) 1885-2025 MHz. ve 2110-2200 MHz. arası frekans bantlarını gelecekte kullanılacak IMT-2000 sistemleri için tanımlamıştır. 1980-2010 MHz. ve 2170-2200 MHz. arasını da gelecekte kullanılacak sistemlerin uydu tarafı için ayırmıştır. ITU, radyo iletim teknolojisi (Radio Transmission Technology-RTT) olarak bilinen hava arayüzü teknolojisi üzerinde çalışmaktadır. Giderek artan geniş bant ve üçüncü jenerasyon sistemlerinin artan interaktif trafiğine karşın yeterli olabilmek için gereken ek spektrum miktarı World Radio Conference 2000 (WRC 2000) de ele alınmıştır.

Radyo arayüz teknolojisi için ITU dünya çapındaki organizasyonlardan 15 tanesini çalışmalara dahil etmiştir. Yapılan çalışmalar sonucunda; CDMA, TDMA ve TDMA/CDMA in birleşimini içeren çoklu erişim yöntemlerinden oluşan esnek bir platformda karar kılınmıştır. İkinci jenerasyon mobil sistemler de TDMA ve CDMA teknolojilerini içermektedir; fakat az da olsa SDMA (Space Division Multiple Access) kullanılmaktadır.

IMT-2000 in ana karakteristikleri karasal ve uydu sistemleri için organize edilmiştir. RF bölümünün (ön yüz) etkileri daha çok mobil terminalin donanım bölümünde olur ve temelbant bölümü de daha çok yazılım ile tanımlanır. RF ve temel banda ek olarak, temel uydu karakteristikleri genel yapıyı ve sistem gereksinimlerini de karşılarlar.

Günümüzde bir çok çok modlu/çok bantlı mobil terminal piyasada bulunmaktadır. IMT-2000 standardı tarafından tanımlanan güç tüketimi, boyut ve maliyet gibi faktörler de göz önünde bulundurularak cihazlar geliştirilmektedir.

IMT-2000 uygulamalarına olan esnek yaklaşım, dünya çapında yer etmiş kablosuz teknoloji platformlarının gereksinimlerini karşılayan tek bir standart dahilinde birden fazla erişim yöntemi seçimi sunmaktadır.

8.1.2 IMT-2000 in Amaçları

IMT-2000 modeli dahilinde, mobil telefon teknolojisi sadece pazara-özel bir ürün özelliği göstermeyecek, standartlaşmış esnek platformlar (dünya genelindeki genel, özel, sabit ve mobil platformlar) üzerine kurulu olacaktır. Bu yaklaşım ile daha uzun ürün ömrü ve maliyet-performans iyileştirmesi sağlanacaktır.

IMT-2000 tarafından mobil kullanıcıların gelecek gereksinimlerini karşılayacak 3G sistemler geliştirirken dikkat edilmesi gereken ana noktalar belirlenmiştir. Bu noktalar:

Yüksek Hız

Hızlı internet erişimi veya çoklu ortam uygulamaları gibi yüksek hızlı geniş bant uygulamaları desteklenmelidir. Geniş bant servisleri pazarının 2010 yılında 10 milyar \$ lara ulaşacağı tahmin edilmektedir. Kullanıcılar kullandıkları servislere kablolu ekipmanlardan ulaştıkları gibi mobil olarak da ulaşabileceklerdir.

Esneklik

Entegre sistemlerin gelecek jenerasyonları, evrensel kişisel numaralama ve uydu telefonu gibi yeni tip servisleri desteklemekle birlikte IMT-2000 uyumlu karasal kablosuz ağlar ile de uyumlu bir dolaşım sağlayacak kadar esnek olmalıdır.

Mali Yeterlilik

Sistem, en az bugünkü mobil haberleşme sistemleri kadar elde edilebilir olmalıdır. ITU tek ve global olan bir standartın maliyetleri düşürerek kullanıcının yararına olacağını tespit etmiştir. Telefonların ve mobil teknolojilerin yaygınlaşması için maliyet faktörü çok önemlidir. Kullanıcılar tarafından kolaylıkla alınabilecek üçüncü jenerasyon cihazlar, en az şimdiki kadar veya daha iyi servis sunmalı ve ucuz olmalıdır. Yeterli hacme ulaşıldığı takdirde, kaçınılmaz olarak fiyatlar düşeceği halde, sistemler pahalı olur ve şimdikinden daha fazla fonksiyonallite sağlamazsa kullanıcılar tarafından satın alınmaz.

Uyumluluk

Her yeni-jenerasyon sistem mevcut ağlara göre gelişen bir çizgide bulunmalıdır. Sayısal sistemlerin 1980 lerin sonları ile 1990 ların başları arasında birinci jenerasyon analog ağların devrini kapatmış olmaları gibi; geçtiğimiz 10 yıl boyunca ikinci jenerasyon hücresel ağların gelişimi için yapılan yatırımlar sonucunda üçüncü jenerasyon sistemlerin ikinci jenerasyon sistemlere uyumluluğu konusu da benzer bir noktaya gelmiştir.

Farklılaşma

IMT-2000 çalışma çerçevesinin tasarımı ile koordineli olarak ITU, üreticileri yeni teknolojiler geliştirmeye teşvik edecek bir rekabet ortamı yaratmanın gerekli olduğuna karar vermiştir. IMT-2000 standartlarının amacı yeni teknolojilerin gelişimi bastırmak değil, tersine uygun ortamı oluşturmaktır.

8.1.3 Evrensel Mobil Haberleşme Sistemi (Universal Mobile Telecommunications System-UMTS)

IMT-2000 çalışma çerçevesi ile geliştirilen yeni 3G mobil sistemlerin en önemlilerinden birisi ETSI tarafından standartlaştırılan UMTS dir. UMTS, UTRA (UMTS Terrestrial Radio Access) nın kullanımını sağlayarak global bir karasal radyo erişim ağı temeline dayanmıştır. Avrupa ve Japonya UTRA yı çiftlenmiş (paired)

1920-1980 MHz. ve 2110-2170 MHz. frekans bandlarında uygular. Avrupa UTRA'yı ayrıca çiftlenmemiş (unpaired) 1900-1920 MHz. ve 2010-2025 MHz. frekans bantlarında da kullanmaya karar vermiştir.

UMTS, TDMA (günümüz mobil haberleşme sistemlerinin %80 i TDMA tabanlıdır) ve CDMA teknolojilerinin ana elementleri ile mobil haberleşme ağları üzerinden geniş bant çoklu ortam servislerini verebilmek için entegre bir uydu haberleşme bileşenini içermektedir. UTRA'nın iletim kapasitesi tüm sistemlerdeki tüm mobil uygulamalar için 114 kbit/sn., makro ve mikro hücreli sistemlerde kısıtlı mobil uygulamalar için 384 kbit/sn., mikro ve piko-hücreli sistemlerde düşük ölçekli mobil uygulamalar için ise 2.048 Mbit/sn. dir. 2.048 Mbit/sn. lik iletim hızı makro hücreli sistemlerde kısa dalga veya paket uygulamaları için de kullanılabilir.

UMTS Hedefleri

UMTS; mesajlaşmadan konuşma, veri ve video haberleşmesine, internet ve intranet erişimine, 2 Mbit/sn. ye kadar yüksek bit hızlı haberleşmesine kadar geniş bir çeşitlilik gösteren mobil servisleri destekler. UMTS'in kablolu ve kablosuz uygulamaların şimdiki pozisyonlarının çok daha ötesinde bir platform sağlaması beklenmektedir.

UMTS global olarak kullanılabilen, kişiselleştirilmiş ve yüksek kalitede mobil haberleşme servisleri sunmak üzere tasarlanmıştır. Tasarım hedefleri arasında şunlar bulunur:

- Ev, ofis ve hücreli servislerin tek bir sistem içerisinde entegre edilmesi ve tek bir kullanıcı terminaline ihtiyaç duyması.
- Konuşma ve servis kalitesinin mevcut sabit ağlar kalitesinde olması.
- Çoklu ortam servislerinin desteklenmesi.
- Servis hazırlığı ve ağ operasyonlarının birbirinden ayrılması.
- Ağ veya servis sağlayıcıdan bağımsız olarak taşınabilirlik
- Dünya nüfusunun %50 sinden fazlasına hizmet verme kapasitesi.
- 144 kbit/sn. ye kadar global radyo kapsama alanı ve 2 Mbit/sn. ye kadar radyo taşıyıcı servisleri.
- Bir frekans bantı içinde rekabete imkan verecek kaynak esnekliği.

Tanım

UMTS; servis sağlayıcı, ağ operatörü, abone ve kullanıcı rollerini birbirinden ayırır. Rollerin ayırımı servis sağlayıcılardan ek ağ yatırımı istenmeksizin yeni servislerin geliştirilmesine imkan tanır. Her UMTS kullanıcısı ağdan bağımsız benzersiz bir kimlik numarasına sahiptir. Birçok kullanıcı ve terminal aynı abonelik ile ilişkili olabilir. Böylelikle tek abonelik ve faturalandırma ile örneğin bir aileye mensup bireylerin kendi terminallerini kullanmalarına olanak tanınır. Aynı şekilde işyerleri için de uygun maliyetli çözümler oluşturulur.

UMTS, uygulamaları standartlaştırmak yerine, esnek servislerin oluşumunu desteklemektedir. Servislerin verilme kararı servis sağlayıcılara ya da ağ operatörlerine bırakılmıştır. Kullanıcı kendi ihtiyaçlarına göre kullanacağı servisleri o servislere abone olarak veya terminali yardımıyla interaktif olarak seçer.

UMTS ağ, yayım, izin, konuma bağlı servisler ve diğer sistem özellikleri desteği sayesinde daha önceden verilen konuşma ve veri servislerine göre oldukça üstündür.

UMTS 2 kbit/sn. den 64 kbit/sn. ye kadar farklı konuşma kodlama-kod çözme (codec) alternatifleri ile imaj, video ve veri kodlamalarını-kod çözmelerini (codec) destekleyen yüksek kalitede radyo bağlantısı sağlar. ISDN in büyük bir kısmını kapsayan ileri veri protokollerini de destekler ve 2 Mbit/sn. ye kadar yüksek bir hızlarını içerir. [21]

Fonksiyonel Model

UMTS fonksiyonel modeli dağıtılmış veri tabanları ve veri işlemeye dayanır. Mevcut UMTS ağları ve UMTS terminallerini değiştirmeksizin yeni servisler eklenebilir. Bu servis-yönelimli model; servislerin yönetim ve işletimi, mobilite ve bağlantı kontrolü ile ağ yönetimi olmak üzere üç ana fonksiyon sağlar.

- Servislerin yönetim ve işletimi

Bir “Servis Veri Fonksiyonu” (SDF) servisle ilgili veriye erişmeyi ve depolamayı sağlar. Bir “Servis Kontrol Fonksiyonu” (SCF) tüm servis ve mobilite kontrol mantığı ile servisle ilgili veri işleme fonksiyonunu içerir. Bir “Servis Bağlaşma Fonksiyonu (SSF) servis mantığını harekete geçirir (örneğin rota bilgisini talep eder). Bir “Arama Kontrol Fonksiyonu” (CCF)

servis taleplerini analiz ve proses eder, aramaları başlatır, devam ettirir ve sona erdirir.

- Mobilite ve bağlantı kontrolü

UMTS, kullanıcı servis profillerini uygun ağ servisleri, radyo özellikleri ve terminal fonksiyonları ile gerçek zamanlı olarak eşleştirir. Bu fonksiyon mobil abone kaydı, doğrulama, fiziksel yer güncelleme, dolaşımdaki bir aboneye çağrı yönlendirme gibi özellikleri yerine getirir.

- Ağ yönetimi

UMTS'de abone verisinin yönetimi ve prosesi, ağın bakımı, faturalama ve trafik istatistikleri geleneksel Telecommunications Management Network (TMN) ile gerçekleşir.

TMN dünya çapındaki haberleşme servis sağlayıcı ağının kontrolü ve izlenmesi için yapılan ulusal ve uluslararası birçok anlaşma ve standart içerir. Bu anlaşmalar sayesinde yüksek servis kalitesi, maliyet azalması ve hızlı ürün entegrasyonu sonuçları elde edilir. TMN kablosuz haberleşmede, kablolu televizyon ağlarında, yüksek band genişlikli haberleşme ağlarında da uygulanır. UMTS için yeni TMS elementleri geliştirilmektedir.

Taşıyıcı Servisleri

UMTS'de dört tip taşıyıcı servisi kullanılmaktadır:

- A sınıfı: Bu taşıyıcı servisi isonkron (gerçek zamanlı) konuşma iletimi için sabit bit hızlı (Constant Bit-Rate-CBR) bağlantılar sağlar. Yüksek kalitede konuşmayı garanti etmek için gereken bant genişliğini sürekli olarak temin eder.
- B Sınıfı: Bu taşıyıcı servisi patlamalı (bursty) trafiğe uyum sağlayan değişken bit hızlı bağlantılar sağlar.
- C Sınıfı: Bu taşıyıcı servisi zamana karşı hassas olan bilinen mevcut veri uygulamalarını desteklemek için kullanılabilecek bağlantı yönelimli bir paket protokolüdür.
- D Sınıfı: Bu taşıyıcı servisi internet veya intranetteki veriye erişmek için uygun olan bir bağlantısız paket taşıyıcı servsidir.

Teknoloji Yaklaşımları

UMTS standardı geliştirilirken UMTS Forum'da ağın radyo arayüzü bölümü için TD-CDMA (time division) ya da W-CDMA (wideband) kullanılmasına ilişkin anlaşmazlıklar olmuştur.

TD-CDMA geleneksel TDMA teknolojisi tarafından sunulan kapasiteyi genişletmek için CDMA in işaret-saçılma (spreading) tekniklerini kullanır. Sayısallaştırılmış ses ve veri 1.6 MHz. lik geniş bir kanalda zaman-bölümlemeli TDMA teknolojisi kullanılarak iletilebilir. TDMA kanalının her bir zaman slotu CDMA teknolojisi kullanılarak kodlanabileceği için zaman slotu başına birden fazla kullanıcı desteklenir. Bu sayede mevcut GSM kullanıcılarının gelecek nesil hücresel standarda ekonomik ve kolay yoldan geçmeleri sağlanır. Aynı zamanda TD-CDMA teknolojisi ile CDMA teknolojisinin dünya çapında kullanılan TDMA tabanlı GSM altyapısına entegre olması sağlanır.

W-CDMA yüksek kapasite avantajına ek olarak en çok kullanılan hücresel teknolojidir. Ocak 1998'de UMTS Forum üyeleri TD-CDMA ile W-CDMA in anahtar elemanlarını birleştirmeye karar vererek bu yeni çözüme UTRA adını vermişlerdir. UMTS in çiftlenmiş (paired) bantlarında (frekans bölmeli dublex) sistem W-CDMA grubu tarafından desteklenen radyo erişim tekniğini benimser. Çiftlenmemiş (unpaired) bantlarda (zaman bölmeli dublex) ise TD-CDMA grubu tarafından desteklenen radyo erişim tekniği benimsenir.

Uygulamalar

UMTS yeni bir hava arayüzü ve yeni radyo bileşenlerinden oluşmaktadır. Bu yeni özelliklerin yeni ağ bileşenleri ve UMTS'den önceki ağların bileşenleri ile modüler bir yolla birleştirilmesi amaçlanmaktadır. Bu sayede operatörlerin mevcut altyapılarını kullanarak UMTS'e yumuşak bir geçiş yapmalarını sağlamak amaçlanmaktadır.

Kullanıcı için, UMTS adaptif çok modlu/çok bantlı terminaller veya global dolaşıma olanak tanıyan ve ikinci jenerasyon sistemlerle de haberleşebilen esnek hava arayüzü olan terminaller sağlar. Terminallere yeni yazılımlar yüklenerek ek özellikler de sağlanır.

8.2 Bluetooth'un Rolü

Hücreli telefon sistemlerinin ileriki jenerasyonu, mevcut sayısal sistemlerin (GPRS, EDGE ve HSCSD) evrimi veya tamamen yeni sistemlerin (UMTS/IMT 2000) gelişimi ile mümkün olacaktır. Yeni jenerasyon sistemler kullanıcılara daha önce mümkün olmayan bir esneklik ve olanak sağlayacaktır. Bluetooth spesifikasyonu mobil telefonlara günümüzde sıklıkla kullanılan telefon servisleri yanında bir çok yeni uygulama alanı açmıştır. Yeni gelişimlerin yaşaması Bluetooth kablosuz teknolojisinin hücreli telefon gibi kablosuz mekanizmaları desteklemedeki başarısı ile orantılıdır. Ulusal ağlar, hareket halindeyken veya herhangi bir lokasyona kablosuz erişim sağlarken; lokal iç bağlantıların da Bluetooth spesifikasyonu gibi bir sistem tarafından yerine getirilmesi avantaj getirecek bir bakış açısidir.

Tanımlanmamış fiziksel bir yerden başka birine telefon servislerinin sağlanabilmesi ve bu yerlerde servisler ile fonksiyonların dağıtılabilmesi için, hibrid bir çözüme gerek duyulur, içinde Bluetooth alıcı-vericisi olan hücreli bir el terminali (handset) ile bu işleyiş yerine getirilebilir. Hücreli telefonlar konuşma iletiminde oldukça fazla kullanılmalarına rağmen, veri iletiminde çok iyi değillerdir. Mevcut ikinci jenerasyon sistemlere yapılan geliştirmeler, 2.5G sistemler olarak anılırlar, veri iletiminin de yüksek hızlarda (genel olarak maksimum 64 kbit/sn. ye kadar) yapılabilmesine olanak tanır. Veri, devre bağlama yerine paket bağlamalı olarak taşınır. Hücreli telefon sistemlerinin üçüncü jenerasyonu paket veriyi taşımak üzere tasarlanmıştır, konuşma da başka bir veri uygulaması olarak ele alınır. Hücreli telefonlar için mümkün olacak birkaç yüz kbit/sn. lik veri hızları, telefonları birer çoğul ortam terminali haline getirir. Bluetooth spesifikasyonu geniş bir yelpazede bulunan servislerin WAN lardan LAN lara ve PDA lara dağıtımı ile geliştirilmiş 2G ve 3G sistemleri desteklemektedir. Bluetooth spesifikasyonu lokal bir iç bağlantı sağladığı gibi ulusal ağlara da bir ara geçit oluşturur.

Ulusal ağlara ve 3G sistemlere erişim için kullanılan telsiz telefon sistemleri birleştirilmiş bir ağ/telsiz servisi sunarlar. Bununla birlikte el terminallerinin (handset) intercom fonksiyonlitesini desteklemesi ve birbirlerine yakın mesafede bulunan iki cihaza da bu özelliklerin eklenmesi gerektiği için verimsiz ve ekonomik olmayan bir yapı meydana gelir.

Bluetooth kablosuz teknolojisi kısa bir mesafede bulunan ve bir pikonette bulunan maksimum sekiz cihazın eş zamanlı olarak birbirleri ile haberleşmelerini sağlar. Birçok pikonet birbirlerine yakın mesafede çalışabilir ve Bluetooth cihazları bir pikonetten diğerine hızla geçebilirler. Bluetooth cihazlarının bir haberleşme sürecini tamamlayana kadar bir pikonetin üyesi olarak kalmaları yeterlidir. Cihazlar bir pikonete hızla ve sık sık katılıp, ayrılabilirler. Birbirine bağlı iki pikonet bir saçılmış ağ (scatternet) oluşturur ve farklı atlama dizileri kullandıkları için aynı bölgede çalışabilirler. Bu sayede küçük gruplardan oluşan birçok Bluetooth cihazının aynı bölgede girişime neden olmaksızın çalışabilmesi sağlanır.

Bluetooth cihazları 1 Mbit/sn. ye kadar veri alıp gönderebilirler. Pratikte aynı anda birden fazla uygulamanın birbirleriyle haberleşmelerine imkan verebilmek için veri hızları bundan daha düşük olur. Bir pikonete dahil olmayan Bluetooth cihazları sürekli olarak diğer Bluetooth cihazlarını dinlerler ve bir pikonetin parçası olabilecek kadar yakın mesafeye geldiklerinde diğer cihazların kendileri ile haberleşebilmeleri için kendilerini tanımlarlar.

3G terminaller web tarama, e-posta gönderme ve alma, video ve ses iletimi gibi değişik şekillerdeki bilginin iletimi sağlayabilen gerçek çoğul ortam terminalleri olacaktır. Ses iletimi her zaman için ana unsur olma önemini koruyacağından dolayı Bluetooth spesifikasyonunda yüksek kalitede iletim sağlayan 64 kbit/sn. lik konuşma kanalları sağlanmaktadır. Ses iletiminin yanısıra paket veri iletimine de imkan tanındığı için çoğul ortam uygulamaları için tam destek sağlanmaktadır.

Bluetooth cihazları aynı anda birden fazla veri bağlantısına ve en fazla üç ses bağlantısına olanak tanıdığı için üç-el terminali (handset) telsiz çoğul ortam/intercom sistemi için gereken fonksiyonalliteyi sağlar. Üç terminal kısıtı ses için geçerli olup, veri değiş tokuşu yapan terminal sayısı pikonet başına sekizdir.

Bluetooth kablosuz teknolojisini kullanan bir baz istasyonu birbirine benzer donanımdaki terminaller ve telefon hattı bağlantısı için iç bağlantı sağlar. Harici bir bağlantı talep edildiğinde sadece iki lokal el terminali (handset) ses bağlantılarına katılabilir. Baz istasyonu lokal cihazlar ile çeşitli ulusal ağlar ve servisler arasında bir ara geçit görevi görür. Herhangi iki el terminali (handset) baz istasyonu olmaksızın birbirlerine bağlanabilirler. Bazı durumlarda örneğin evde kullanılan bir bilgisayar

Bluetooth spesifikasyonu ile baz istasyonuna bağlanır ve herhangi bir uzak mesafeden bu baz istasyonu çağrılarak bilgisayardan veri alınabilir.

Bu senaryo Bluetooth ve 3G sistemlerin bütünler fonksiyonalitesinin altını çizmektedir. 3G sistemi belirli bir fiziksel yere bağlantı sağlarken, Bluetooth kablosuz teknolojisi de lokal cihazlara son iletim için kullanılmaktadır. Bu durum 3G ağındaki gereksiz trafiğin önüne geçerken, sabit ve mobil servislerin birlikte kullanımları için de RF girişimini minimumda tutan uygun maliyetli bir çözüm sunar.

8.3 Özet

IMT-2000; uluslararası uyumluluk, global dolaşım, çoğul ortam uygulamalarının, internet erişiminin ve kişiselleştirilebilen servislerin yüksek hızda iletimi için giderek artan global ekonomi ihtiyaçlarını adreslemektedir. Günümüzde bütün bu servisler için bir pazar bulunmakta ve hızla büyümektedir. IMT-2000 günümüzdeki 2G ağlardan 3G ağlara geçişi sağlayacak standartları ortaya koymaktadır.

Bluetooth kablosuz teknolojisi küçük boyutu, kayda değer fonksiyonalitesi ve esnekliği, çok düşük maliyeti ile birçok el tipi cihaz ve uygulamada yerini almaktadır. Hücresel telefonların yeni jenerasyonları ulusal bir kapsama alanı ve mobilite sağlarken lokal bağlantılı cihazlar için düşük maliyetli bir iç bağlantı hizmeti sunamayacaktır. Bluetooth spesifikasyonu ile bağdaştırıldığı takdirde ise yerel cihazlar da bulundukları yere bağlı olmaksızın ve hareket halindeyken de bağlantı durumuna geçebileceklerdir. Bluetooth kablosuz teknolojisi ile hücresel sistemlerin günümüz sınırlarının ötesine geçerek, kullanım alanlarının hızla artacağı aşıkardır. [9,22]

9. SONUÇLAR ve TARTIŞMA

Son yıllarda bilgi teknolojileri alanında yaşanan hızlı gelişmeler mobil haberleşmeye ve kablosuz teknolojilere de yansımış; kablosuz haberleşmenin çağımızın en önemli konularından birisi haline gelmesine yol açmıştır. Ancak kişisel ve iş amaçlı kullanım için sayısız elektronik cihaz üretilmiş olmasına rağmen, çok yakın zamana kadar kişisel alan ağlarında (Personal Area Networks) yerlerini alan cihazların kendi aralarında iletişim kurmasını sağlayacak yaygın bir teknoloji bulunamamıştır. Kullanılan cihaz sayısı arttıkça cihazlar arasında kablolarla ihtiyaç duymadan veri ve ses haberleşmesi yapabilecek bir teknolojiye olan gereksinim de hızla artmıştır.

Bluetooth teknolojisi bu önemli boşluğu doldurmakta; düşük güç tüketimli, ucuz ve cihazlara kolaylıkla entegre edilmeye imkan veren bir teknoloji olarak kablosuz veri ve ses haberleşmesinin kapılarını açmaktadır.

Bluetooth teknolojisinin piyasaya ilk sunulduğu 1999 yılının Aralık ayından itibaren çok sayıda üretici Bluetooth teknolojisini ürünlerine entegre etmiştir. Cahners In-Stat Group tarafından 2000 yılı Temmuz ayında yapılan bir araştırmaya göre 2000-2002 yılları arasında Bluetooth kullanan ürünlerin gelişimi şu şekilde olmuştur:

2000-2001 döneminde mobil telefon adaptörleri, dizüstü ve masaüstü bilgisayarlar için adaptörler ve PC Card'lar, cep telefonları, mikrofon-kulaklık setleri ve PDA'ler kullanıcıları Bluetooth ile tanıştırmıştır.

2001-2002 döneminde ise anakartında elektronik Bluetooth devreleri içeren bilgisayarlara, Bluetooth kullanan yazıcılara, faks makinelerine, dijital fotoğraf makinelerine, tıbbi ürünlere, endüstriyel çözümlere ağırlık verilmiştir. Örneğin 2002 yılı başlarında otomotiv sektörü için lastik üretimi yapan Nokian Renkaat adlı Finlandiya şirketi “Akıllı Lastik” projesini tamamlamıştır. Bu proje kapsamında Bluetooth çipinin içine monte edildiği akıllı lastik, otomobil kullanılırken sürücüye yol, lastik basıncı ve sürtünme değerlerini Bluetooth teknolojisi sayesinde iletmekte; yolda giderken oluşabilecek herhangi bir problemi veya tehlikeyi, önceden algılayarak sürücünün cep telefonuna acil durum mesajı gönderebilmektedir. Bu

işlemin gerçekleşebilmesi için gerekli tek şey sürücünün cep telefonunda da Bluetooth çipinin olmasıdır.

Türkiye’de ise en çok rağbet gören Bluetooth ürünleri Bluetooth mikrofon-kulaklık setleri, cep telefonları, USB arabirimli Bluetooth erişim cihazlarıdır. Son dönemde de Bluetooth uyumlu ana kartlar ilgi çekmeye başlamıştır.

IDC’ye göre 2003 yılı Bluetooth’un patlama yılı olacaktır. Gartner Grup’a göre de 2005 yılı sonuna kadar kişisel ve iş amaçlı kullanım için 560 milyon Bluetooth uyumlu cihaz satın alınmış bulunacaktır.

Bluetooth, 2.4 GHz. lisanslanmamış ISM frekans bandında çalışması, saniyede maksimum 1 Mbit lik veri transfer hızı, düşük güç tüketimi, düşük maliyeti, 10-100 m. etki alanı, kızıl ötesi haberleşmede olduğu gibi haberleşecek iki noktanın birbirini görme zorunluluğu olmaması gibi olumlu özelliklerine rağmen, başka bir kablosuz haberleşme teknolojisi olan IEEE 802.11b teknolojisi ile kullanıcı gözünde ciddi ölçüde rekabet etmektedir. Ancak Bluetooth’un temelde cihazlar arasında kısa mesafelerde veri ve ses haberleşmesini sağladığı, 802.11b teknolojisinin ise kablosuz bir LAN özelliği taşıdığı göz önüne alınırsa iki teknolojinin ortaya çıkma amaçlarının farklı olduğu anlaşılmaktadır.

Bluetooth gibi 2.4 GHz. radyo frekansını kullanan 802.11b teknolojisi, Kablosuz Ethernet (Wireless Ethernet) olarak da bilinmektedir; hem veri transfer hızı hem de etki alanı büyüklüğü Bluetooth’a göre 10 kat daha fazladır. Eş zamanlı kullanıcıların sayısı yüksektir. Diğer yandan, Bluetooth ile karşılaştırılacak olursa, daha pahalıdır ve daha fazla güç tüketir. Ayrıca 802.11b donanımı, küçük mobil cihazlarda kullanım için gereken uygun boyutlara sahip değildir. 40 bitlik şifreleme ile gerçekleştirdiği güvenlik özellikleri ise dezavantajları arasındadır.

Bluetooth’un sadece 8 kullanıcı kapasitesi ile sınırlı olması kablosuz LAN uygulamaları için bir problem olarak düşünülebilir. 802.11b’nin yaklaşık 100 metrelik etki alanına ulaşmak için Bluetooth vericileri elektrik güçlerini kısa sürede tüketmek zorunda kalacaklardır. Ayrıca Bluetooth cihazlarının, 802.11b kullanan cihazlarla aynı frekansı kullanmaları nedeniyle de çeşitli problemler çıkacağı öngörülmektedir.

Dünya genelinde birçok işyerinde, havaalanlarında ve hatta hastanelerde 802.11b ile çalışan kablosuz ağ uygulamaları uygulanmaya başlanmıştır. Bluetooth iş

dünyasında, LAN uygulamalarının kablosuz hale geçirilmesi konusunda 802.11b'ye göre daha geride olmasına karşın, günlük hayatımızdaki cihazların birbirleri ile haberleşmesini sağlamak konusunda sunduğu ve sunacağı birçok avantaj vardır.

2.4 GHz'lik diğer teknoloji de Bluetooth ile büyük benzerlikler taşıyan EvRF (Home RF) dir. EvRF özel veri ağlarında kullanılabilir. Ayrıca sistemi koordine eden ve telefon şebekesine (ses ve veri) bir ara geçit sunan bir bağlantı noktasının altında da EvRF kullanılabilir. Atlama frekansı 8 Hz'dir. (Bir Bluetooth bağlantısında ise bu değer 1600 Hz'dir.)

Bluetooth'u yavaşlatıcı ve engelleyici faktörler arasında sağlıkla ilgili endişeler ve gürültü konusu da bulunur. Bluetooth, düşük gücü dolayısıyla hiçbir sağlık sorununa yol açmaz; ancak satıcıların bu mesajı kullanıcılara duyurmaları ve anlatmaları gerekmektedir. ISM bandının birçok cihaz tarafından giderek artan kullanımı ile gürültü oluşacaktır; ancak Bluetooth'un yüksek hızlı frekans atlamalı tekniği gürültünün etkisini azaltır.

Tüm bu faktörler Bluetooth'un başarısızlığa uğrayacağı anlamına gelmemekte, ancak gerçek potansiyeline ulaşmasının bugünkü tahminlerden daha fazla zaman alabileceğini göstermektedir. Unutulmaması gereken bir nokta, Bluetooth'un fiyat avantajının diğer teknolojilerde bulunmamasıdır. Birkaç yıl içinde Bluetooth çiplerinin 5 dolar gibi bir fiyatla satılması beklenmektedir.

Bluetooth 2005 yılına kadar tüketiciden-işletmeye elektronik ödeme (POS, bilet kesme ve otomat makineleri) gibi tamamen yeni ve günlük hayatı kolaylaştıran fırsatlar yaratacaktır. Bluetooth kullanımının artmasıyla birlikte, bugün çok zor gibi görünen bir çok şeyi yapmak kolaylaşacaktır. Örneğin yolda giderken, arabada bulunan bir Bluetooth çipi sayesinde gişede durmaya gerek kalmadan uzaktan otomatik ödeme yapılabilir, ya da yine benzer bir çipe sahip dijital fotoğraf makinesiyle çekilen fotoğraflar, hiç zaman kaybedilmeden dizüstü bilgisayar aracılığıyla e-posta olarak gönderilebilecektir. Hatta, cep telefonu ya da PDA kullanarak kredi kartından ödeme yapılarak otomat makinelerinden içecek alınabilecek, böylelikle bozuk para taşıma gereksinimi ortadan kalkacaktır.

Bluetooth'a yatırım yapan teknoloji devi şirketlerden Apple, Temmuz 2002 de Mac OS X işletim sistemine Bluetooth desteğini eklemiştir. Benzer şekilde Microsoft da

Ekim 2002 de Windows XP işletim sistemine Bluetooth desteğini eklediğini duyurmuştur.

Kullanım kolaylığı, fayda ve düşük maliyeti birleştiren Bluetooth ürünleri başarıya ulaşacak; Türkiye’de de Bluetooth ürünlerinin kullanımı giderek yaygınlaşacaktır.

KAYNAKLAR

- [1] **Biesecker K.**, 2000. The Promise of Broadband Wireless, *IT Pro*, November December, 31-36.
- [2] **Miller B.A. and Bisdikian C.**, 2001. Bluetooth Revealed, Prentice Hall, USA.
- [3] **AU System**, 2000. Bluetooth Whitepaper 1.1
- [4] **Sönnerstam Dan**, 1998. Comprehensive Description of the Bluetooth System, Ericsson Bluetooth Document.
- [5] **www.palowireless.com**, Bluetooth Articles, Bluetooth Radio
- [6] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Radio Specification.
- [7] **Riku Mettala**, 1999. Bluetooth Protocol Architecture, Bluetooth White Paper, Nokia.
- [8] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Baseband Specification.
- [9] **Müller Nathan J.**, 2001. Bluetooth Demystified, McGraw-Hill, USA.
- [10] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Link Manager Protocol.
- [11] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Logical Link Control and Adaptation Protocol.
- [12] **International Business Machines Corporation**, 1999. Discovering Devices and Services in Home Networking
- [13] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Service Discovery Protocol.
- [14] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, RFCOMM
- [15] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, IrDA Interoperability.
- [16] **Suvak Dave**, 2000. IrDA and Bluetooth Comparison, Extended Systems, Inc.

- [17] **Bluetooth SIG, Inc.**, 2001. Specification of the Bluetooth System, Telephony Control Protocol Specification.
- [18] **Müller Thomas**, 1999. Bluetooth Security Architecture, Bluetooth White Paper, Nokia.
- [19] **Jakobsson Markus and Wetzel Susanne**, 2001. Security Weaknesses in Bluetooth.
- [20] **Stripp Jeff**, 2001. Bluetooth: Value Adds and Opportunities, Mindbranch, Inc.
- [21] **www.wired.com**, 3G Spectrum Pricetag Soars by Elisa Batista.
- [22] **Widcomm Inc.**, 2001. 3G & Bluetooth Whitepaper.

ÖZGEÇMİŞ

1974 yılında Adana’da doğdu. İlk, orta ve lise öğrenimini Adana’da tamamladıktan sonra 1991 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünü kazandı. Üniversite eğitimi boyunca haberleşme derslerine ağırlık verdi. 1995 yılında “Telefon Hattı Ölçümlerinin PC ile Yapılması” konulu bitirme projesinde çalışarak lisans eğitimini tamamladıktan sonra aynı yıl Escort Computer’de ArGe Mühendisi olarak çalışma hayatına atıldı. 1996 yılında İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği Bölümü, Biyomedikal Mühendisliği yüksek lisans programına girerek; haberleşme konularında çalışmaya devam etti. Halen Enter Bilgisayar A.Ş. de İş Geliştirme Müdürü olarak çalışmakta; mobil teknolojiler üzerine geliştirilen projelerde yer almaktadır. Amatör olarak müzik, sinema ve dalgıçlık ile ilgilenmekte; iyi derecede İngilizce ve orta derecede Almanca bilmektedir.