



**KAHRAMANMARAS ST İMAM NİVERSİTESİ**  
**FEN BİLİMLERİ ENSTİTS**  
**ELEKTRİK-ELEKTRONİK MHENDİSLİĐİ ANABİLİM DALI**

## **BLUETOOTH ZERİNDEN GVENLİ VERİ İLETİMİ**

**MEHMET ALİ ZELİK**

**YKSEK LİSANS TEZİ**

**KAHRAMANMARAS**  
**OCAK - 2006**



**KAHRAMANMARAS ST İMAM NİVERSİTESİ  
FEN BİLİMLERİ ENSTİTS  
ELEKTRİK-ELEKTRONİK MHENDİSLİĐİ ANABİLİM DALI**

**BLUETOOTH ZERİNDEN GVENLİ VERİ İLETİMİ**

**MEHMET ALİ ZELİK**

**YKSEK LİSANS TEZİ**

**KAHRAMANMARAS  
OCAK - 2006**

**KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ**  
**FEN BİLİMLERİ ENSTİTÜSÜ**  
**ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI**

**BLUETOOTH ÜZERİNDEN GÜVENLİ VERİ İLETİMİ**

**Mehmet Ali ÖZÇELİK**

**Kod No :**

**Bu Tez 17/ 01 /2006 Tarihinde Aşağıdaki Jüri Üyeleri Tarafından  
Oy Birliği ile Kabul Edilmiştir.**

.....  
**Prof.Dr. M.Kemal KIYMIK**

**DANIŞMAN**

.....  
**Yrd.Doç.Dr.Abdülhamit SUBAŞI**

**ÜYE**

.....  
**Yrd.Doç.Dr.M.Metin KÖSE**

**ÜYE**

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

.....  
**Prof.Dr.Özden GÖRÜCÜ**

**Enstitü Müdürü**

Bu çalışma.....tarafından  
desteklenmiştir.

Proje No:.....

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

| <b>İÇİNDEKİLER</b>                                             | <b>SAYFA</b> |
|----------------------------------------------------------------|--------------|
| <b>İÇİNDEKİLER.....</b>                                        | <b>I</b>     |
| <b>ÖZET.....</b>                                               | <b>V</b>     |
| <b>ABSTRACT.....</b>                                           | <b>VI</b>    |
| <b>ÖNSÖZ.....</b>                                              | <b>VII</b>   |
| <b>ÇİZELGELER DİZİNİ.....</b>                                  | <b>VIII</b>  |
| <b>ŞEKİLLER DİZİNİ .....</b>                                   | <b>IX</b>    |
| <b>SİMGELER VE KISALTMALAR DİZİNİ.....</b>                     | <b>XI</b>    |
| <b>1. GİRİŞ.....</b>                                           | <b>1</b>     |
| <b>1.1. WiFi / IEEE 802.11.....</b>                            | <b>1</b>     |
| <b>1.2. İrda Teknolojisi.....</b>                              | <b>2</b>     |
| <b>1.3. DECT Teknolojisi.....</b>                              | <b>3</b>     |
| <b>1.4 Home RF Teknolojisi.....</b>                            | <b>4</b>     |
| <b>1.5. Bluetooth Teknolojisi.....</b>                         | <b>5</b>     |
| <b>2. ÖNCEKİ ÇALIŞMALAR.....</b>                               | <b>7</b>     |
| <b>3. MATERYAL ve METOD.....</b>                               | <b>8</b>     |
| <b>3.1. MATERYAL.....</b>                                      | <b>8</b>     |
| <b>3.1.1. Bluetooth Teknolojisi ile İlgili çalışmalar.....</b> | <b>8</b>     |
| <b>3.1.2. Bluetooth ismi.....</b>                              | <b>9</b>     |
| <b>3.1.3. Bluetooth’un Temel Özellikleri .....</b>             | <b>10</b>    |
| <b>3.1.3.1. Birlikte Çalışabilirlik.....</b>                   | <b>10</b>    |
| <b>3.1.3.2. Kısa Mesafe Kablosuz Haberleşme Yapısı.....</b>    | <b>10</b>    |
| <b>3.1.3.3. Açık Standart Yapısı.....</b>                      | <b>10</b>    |
| <b>3.1.3.4. Ses ve Veri Haberleşmesi.....</b>                  | <b>10</b>    |
| <b>3.1.3.5. Tüm Dünyada Uyumlu Olması .....</b>                | <b>11</b>    |
| <b>3.1.4. Teknolojik Alt Yapı.....</b>                         | <b>11</b>    |
| <b>3.1.4.1. Kablolu ve Kablosuz Haberleşme.....</b>            | <b>11</b>    |
| <b>3.1.4.2. Bluetooth Radyo Teknolojisi.....</b>               | <b>12</b>    |
| <b>3.1.4.3. Frekans Atlama Tekniği.....</b>                    | <b>12</b>    |
| <b>3.1.4.4. Modülasyon Tekniği.....</b>                        | <b>13</b>    |
| <b>3.1.4.5. Bluetooth Radyo Güç Sınıfları.....</b>             | <b>13</b>    |
| <b>3.1.4.6. Master - Slave Yapısı.....</b>                     | <b>13</b>    |

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>3.1.5. Bluetooth Şebeke Yapısı.....</b>                                | <b>14</b> |
| <b>3.1.5.1. Piconet.....</b>                                              | <b>14</b> |
| <b>3.1.5.2. Scatternet.....</b>                                           | <b>15</b> |
| <b>3.1.5.3. Ses ve Veri.....</b>                                          | <b>16</b> |
| <b>3.1.5.4. Güvenlik.....</b>                                             | <b>16</b> |
| <b>3.1.6. Bluetooth Protokol Mimarisi.....</b>                            | <b>17</b> |
| <b>3.1.6.1. Genel Bakış.....</b>                                          | <b>17</b> |
| <b>3.1.6.1.1. Protokol Nedir?.....</b>                                    | <b>17</b> |
| <b>3.1.6.1.2. Bluetooth Protokol Mimarisi Tanımı.....</b>                 | <b>17</b> |
| <b>3.1.6.1.3. OSI Referans Modeli.....</b>                                | <b>18</b> |
| <b>3.1.6.1.4. Bluetooth Protokol Yığını.....</b>                          | <b>19</b> |
| <b>3.1.6.2. Bluetooth Radyo.....</b>                                      | <b>20</b> |
| <b>3.1.6.3. Temel Bant Katmanı.....</b>                                   | <b>21</b> |
| <b>3.1.6.4. LMP (Link Yönetim Protokolü).....</b>                         | <b>21</b> |
| <b>3.1.6.5. HCI (Host Control Interface).....</b>                         | <b>22</b> |
| <b>3.1.6.6. L2CAP (Logical Link Control and Adaption Protocol).....</b>   | <b>22</b> |
| <b>3.1.6.7. RFCOMM.....</b>                                               | <b>23</b> |
| <b>3.1.6.8. SDP (Service Discovery Protocol).....</b>                     | <b>23</b> |
| <b>3.1.7. Telefon Kontrol Protokolleri ve Uyarlanmış Protokoller.....</b> | <b>24</b> |
| <b>3.1.7.1. TCS Katmanı.....</b>                                          | <b>24</b> |
| <b>3.1.7.2. TCS-BIN.....</b>                                              | <b>24</b> |
| <b>3.1.7.3. AT Komutları.....</b>                                         | <b>25</b> |
| <b>3.1.8. Uyarlanmış Protokoller.....</b>                                 | <b>25</b> |
| <b>3.1.8.1. PPP.....</b>                                                  | <b>25</b> |
| <b>3.1.8.2. TCP/UDP/IP.....</b>                                           | <b>25</b> |
| <b>3.1.8.3. IrDA.....</b>                                                 | <b>25</b> |
| <b>3.1.8.4. OBEX.....</b>                                                 | <b>26</b> |
| <b>3.1.9. Temel Bant Katmanı.....</b>                                     | <b>26</b> |
| <b>3.1.9.1. Genel Bilgi .....</b>                                         | <b>26</b> |
| <b>3.1.9.2. Frekans Bandı ve RF Kanalları.....</b>                        | <b>27</b> |
| <b>3.1.9.3. Zaman Dilimleri.....</b>                                      | <b>27</b> |
| <b>3.1.9.4. Kanal Tanımı.....</b>                                         | <b>28</b> |

|                                                           |    |
|-----------------------------------------------------------|----|
| 3.1.9.5. Modülasyon ve Bit Hızı.....                      | 29 |
| 3.1.9.6. Fiziksel Linkler.....                            | 29 |
| 3.1.9.7. ACL.....                                         | 29 |
| 3.1.9.8. SCO.....                                         | 29 |
| 3.1.10. Bluetooth Adres Çeşitleri.....                    | 30 |
| 3.1.11. Bluetooth Paket Yapıları.....                     | 30 |
| 3.1.11.1. Genel Paket Formatı.....                        | 30 |
| 3.1.11.2. Erişim Kodu.....                                | 31 |
| 3.1.11.3. Başlangıç (Preamble).....                       | 32 |
| 3.1.11.4. Senkronizasyon Kelimesi.....                    | 32 |
| 3.1.11.5. Kuyruk (Trailer).....                           | 33 |
| 3.1.11.6. Paket Başlığı (Packet Header) .....             | 33 |
| 3.1.11.7. Aktif Üye Adresi (AM_ADDR).....                 | 33 |
| 3.1.11.8. Paket Tipi (TYPE).....                          | 34 |
| 3.1.11.9. Akış Kontrol Alanı (Flow) .....                 | 34 |
| 3.1.11.10. Doğrulama Alanı (ARQN).....                    | 34 |
| 3.1.11.11. Sıralama Alanı (SEQN).....                     | 34 |
| 3.1.11.12. Hata Kontrol Alanı (HEC).....                  | 34 |
| 3.1.11.13. Kullanıcı Verisi (Payload .....                | 35 |
| 3.1.11.14. Kullanıcı Verisi Başlığı (Payload Header)..... | 35 |
| 3.1.11.15. Veri Gövdesi (Payload Body).....               | 35 |
| 3.1.11.16. CRC Alanı.....                                 | 35 |
| 3.1.11.17. Paket Tipleri.....                             | 35 |
| 3.1.11.18. Ortak Paket Tipleri.....                       | 36 |
| 3.1.11.19. SCO Paketleri.....                             | 38 |
| 3.1.11.20. ACL Paketleri.....                             | 39 |
| 3.1.11.21. Lojik Kanallar.....                            | 40 |
| 3.1.11.22. Bluetooth Link Denetleyici Durumları.....      | 41 |
| 3.1.12. Şifreleme.....                                    | 41 |
| 3.1.12.1. Şifreleme Modları.....                          | 42 |
| 3.1.12.2. Şifreleme Anahtar Boyu.....                     | 42 |
| 3.1.12.3. Şifreleme Mekanizmasını Başlatma.....           | 43 |

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| 3.1.12.4. Şifreleme Mekanizmasını Sonlandırma.....                             | 44 |
| 3.1.13. Bluetooth Fonksiyonlarının Bluetooth Güvenliğinde Kullanılması.....    | 44 |
| 3.1.14. Bilgi Güvenliği ve Kriptoloji.....                                     | 45 |
| 3.1.14.1. Kriptolojinin Hedefleri.....                                         | 46 |
| 3.1.14.2. Şifreleme.....                                                       | 46 |
| 3.1.14.3. Şifrelemenin Temel Elemanları.....                                   | 46 |
| 3.1.14.4. Gizli Anahtar (Simetrik) Yöntemleri.....                             | 48 |
| 3.1.14.5. Safer Algoritması.....                                               | 50 |
| 3.1.14.6. Açık (Asimetrik) Anahtar Şifreleme.....                              | 50 |
| 3.1.15. Ağ Sistemlerine Yapılabilecek Güvenlik Saldırıları.....                | 52 |
| 3.1.15.1. Pasif Saldırılar.....                                                | 52 |
| 3.1.15.2. Aktif Saldırılar.....                                                | 53 |
| 3.1.16. J2ME (Java 2 Micro Edition).....                                       | 53 |
| 3.1.16.1. J2ME’ de Tanımlanmış Profiller.....                                  | 56 |
| 3.1.16.2. Borland Jbuilder 9/X.....                                            | 59 |
| 3.2. METOD.....                                                                | 60 |
| 3.2.1. DES algoritması .....                                                   | 60 |
| 3.2.2. Rijndael (AES) Algoritması.....                                         | 62 |
| 3.2.3. Uygulama Geliştirmede Emülatörlerin Kullanımı.....                      | 63 |
| 3.2.4. Geliştirilen Uygulamanın Gezgin Telefona Aktarılması.....               | 64 |
| 4. BULGULAR VE TARTIŞMA.....                                                   | 66 |
| 4.1. İki Gezgin Telefon Arasında Bluetooth Üzerinden Güvenli Veri İletimi...   | 66 |
| 4.2. İki Bilgisayar (PC) Arasında Bluetooth Üzerinden Güvenli Veri İletimi.... | 73 |
| 5. SONUÇ ve ÖNERİLER.....                                                      | 83 |
| KAYNAKLAR.....                                                                 | 85 |
| ÖZGEÇMİŞ.....                                                                  | 88 |

**KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ  
ELEKTRİK – ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI**

**YÜKSEK LİSANS TEZİ**

**ÖZET**

**BLUETOOTH ÜZERİNDEN GÜVENLİ VERİ İLETİMİ**

**Mehmet Ali ÖZÇELİK**

**DANIŞMAN : Prof.Dr. M. Kemal KIYMIK**

**Yıl : 2006 Sayfa : 88**

**Jüri :Prof.Dr. M. Kemal KIYMIK  
:Yrd.Doç.Dr. Abdulhamit SUBAŞI  
:Yrd.Doç.Dr. M. Metin KÖSE**

Bluetooth, kısa mesafede kablosuz iletişim ortamı sunan ve 2,4 Ghz endüstriyel-bilimsel-tıbbi (ISM) radyo frekans bandını kullanan bir teknolojidir. Bluetooth teknolojisi düşük güç tüketimli, ucuz ve tüm cihazlara entegre edilmeye imkan veren bir teknikle kablosuz veri ve ses iletişimi sağlamaktadır.

Bluetooth iletişim ortamının kablosuz olması ve ortamın tüm kullanıcılara açık olması sistemde güvenlik açıkları meydana getirmektedir. Bu nedenden ötürü kablosuz ağ ortamı olan bluetooth'a özgü güvenlik protokol ve yöntemleri geliştirilmektedir.

Bu çalışmada bluetooth teknolojisi sisteminin yapısı açıklanmış, kullandığı güvenlik yöntemlerini incelenmesi, sistemin güvenlik açıkları tesbit edilmeye çalışılmıştır. Sistemi daha güvenli hale getirmek için güvenlik mekanizmalarının nasıl geliştirilmesi gereği üzerinde durulmuş ve yeni yöntem uygulanmıştır.

**Anahtar Kelimeler:** Bluetooth, Bluetooth Güvenliği, Kriptografi, Şifreleme, GizliAnahtar.

**UNIVERSITY OF KAHRAMANMARAŞ SÜTÇÜ İMAM  
INSTITUTE OF NATURAL AND APPLIED SCIENCES  
DEPARTMENT OF ELECTRIC – ELECTRONIC ENGINEERING**

**MSc THESIS**

**ABSTRACT**

**SECURE DATA TRANSMISSION OVER BLUETOOTH**

**Mehmet Ali ÖZÇELİK**

**SUPERVISOR :Prof.Dr. M. Kemal KIYMIK**

**Year : 2006      Pages : 88**

**Jury : Prof.Dr. M. Kemal KIYMIK  
: Assist.Prof.Dr. Abdulhamit SUBAŞI  
: Assist.Prof.Dr. M. Kemal KÖSE**

**Bluetooth is a technology that provides wireless communication in short distance and uses 2.4 GHz Industrial-Scientific-Medical (ISM) radio-frequency band. Bluetooth technology supplies wireless data and voice communication with the technique enabling to integrated to all equipments and having low power consumption and beingcheap.**

**That the enviorenment of bluetooth communication is wireless and open for all users causes lack in security. Because of these reasons, security protocols and methods that are peculiar to wireless network bluetooth area have been developed.**

**In this thesis, the structure of bluetooth technology system was explained, the security methods that bluetooth technology uses were investigated and security lacks of the system were tried to be found out. To make the system more secure, We concentrated how the security mechanisms can be improved and new methods were applied.**

**Keywords : Bluetooth, Bluetooth Security, Cryptography, Encryption ,Symmetric Key**

**ÖNSÖZ**

Kablosuz veri iletim teknolojilerinden olan bluetooth kısa mesafede bilgisayar, klavye, PDA, gezgin telefon, yazıcı v.s sayısal giriş/çıkış birimlerinin ara bağlantı olmadan ana sisteme bağlanmasını sağlayan bir teknolojidir.

Bluetooth haberleşme ortamının kablosuz ve radyo dalgaları üzerinden yapılması sistemde güvenlik problemleri meydana getirmektedir. Bu çalışmada bluetooth güvenlik yapısı eksikleri ve giderilmesi üzerinde durulmuştur.

Çalışmalarım sırasında bilgi ve tecrübeleriyle yardımlarını esirgemeyen danışman hocam Prof.Dr. M.Kemal KIYMIK'a ve Sayın Yrd.Doç.Dr. Abdülhamit SUBAŞI'na, teşekkürlerimi sunarım.

Bu alanda yaptığım çalışmada desteklerini esirgemeyen Sayın Mustafa KARABULUT'a ve Serdar AKAR'a teşekkürlerimi iletirim.

**Ocak-2006**  
**KAHRAMANMARAŞ**

**MEHMET ALİ ÖZÇELİK**

## ÇİZELGELER DİZİNİ

## SAYFA

|             |                                                       |    |
|-------------|-------------------------------------------------------|----|
| Çizelge 3.1 | Güç sınıfları .....                                   | 13 |
| Çizelge 3.2 | Bluetooth protokolleri ve bulundukları katmanlar..... | 20 |
| Çizelge 3.3 | RF kanalları ve frekans bandı.....                    | 27 |
| Çizelge 3.4 | Erişim kodU tipleri ve LAP.....                       | 32 |
| Çizelge 3.5 | Bluetooth paket tipleri.....                          | 36 |
| Çizelge 3.6 | Link kontrol paketleri.....                           | 37 |
| Çizelge 3.7 | SCO paket tipleri .....                               | 39 |
| Çizelge 3.8 | ACL paket çeşitleri.....                              | 40 |
| Çizelge 3.9 | Şifreleme işlemi için PDU türleri.....                | 41 |

## ŞEKİLLER DİZİNİ

## SAYFA

|             |                                                                      |    |
|-------------|----------------------------------------------------------------------|----|
| Şekil 3.1.  | Bluetooth sistemi yapısı.....                                        | 8  |
| Şekil 3.2.  | Bluetooth kullanım alanları.....                                     | 9  |
| Şekil 3.3.  | Tipik Bluetooth modülleri.....                                       | 11 |
| Şekil 3.4.  | Bluetooth frekans atlama örneği.....                                 | 12 |
| Şekil 3.5.  | Bir piconet'in ve scatternet'in şematik gösterimi.....               | 14 |
| Şekil 3.6.  | Scatternet durumu.....                                               | 15 |
| Şekil 3.7.  | Bir bluetooth master biriminin slave olarak rol alması.....          | 15 |
| Şekil 3.8.  | OSI – Bluetooth karşılaştırması.....                                 | 18 |
| Şekil 3.9.  | Bluetooth protokol yığını.....                                       | 20 |
| Şekil 3.10. | SDP çalışma biçimi.....                                              | 24 |
| Şekil 3.11. | Link katmanı.....                                                    | 27 |
| Şekil 3.12. | TDD ve zamanlama.....                                                | 28 |
| Şekil 3.13. | Çok dilimli paketler.....                                            | 28 |
| Şekil 3.14. | Genel paket formatı.....                                             | 31 |
| Şekil 3.15. | Erişim kodu formatı.....                                             | 31 |
| Şekil 3.16. | Başlangıç alanı.....                                                 | 32 |
| Şekil 3.17. | Kuyruk.....                                                          | 33 |
| Şekil 3.18. | Paket başlık formatı.....                                            | 33 |
| Şekil 3.19. | Kullanıcı verisi başlık formatı.....                                 | 35 |
| Şekil 3.20. | FHS kullanıcı verisi formatı.....                                    | 37 |
| Şekil 3.21. | DV Paket formatı.....                                                | 38 |
| Şekil 3.22. | Şifreleme modu için anlaşmaya varma.....                             | 42 |
| Şekil 3.23. | Şifreleme anahtar boyutunun belirlenmesi.....                        | 43 |
| Şekil 3.24. | Şifreleme mekanizmasını başlatma.....                                | 43 |
| Şekil 3.25. | Şifreleme anahtar mekanizmasının sonlandırılması.....                | 44 |
| Şekil 3.26. | Kriptolojik şifreleme işlemi.....                                    | 47 |
| Şekil 3.27. | Bir mesajın dinlenmesini önlemek için anahtar ile şifreleme...       | 47 |
| Şekil 3.28. | Tek anahtar şifreleme.....                                           | 48 |
| Şekil 3.29. | İki farklı anahtar ile şifreleme ve şifre çözme.....                 | 48 |
| Şekil 3.30. | Gizli (Simetrik) anahtarlı şifreleme.....                            | 49 |
| Şekil 3.31. | Açık (Asimetrik) anahtar şifreleme.....                              | 51 |
| Şekil 3.32. | Güvenlik saldırılarının sınıflandırılması.....                       | 52 |
| Şekil 3.33. | MIDlet yaşam döngüsü.....                                            | 57 |
| Şekil 3.34. | MIDP kullanıcı ara birimi nesneleri.....                             | 58 |
| Şekil 3.35. | J Builder uygulama geliştirme ortamı ve emülatörler.....             | 59 |
| Şekil 3.36. | J Builder (mobile set 3.0)'in kullanıcı arabirimi oluşturma araçları | 59 |
| Şekil 3.37. | ECB modu.....                                                        | 60 |
| Şekil 3.38. | CFB modu.....                                                        | 61 |
| Şekil 3.39. | OFB modu.....                                                        | 61 |
| Şekil 3.40. | Uygulama geliştirmede emülatörlerin kullanım döngüsü.....            | 64 |
| Şekil 3.41. | Geliştirilen uygulamanın gezgin telefona aktarılması.....            | 64 |
| Şekil 4.1.  | J Builder uygulama geliştirme ortamı ve emülatörler.....             | 66 |
| Şekil 4.2.  | J Builder'in kullanıcı ara birimi oluşturma araçları.....            | 67 |
| Şekil 4.3.  | Emülatör görüntüleri.....                                            | 68 |

|             |                                                                                               |    |
|-------------|-----------------------------------------------------------------------------------------------|----|
| Şekil 4.4.  | Mesaj gönderici ve mesaj alıcı konumları seçimi.....                                          | 68 |
| Şekil 4.5.  | Cihaz keşif.....                                                                              | 68 |
| Şekil 4.6.  | Mesaj gönderici emülatörün cihaz keşif araması.....                                           | 69 |
| Şekil 4.7.  | Bluetooth cihaz sorgulamasında bulunan cihaz.....                                             | 70 |
| Şekil 4.8.  | Gönderilecek verinin ve veri anahtarı şifresinin girilmesi.....                               | 70 |
| Şekil 4.9.  | Mesaj gönderici emülatörün veriyi gönderme istemi.....                                        | 71 |
| Şekil 4.10. | Mesaj gönderici emülatörün veriyi şifreleyerek, mesaj alıcı emülatöre göndermesi.....         | 71 |
| Şekil 4.11. | Alınan şifreli verinin çözülme işlemi.....                                                    | 72 |
| Şekil 4.12. | Mesaj gönderici emülatör tarafından gönderilen verinin, mesaj alıcı emülatörde çözülmesi..... | 72 |
| Şekil 4.13. | Bluesoleil display görüntüsü.....                                                             | 74 |
| Şekil 4.14. | Cihaz keşif tarama sonucu.....                                                                | 74 |
| Şekil 4.15. | İki PC arasında bağlantının sağlanması için giriş anahtar değerlerinin girilmesi.....         | 75 |
| Şekil 4.16. | Bayık PC'sinde girilen anahtar değerinin diğer PC'de girilmesi.....                           | 76 |
| Şekil 4.17. | Aynı anahtar değerlerinin girilmesi sonucu bağlantının yapılması..                            | 76 |
| Şekil 4.18. | Bayık PC'sinin dosya transferini kabul etmesi.....                                            | 77 |
| Şekil 4.19. | Veri paylaşımı sağlayacak "Remote Shared Folder" in açılması.....                             | 77 |
| Şekil 4.20. | Şifrelenecek metnin girilmesi.....                                                            | 78 |
| Şekil 4.21. | Şifreleme (encrypt) anahtarının belirlenmesi.....                                             | 78 |
| Şekil 4.22. | Şifreleme (encrypt) anahtarının girilmesi.....                                                | 78 |
| Şekil 4.23. | Girilen metnin şifrlenmesi işlemi.....                                                        | 79 |
| Şekil 4.24. | Şifrelenen metnin word halindeyken Bayık PC'sine aktarılması.....                             | 79 |
| Şekil 4.25. | Şifreli metnin alındığı share klasörü.....                                                    | 79 |
| Şekil 4.26. | Alınan şifreli metnin görüntüsü.....                                                          | 80 |
| Şekil 4.27. | Alınan şifreli metnin şifreleme/deşifreleme arayüzüne aktarılması..                           | 80 |
| Şekil 4.28. | Şifreli metnin çözülmesi (decrypt) için anahtar değerinin istenmesi                           | 81 |
| Şekil 4.29. | Şifre çözme (decrypt) işlemi için anahtar değerinin girilmesi.....                            | 81 |
| Şekil 4.30. | Alınan şifreli metnin tekrar orijinal haline gelmesi (decrypt).....                           | 82 |

## SİMGELER VE KISALTMALAR DİZİNİ

|                |                                                      |
|----------------|------------------------------------------------------|
| <b>3G</b>      | <b>: 3rd Generation</b>                              |
| <b>ACL</b>     | <b>: Asynchronous Connectionless</b>                 |
| <b>ACO</b>     | <b>: Asynchronous Connection-Oriented</b>            |
| <b>ADPCM</b>   | <b>: Adaptive Different Pulse Code Modulation</b>    |
| <b>AES</b>     | <b>: Advanced Encryption Standard</b>                |
| <b>AM_ADDR</b> | <b>: Aktif Üye Adresi</b>                            |
| <b>ANSI</b>    | <b>: American National Standard Institute</b>        |
| <b>AR_ADDR</b> | <b>: Erişim İstek Adresi</b>                         |
| <b>ARQN</b>    | <b>: Doğrulama Alanı</b>                             |
| <b>AWT</b>     | <b>: Abstract Windows Toolkit,</b>                   |
| <b>BD_ADDR</b> | <b>: Bluetooth Device Address</b>                    |
| <b>BT</b>      | <b>: Bandwidth Time</b>                              |
| <b>CAC</b>     | <b>: Channel Access Code</b>                         |
| <b>CBC</b>     | <b>: Cipher Block Chaining</b>                       |
| <b>CDC</b>     | <b>: Connected Device Configuration</b>              |
| <b>CFB</b>     | <b>: Cipher Feedback</b>                             |
| <b>CLDC</b>    | <b>: Connected, Limited Device Configuration</b>     |
| <b>COF</b>     | <b>: Ciphering Offset</b>                            |
| <b>CP</b>      | <b>: Control Point</b>                               |
| <b>CRC</b>     | <b>: Cyclic Redundancy Check</b>                     |
| <b>CRC</b>     | <b>: Cyclic Redundancy Check</b>                     |
| <b>DAC</b>     | <b>: Device Access Code</b>                          |
| <b>DECT</b>    | <b>: Digital European Cordless Telecommunication</b> |
| <b>DES</b>     | <b>: Data Encryption Standard</b>                    |
| <b>DH</b>      | <b>: Data High rate</b>                              |
| <b>DM</b>      | <b>: Data Medium rate</b>                            |
| <b>DSA</b>     | <b>: Digital Signature Algorithm</b>                 |
| <b>DSSS</b>    | <b>: Direct Sequence Spread Spectrum</b>             |
| <b>ECB</b>     | <b>: Electronic Codebook</b>                         |
| <b>ETSI</b>    | <b>: Avrupa Telekomünikasyon Standart Enstitüsü</b>  |
| <b>FEC</b>     | <b>: İleri Hata Düzeltme</b>                         |
| <b>FHSS</b>    | <b>: Frequency Hopping Spectrum</b>                  |
| <b>FIR</b>     | <b>: Fast Infrared Standard</b>                      |
| <b>GAP</b>     | <b>: Generic Access Protocol</b>                     |
| <b>GFSK</b>    | <b>: Gaussian Frequency Shift Keying</b>             |
| <b>GIAC</b>    | <b>: General Inquiry Access Code</b>                 |
| <b>GSM</b>     | <b>: Global System for Mobile Communication</b>      |
| <b>HCI</b>     | <b>: Host Controller Interface</b>                   |
| <b>HEC</b>     | <b>: Header Error Check</b>                          |
| <b>IAC</b>     | <b>: Inquiry Access Code</b>                         |
| <b>IBM</b>     | <b>: International Business Machines</b>             |
| <b>IDEA</b>    | <b>: International Data Encryption Algorithm</b>     |
| <b>IEEE</b>    | <b>: Institute of Electric Electronic Engineers</b>  |
| <b>IRDA</b>    | <b>: Infrared Data Association</b>                   |
| <b>IrOBEX</b>  | <b>: Infrared Object Exchange Protocol</b>           |
| <b>ISM</b>     | <b>: Industrial Scientific Medical</b>               |

|                |                                                            |
|----------------|------------------------------------------------------------|
| <b>J2ME</b>    | : <b>Java Second Micro Edition</b>                         |
| <b>J2SE</b>    | : <b>Java 2 Standart Edition</b>                           |
| <b>L2CAP</b>   | : <b>Logical Link and Adaptation</b>                       |
| <b>LAN</b>     | : <b>Local Area Network</b>                                |
| <b>LANAP</b>   | : <b>Lan Access Profile</b>                                |
| <b>LC</b>      | : <b>Link Controller</b>                                   |
| <b>LM</b>      | : <b>Link Manager</b>                                      |
| <b>LSB</b>     | : <b>Least Significant Bit</b>                             |
| <b>LT_ADDR</b> | : <b>Logical Transport Address</b>                         |
| <b>MAC</b>     | : <b>Message Authentication Code</b>                       |
| <b>MIC</b>     | : <b>Message Integrity Code</b>                            |
| <b>MIDP</b>    | : <b>Mobile Information Device Profile</b>                 |
| <b>MSB</b>     | : <b>Most Significant Code</b>                             |
| <b>NAP</b>     | : <b>Non Significant Adress Part</b>                       |
| <b>NIST</b>    | : <b>National Institute of Standarts and Technology</b>    |
| <b>OFB</b>     | : <b>Output Feedback</b>                                   |
| <b>OSI</b>     | : <b>Open Systems Interconnecti</b>                        |
| <b>PAN</b>     | : <b>Personal Area Networks</b>                            |
| <b>PC</b>      | : <b>Personel Computer</b>                                 |
| <b>PDA</b>     | : <b>Personal Digital Assistant</b>                        |
| <b>PDU</b>     | : <b>Protocol Data Unit</b>                                |
| <b>PGP</b>     | : <b>Pretty Good Privacy</b>                               |
| <b>PGP</b>     | : <b>Pretty Good Privacy</b>                               |
| <b>PIN</b>     | : <b>Personel Identification Number</b>                    |
| <b>PM_ADDR</b> | : <b>Park Adresi</b>                                       |
| <b>PPP</b>     | : <b>Point-to-Point Protocol</b>                           |
| <b>RC</b>      | : <b>Rivest's Cipher</b>                                   |
| <b>RF</b>      | : <b>Radio Frequency</b>                                   |
| <b>RMI</b>     | : <b>Remote Method Invocation</b>                          |
| <b>RNG</b>     | : <b>Random Number Generator</b>                           |
| <b>RSA</b>     | : <b>Rivest-Shamir-Adleman)</b>                            |
| <b>SCO</b>     | : <b>Synchronous Connection Oriented</b>                   |
| <b>SDP</b>     | : <b>Service Discovery Protocoli</b>                       |
| <b>SEQN</b>    | : <b>Sıralama Alanı</b>                                    |
| <b>SIG</b>     | : <b>Special Interest Group</b>                            |
| <b>SNR</b>     | : <b>Signal to Noise Radio</b>                             |
| <b>SPP</b>     | : <b>Serial Port Profile</b>                               |
| <b>SRES</b>    | : <b>Signed Response</b>                                   |
| <b>SWAP</b>    | : <b>Shared Wireless Access Protocol</b>                   |
| <b>TCP/IP</b>  | : <b>Transmission Control Protocol / Internet Protocol</b> |
| <b>TDMA</b>    | : <b>Time Division Multiple access</b>                     |
| <b>UA/UI</b>   | : <b>User Asynchronous or User Isochronous data</b>        |
| <b>UAP</b>     | : <b>Upper Address Part</b>                                |
| <b>UDP</b>     | : <b>User Datagram Protocol</b>                            |
| <b>US</b>      | : <b>User Synchronous data</b>                             |
| <b>WAP</b>     | : <b>Wireless Aplicarion Protocol</b>                      |
| <b>WLAN</b>    | : <b>Wireless Local Area Network</b>                       |
| <b>XOR</b>     | : <b>Mod 2 Adding</b>                                      |

## 1.GİRİŞ

Bilgisayar ve diğer elektronik cihazların ağ uygulamalarında önemli anahtar sözcüklerden birisi veriyi taşıyan elektriksel işaretlerin taşındığı iletim ortamıdır. Bu ortam kablo üzerinden sağlanabildiği gibi kablosuz olarak da gerçekleşebilir; veya her ikisi bütünleşik olarak bir ağ içerisinde bulunabilir. Kabloya dayalı uygulamalarda uç sistemler arasında birebir kablo bağlantısı vardır; bu kablo yerine UTP/STP yerine göre fiber optik olabilmektedir. Kablosuz ağ bağlantısı iletişimde bulunacak sistemler arasında herhangi bir fiziksel kablo bağlantısı olmadan veri alışverişinde bulunulmasını sağlar. Uygulamada çok değişik amaçlı kablosuz ağ erişimlerine ihtiyaç duyulmaktadır. Örneğin hiçbir kablo bağlantısı yapılmadan bir LAN kurulabilir; veya bir bilgisayar sistemiyle fare, yazıcı, çizici gibi çevre birimler ana sistem kablosuz şekilde birbirine bağlanabilir; araya kablo çekilmesinin zor, pahalı veya izin verilmediği durumlarda iki bina arasında noktadan noktaya kablosuz hat bağlantısı yapılabilir; ya da cep telefonlarında olduğu gibi yer değiştiren sistemlerin iki yönlü haberleşmesi sağlanabilir.

Kablosuz ağ teknolojileri diğer tabirle telsiz ağ teknolojileri denildiğinde alış-veriş band genişlikleri aynı olmasa da iki yönlü iletişim akla gelir. Çünkü uç sistemler arasında veri aktarımına ek olarak kontrol işaretleri ve onaylama bilgileri gibi iki yönlü aktarım gereksinimi vardır. Günümüzde kablosuz ağ denildiğinde ilk akla gelen sözcükler WLAN, HiperLAN, Bluetooth, GSM, WAP, LMDS, İrda gibi sözcükler gelmektedir; bunlara ek olarak WAP, DECT, 3G, Edge gibi kavramlarda vardır ( Çölkesen ve ark., 2002).

Geliştirilen bu iletişim teknikleri ile birlikte bir sıra farklı iletişim teknolojileride geliştirilmiş durumdadır. Bunların da kendilerine göre avantaj ve dezavantajları vardır. Kullanım alanına ve amacına göre bu teknolojiler birbirinden farklılık arz etmektedir. Günümüzde kullanılan, geliştirilen ve kullanılacak olan bu teknolojiler hakkında genel bir bilgi verilecek olursak kıyaslama yapmak daha da kolaylaşacaktır.

### 1.1. WiFi / IEEE 802.11

**Kullanım Alanları:** Sabit ağ-telefon, mobil İnternet erişimi.

**Avantajları:** Yüksek veri aktarım hızı, dünya çapında yaygınlık, ağ yapıları mümkün.

**Dezavantajları:**Yüksek arıza riski, ses aktarımı yok.

Bu karmaşık tanımlamanın ardında kablosuz yerel ağ yapıları (Wireless Local Area Networks-WLAN) için geliştirilen uluslararası bir standart var. Standart 1990 yılından bu yana, bir Amerikan norm birliği olan Institute of Electrical and Electronically Engineers (IEEE) tarafından geliştiriliyor. IEEE 802.11 standardı, 1997 yılında tamamlanmış. Sistemde lisanssız ISM bandından 2,4 GHz bandı kullanılıyor. Bluetooth sisteminde de aynı bant genişliği kullanılıyor. Ancak mikrodalga fırınlar gibi araçlarda da aynı bant genişliği kullanıldığından, çeşitli arızalarla karşılaşmak mümkün. 1999 yılında, 802.11a ve 802.11b geliştirildi. Bu iki standardın amacıysa, bant genişliklerini yükseltmekti. Ancak her ikisi de farklı amaca hizmet ettiler. 802.11a, daha yüksek bant genişliklerinin elde

edildiği 5 GHz bandına sahip. Buna karşılık 802.11b ise, 802.11 standardına uyumlu bir gelişim sunuyor. 802.11b ile gerçekleştirilen transferler 11 MBit/sn'lik bir hıza ulaşıyor.

IEEE 802.11 standardını iki işletim sisteminde kullanmak mümkün. Ad-hoc modunda cihazlar peer to peer tipi bir ağda birbirleri ile doğrudan iletişime geçebiliyorlar. Bu sayede problemsiz bir şekilde küçük alanlar içinde, düşük katılımlı yerel ağlar kurulabilir. Ne var ki aktarım çoğu zaman şifrelenmeden gerçekleşiyor.

Kızılötesi modunda iletişim, tüm idare işlerinin yönetildiği bir erişim noktası üzerinden gerçekleşiyor. Network kartları doğrudan birbirleri ile değil Access Point (erişim noktası) ile bağlantı kuruyorlar. Access Point bilgi paketlerini başka bir network kartına ya da başka bir Access Point'e yönlendiriyor.

802.11 sistemi, diğer sistemlerden daha çok sevildi. Yüksek aktarım hızı nedeniyle bu standart daha iyi bir parazit önleme oranına (Signal to Noise Ratio / SNR) ihtiyaç duyar. Sonuç olarak sistemin etkilenme hassasiyeti artar ve diğer sistemlere oranla menzili düşer. IEEE 802.11 sisteminin kapalı alanlarda menzili 30, açık alanlarda ise 300 metredir. Etkilenme hassasiyetini düşürmek için 802.11 standardında iki mekanizma bulunuyor. Bunlardan ilki FHSS (Frequency Hopping Spread Spectrum)'da asıl sinyal bir taşıyıcı sinyal üzerine modüle edilir. Taşıyıcı sinyal belli bir sıraya göre sürekli olarak frekansı değiştirir, ikincisi ise DSSS (Direct Sequence Spread Spectrum). Bu mekanizmada bütün bant genişliği kullanılır ve kullanılan bant genişliğini zaman aralıklarına göre parçalara böler. DSSS diğer çözüme göre daha yaygın kullanılıyor.

Yüksek band genişliği gerektiren LAN uygulamaları, daha geniş kapsama alanı gerektiren uygulamalar, güvenilirlik gerektiren uygulamalar, dosya eklemeli e-mail alma-gönderme, web tarama ve dosya paylaşımı gibi uygulamalarda Wi-Fi (802.11b) kullanımı daha uygundur.

Bu teknoloji bir bina içerisindeki LAN yapısını kablosuz bir şekilde yeniden dizayn etmeyi öngörür. İletim kapasitesi ve eş zamanlı kullanıcıların sayısı yüksektir.

## 1.2.İrda Teknolojisi

**Kullanım Alanlar:** Cep telefonları, PDA'lar, dizüstü bilgisayarlar ve uzaktan kumandalar.

**Avantajı:** Yaygınlık.

**Dezavantajları:** Düşük menzil, yüksek arıza riski, konuşma desteğinin olmaması.

Bu kısaltmanın açılımı "Infrared Data Association" anlamına geliyor. 1993 yılında, aralarında Hewlett Packard ve IBM'in de bulunduğu yaklaşık 30 firma, kızılötesi ışınlarla veri aktarımını standartlaştırmak için bir araya geldi. İlk standart kızılötesi ara birimi (SIR), 115,2 Kbps'lik aktarım hızına sahipti. Daha sonra FAsT Infrared Standard (FIR) geliştirildi. FIR ile 4 Mbit/sn'lik aktarım hızına ulaşıldı.Yeni duyurulan "Very Fast Infraredstandardı " (VFIR) ile 16 Mbit/sn'lik hızlarla veri aktarımı mümkün hale gelmiştir.

IrDA sisteminde verici olarak, dalga boyu 850-900 nm olan ve ışını 30 derecelik açıyla yayan bir diyot kullanılıyor. Alıcının menzili, teorik olarak bir metre. Ancak kızılötesi ışınlar, normal ışık ve yansıtıcı cisimler gibi etkenlerden kolayca etkilenirler. Bu nedenle pratikte durum farklı: Parlak güneş ışığı altında menzilleri çok kısa, evlerde kullanılan yapay ışık altında ise menzilleri daha uzundur.

Bağlantı herhangi bir cihaz üzerinden kurulabilir. Aktif halde olduklarını belirtmek için IrDA arabirimleri, her iki saniyede bir, bir ışık demeti yayınlarlar. Eğer civarda başka bir IrDA cihazı bulunuyorsa, bu sinyalleri, algılar ve böylece bağlantı kurulur, ilk aşamada cihazlar birbirlerine kendi özelliklerini bildiren verileri gönderirler.

Daha sonra Tiny Transport protokolü üzerinden asıl veri alışverişi gerçekleşir. Bu protokolün üzerine farklı üç protokol daha kurulur: Yerel ağ girişi için IrLAN, veri alışverişi için Infrared Object Exchange Protocol (IrOBEX "Very Fast Infrared" standardı (VFIR)), seri ve paralel arabirimlerin oluşturulması için Ir-COMM. Sonuncu protokole mobil internet erişimi için ihtiyaç duyulur. IrDA özellikle cep telefonu ve PDA pazarında yaşanan patlamadan sonra popüler oldu. IrDA hem mobil internet erişimi için hem de masaüstü bilgisayarı ile dizüstü bilgisayarı arasında veri alışverişi için kullanılıyor. IrDA'nın kablolu-kablosuz güçlü rakipleri var. USB arabirimleri şu sıralar çok yaygın. Üstelik IrDA'ya oranla daha çok destekleniyor. Bunun yanı sıra, kablosuz bağlantı teknolojisi Bluetooth, daha yaygın ve endüstriyel anlamda daha çok tercih ediliyor.

### 1.3.DECT Teknolojisi

**Kullanım alanları:** Sabit ağ telefonları, mobil internet erişimi.

**Avantajları:**Yaygınlık, 120 iletişim kanalı, düşük arıza riski

**Dezavantajı:** Frekans birliği yok

1992 yılında Avrupa Telekomünikasyon Standart Enstitüsü (ETSI), Digital European Cordless Telecommunication (DECT) için ETS 300 175 standardını hazırladı. Günümüzde bu standart 100'den fazla ülkede kullanılıyor. 1994 yılında hazırlanan Generic Access Protocol'ü (GAP) ile bütün DECT cihazları birbirleriyle kombine edilebiliyor. DECT sistemini diğer mobil iletişim sistemlerinden ayıran özellik, merkezi bağlantılarının bir merkezde toplanmasıdır. Kaynakların yönetimi cihazlar üzerinden kontrol ediliyor. DECT sistemi, temel istasyon ile mobil parça arasında, noktadan noktaya bağlantı mantığı üzerine kurulmuş. Buna göre iletişim, ancak bir temel istasyon ile mobil parça arasında kurulabilir, iki mobil parça arasında, doğrudan bağlantı kurmak mümkün olmuyor.

Avrupa içinde DECT, 1.880 ile 1.900 MHz frekans aralığında çalışıyor. Mevcut frekans aralığı bir multi-carrier yöntemi ile on kanala ayrılıyor. Bir frekans yelpazesi içinde çeşitli taşıyıcı frekanslar aynı anda gönderiliyor. Bir frekansın devre dışı kalması durumunda, yeteri kadar yedek frekans hazır bulunuyor. Bu kanallar TDMA (Time Division Multiple Access) ile, her biri 417 ns süren 24 zaman aralığına bölünüyor. Bu sayede birçok cihaz, aynı anda aynı frekansta yayın yapabiliyor. Cevap sinyali de aynı şekilde Time Division Duplex tarafından organize ediliyor: Temel istasyon ile mobil parça sırası ile verilerini gönderiyor. Adaptive Different Pulse Code Modulation (ADPCM) kodlama yöntemi sayesinde, yüksek iletişim kalitesi elde ediliyor. ADPCM yönteminde, konuşma sesi ve müzik yüzde 50 oranında sıkıştırılıyor.

Veri aktarımı için, her bir zaman aralığı başına 32 KBit/sn'lik aktarım hızı kullanılıyor. Ses aktarımından farklı olarak veri aktarımı sırasında, güvenli iletişim için bir kontrol uygulanıyor. Bu kontrol nedeniyle veri aktarım hızı 24 KBit/sn'ye düşüyor. Ancak veri aktarımı için 23 farklı kanalı birbirlerine bağlamak mümkün. Bu şekilde iletişim hızı 552 KBit/sn'ye kadar çıkıyor, internet gezintilerinde ihtiyaç duyulan asimetrik aktarım olanağı, bu teknolojiye de kullanılabilir. Kapalı mekanlarda DECT sisteminin menzili 40 metre. Açık alanlarda ise 350 metre.

DECT sisteminin sağladığı en önemli avantaj, frekans bantlarının rezerve edilmesi ve müdahale yöntemlerinin belirlenmesidir. Bu sayede Bluetooth gibi sistemlerde meydana gelen arızaların önüne geçiliyor, ayrıca kullanım da belirgin ölçülerde kolaylaşıyor. Bir ağdan diğerine aktarım da sorunsuz gerçekleşiyor. "Handover" adı verilen aşama, kullanıcıya fark ettirilmeden otomatik olarak gerçekleşiyor.

DECT bir ağın kendisini değil, ağa girişi tarif eder. Bu nedenle sistemi ISDN, LAN ya da GSM gibi pek çok ağ için kullanmak mümkün.

Sistemin en önemli dezavantajı, DECT standardı için dünya çapında çok farklı frekans alanlarının kullanılmasıdır. Örnek olarak Avrupa'da üretilen DECT cihazları, Amerika'da üretilenlerle uyumlu değildir. Üstelik çözümlerin birçoğu ISDN'e göre hazırlanmış durumda. Bir başka olumsuzluk ise, cihazın fiyatının oldukça yüksek olması.

Bütün bunlara rağmen DECT sisteminin geleceği parlak gözüküyor. DECT teknolojisi şu anda, Avrupa'daki kablosuz telefonlar için en geçerli standart durumunda. Aynı şekilde "Wireless Local Loop" adı verilen kablosuz çözümler de DECT pazar payının yüzde 30'unu elinde tutuyor. Bir başka kullanım alanı da web-pad gibi kablosuz veri aktarım durumları. Ancak, burada kullanılan ürünlerin düşük performansları ve yüksek fiyatları, sistemin yaygınlaşmasını engelliyor. DECT cihazlarının UMTS' de de kullanılması mümkün.

#### 1.4.Home RF Teknolojisi

**Kullanım alanları:** Küçük ağlar, mobil internet erişimi.

**Avantajları:** Yüksek veri aktarım hızı, servis kalitesi, bant genişliği rezervasyonu

**Dezavantajı:** Uyumlu cihaz az

1999 yılında "Home RF Working Group" kablosuz çözümler üretebilmek amacıyla DECT ve IEEE 802.11 standartlarını bir araya getirdi. Kablosuz İnternet Erişim Protokolü (Shared Wireless Access Protocol-SWAP) olarak adlandırılan çözüm, son kullanıcılara yönelik. Sistemin içinde yer alan DECT sistemi konuşma hizmetlerini, paket tabanlı veri iletimini ve Streaming Media gibi uygulamalarda ihtiyaç duyulan kesin aktarım hızı hizmetlerini garanti ediyor.

Home RF, ISM frekans sınırı içinde 2,4 GHz ile, maksimum 100 mW'lık performansla yayın yapıyor. Tıpkı IEEE 802.11 gibi Home RF de Frequency Hopping Spread Spectrum mekanizmasını kullanıyor. Home RF sistemi 10 Mbit/sn' lik veri aktarım hızına ulaşabiliyor, iletişimi hem peer to peer olarak hem de bir kontrol noktası (Control

Point "CP") üzerinden kurmak mümkün. Buradaki Control Point, IEEE 802.11 standardında kullanılan Access Point uygulamasına benziyor. Konuşma için kullanılan Control Point, aynı anda sekiz telefon görüşmesini yapabilecek kapasitede olmalı. Bir ağa 256 CP bağlanabilir. Güvenlik nedeniyle her ağ yapısının ayrı bir ağ-ID'si (Network ID) bulunuyor. Bu ID'nin gizli tutulmasıyla, ağ dışardan izinsiz girişler önlenir. Teorik olarak Home RF çok başarılı olmalıydı, ancak endüstrinin çıkarları farklı yönlerde olduğu için, sistem pratikte fazla tutulmadı, gelecekte yerini tamamen başka teknolojiye bırakacak gibi görünüyor.

Home RF özel veri network'lerinde kullanılabilir. Ayrıca sistemi koordine eden ve telefon şebekesine (ses ve veri) bir gateway sunan bir bağlantı noktasının altında da Home RF kullanılabilir. Sıçrama frekansı 8 Hz'dir.

### 1.5. Bluetooth Teknolojisi

**Kullanım alanları:** Bilgisayarlar, cep telefonları, donanımların kablosuz bağlantıları.

**Avantajı:** Geniş endüstriyel destek

**Dezavantajları :** Uyumlu cihaz az, düşük menzil, düşük aktarım hızı.

1994 yılında Ericsson, cep telefonları ve cep telefonu aksesuarları arasında kablosuz iletişim kurabilecek düşük güç tüketimli, düşük maliyetli bir radyo arabirimi üzerinde araştırma yapmaya karar verdi. Bu karar Bluetooth teknolojisinin kapılarını açan adımdı. Benzer şekilde bir cep telefonu ve bir taşınabilir bilgisayar arasında kablosuz iletişim kurmak için de her iki cihaza küçük bir radyo alıcısı yerleştirilebilirdi. Bir yıl sonra mühendislik çalışmaları başladı ve Bluetooth teknolojisinin gerçek potansiyeli daha net bir şekilde görülebilir oldu. Cihazlar arası iletişimde kabloları kaldırmak amacıyla start alan bir fikir zamanla yepyeni imkanları da gözler önüne serdi: Bluetooth uygulamaları; mevcut veri ağlarına uzanan evrensel bir köprü, çevre birimleri için bir arabirim ve küçük çaplı cihaz ağları oluşturmak için bir araç olarak da kullanılabilirdi. 1998 Şubat ayında Special Interest Group (SIG) kuruldu. SIG çatısı altında 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia ve Toshiba gibi öncü firmaların yanı sıra binlerce irili ufaklı üye firma da yer almaktadır. SIG'nin başlangıçtaki görevi, teknolojinin sadece tek bir şirket tarafından sahiplenilmesini önlemek amacıyla, kısa menzilli radyo iletişimi sahasında yaşanan teknik gelişmeleri izlemek ve açık, global bir standardın oluşmasını sağlamaktır. Yapılan çalışmaların neticesinde 1999 Temmuz ayında ilk Bluetooth spesifikasyonu çıkarıldı. SIG'nin önemli çalışmaları arasında bu spesifikasyonun geliştirilmesi yer alıyor. Kuruluşun önde gelen diğer görevleri ise birlikte çalışabilirlik gereksinimleri, frekans bandı harmonizasyonu ve teknolojinin kitlelere tanıtılmasıdır.

Belirtilen kablosuz teknolojilerde iletişim ortamı olarak havanın kullanılması beraberinde ciddi güvenlik problemleri getirmekte, ortamın tüm kullanıcılara açık olması, sisteme yetkisiz girişlerin daha kolay yapılabilmesine neden olmaktadır. Telsiz teknolojilere özel farklı güvenlik protokol ve yöntemleri geliştirilerek de bu riskler azaltılmaya çalışılmaktadır (Çomakçı, 2004).

Bir telsiz teknolojisi olan Bluetooth'un kullandığı güvenlik mekanizmalarını inceleyerek, sistemin güvenlik açıklarının bulunması ve bu açıkların kısmen giderilmesi ve

mevcut güvenlik protokollerinde ne gibi değişiklikler yapılması gerektiği yapmış olduğumuz bu çalışmanın amacını oluşturmaktadır.

Bu amaca ulaşabilmek için öncelikle Bluetooth teknolojisi sistem yapısı ve güvenliği incelenmiş, bu teknolojinin bağlantı konumları, ağ ve paket yapıları üzerinde durularak Bluetooth teknolojisinin daha iyi anlaşılması ve bir iletişim standardı olarak daha iyi değerlendirmemize yol açmıştır.

Çalışmanın ikinci aşamasında bluetooth güvenliğini sağlayabilmek için bilgi güvenliği, kriptoloji kavramları üzerinde yoğunlaşmış, günümüze kadar yapılmış güvenlik yöntemleri ve algoritmaları araştırılarak bilgi birikimi oluşturulmuştur.

Çalışmamızın üçüncü aşamasında ise bluetooth güvenlik açıkları belirlenmiş sistemdeki bu açıkların giderilmesi için yöntem çalışılması yapılmış önerdiğimiz yöntem yazılımsal olarak irdelenmiştir.

Çalışmamızın dördüncü aşamasında ise bluetooth ortamında iletilecek verinin iki bilgisayar ve iki gezgin telefon arasında güvenli bir şekilde yapılmasına olanak veren yazılımsal yöntemler deneysel ortamda bluetooth donanım yapısı üzerinden uygulaması gerçekleştirilmiştir.

Çalışmamızın son bölümünde ise yapılan tez çalışmasının Bluetooth güvenliğine katkıları değerlendirilmiş, önerilen yazılımsal yöntemler ışığında Bluetooth'un mevcut güvenlik yapısı irdelenerek bu yapı daha güçlendirilmiştir.

## 2. ÖNCEKİ ÇALIŞMALAR

İlhan (2002), "Bluetooth Şifrelemesi ve Kanal tasarımı" isimli yüksek lisan tezinde Bluetooth telsiz iletişimi, Bluetooth katman yapıları, Paket tipleri, Bluetooth için kanal ve modülasyon seçimi yapılarak katmanlardaki uygulamaların yazılımları oluşturulması, iki Bluetooth birim arasındaki trafik akışı, verici ve alıcı için kanal tasarımı simülasyonu matlab ortamında gerçekleştirilmiştir.

Formsan (2002), "Bluetooth ağ bileşenlerinin Symbian işletim sistemi için yeniden kullanılabilir olması" konulu çalışmanın ilk bölümünde Symbian işletim sistemi detaylı olarak anlatılmıştır. Symbian işletim sisteminin genel teknoloji özellikleri, kullanıcı arabirimleri iletişim alt sistemleri anlatılmıştır. Beşinci bölümde Bluetooth teknolojisi incelenmiş ve altıncı bölümde Bluetooth ağlar için yazılım bileşenleri anlatılmıştır (Aksu, 2005)

Piroumian (2002), "J2ME kablosuz platform programcılığı" isimli bu kitabın ilk bölümünde Javanın sürümleri (J2SE, J2EE, J2ME) anlatılıp Java 2 Micro Edition ortamı, konfigürasyonlar, profiller anlatılmıştır. İkinci bölümde uygulama geliştirme, derleme ve J2ME kablosuz uygulama geliştirme araçlarının kullanılması anlatılmıştır. Üçüncü bölümde MIDP uygulama programlarının yapısı, MIDlet program yapısı anlatılıp ilerleyen bölümlerde ise verilerin saklanması, kablosuz internet ve ağ konuları anlatılmış bunlarla ilgili örnekler verilmiştir (Aksu, 2005).

Mallick (2003), "Mobil ve kablosuz tasarım esasları" konulu kitabın ilk bölümünde mobil aygıtlar, mobil uygulamalar, kablosuz ağlar, mobil uygulamaların mimarisi, mobil ve kablosuz ortamların güvenliği anlatılmıştır. İlerleyen bölümlerde kablosuz internet uygulamaları mimarisi ve esasları anlatılmış, son kısımda ise birçok faydalı teknoloji tanıtılmıştır (Aksu, 2005).

Klingsheim(2004), "J2ME Bluetooth programlama" tezinin ilk bölümünde Bluetooth sistem mimarisi ve güvenliği anlatılıp Java 2 Micro Edition ortamı CLDC, MIDP, MIDlet program yapısı, J2ME ve JABWT yapısı anlatılmış, örnek programlama örnekleri yapılmıştır.

Gehrmann ve ark., (2004), "Bluetooth güvenliği" kitabında Bluetooth sistem yapısı ve güvenliği detaylı olarak anlatılmış Bluetooth şifreleme ve algoritmik yapılarının detaylarına inilmiştir.

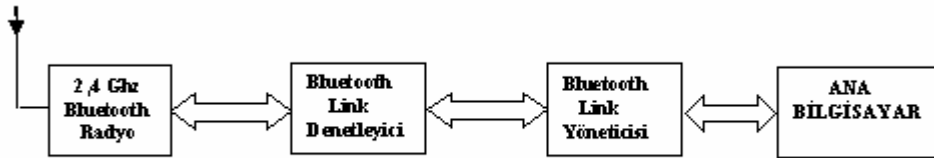
Engin Çomakçı (2004), "Bluetooth Güvenlik Mimarisinin İncelenmesi ve Geliştirilmesi" isimli yüksek lisans tezinde Bluetooth mimarisi, kriptoloji, Bluetooth güvenlik yönetimi, Bluetooth algoritmik yapısının kıyaslanması yapılarak CCMP protokolü önerilmiştir.

Bu çalışmada ise Bluetooth teknolojisi ve güvenlik yapısı incelenmiş, bilgi güvenliği, kriptoloji konularında bilgiler verilerek, oluşturulan yazılımların Bluetooth güvenliğini artırıcı bir durum meydana getirilmiştir

**3. MATERYAL VE METOD****3.1. MATERYAL****3.1.1. Bluetooth Teknolojisi ile İlgili Çalışmalar**

Son yıllarda bilişim teknolojileri alanında meydana gelen hızlı gelişmeler mobil haberleşme ve kablosuz teknolojiler sahasına yansımış ve kablosuz iletişimin en popüler teknolojilerden biri haline gelmesini sağlamıştır. Son yıllarda ev, ofis kullanımı ve kişisel kullanım için sayısız elektronik cihaz üretilmiş olmasına rağmen, Kişisel Alan ağlarındaki (Personal Area Networks) cihazların kendi aralarında iletişim kurmasını sağlayacak, yaygın bir teknoloji ortaya çıkmamıştır. Cihazlar arasında kablolarla ihtiyaç duymadan veri ve ses transferi yapabilecek bir teknolojiye olan gereksinim her geçen gün daha büyük bir hızla artmıştır.

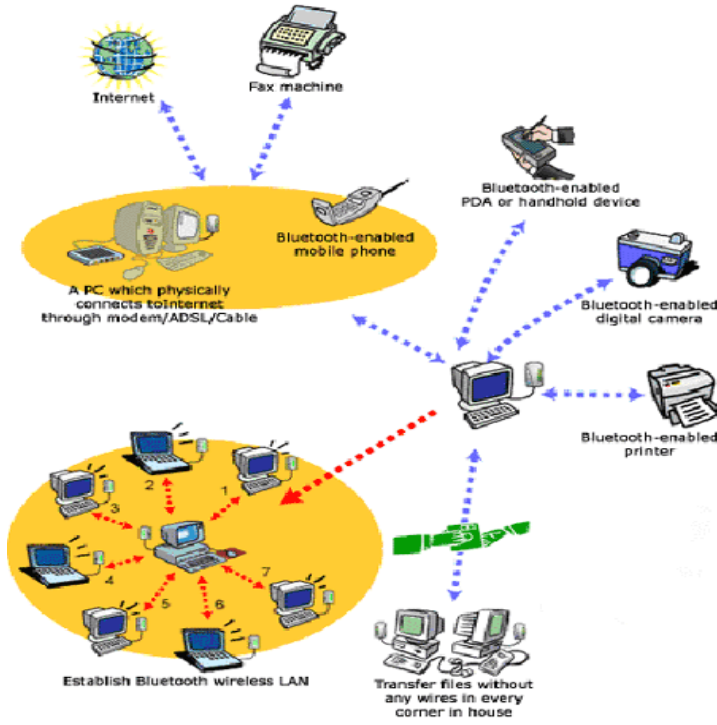
Bluetooth, kablosuz haberleşme sahasındaki boşluğu doldurmakta; ucuz ve tüm cihazlara uyumlu çalışmaya imkan veren teknikle kablosuz veri ve ses iletişimin kapılarını açmaktadır. Bluetooth teknolojisi tanım olarak, kısa mesafede kablosuz ses ve veri haberleşmesine dünyanın her yerinde açık standartlar sunan bir teknolojidir. Bluetooth teknolojisi, düşük maliyetli, düşük güçlü, kısa mesafe radyo teknolojisidir ve kulaklıklılı telefonlar, PDA (Personal Digital Assistant) cihazları ve diz üstü bilgisayarlar gibi haberleşme cihazlarının kendi aralarında haberleşmesi için kablonun yerini alır. Bluetooth haberleşmesi, 2.4 GHz’ de ve lisans gerektirmeyen ISM bandında (endüstriyel, bilimsel ve tıp uygulamalarına ayrılmış frekans bandı) gerçekleşmektedir. Maksimum veri akış hızı 1 Mbit / sn’dir. Şekil 3.1’ de Bluetooth sistemi yapısı görülmektedir.



Şekil 3.1. Bluetooth sistemi yapısı

Bluetooth sistemi yapısı radyo birimi, link kontrol birimi, link yönetimi ve kullanıcı uç cihazı arayüz fonksiyonlarına destek veren bir birimden oluşmaktadır. Ana bilgisayar kontrol arayüzü (HCI – Host Controller Interface) ana birimin Bluetooth donanımına erişmesi için bir araç vazifesi görür. Örneğin, ana birim bir dizüstü bilgisayar ve kişisel bilgisayarın (PC) içine yerleştirilmiş bir PC kartta bir Bluetooth cihazı olabilir. Ana birimden Bluetooth modülüne gönderilen tüm komutlar ve modülün ana birime verdiği cevaplar HCI vasıtasıyla iletilir.

Bağlantıyı sağlamak için iki adet Bluetooth ile donatılmış cihazın birbirlerine 10 metrelik bir mesafe kadar yaklaşmaları gerekir. Bluetooth telsiz tabanlı bir bağlantı kullandığından, iletişim kurmak için görüş hattı bağlantısına ihtiyaç duymaz. Diz üstü bilgisayarınız, bilgiyi yan odadaki yazıcıya gönderebilir ya da evinizin alarm sistemini cep telefonuyla kontrol edebilirsiniz. Şekil 3.2’ de Bluetooth kullanım alanları verilmektedir.



Şekil 3.2. Bluetooth kullanım alanları ( Anonim, 2005)

Bluetooth vasıtasıyla özel amaçlı haberleşme ağlarının kurulması, tüm kişisel cihazların arasında senkronizasyonun kablosuz olarak sağlanması çok kolaydır. Bluetooth teknolojisi yalnız donanım değil birlikte çalışabilirlik ve yazılım ihtiyaçlarını da karşılamaktadır. Ayrıca Bluetooth'un kabul gördüğü tek sektör telekom endüstrisi değildir. Bilgisayar, ev eğlencesi, otomotiv, sağlık, oyuncak ve daha pek çok farklı sektör Bluetooth çözümlerine büyük ilgi göstermektedir.

### 3.1.2. Bluetooth İsmi

Bluetooth, kısa mesafedeki aygıtları birbirine bağlayan bir kablosuz teknolojidir ve adını Viking savaşçısı Harald'dan almıştır. Bu kişi, Norveç ile Danimarka'yı birleştirmesi ile tanınmaktadır. Kral Harald'ın farklı politikaları bir araya getirmesi gibi bluetooth'da cep telefonları, bilgisayarları, PDA'ları, yazıcıları kablosuz olarak bir araya getirir.

1994 yılında İsveç hareketli cep telefonu üreticisi Ericsson, cep telefonları ve cep telefonu aksesuarları arasında kablosuz iletişim sağlayabilecek düşük güç tüketimli, düşük maliyetli bir radyo arabirimi üzerinde araştırma yapmaya karar vermesi Bluetooth teknolojisinin kapılarını açan bir adımdır.

Daha sonra mühendislik çalışmaları başladı ve Bluetooth teknolojisinin gerçek potansiyeli daha net bir şekilde görülmesini sağladı. Cihazlar arası iletişimde kabloları kaldırmak amacıyla ortaya atılan bir fikir zamanla yepyeni imkanları da gözler önüne serdi: Bluetooth uygulamaları; mevcut veri network'lerine uzanan evrensel bir köprü, çevre birimleri için bir arayüz ve küçük çaplı cihaz network'leri oluşturmak için bir araç olarak da kullanılabilir.

1998 yılının başlarında bilgisayar ve telekomünikasyon endüstrisinin Bluetooth teknolojisiyle ilgilenen öncü firmaları Bluetooth SIG (Special Interest Group) organizasyonu altında birleştiler. SIG' in kurucu firmaları Ericsson, Intel, IBM (International Business Machines), Nokia ve Toshiba dır. 1999 yılının aralık ayında da 3Com, Lucent Technologies, Microsoft ve Motorola firmalarının katılımıyla SIG genişletilmiştir. SIG nin temel amacı Bluetooth teknolojisinde yaşanan gelişmeleri yakından izlemek ve bu teknoloji için açık, global bir spesifikasyonun oluşmasını sağlamaktır. Kuruluşun diğer çalışmaları arasında frekans bandı uyumu ve teknolojinin kitlelere tanıtılması yer almaktadır. SIG organizasyonu kendi içinde her biri teknolojinin belli bir kısmına (yazılım, hava ara yüzü gibi) odaklanmış, çeşitli çalışma gruplarına ayrılmıştır.

### **3.1.3. Bluetooth'un Temel Özellikleri**

#### **3.1.3.1. Birlikte Çalışabilirlik**

Bluetooth spesifikasyonlarında farklı üretici firmaların farklı cihazlarının aynı profili kullandıkları sürece birlikte çalışabilirliği garanti altına alınmıştır. Profiller, Bluetooth protokol yığınının birlikte çalışabilirlik çözümleri sunmak için nasıl kullanılabileceğini ortaya koymaktadır. Örneğin, bir farenin bir cep telefonu kulaklığı ile haberleşmesi gerekli olmadığı için, fare ve kulaklık farklı profilleri esas alarak tasarlanabilir

#### **3.1.3.2. Kısa Mesafe Kablosuz Haberleşme Yapısı**

Günümüzde, bilgi işlem ve haberleşme cihazları arasında sayısal haberleşme genellikle kablolar vasıtasıyla gerçekleştirilmektedir. Bu kablolar da çeşitli şekillerde, çeşitli boyutlarda ve çeşitli sayıda pinleri olan konnektörlere bağlanıyorlar ki bu da kullanıcı için oldukça külfetli olmaktadır.

Bluetooth teknolojisi ile haberleşecek olan cihazlar, kablosuz olarak bir hava- ara yüzü vasıtasıyla radyo dalgalarını kullanarak bağlantı kurabilmektedirler. Bu teknoloji özellikle kısa mesafe (yaklaşık 10 metre) haberleşmesi için tasarlanmıştır. Bunun nedeni, teknolojiyi küçük, taşınabilir, batarya ile beslenen cihazlar için, çok az güç tüketimi sayesinde, cazip hale getirmektir.

#### **3.1.3.3. Açık Standart Yapısı**

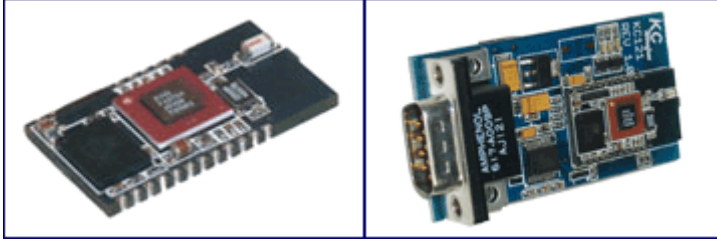
Bluetooth SIG, Bluetooth kablosuz haberleşme teknolojisini herkese açık, telif hakkı olmayan bir teknoloji olarak tanımlamıştır. SIG'nin kuruluşundan itibaren bu açık standart yapısını benimsemesinin nedeni teknolojinin daha geniş kitleler tarafından kabulünü sağlamaktır.

#### **3.1.3.4. Ses ve Veri Haberleşmesi**

Bluetooth kablosuz haberleşme teknolojisi, hem ses hem de veri trafiğini taşıyacak yapıya sahip, bütün cihazlara bu her iki içeriği de kullanma olanağı veren ideal teknolojidir.

### 3.1.3.5. Tüm Dünyada Uyumlu Olması

Telefon sistemleri ülke içinde tanımlı olan frekans kısıtlamalarına uyumlu olmalıdır. Ayrıca telefon standartları da ülkeden ülkeye değişiklik göstermektedir. Radyo frekans spektrum kullanımı genellikle lisans gerektirmektedir. Bununla birlikte, radyo frekans spektrumunun bazı bölgeleri lisanssız olarak tüm dünyada kullanılabilir. Böylece, Bluetooth teknolojisi de bu lisanssız bölgede çalışmaktadır. Bluetooth teknolojisini kullanan cihazlar dünyanın neresinde olursa olsun herhangi bir ek donanım ve yazılım gerektirmeden çalışmaktadır. Şekil 3.3’de Bluetooth modülleri görülmektedir.



Şekil 3.3. Tipik Bluetooth modülleri (Anonim, 2005)

SIG bünyesinde yürütülen Bluetooth Yeterlik Programının (Bluetooth Qualification Program) amacı cihazların hangi ülkede ya da hangi üretici tarafından üretildiğinden bağımsız olarak birlikte çalışabilir olmalarını sağlamaktır. Bluetooth sertifikasyonu almak isteyen her cihazın geçmek zorunda olduğu testler sırasında cihaz şu konulardaki yeterliliğini ve uyumunu kanıtlamalıdır: Radyo link kalitesi, alt katman protokolleri, profiller ve son kullanıcı için bilgiler.

### 3.1.4. Teknolojik Alt Yapı

#### 3.1.4.1. Kablolu ve Kablosuz Haberleşme

Kablolu ağlar ile yüksek oranda veri taşınmaktadır. Telefon sistemlerinde, koaksiyel kablolu sistemlerde, Yerel Alan Ağları’nda (Local Area Networks) ve internet haberleşmesinin bir kısmında bağlantı telleri ve kablolar kullanılmaktadır. Pek çok televizyon kablolu sistemlere, pek çok bilgisayar, telefon hatlarına ve Ethernet ağı gibi kablolu ağlara bağlanmaktadır.

Kablosuz haberleşme teknolojisi ise, özellikle son yıllarda cihazlar arasında kablolarla ihtiyaç duyulmadan ses ve veri transferinin yapılmasını sağlayacak bir teknolojiye duyulan gereksinimin artması sonucu doğmuştur. Aslında kablosuz haberleşme yeni bir kavram değildir ama son yıllarda büyük gelişme göstermiştir. Geniş alana yayın yapan radyo ve televizyonlar, uydular, hücresel telefonlar, uzaktan kumandalı televizyonlar, otomobil kapısı kilitleri kablosuz sistemlere örnek teşkil ederler. Bu sistemlerde genellikle radyo dalgaları kullanılmakla birlikte, ışık spektrumunun kızıl ötesi ve görünür olmayan bölgelerinin kullanımı da mümkündür. Bluetooth kablosuz haberleşme teknolojisi ise haberleşme için radyo frekans (radio-frequency – RF) teknolojisini kullanmaktadır.

### 3.1.4.2. Bluetooth Radyo Teknolojisi

RF teknolojileri, radyo dalgalarını üretmek için frekans modülasyonunu kullanırlar. Frekans modülasyonlu (FM) radyo yayınları, frekans spektrumunun 88 megahertz (MHz) ile 108 MHz arasındaki kısmını, bazı kablosuz telefonlar 900 MHz bölgesini kullanırken, Bluetooth kablosuz haberleşme teknolojisi 2.4 GHz'lik lisanssız bölgeyi kullanır. Frekans spektrumunun 2.4 GHz'lik kısmı lisanssız olmasına rağmen bu bölgenin de bazı düzenleyici kuralları vardır. Bunlar:

Spektrum 79 kanala ayrılmıştır. (bazı ülkelerde 23 kanal kullanılmaktadır).

Her kanal için bant genişliği 1 MHz ile sınırlandırılmıştır.

Frekans atlama tekniği, yaygın spektrum haberleşmesinde kullanılmalıdır.

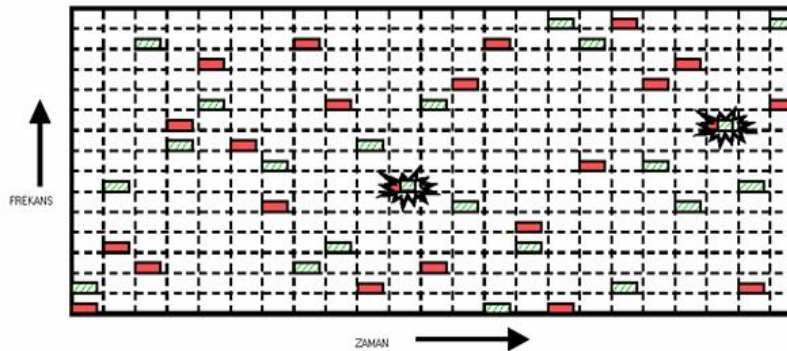
Girişim etkisi uygun bir şekilde yürütülmelidir.

### 3.1.4.3. Frekans Atlama Tekniği

Bluetooth teknolojisinde, daha güvenilir ve daha etkili bir haberleşme için frekans atlama mekanizması kullanılmaktadır. Bluetooth radyosu trafiğin oldukça yoğun olduğu ISM bandında çalıştığı için, herhangi bir etkileşim halinde, kaynak tarafından geçici olarak bloke edilmesi mümkündür. Bluetooth teknolojisi kaybedilen paketlerin tekrar gönderilmesini sağlamasına rağmen onların da tekrar bloke olması ihtimaline karşı, bu paketlerin yeni bir kanaldan gönderilmesi daha verimli olacaktır.

Bluetooth radyo frekans işlemleri 2.402 GHz den başlar; 2.480 GHz de son bulur. 1 MHz'lik aralıklara ayrılmış 79 frekans atlama sayesinde frekans spektrumu genişletilir. Saniyede ortalama 1600 atlamaya izin veren full-duplex sinyal iletişim tekniği kullanılır. Eğer bir Bluetooth cihazının paket iletimi başka bir cihaz tarafından bozuluyorsa, paket master tarafından belirlenen başka bir frekansta tekrar gönderilir. Şekil 3.4 de şematik olarak bu frekans atlama gösterilmiştir. Burada, birinci cihazın ve ikinci cihazın paketleri aynı frekansı kullanmak istiyorlar.

Bluetooth radyo haberleşmesinde RF verimi, 10 metre mesafeli versiyonda 0 dBm , daha uzun mesafeli versiyonda ise -30 ile +20 dBm olarak belirlenir.



Şekil 3.4 . Bluetooth frekans atlama örneği (Anonim, 2002)

**3.1.4.4. Modülasyon Tekniği**

Bluetooth sisteminde kullanılan modülasyon metodu GFSK(Gaussian Frequency Shift Keying) tekniğidir. İşletim bandı 83.5 MHz, 1 MHz aralıklı kanallara ayrılmıştır ve maksimum kanal bant genişliğini elde etmek için her bir kanal, GFSK modülasyon tekniği ile 1 Mbit/sn ile sinyalleşmektedir. İkili sistemde "1" nominal taşıyıcı frekanstan pozitif frekans sapmasını belirtmektedir. Buna frekans atlama algoritması kullanılarak karar verilir. İkili sistemde '0' ise negatif frekans sapmasını belirtmektedir.

GFSK ile en iyi verimi elde etmek için, kabul edilebilir bir hata olasılığı ile, bant genişliği bit hızının 0.5'i olarak alınır. Modülasyon indeksi ise 0.28 ile 0.35 arasında seçilir. Bluetooth standartlarına göre, herhangi bir andaki minimum frekans sapması 115 KHz'dir. Ayrıca, sıfır geçiş hatası (zero crossing error), sembol periyodunun 1/8'inden az olmak durumundadır. GFSK, frekans değişimlerini düzeltmek için, Gauss filtresi kullanır. Böylece, modüle edilmiş taşıyıcı frekans, Gauss zarfı ile düzgün bir şekil alır.

**3.1.4.5. Bluetooth Radyo Güç Sınıfları**

Bluetooth standartları, üç farklı tipte güç sınıfına müsaade etmektedir. Bu güç sınıfları Bluetooth cihazlarının farklı mesafelerde bağlantı kurmalarına imkan tanır. Çizelge 3.1 de bu güç sınıflarının maksimum çıkış güçleri ve mesafeleri gözükmektedir.

Çizelge 3.1.Güç sınıfları

| Güç Sınıfı | Maksimum Çıkış Gücü | Mesafe      |
|------------|---------------------|-------------|
| 1          | 100 mW (20 dBm)     | ~ 100 metre |
| 2          | 2.5 mW (4 dBm)      | ~ 35 metre  |
| 3          | 1 mW (0 dBm)        | ~ 10 metre  |

Bluetooth bağlantısı için ayrıca minimum mesafe de söz konusudur. Eğer radyolar birbirine çok yakın konulurlarsa, bazı alıcılar doyma noktasına gelebilir ve birkaç Bluetooth radyosu kısa uzunluktaki hatlarda güvenilir olmayabilir. Bu minimum mesafe yaklaşık olarak 10 cm'dir. 100 m' lik hatlar 1.sınıf yüksek güçlü radyolara ihtiyaç duyarlar.

Bununla birlikte, düşük ve yüksek güçlü cihazların farklı mesafelerde kombinasyonları kullanılarak da piconetler (En küçük Bluetooth şebekesi) oluşturulabilir.

**3.1.4.6. Master – Slave Yapısı**

Bluetooth şebekesinde neredeyse tüm birimler özdeştir ve 48 bitlik adres dışında donanım ve yazılımları aynıdır. Bağlantı ilk kurulduğu zaman geçici bir başlangıç ünitesi tahsis edilmektedir. Bağlantıyı kurmaya başlayan ve trafiği en fazla 7 üniteye kadar kontrol edebilen bu sistem master adını almaktadır. Her bağlantı yolu şebekesi ise slave olarak adlandırılmaktadır.

Bluetooth cihazları, her bir paketten sonra yeni bir frekansa atladıkları zaman mutlaka kullanacakları frekans sırası ile uyum sağlamak zorundadırlar. Bluetooth cihazları iki farklı modda çalışabilmektedir; master olarak veya slave olarak. Frekans atlama sırasını

belirleyen master'dır. Slave'ler master ile eş zamanlı olarak onun frekans atlama sırasını takip ederler.

Her bir Bluetooth cihazının kendine özgü bir Bluetooth cihaz adresi ve Bluetooth saati vardır. Bluetooth spesifikasyonunun temel bant katmanı, Bluetooth cihaz adresi ve Bluetooth saatinden frekans atlama sırasını hesaplayan bir algoritma tanımlamaktadır. Slave'ler master'a bağlandıkları zaman onlara Bluetooth cihaz adresi ve master'ın saati belirtilir. Onlar da bu bilgileri frekans atlama sırasını hesaplamak için kullanırlar. Çünkü, bütün slave'ler master'ın saatini ve adresini kullanmaktadırlar ve master'ın frekans atlama sırasıyla eş zamanlı olarak çalışmaktadırlar.

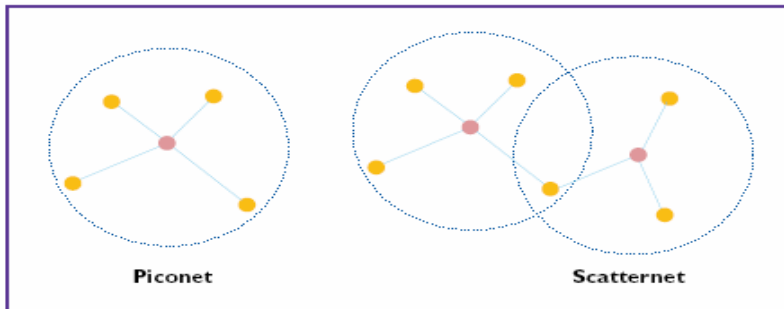
Frekans atlama sırasını kontrol etmeye ek olarak, cihazların ne zaman gönderme yapabileceğini de master kontrol eder. Master, dilimleri (slotları) ses veya veri trafiği için tahsis ederek, slave'lere iletim için izin verir. Data trafik dilimlerinde, slave'ler yalnızca master tarafından yapılan bir gönderime cevap verme yetkisine sahiptir; onun dışında iletim yapamazlar. Ses trafik dilimlerinde ise, slave'ler master'a cevap versin veya vermesin düzenli olarak, ayrılmış dilimlerde gönderim yapmak durumundadırlar.

Master, toplam elde edilebilir bant genişliğinin slave'ler arasında nasıl bölündüğüne, her bir slave ile ne kadar sıklıkla haberleştiğine bağlı olarak karar verir. Her bir cihazın alacağı zaman dilimi sayısı, o cihazın veri transfer gereksinimine bağlıdır. Zaman dilimlerini bir çok cihaz arasında paylaştıran sisteme zaman bölmeli çoğullama (Time Division Multiplexing – TDM) denir.

### 3.1.5. Bluetooth Şebeke Yapısı

#### 3.1.5.1. Piconet

Bluetooth teknolojisini kullanan cihazlar, ad-hoc biçimiyle bağlantı kurmaktadırlar. Birbirlerinin kapsama alanı içerisinde bulunan Bluetooth birimleri noktadan noktaya ya da noktadan çok noktaya bağlantı kurabilirler. İki veya daha fazla bluetooth birimi birbiriyle bağlantı kurduğunda bunlar bir şebeke oluştururlar ve Bluetooth standartlarında bu şebekeye 'piconet' adı verilir. Piconet birbirine bağlı iki birimle (dizüstü bilgisayar ve hücresel telefon gibi) başlar, birbirine bağlanmış sekiz birime kadar genişleyebilir. Bütün Bluetooth cihazları eşdeğer olmalarına rağmen, piconet oluştururken piconet bağlantısı süresince bir birim master, diğerleri slave olarak rol alır. Bu durum Şekil 3.5 'de verilmektedir.



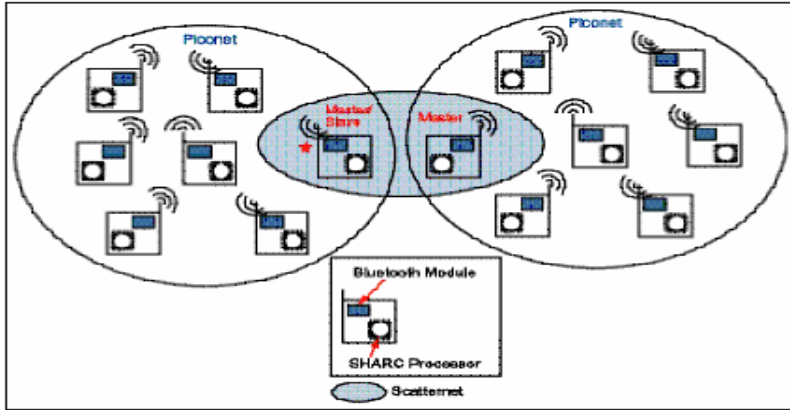
Şekil 3.5. Bir piconet'in ve scatternet'in şematik gösterimi (Bhagwat, 2001)

Piconet içerisinde bir slave sadece kendi master'ı ile haberleşebilir. Piconet içerisindeki tüm birimler master'ın saatini ve Bluetooth adresini kullanarak hesaplanan aynı frekans atlama sırasını paylaşırlar.

### 3.1.5.2. Scatternet

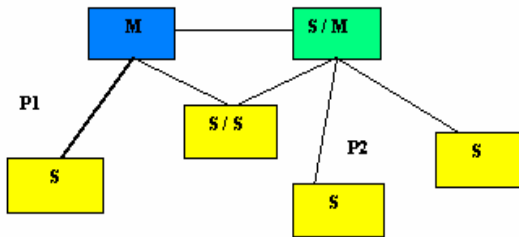
Birçok piconet aynı alanı kapsıyor olabilir. Her bir piconet farklı master'a sahip olduğu için piconet'lerin frekans atlamaları birbirinden bağımsızdır. Birden fazla piconet'in birbirine bağlanmasıyla oluşan şebeke yapısına 'scatternet' adı verilir. Standartların piconet içerisindeki slave sayısını 7 ile sınırlandırmasına rağmen, scatternet yapısı kullanılarak ağ içerisindeki birim sayısı artırılabilir ve daha geniş bir kapsama alanı elde edilebilir. Eğer bir birim birden fazla piconet'e ait ise, mutlaka zaman-paylaşımlı (time sharing) olmalıdır. Bunun anlamı, bu birim birkaç dilim bir piconet'te birkaç dilim diğer piconet'te harcar. Şekil 3.6'da bir scatternet durumu verilmiştir.

Bluetooth v1.1 standartlarına göre, bir Bluetooth ünitesi, iki farklı piconet'te slave olarak rol alabilir fakat, master olarak sadece bir piconet'te görev alır. Eğer bir master iki piconet'te master ise bu piconet'ler eşzamanlı olmalı ve aynı atlama sırasını kullanmalıdır. Başka bir deyişle bu iki piconet tek ve aynı piconet olmalıdır.



Şekil 3.6. Scatternet durumu ( Keon loo ve ark.; 2001)

Bir master ya da slave başka bir piconet'in master'ı tarafından çağırılarak (paging) o piconet'te slave olarak rol alabilir. Şekil 3.7 de örnek olarak master  $M_1$ , master  $M_2$ 'yi çağırmakta ve böylece master  $M_2$  iki role sahip olmaktadır; birinci piconet'te slave, ikinci piconet'te master.



Şekil 3.7. Bir Bluetooth master biriminin slave olarak rol alması.

**3.1.5.3. Ses ve Veri**

Bluetooth teknolojisi hem zamanın önemli olduğu veri haberleşmesine, hem de zaman duyarlılığı olmayan fakat yüksek hızlı paket data haberleşmesine imkan tanır. Bu verileri taşımak üzere, cihazlar arasında iki farklı tipte link tanımlanmıştır. Bu linkler ses haberleşmesi için eş zamanlı bağlantı hattı (SCO-Synchronous Connection Oriented) ve veri haberleşmesi için eş zamanlı olmayan bağlantı (ACL- Asynchronous Connectionless) hattıdır.

SCO bağlantı tipi, master ve slave arasında full-duplex olarak gerçekleştirilir. SCO hatları, 64 Kbit/sn hızda çalışır ve 3 taneye kadar full-duplex eş zamanlı ses kanalı veya eş zamanlı olmayan veri ile eş zamanlı sesi aynı anda destekleyen bir kanal kullanır. Bu ses kanalları modern bir hücresel telefon sisteminden beklenebilecek kalitede haberleşme imkanı sunar.

ACL bağlantı tipi master ile herhangi bir slave arasındaki iletişimi sağlar. ACL veri paketleri, taşınacak bilgiye ek olarak 72 bit erişim kodu, 54 bit paket başlığı ve 16 bit CRC (Cyclic Redundancy Check) kodu içermektedir. Farklı miktarlarda verinin taşınmasına olanak sağlayan çeşitli paket tipleri mevcuttur. Bu paket tiplerinden en fazla veri taşıyan 5 bölmeli DH5 paketleridir. DH5 paketleri 339 bayt ya da 2712 bit veri taşıyabilir. 2712 bit'lik bilgi için 2858 adet bit gönderilir.

DH5 paketlerinin 5 bölmesinden minimum bir tanesi cevap için ayrılır. Dolayısıyla, bir doğrultuda gönderilebilecek maksimum veri miktarı 723.2 Kbit/sn dir. Bununla birlikte dönüş yönünde gönderilen veri miktarı 57.6 Kbit/sn olduğu için bu hat asimetrik bir hatır. Eğer 5 bölmenin hepsi iki yönde de veri gönderirse 433.9 Kbit/sn'lik simetrik, eşzamanlı olmayan bir haberleşmeyi destekleyen bir hat elde edilir.

**3.1.5.4. Güvenlik**

Bluetooth cihazlarının gizlice dinlenmesi ya da mesajların çıkış noktasının değiştirilmesi gibi tehlikelerin önüne geçmek amacıyla Bluetooth cihazları bazı güvenlik özellikleri içermektedir. Başlıca güvenlik yöntemleri şunlardır:

İletişim Şifresi; bağlantıların gizliliğini sağlamak ve gizlice dinlenilmeyi önlemek için kullanılır.

Karşıla-yanıtla prosedürü; mesajların çıkış noktasının değiştirilmesi ve kritik bazı verilerle fonksiyonlara ulaşılması gibi olaylara engel olur.

Oturum anahtarlarının üretimi; bağlantı sırasında oturum anahtarları istenildiği zaman değiştirilebilir.

Frekans sıçraması ve mesafenin kısa olması; sinyallerin yakalanmasını önlemede yardımcı bir etkidir.

Bluetooth güvenlik algoritmalarında aşağıdaki yöntemler kullanılır:

Kullanıcıya özel 128 bit'lik bir anahtar başlangıçta üretilir. Bu anahtar gizlidir ve hiçbir zaman açıklanmaz.

Bluetooth biriminde pseudo-random bir süreç sonunda 128 bitlik her yeni işlem için farklı olan rasgele bir sayı üretilir.

Bluetooth cihaz adresi (BD\_ADDR) de güvenlik algoritmalarında kullanılmaktadır.

48 bitlik ve her cihaz için ayrı olan bu adres, sıradan sorgulama prosedürü ile öğrenilebilir.

### **3.1.6. Bluetooth Protokol Mimarisi**

#### **3.1.6.1. Genel Bakış**

##### **3.1.6.1.1. Protokol nedir?**

Protokoller cihazların birbiriyle bilgi alışverişinde bulunabilmeleri için üzerinde fikir birliğine varılmış kurallar bütünüdür. Ağ topolojilerinin bütün tipleri için, mesajların linkler üzerinde nasıl iletileceğine ilişkin kurallar ve protokoller tanımlanmıştır. Protokoller bu mesajların biçimleri ile adres, hata kontrolü ve kullanıcı bilgisi gibi bilgiler için hangi alanların ayrıldığı bilgilerini de tanımlarlar.

Genel kabul gören protokoller olmadığı takdirde yazılım ve donanım üreticileri kendi yöntemlerini geliştirerek üretim yapacakları için ağlar düzgün çalışmazlar. Aynı ağda bulunan cihazların birbiriyle haberleşmesi için protokoller mutlaka olmalıdır. 1960'ların sonlarına doğru TCP/IP (Transmission Control Protocol / Internet Protocol) üzerinde çalışılmaya başlanmış, bu sayede farklı üreticiler tarafından üretilen cihazların birbiriyle haberleşebilmesi sağlanmıştır. Günümüzde ise TCP/IP katmanını içeren bütün bilgisayar yapıları internet üzerinden birbiri ile haberleşebilmektedir.

##### **3.1.6.1.2. Bluetooth Protokol Mimarisi Tanımı**

Bluetooth SIG tarafından tanımlanan Bluetooth standartları, donanım, yazılım, kısa mesafe kablosuz bağlantı için birlikte çalışabilirlik gerekleri ve plansız (ad hoc ) ağ oluşturmayı tanımlamaktadır. Tanımlamalar iki ana birime ayrılabilir; protokoller ve profiller. Protokoller alt katmandan üst katmana doğru sıralanan, teknolojinin nasıl çalıştığını tanımlayan kısımdır. Profiller ise teknolojinin nasıl kullanıldığını tanımlar.

Bluetooth protokol yığını üç gruba ayrılabilir. Taşıma protokolleri (Transport Protocols), özel yazılım protokolleri (Middleware Protocols) ve uygulama protokolleri (Application Protocols). Taşıma protokol grubu, Bluetooth cihazlarının birbirlerini konumlandırmaları ve yüksek katman protokol ve uygulamalarının bilgiyi taşıma protokollerinden geçirmesine imkan veren, fiziksel ve lojik linklerin yaratılması, yapılandırılması,ve yönetilmesi için imkan sunan protokollerden oluşmuştur. Bu gruptaki protokoller içerisinde; radyo, temel bant, link yönetim protokolü, L2CAP (Logical Link and Adaptation) ve HCI (Host Controller Interface) bulunur.

Özel yazılım protokolleri, var olan ve yeni uygulamaların Bluetooth linklerinde çalışabilmesi için gerekli olan ek taşıma protokollerini kapsayan bir gruptur. Özel yazılım protokolleri hem üçüncü kullanıcı ve endüstri standartları protokollerini hem de SIG tarafından geliştirilen protokolleri içerir. Özel yazılım protokolleri grubu öncelikli olarak internetle ilgili protokolleri (PPP, IP, TCP gibi), kablosuz uygulama protokollerini ve IrDA den uyarlanmış nesne değiş tokuş protokollerini (object exchange protocols) kapsar. Ayrıca, normalde seri port ara yüzü ile işleyen uygulamaların Bluetooth taşıma protokolleri üzerinden olmasına imkan veren bir seri haberleşme emülasyon protokolü olan RFCOMM, grup yönetimi ve baz istasyonlarına, kablosuz telefonlara taşınabilirlik desteği sağlama gibi telefon kontrol işlemlerini üstlenen telefon kontrol protokolü ve son olarak, cihazların birbirinin servislerini keşfetmesini ve bu servislere nasıl erişileceğine dair bilgi verilmesi işlemlerini yapan servis keşif protokolü (SDP-Service Discovery Protocol) de bu gruptandır.

Uygulama protokol grubu da Bluetooth linklerini kullanan gerçek uygulamaları kapsar. Bu uygulamalar, modem çeviricisi uygulaması ya da web browsing kullanıcısı gibi Bluetooth taşıması ile ilgili olmayan miras (legacy) uygulamaları ya da telefon cihazını kontrol etmek için telefon kontrol protokolünü kullanan kablosuz haberleşme ile ilgili uygulamaları içermektedir.

### 3.1.6.1.3. OSI Referans Modeli

Bluetooth teknolojisi OSI (Open Systems Interconnect) referans modeli ile birebir modellenememesine rağmen, Bluetooth protokol yığını ile OSI referans modelini Bluetooth protokol yığınındaki görev dağılımını ifade etmek amacı ile, birbiri ile ilişkilendirebiliriz. Şekil 3.8’ de OSI referans modeli ile Bluetooth protokol yığınının karşılaştırılması şematik olarak gösterilmiştir.

|                            |                                  |
|----------------------------|----------------------------------|
| <b>Uygulama Katmanı</b>    | <b>Uygulamalar</b>               |
| <b>Sunum Katmanı</b>       | <b>RFCOMM / SDP</b>              |
| <b>Oturum Katmanı</b>      | <b>L2CAP</b>                     |
| <b>İletim Katmanı</b>      | <b>Host Kontroller Interface</b> |
| <b>Network Katmanı</b>     | <b>Link Yönetim</b>              |
| <b>Veri Link Katmanı</b>   | <b>Link Denetçisi</b>            |
| <b>Fiziksel Katman</b>     | <b>Temel Bant</b>                |
|                            | <b>Radyo</b>                     |
| <b>OSI Referans Modeli</b> | <b>Bluetooth</b>                 |

Şekil 3.8. OSI – BLUETOOTH karşılaştırması (Gurovski ve ark.; 2002)

Fiziksel katman, haberleşme ortamı ile kanal kodlaması ve modülasyonu da kapsayarak elektriksel bir ara yüz oluşturmaktadır. Dolayısıyla radyo katmanı ve temel

bant katmanının bir bölümünü kapsamaktadır.

Data Link katmanı, belli bir link üzerinden iletim, çerçeveleme ve hata kontrolü ile görevlidir. Dolayısıyla, hata kontrolü ve düzeltmesini de içererek, Link Kontrol katmanı ve Temel bant katmanının üst kısmı ile örtüşmektedir.

Network katmanı, ortamdan ve belli bir ağ topolojisinden bağımsız olarak, ağ üzerinden veri transferinden sorumludur. Link kontrol katmanının üst kısmını ve link yönetim katmanının bir kısmını kapsamaktadır.

Transport katmanı, Network katmanından uygulama tarafından belirlenen seviyeye transfer olan verinin güvenilirlik ve çoğullamasından sorumludur. Dolayısıyla, link yönetim katmanının üst kısmı ve gerçek veri transfer mekanizmasını sağlayan HCI katmanı ile örtüşmektedir.

Session katmanı, yönetim ve veri akış kontrolü ile ilgili servislerden sorumludur. L2CAP katmanı ve RFCOMM / SDP katmanının alt kısmı ile örtüşmektedir.

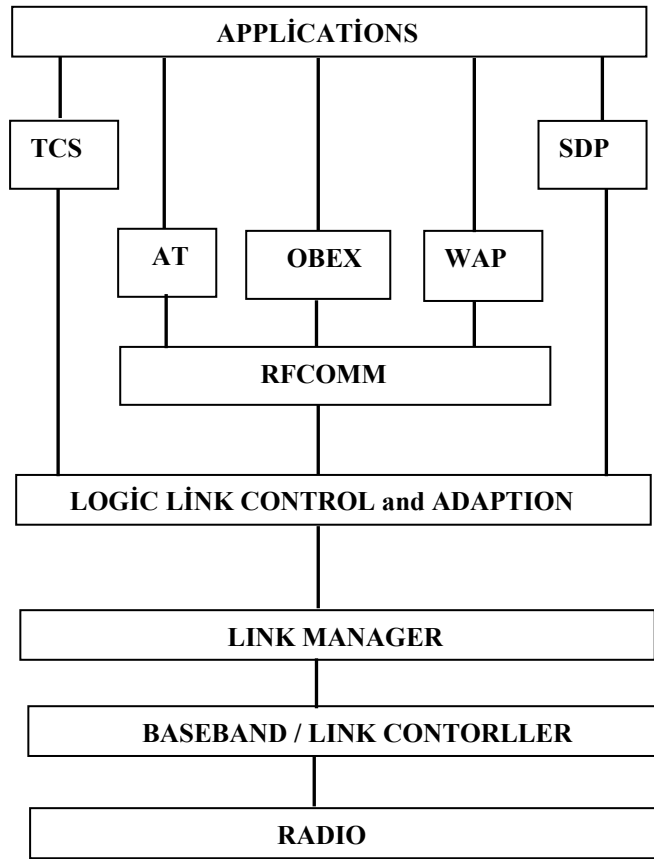
Presentation katmanı, data birimlerine servis yapılarını ekleyerek Application katmanı için genel bir sunum sağlamaktadır. Dolayısıyla, RFCOMM/SDP katmanı ile benzeşmektedir.

Son olarak, Application katmanı, ana bilgisayar uygulamaları arasındaki haberleşmenin yönetimi ile görevlidir. Uygulamalar katmanı ile örtüşmektedir.

#### **3.1.6.1.4. Bluetooth Protokol Yığını**

Bluetooth protokol yığına baktığımızda, LMP ve L2CAP gibi Bluetooth'a özel protokolleri ve "Obje Değiş-Tokuş Protokolü" (OBEX – Object Exchange Protocol) ve UDP (User Datagram Protocol) gibi Bluetooth'a özgü olmayan protokollerden oluştuğunu görürüz (Şekil 3.11). Bu yapıda, protokoller ve tüm protokol yığını tasarlanırken, ana prensip var olan protokollerin üst katmanlarda mümkün olduğunca fazla, tekrar kullanımına imkan sağlamak olmuştur. Protokollerin tekrar kullanılması, bilinen mevcut uygulamaların Bluetooth teknolojisi ile uyumlu olarak çalışmasına neden olmuştur. Böylece, Bluetooth spesifikasyonu ile uyumlu donanım ve yazılım sistemlerinin avantajlarından, üreticiler tarafından geliştirilmiş pek çok uygulama yararlanabilme şansına sahip olmaktadır. Ayrıca, Bluetooth spesifikasyonunun açık bir altyapıya sahip olması dolayısıyla, üreticiler kendi uygulama protokollerini, Bluetooth teknolojisine has protokollere uygun bir hale getirebilmekte ve pek çok yeni uygulama geliştirebilmektedirler (Gurovski ve ark.; 2002).

Farklı uygulamalar, farklı protokol katmanlarında çalışabilmektedir. Fakat, birbirinden farklı bu katmanların her biri ortak bir Bluetooth veri linkini ve fiziksel katmanı kullanmaktadır. Uygulamalar, Şekil 3.9 daki protokol yığınındaki protokollerin tümünü kullanmazlar; çoğunlukla bir veya daha fazla dikey dilimi kullanırlar. Genellikle ek dikey dilimler de ana uygulamayı destekleyen servislerden oluşmaktadır



Şekil 3.9. Bluetooth protokol yığını (Gurovski ve ark.; 2002).

Bluetooth protokol yığını, Bluetooth SIG'nin protokolleri belirlerken aldığı göreve ve protokollerin amaçlarına göre ayrıldığında dört katmanda gruplandırılabilir. Bu gruplandırma şematik olarak, Çizelge 3.2 de gösterilmiştir.

Çizelge 3.2. Bluetooth protokolleri ve bulundukları katmanlar

| PROTOKOL KATMANI             | YIĞINDAKİ 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 |

Çizelge 3.2' deki protokollere ek olarak spesifikasyon, temel bant kontrolörü ve link yöneticisine (LMP), bir komut arayüzü sunan ve donanım durumu ve kontrol kaydedicilerine erişim sağlayan HCI (Host Controller Interface) protokolünü tanımlamıştır.

### 3.1.6.2. Bluetooth Radyo

Radyo Katmanı, Bluetooth protokol mimarisinin en alt seviyesinde bulunur. Bluetooth radyo katmanı yayılan spektrum tekniğini ve frekans atlama tekniğini başarıyla

kullanır. Bazı ülkelerde 1 MHz' lik 79 atlama (hop) kullanılırken, bazılarında 23 atlama kullanılmaktadır. Bluetooth radyo, modülasyon tekniği olarak GFSK ( Gaussian Frequency Shift Keying) kullanır. Bunun yanında, güç sınıflarını ve alıcı – verici karakteristiklerini tanımlayan bir katmandır.

### **3.1.6.3. Temel Bant Katmanı**

Temel bant katmanı Bluetooth protokol mimarisinin fiziksel katmanıdır. Fiziksel kanalları ve linkleri yönetir. Temel bant katmanı protokol yığnında Bluetooth radyo katmanının üzerinde bulunmaktadır. Kanal kodlaması ve kod çözmesi, hata düzeltme, veri temizleme, hop seçimi ve güvenlik işerinden de sorumludur.

Temel bant katmanı Link kontrol katmanı ile birlikte, piconet oluşturan Bluetooth üniteleri arasında fiziksel RF linki oluşmasını sağlamaktadır. Bluetooth RF sistemi, paketlerin belirli frekanslardaki belirli zaman bölmelerinde aktarıldığı FHSS (Frequency Hopping Spread Spectrum) yöntemini kullandığı için, bu katman farklı Bluetooth cihazlarının saatleri ve transfer atlama frekanslarının eşzamanlı olmasını sağlayan sorgulama ve çağrı prosedürlerini kullanır.

Temel bant katmanı iki farklı fiziksel link tanımlar. Bunlar: SCO (Synchronous Connection Oriented – Eşzamanlı Bağlantı Yönelimli) ve ACL (Asynchronous Connection Less- Eşzamanlı Olmayan Bağlantısız) linkleridir. SCO linki piconet'te master ile tek bir slave arasında kurulan, noktadan- noktaya simetrik bir linktir. Master ayrılmış zaman dilimlerini belirli aralıklarla kullanarak SCO linkini korur. Dolayısıyla, SCO linki devre-anahtarlamalı bir bağlantı sağlar ve temel olarak ses bilgisini taşır. Master aynı anda en fazla üç SCO linkini destekleyebilir. SCO paketleri asla geri gönderilmezler ve 64 Kbit/sn ses iletimi için kullanılırlar. ACL linki master ile piconet'teki tüm slave'ler arasında kurulan noktadan- çoklu noktaya bir linktir. Master, SCO linkleri için ayrılmamış zaman aralıklarında (time-slot) her bir aralık herhangi bir slave'e (bir SCO linki tarafından ayrılmış slave'lerde dahil) temel oluşturacak şekilde bir ACL link'i kurar. ACL link, veri değiş-tokuşunun rastgele olduğu paket- anahtarlamalı bağlantı sağlamaktadır. Herhangi iki cihaz arasında, sadece bir ACL link ortaya çıkabilir. Pek çok ACL paketi için paket geri iletimi uygulanmaktadır. Bütün ses ve veri paketleri, İleri Hata Düzeltme (FEC) veya Cyclic Redundancy Check (CRC) hata düzeltme tekniklerinin değişik seviyelerini içerebilir ve şifrelenebilir.

### **Ses (Audio)**

Ses bilgisi bir veya daha fazla Bluetooth cihazı arasında transfer edilebilir ve çeşitli kullanım modellerini mümkün kılar. SCO paketlerindeki ses verisi, temelband üzerinden doğrudan yönlendirilir; L2CAP üzerinden geçmez. Bluetooth içerisindeki ses modeli görece olarak basittir; herhangi iki Bluetooth cihazı sadece bir ses link'i açarak birbirleri arasında ses verisi alışverişinde bulunabilirler.

### **3.1.6.4. LMP (Link Yönetim Protokolü)**

Link yönetim yazılımı, bir mikroişlemci üzerinde çalışmaktadır ve Bluetooth cihazları arasındaki haberleşmeyi yönetir. LMP piconet yönetimi, link kurulması ve

konfigürasyonu ve güvenlik fonksiyonlarından sorumludur. LMP, master ve slave arasında ve SCO/ACL linklerinin kurulmasında anahtar görevi görür. Ayrıca, Bluetooth radyo cihazının görev dönüşümlerini, bağlantı durumlarını ve güç modlarını da kontrol eder.

Link yöneticisi uzaktaki link yöneticilerini araştırır ve onlarla LMP yi kullanarak haberleşir. LMP, PDU (Protocol Data Unit) lardan meydana gelmiştir. PDU'lar bir cihazdan diğerine AM\_ADDR ve paket başlığı ile gönderilmektedir.

### **3.1.6.5. HCI (Host Controller Interface)**

Radyo, temel bant ve link yöneticisi birlikte aynı Bluetooth modülünün içerisinde paketlenir. Daha sonra modül bir host (ana bilgisayar) cihazına iliştilererek, cihazın Bluetooth kablosuz haberleşme teknolojisini kullanabilmesine imkan verir. Bu konfigürasyonda host, L2CAP ve protokol yığınının ilgili üst katmanlarını içermektedir. Modül hosta, "host taşıma" denen USB (Universal Serial Bus), bir RS-232 portu ya da UART gibi bazı fiziksel arayüzler ile eklenir. Spesifikasyon farklı üreticilerin Bluetooth modüllerinin birlikte çalışabilirliğini mümkün kılmak için, ortak bir arayüz tanımlamıştır. Bu ortak arayüz, hostu modüle bağlayan özel fiziksel arayüzlerden bağımsız olarak, modüldeki protokol yığınının alt katmanlarına erişim imkanı sunar. HCI (Host Controller Interface), uygulamalar dahil yığının üst katmanlarının, temel bant, link yöneticisi ve diğer donanım kütüklerine tek bir standart arayüz ile ulaşmasını sağlar. HCI yığının üst katmanlarını cihaz sorgu işlemi ya da gelen transimiyonun sinyal gücünü okuma gibi bazı konularda bilgilendirebilir. Host tarafından gönderilen ya da alınan hem eşzamanlı hem de eş zamanlı olmayan trafik, HCI üzerinden geçer.

HCI katmanı L2CAP katmanının altında yerleştiği için, spesifikasyonun gerekli bir parçası değildir. Host cihazlar ile çeşitli üreticiler tarafından geliştirilmiş Bluetooth modülleri arasında birlikte işlerliği sağlamak amacı ile geliştirilmiştir. Ürün uygulamaları, Bluetooth hava arayüzü ile tam uyumu desteklemek için, HCI spesifikasyonları ile bağdaşmak zorunda değildir.

### **3.1.6.6. L2CAP (Logical Link Control and Adaption Protocol)**

Veri uygulamalarından gelen trafik ilk olarak, L2CAP (Logical Link Control and Adaptation Protocol) katmanına yönlendirilir. L2CAP katmanı, temel Bluetooth katmanlarının üzerinde protokol çoğullaması için, paket segmentasyonu ve yeniden yapılandırması için ve servis kalitesi bilgisini taşımak için kullanılır. Bu katman, iki cihaz arasındaki linkin paket çoğullaması yöntemi ile aynı anda pek çok uygulama tarafından kullanılmasına imkan sağlar. Ayrıca uygulama tarafından gelen paket boyutlarını temel bant tarafından alınan paket boyutlarına küçültür. L2CAP katmanının alabileceği maksimum paket büyüklüğü 64 kbyte'dır ve o bunu 2745 bite küçültür.

L2CAP katmanı sayesinde, yüksek seviye katmanları ne radyo ne de temel bant seviyelerinin frekans atlama olaylarının, ne de iletilen özel paket biçimlerinin farkında olmak zorunda değildir. Çünkü L2CAP katmanı yüksek seviyeli protokolleri ve uygulamaları alt seviyedeki protokollerin detaylarından korur.

L2CAP ayrıca, temel banttaki küçük paket yapılarını birleştirip bunları uygulamalara

sunma görevini yapar. L2CAP, maksimum link bant genişliği, gecikme süresi, gecikme değişimleri gibi bazı parametrelerde uygulamaların servis kalitesi istemesine imkan tanır. L2CAP, linkin bunu sağlayıp sağlayamayacağını kontrol eder ve mümkün ise gerçekleştirir. Kısaca, L2CAP katmanı, uygulamalara ve yüksek seviye katmanlarına "Network" katmanı fonksiyonlarını sunar.

### **3.1.6.7. RFCOMM**

Seri portlar bilgisayar ve haberleşme cihazları için günümüzde en çok kullanılan ortak arayüzdür. Bir çok seri haberleşme uygulaması seri portlardan veri transferi yapmak için kabloları ihtiyaç duyar. Bluetooth kablosuz haberleşme teknolojisinin temel amacı kabloları kaldırmak olduğu için, seri haberleşme ve ilgili uygulamaların kablosuz olarak gerçekleştirmesine imkan verir. Noktadan noktaya dosya veya nesne transferi, veri senkronizasyonu genellikle seri haberleşmeyi kullanan bazı uygulamalardır.

Bluetooth kablosuz linkleri üzerinden seri haberleşmeyi sağlamak için, protokol yığını RFCOMM isimli bir protokol tanımlamaktadır. RFCOMM protokolü, kablolu modeli kullanan seri haberleşme uygulamaların kolaylıkla kablosuz seri haberleşmeye uyarlanması için uygulamalara sanal bir seri port tanımlamaktadır. Herhangi bir uygulama RFCOMM'u standart kablolu seri port gibi kullanabilir; buna örnek olarak senkronizasyon, çevirmeli ağ bağlantısı gibi uygulamaların önemli değişikliklere uğramadan gerçekleştirilmesi verilebilir.

Dolayısıyla, RFCOMM protokolünün işlevi, seri port tabanlı uygulamaların, Bluetooth taşımacılığından yararlanmasını sağlamaktır.

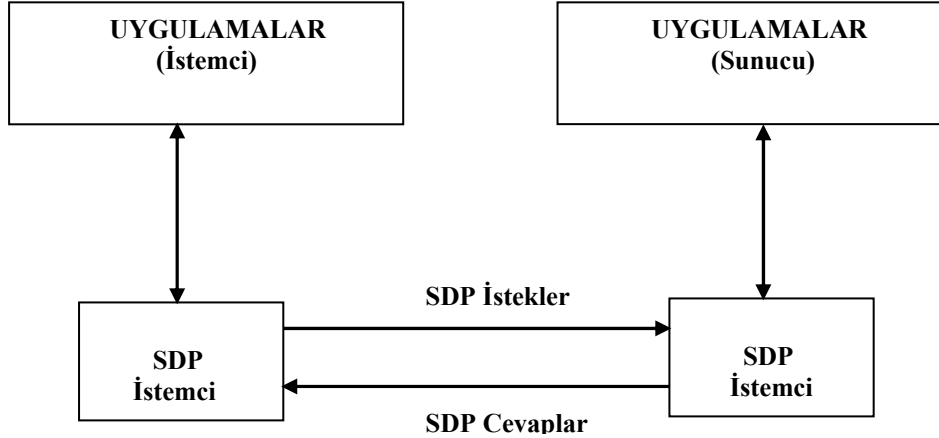
RFCOMM, ETSI 'nin (European Telecommunications Standards Institute) TS 07.10 standardına göre modellenmiştir. Bu standart tek bir seri link üzerinden çoğullanmış seri haberleşmeyi tanımlamaktadır. Bluetooth spesifikasyonu, ETSI 07.10 standardını kullandığı gibi Bluetooth' a özgü bazı özelliklerde tanımlamaktadır. Seri haberleşme sayısal cihazlarda çok yaygın olduğu için, RFCOMM'un uygulamalara kattığı seri port özelliği onu protokol yığınının önemli bir parçası yapar.

### **3.1.6.8. SDP (Service Discovery Protocol)**

Ethernet LAN'lar gibi geleneksel ağlarda dosya hizmetleri, yazıcı hizmetleri, köprüler (bridges) ve geçitler (gateways) gibi servisler ağ içindeki sunucu (server) denilen bazı cihazlar tarafından sağlanır; böylece diğer cihazlar bu hizmetlerden yararlanabilir. Genellikle istemciler (clients) bu ağ hizmetlerini bazı statik konfigürasyonlarla gerçekleştirirler; bu konfigürasyon da statik olarak ağ yöneticisi tarafından sağlanır.

Dinamik ad-hoc ağlarda ise bunlar Bluetooth kablosuz haberleşme teknolojisi ile gerçekleştirilebilir; statik konfigürasyon gereksizdir. Bluetooth teknolojisinde son kullanıcı ağa dahil olmak için gerekli konfigürasyonu kendisi yapar. Bluetooth bunun için, kendine özgü SDP (Service Discovery Protocol) 'ye ihtiyaç duyar. Böylece elde edilebilir servisler hareket halindeki cihazların RF yakınlığına bağlı olarak dinamik olarak değişir. SDP uygulamaların, uzaktaki bir Bluetooth cihazından hangi servislerin alınabileceğini keşfetmeleri ve bu servislerin özelliklerini belirlemeleri için bir araç görevini üstlenir.

SDP, istek/cevap modelini kullanır; her bir hareket bir istek PDU'su (Protokol Data Unit) ve bir cevap PDU'su içerir. SDP Bluetooth L2CAP taşıma protokolü ile birlikte kullanıldığı zaman, her bir bağlantı için SDP sunucusuna verilen sadece bir istek PDU'su göze çarpar. Başka bir ifadeyle, istemci aynı L2CAP bağlantısı üzerinden başka bir istekte bulunmadan önce mutlaka her bir isteğine cevap almış olmalıdır. SDP protokolünün çalışma biçiminin şematik olarak Şekil 3.10'da görüldüğü gibidir.



Şekil 3.10. SDP çalışma biçimi (Gurovski ve ark.; 2002).

### 3.1.7. Telefon Kontrol Protokolleri ve Uyarlanmış Protokoller

#### 3.1.7.1. TCS Katmanı

Bluetooth kablosuz haberleşme teknolojisinin önemli avantajlarından biri de veri trafiği kadar ses trafiğini de iyi bir şekilde taşıyabilmesidir. Bluetooth TCS (Telephone Control Specification) katmanı, çağrı kontrolü ve grup yönetimini de kapsayan telefon fonksiyonlarını desteklemek için tasarlanmıştır. Bu çağrılar genellikle ses çağrılarıdır ve TCS burada çağırma parametrelerini ayarlamak için kullanılmaktadır. Bir kere bağlantı kurulduğu zaman, Bluetooth ses kanalı çağrılardaki ses içeriğini taşır. TCS aynı zamanda çevirmeli ağ bağlantısı profili gibi veri çağrıları kurmak içinde kullanılabilir; bu durumda çağrı içeriği L2CAP üzerinden standart data paketleri ile taşınır.

TCS protokolleri ITU-T (International Telecommunications Union – Telecommunication) Q.931 spesifikasyonları ile uyumludur. Bu protokoller ikili kodlama kullandıklarından dolayı, spesifikasyon içerisinden TCS-BIN olarak isimlendirilmişlerdir. Spesifikasyonun geliştirilmesi sırasında SIG ikinci bir protokol (TCS-AT) önerdi; ve TCS-AT, RFCOMM üzerinden geçen bir modem kontrol protokolü (AT komutları) olarak tanımlandı.

#### 3.1.7.2. TCS-BIN

TCS-BIN Bluetooth cihazları arasında konuşma ve veri çağrılarının kurulması için çağrı kontrol işaretleşmesini tanımlayan bir bit tabanlı protokoldür. TCS-BIN protokolü, çağrı kontrol fonksiyonlarını, grup yönetimi fonksiyonlarını ve cihazların gerçekte bağlantı kurulmadan çağrı işaretleşme bilgisi değişimi yapabilmelerini sağlayan metodu

içermektedir.

### **3.1.7.3. AT Komutları**

Bluetooth teknolojisinde kullanılan AT Komutları, ITU-T V.250 ve ETS 300 196 prosedürlerine dayanır. Ayrıca, faks servisleri için kullanılan komutlarda uygulama tarafından belirlenmiştir. Pek çok profil (faks, çevirmeli ağ bağlantısı, kulaklıklılı telefon gibi) TCS-BIN protokolünü kullanmak yerine, RFCOMM üzerinden AT komutlarını kullanmayı tercih eder.

### **3.1.8. Uyarlanmış Protokoller**

#### **3.1.8.1. PPP**

PPP, RFCOMM üzerinde çalışarak noktadan noktaya bağlantı kurmak için tasarlanmıştır. PPP, IETF (Internet Engineering Task Force) noktadan noktaya protokolüdür. PPP ağ yapısının anlamı, IP paketlerini PPP katmanından alarak LAN'a yerleştirmektir. Bluetooth linki üzerinden ağ erişim noktasına bağlanmak için internet PPP (Point-to-Point Protocol) protokolünü kullanır. PPP bağlantısı kurulduktan sonra standart internet protokolleri ağla etkileşim için kullanılır.

#### **3.1.8.2. TCP/UDP/IP**

Bu protokollerin standartları IETF tarafından tanımlanmıştır. Günümüzde dünyada en çok kullanılan protokol ailesidir. TCP/IP yığını yazıcılar, el bilgisayarları, mobil telefonlar gibi pek çok cihazda bulunmaktadır. Bu protokollere erişim, geleneksel socket programlama arayüz modeli kullanıldığı halde işletim sisteminden bağımsızdır. Bluetooth cihazlarında bu standartların uygulanması, internete bağlı herhangi bir cihaz ile haberleşmeyi mümkün kılmaktadır. Bu Bluetooth cihazı bir hücresel telefon ya da internet için köprü (bridge) görevi gören bir veri erişim noktası olabilir. TCP/IP/PPP, Bluetooth 1.0 ve OBEX'in gelecekteki versiyonları için, internet köprüsünü kullanım senaryolarında yer almaktadır.

#### **3.1.8.3. IrDA**

IrDA (Infrared Data Association ), kablosuz cihazlar arasında veri alış verişi ve senkronizasyonu için protokoller tanımlar. SIG, IrDA protokollerinin ve veri modellerinin pek çoğunu olduğu gibi kullanır; çünkü IrDA ve Bluetooth kablosuz haberleşme teknolojisi, bazı önemli ortak özellikleri, kullanım senaryolarını ve uygulamalarını paylaşmaktadır.

Verinin cihazlar arasında alışverişinde en temel gereksinim, biçim(format) tanımını hem sentaks hem de semantik açıdan yapmaktır. OBEX (Object Exchange) ve IrMC (Infrared Mobile Communications) protokolleri IrDA tarafından tanımlanmış protokollerdir. IrMC, aynı nesneler arasında senkronizasyonu sağlamaktadır.

#### **3.1.8.4. OBEX**

IrOBEX (Infrared Object Exchange ) ya da kısaca OBEX protokolü, IrDA tarafından nesneleri basit ve anında değiş tokuş etmek amacıyla geliştirilmiş bir oturum protokolüdür. OBEX, HTTP' ye benzer temel bir fonksiyonu bir istemci-sunucu modeli kullanarak ve iletim mekanizmasından bağımsız olarak daha basit bir şekilde gerçekleştirmektedir. OBEX ayrıca, nesneleri ve operasyonları sunmak için bir model tanımlamaktadır. Ek olarak, OBEX protokolü, dosya-listeleme nesnesi tanımlar; bu nesne uzak cihazlardaki dosyaların içeriğinde tarama yapmak için kullanılır. İlk aşama da RFCOMM OBEX için tek transfer katmanı olarak kullanılmıştır. Gelecekteki uygulamaların, TCP/IP kullanması da beklenmektedir.

#### **İçerik Formatları**

VCard, vCalender "Internet Mail Consortium" tarafından kontrol edilen açık spesifikasyonlardır. Bu spesifikasyonlar sırası ile elektronik iş kartı ve kişisel takvim girdileri ile düzenlemelerinin formatını tanımlarlar. vCard ve vCalender herhangi bir iletim mekanizması tanımlamaz; aktarılan veriye bağlı olan biçimi tanımlar. vCard ve vCalender'i benimseyerek, iyi tanımlanmış ve desteklenen biçimlerin yardımıyla SIG, kişisel bilgilerin alışverişini daha iyi yapacaktır. vCard ve vCalender spesifikasyonları Internet Mail Consortium tarafından elde edilebilir ve IETF tarafından geliştirilmiştir.

Bluetooth teknolojisinde OBEX tarafından aktarılan diğer içerik formatları arasında vNote ve vMessage vardır. Bu içerik formatları da açık standartlardır ve mesaj ve notların alışverişi için kullanılırlar. Bu formatlar, cihazlar arasında veri senkronizasyonu yaparken gereken kütük dosyaları için de format tanımlayan, IrMC spesifikasyonu tarafından tanımlanmıştır.

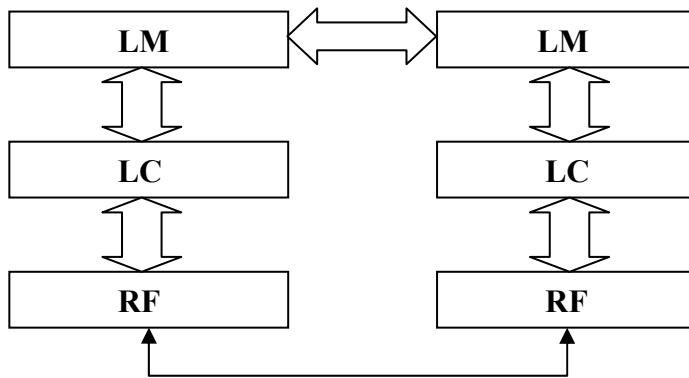
#### **3.1.9. Temel Bant Katmanı**

##### **3.1.9.1. Genel Bilgi**

Temel bant katmanı, Bluetooth protokol mimarisinde OSI referans modelinin fiziksel katmanına karşılık gelir. Güvenlik, hop seçimi, hata düzeltme ve veri temizleme gibi görevleri vardır. Bunlara ek olarak, cihazlar arasındaki fiziksel kanalları ve linkleri yönetir ve kontrol eder. Temel bant katmanı protokol yığınının radyo katmanı üzerinde yer almaktadır. Temel bant protokolü bir link denetleyicisi (LC-Link Controller) olarak tasarlanmıştır.

Link Denetleyicisi, bir üst katmanda yer alan, Link Yöneticisi (LM-Link Manager) ile birlikte, link bağlantısı ve güç kontrolü gibi link seviyesi işlemlerini yerine getirmek için ortak çalışır. Şekil 3.11' de Link katman yapısı görülmektedir.

Bu katman eşzamanlı ve eşzamanlı olmayan linkleri kontrol eder ve yönetir. Ayrıca, sorgu (inquiry) ve çağrı(paging) işlemleri bu katmanda gerçekleşir. Yerel ve uzak Link Denetleyicileri, LM tarafından komut verildikten sonra, linki paket paket kurar ve daha sonra kurulan linki korur.



Şekil 3.11. Link katmanı

### 3.1.9.2. Frekans Bandı ve RF Kanalları

Bluetooth teknolojisi 2.4 GHz ISM bandında çalışmaktadır. Bu bant lisanssız ve herkese açık olmasına rağmen, gerçek frekans aralığı ve bant genişliği ülkeden ülkeye değişebilir. Amerika’da ve Avrupa’da 1 MHz aralıklarla yerleşmiş 79 RF kanalı bulunan, 83.5 MHz lik bant genişliğine sahip bir bant kullanılırken, Japonya, İspanya ve Fransa’da 1 MHz aralıklarla dizilmiş 23 RF kanalına sahip, daha küçük bir bant kullanılmaktadır. Çizelge 3.3’de kullanılan frekans bantlarının ülkelere göre durumu görülmektedir.

Çizelge 3.3. RF kanalları ve frekans bandı

| ÜLKE          | FREKANS ARALIĞI     | RF KANALLARI               |                  |
|---------------|---------------------|----------------------------|------------------|
| Avrupa ve USA | 2400 – 2483.5 Mhz   | $f = 2402 + k \text{ Mhz}$ | $k = 0 \dots 78$ |
| Japonya       | 2471 – 2497 Mhz     | $f = 2473 + k \text{ Mhz}$ | $k = 0 \dots 22$ |
| İspanya       | 2445 – 2475 Mhz     | $f = 2449 + k \text{ Mhz}$ | $k = 0 \dots 22$ |
| Fransa        | 2446.5 – 2483.5 Mhz | $f = 2454 + k \text{ Mhz}$ | $k = 0 \dots 22$ |

### 3.1.9.3. Zaman Dilimleri

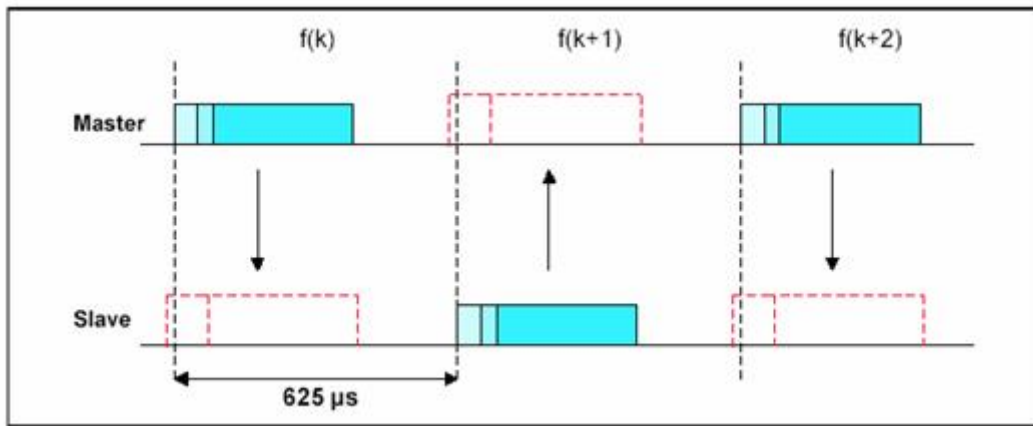
Kanal her biri 625  $\mu$ s uzunluğunda zaman aralıklarına bölünmüştür. Zaman aralıkları piconet master’ının Bluetooth saatine göre numaralandırılır. Dilimlerin numaraları 0 ile  $2^{27}-1$  arasında değişir. Zaman dilimlerinde master ve slave paketleri gönderebilir. Master ve slave gönderdiğinde kullanılan TDD (Time Division Duplex) şeması Şekil 3.14’de görülmektedir.

Master paketleri göndermeye çift numaralı zaman dilimlerinden başlar iken, slave tek numaralı zaman dilimlerinden başlar. Paket başlangıcı zaman dilimi başlangıcına göre ayarlanır. Master ya da slave tarafından gönderilen paketlerin uzunluğu maksimum 5 zaman dilimi olabilir. Paket süresince RF atlama frekansı sabit kalmalıdır. Tek bir paket için kullanılan RF atlama frekansı o andaki Bluetooth saati değerinden türetilir. Çok dilimli paketler (multi-slot packets) için, tüm pakette kullanılan RF atlama frekansı, paketin birinci dilimindeki Bluetooth saatinin değerinden türetilir. Eğer bir paket birden fazla

zaman dilimi içeriyorsa, paket gönderiminin başladığı zaman dilimindeki atlama frekansı, atlama frekansı olarak alınır.

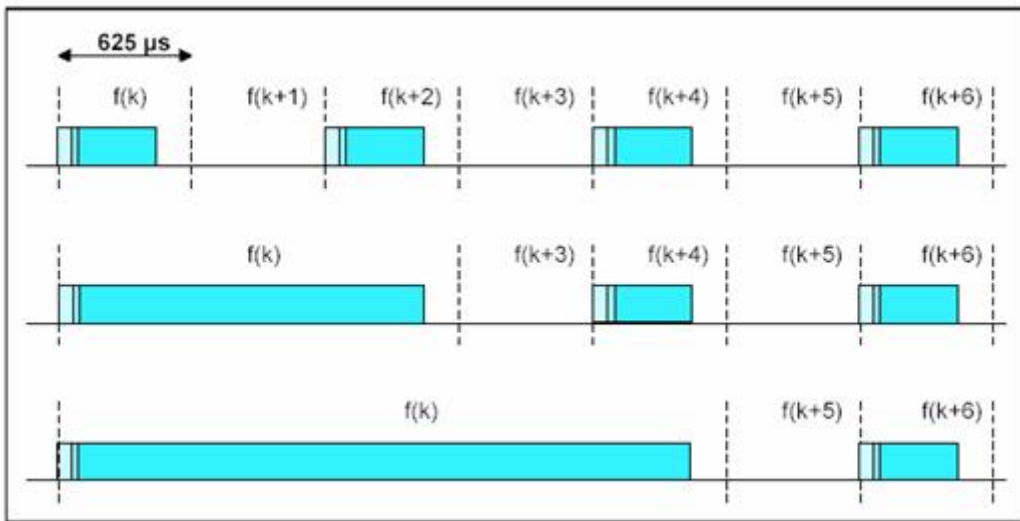
#### 3.1.9.4. Kanal Tanımı

Kanal, 79 veya 23 RF kanalı boyunca rasgele belirlenen atlama sırası (hopping sequence) ile ifade edilir. Atlama sırası, master'ın Bluetooth cihaz adresi ile belirlenir ve her bir piconet için tektir. Atlama sırasındaki faz masterin Bluetooth saati tarafından belirlenir. Kanal zaman aralıklarına bölünmüştür. Her bir aralık RF atlama frekansına karşılık gelmektedir; ardışık atlamalar farklı RF atlama frekansına denk gelir. Nominal atlama oranı (hop rate) 1600hop/sn dir. Piconet içerisindeki Bluetooth üniteleri kanal ile senkronize zaman ve atlamaya sahiptir. Şekil 3.12' de TDD ve zamanlama yapısı görülmektedir.



Şekil 3.12 . TDD ve zamanlama

Tek paketlerdeki ve çok-dilimli paketlerdeki atlama yapısı Şekil 3.13'de gösterildiği gibidir.



Şekil 3.13. Çok-Dilimli paketler (Subramani ve ark., 2003).

**3.1.9.5. Modülasyon ve Bit Hızı**

Gönderilen verinin sembol hızı 1 Mbit/sn'dir. 0.5 BT (Bandwidth Time) değeri ile Gaus şekilli ikili FSK (Frequency Shift Keying) modülasyonu kullanılır. Maksimum frekans değişimi 140 KHz ile 175 KHz arasında olmalıdır.

**3.1.9.6. Fiziksel Linkler**

Master olarak çalışan cihaz ile slave rolündeki cihaz arasında bir link kurulur. Link kurulduktan sonra, iki temel tipte veri paketi alışverişi yapılır; bu paketler arasında önemli bir fark vardır ve ACL ve SCO link tipleri ile karakterize edilirler.

**3.1.9.7. ACL**

Bağlantı kurulu olduğu sürece, master ile slave arasında ACL linki vardır. Master, herhangi bir anda farklı slave'lere doğru, birden fazla ACL linkine sahip olabilir; fakat iki cihaz arasında sadece bir link kurulur. Master her zaman aynı slave'e düzenli olarak gönderim yapmaz. Dolayısıyla, ACL linki veri alışverişinin rasgele olduğu ve veri yığının üst katmanlarından elde edilebilir olduğu zaman, paket-anahtarlama bağlantı sağlamaktadır. Hangi slave'e veri gönderileceği ya da hangi slave'den veri alınacağı, master'a bağlıdır ve hem zaman uyumlu (eşit zaman aralıklı) hem de zaman uyumsuz servisler mümkündür. Pek çok ACL paketi gönderilen verinin doğruluğunu kontrol etmek için, hata kontrolü ve yeniden iletim işlemlerini gerçekleştirmektedir.

ACL linkleri, veriyi LMP ve L2CAP katmanlarının ikisinden alır ya da ikisine verir. Bütün kullanıcı verisi L2CAP üzerinden geçer ve L2CAP paketleri gibi Temel bant katmanına geçer. Linklerin konfigürasyonu ve kontrolü iki zıt Link Yöneticisi(LM) tarafından yapılır ve ilgili komut ve kontrol verisi temel bant katmanına LMP paketleri gibi geçer. Veri, DH (Data High rate) ve DM (Data Medium rate) paketlerinde taşınır. DM paketleri daha az veri taşır ama hata koruması sağlar.

Eğer slave önceki Master-to-Slave diliminde adreslenmiş ise, sonraki Slave-to-Master diliminde sadece ACL paketi ile cevap verebilir. Eğer slave paket başlığındaki slave adresini çözemez ise, o paketin adreslenip adreslenmediğinden emin olamaz ve cevap vermesine izin verilmez. "Broadcast" paketleri, belli bir slave'e adreslenmemiş ACL paketleridir; dolayısıyla her slave tarafından alınabilirler.

**3.1.9.8. SCO**

SCO linki, ayrılmış kanal bant genişliği ve periyodik veri alış verişi ile, master ile slave arasında simetrik (aynı anda alma-verme) bir link kurar. Master rezerve edilmiş zaman bölmelerinde SCO linkleri kurar. Böylece, SCO linki düzenli veri alış verişi olduğunda devre-anahtarlama bağlantı sağlar. Bu link ses gibi eşit zaman aralıklı (zaman sınırlı) bilgiler için kullanılır.

Master aynı slave'e ya da farklı slave'lere maksimum üç SCO linkini destekleyebilir. Slave aynı master'den gelen üç SCO linkini destekleyebilir. SCO verisinin zaman sınırlı yapısı nedeniyle, SCO paketleri asla yeniden gönderilmezler. Master SCO paketlerini slave'e Tscs parametresi ile belirlenen düzenli aralıklarla gönderir. Bu "SCO süresi" olarak

adlandırılır ve bölmelerde (slot) hesaplanır. Slave'in paket başlığını doğru çözdüğü ve beklenildiği gibi adreslenmediği keşfedildiği sürece, her zaman rezerve edilmiş zaman bölmesinde SCO paketi ile cevap vermesine izin vardır. Eğer hatalardan dolayı paket yanlış çözülürse, bölme rezerve edilmiş ise slave cevap verebilir. Gerçekte, normal işlemlerde, Master'ın rezerve edilmiş bölmede herhangi bir yere iletim yapma izni yoktur. Ancak, "broadcast" LMP mesajlarının SCO linkleri üzerinde önceliği vardır.

SCO linki, master'dan slave'e LM komutu ile kurulur. Bu mesaj, rezerve edilmiş dilimi belirlemek için SCO zamanı Tsc0 veya başlangıç konumu Dsc0 gibi zamanlama parametrelerini içerir. Cihaz, SCO linkinin içeriğini korumak için SCO bölmeleri civarındaki ACL trafiğini planlamak zorundadır. İstisna olarak, Link Yöneticisi kontrol paketleri SCO linkinin üzerine yazma iznine sahiptirler.

### 3.1.10. Bluetooth Adres Çeşitleri

Bluetooth cihazlarına dört tip adres verilebilir. Bu adres çeşitleri: BD\_ADDR, AM\_ADDR, PM\_ADDR ve AR\_ADDR'dir.

**BD\_ADDR (Bluetooth Cihaz Adresi) :** Her Bluetooth alıcısı donanım vasıtasıyla kırkık içine yazılan 48 bit uzunluğunda tek bir cihaz adresine sahiptir. Bu adres üç kısımdan oluşmaktadır. Bunlar: LAP(en az anlamlı ilk 24 bit), NAP (24-31 bitleri arası önemsiz adres kısmı) ve UAP(en anlamlı son 8 bit)'dir.

**AM\_ADDR (Aktif Üye Adresi) :** Bu adres, 3 bit uzunluğunda lojik bir adrestir. Örneğin, piconet kapsama alanı dışına çıkmış bir üye bu adresini kaybeder ve yeniden katılmak ister ise, kendisine kullanılmayan rasgele bir AM\_ADDR adresi verilir. Bir piconet'te maksimum yedi slave ve bir master olabileceğine göre, 3-bitlik adresleme ile, 0-7 arası numaralandırılmış adresler birimlere atanabilir. 0 numaralı adres master tarafından 'broadcast' paketleri için kullanılır.

**PM\_ADDR (Park Adresi) :** Bu adres 8 bit uzunluğunda lojik bir adrestir. Aktif olmayan, dinlenmeye çekilmiş slave birimlerine atanan geçici bir adrestir. Böylece bu adres ile park halindeki slave'ler birbirinden ayırt edilebilir.

**AR\_ADDR (Erişim İstek Adresi) :** Bu adres daha önce park halinde bulunan bir slave birim tarafından, slave master'a yarım zaman bölmesinde şebekeye dahil edilme mesajını gönderirken kullanılır. Bu adresin ömrü park süresi kadardır; slave biriminin şebekeye katılma isteği kabul edildikten sonra bu adresin geçerliliği kaybolur.

### 3.1.11. Bluetooth Paket Yapıları

#### 3.1.11.1. Genel Paket Formatı

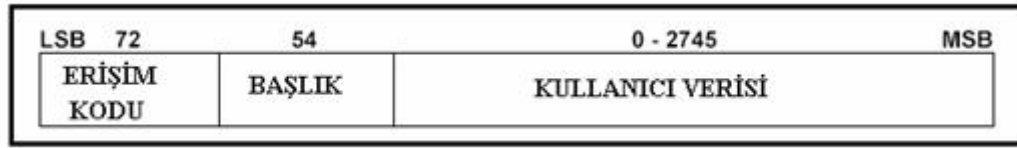
Temel bant spesifikasyonunda paketleri ve mesajları tanımlarken, bit sıralaması "Little Endian" formatındadır. Bu formata göre şu kurallar geçerlidir:

- En az anlamlı bit (Least Significant Bit – LSB), b<sub>0</sub> bitine tekabül eder.
- İletim ortamına gönderilen ilk bit LSB'dir.

- Tüm paket biçimlerinde LBS en solda yer alır.

Temel bant denetleyicisi üst katmanlardan gelen, ilk biti  $b_0$  olarak yorumlar; bu bit iletim ortamına gönderilecek ilk bittir. Temel bant seviyesinde yaratılan paket başlık(header) alanı ve kullanıcı verisi (payload) başlık uzunluğu gibi veri alanları ilk olarak LSB tarafından iletilir. Örneğin,  $b_0b_1b_2=110$  gibi 3 bit'lik bir parametrenin iletileceğini farz edelim. İlk olarak 1 bit'i gönderilir; 0 bit'i en son iletilir.

Piconet kanalındaki veri paketler şeklinde taşınır. Genel paket formatı Şekil 3.14'de gösterildiği gibidir. Her bir paket üç kısımdan oluşur: Erişim kodu (access code), başlık (header) ve kullanıcı verisi (payload).

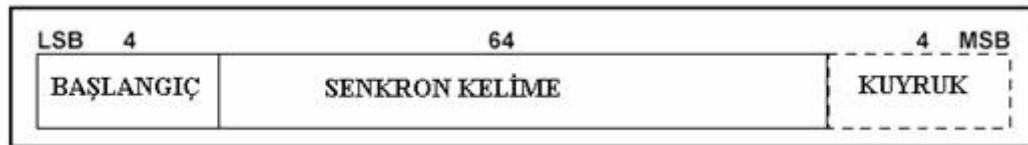


Şekil 3.14. Genel paket formatı (Feifer P. ve ark., 2004).

Erişim kodu ve başlık alanı sırasıyla 72 bit'lik ve 54 bit'lik sabit uzunluğa sahiptir. Kullanıcı verisi ise 0 ile 2745 bit arasında değişebilen değişken bit uzunluğudur. Bir paket fonksiyonuna göre sadece erişim kod alanını, hem erişim kod alanını hem de başlık alanını ve her üç alanı da içerebilmektedir.

### 3.1.11.2. Erişim Kodu

Bluetooth şebekelerinde master ve slave birimler arasındaki iletişim için kullanılan her türlü paket mutlaka erişim kodu taşınmalıdır. Eğer iletilen paket başlık kısmını içeriyorsa erişim kod alan uzunluğu 72-bit olur, aksi takdirde 68-bit uzunluğunda olur. Yani paket yapısında başlık kısmının olması durumunda 4-bitlik kuyruk alanı (Trailer) erişim koda eklenmektedir, aksi halde kuyruk kısmı yer almaz. Bir piconet şebekesinde iletilen bütün paketler aynı kanal erişim koduna sahiptirler, böylece erişim kodu piconeti tanımlar. Erişim kodu DC ofset kompanzasyonu, senkronizasyon tanımlama için kullanılır. Erişim kod formatı şekil 3.15'de verilmiştir.



Şekil 3.15. Erişim kodu formatı (İlhan, 2002)

Erişim kodu aynı zamanda anons (paging) ve sorgu (inquiry) prosedürleri içinde kullanılır. Erişim kodu üç alandan oluşmaktadır: başlangıç alanı (preamble), senkron kelime alanı ve kuyruk alanı (trailer). Bluetooth teknolojisi üç erişim kod tipi tanımlar

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

Bu erişim kodları Bluetooth cihazlar arasında farklı işlemler için kullanılır. CAC piconeti belirler ve her piconet için tekildir. Kanal erişim paketi piconet şebekesinde taşınan tüm paketlerde yer alır. Cihaz erişim kodu (DAC) ise anons (paging) ve anonsa cevap gibi özel amaçlı işaretlemeler için kullanılır.

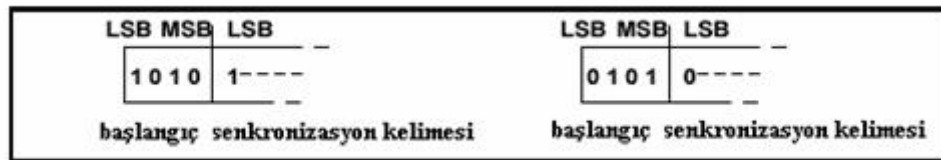
Sorgu erişim kodu iki çeşittir. Bunlardan biri genel sorgu erişim kodu (GIAC) diğeri ise atanmış sorgu erişim kodu (DIAC) dur. GIAC kapsama alanı içindeki cihazların belirlenmesinde kullanılır. DIAC ise ortak bir karakteristiğe sahip birimlerden oluşan bir grup için kullanılır. Kanal erişim kodu başlık alanı gerektirirken diğer erişim kodu gerektirmez. Farklı erişim kod tipleri farklı bluetooth cihaz adresinin LAP alanını kullanır. LAP alanı senkronizasyon kelimesinin oluşturulmasında kullanılır. Erişim kod tipleri ve bu tiplerin kullandıkları LAP türleri Çizelge 3.4’de verilmiştir.

Çizelge 3.4. Erişim kodu tipleri ve LAP

| Erişim Kod Tipi | LAP (24-bit)        | Kod uzunluğu |
|-----------------|---------------------|--------------|
| CAC             | Master              | 72           |
| DAC             | Anons Edilmiş Birim | 68 / 72      |
| GIAC            | Rezerve Edilmiş     | 68 / 72      |
| DIAC            | Atanmış             | 68 / 72      |

### 3.1.11.3. Başlangıç (Preamble)

Başlangıç alanı DC kompanzasyonu sağlamak için kullanılan, 4 bit uzunluğunda bir yapıdır. Senkronizasyon kelimesinin en az anlamlı bitinin 1 veya 0 olmasına göre, 4 bit’lik sıralama 1010 veya 0101 şeklinde olabilir. Şekil 3.16’da bu yapı gösterilmektedir.



Şekil 3.16. Başlangıç alanı

### 3.1.11.4. Senkronizasyon Kelimesi

Senkronizasyon kelimesi 24 bit’lik LAP (en düşük anlamlı ilk 24 bit) alanından türetilen 64 bit uzunluğunda bir kod kelimesidir. CAC erişim kod türü için şebeke içerisindeki her birim master’a ait LAP alanını kullanır. DAC için slave birim kendi LAP alanını kullanırken, GIAC ve DIAC için rezerve edilmiş ve atanmış LAP alanları kullanılmaktadır. Ek olarak, senkronizasyon kelimesinin iyi oto korelasyon özellikleri, senkronizasyon işleminin zamanlamasını iyileştirmektedir.

### 3.1.11.5. Kuyruk (Trailer)

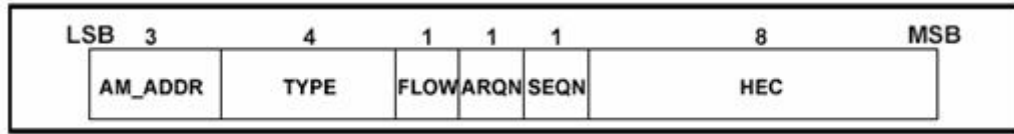
Paket başlığı, erişim kod alanını izlediği sürece, kuyruk alanı pakete eklenmektedir. Bu durum CAC tipi erişim kodunda görülür. Bununla birlikte, eğer DAC ve IAC kodları çağrı ve sorgu cevabı prosedürlerinde alınıp verilen FHS paketlerinde kullanılıyorsa kuyruk kısmı DAC ve IAC erişim kodlarında da kullanılır. Kuyruk kısmı 4 bit'ten oluşmaktadır. Bit dizilişi en anlamlı bitin( Most Significant Bit – MSB) 0 ya da 1 olmasına göre 1010 ya da 0101 olabilir. Şekil 3.17’de anlamlı bitin 0 ya da 1 olması durumundaki kuyruk yapısı görülmektedir.



Şekil 3.17. Kuyruk

### 3.1.11.6. Paket Başlığı (Packet Header)

Paket başlık alanı link denetleyici (LC) bilgisi taşımakta olup altı parçadan oluşur. Paket başlık formatı Şekil 3.18’de verilmiştir.



Şekil 3.18. Paket Başlık Formatı

Toplam paket başlık alanı 18-bit uzunluğundadır. Temel prensibi her biti üç kez tekrarlayan 1/3 FEC algoritması kullanılarak paket başlık alanı 54-bit uzunluklu yapılır. FEC tekrarlama algoritmasının temel kullanım amacı önemli bilgiler taşıyan paket başlık alanını hatalara karşı daha dayanıklı yapmaktır. Böylece hedef alıcıya hatalardan dolayı ulaşmayan paketlerin oranı da azalır ( İlhan, 2002).

### 3.1.11.7. Aktif Üye Adresi (AM\_ADDR)

AM\_ADDR, piconet içerisinde aktif olan bir üyeye ait üye adresini belirtmektedir. Piconet’te bir veya birden fazla slave tek bir master’a bağlanmıştır. Slave’leri birbirinden ayırt etmek için, her bir slave’e slave aktif olduğu zaman kullanılan 3 bitlik geçici bir adres atanır. Master ve slave arasında iletilen tüm paketler slave birimine ait olan bu adres bilgisini taşımaktadır. Tüm bit’lerin 0 olduğu 000 adresi master’dan tüm slave’lere gönderilen ‘broadcast’ paketi için rezerve edilmiştir. İstisna olarak, sadece FHS paketleri bu adresi kullanabilir. Piconet ile bağlantısı kesilen veya park (dinlenme) durumuna geçen bir slave AM\_ADDR adresini kaybeder. Eğer bu slave piconet’e tekrar katılmak isterse master tarafından kendisine yeni bir AM\_ADDR adresi verilir.

**3.1.11.8. Paket Tipi (TYPE)**

On altı farklı tipte paket tanımlanabilmektedir. Hangi paket tipinin kullanıldığını 4 bit paket tipi kodu belirler. Paket tipi kodunun yorumlanması, paket ile ilgili fiziksel link tipine bağlı olarak değişir. İlk olarak paket SCO linki üzerinden mi ACL linki üzerinden mi gönderiliyor ona karar verilir. Daha sonra, hangi tip ACL ya da SCO paketinin alındığı belirlenir. Ayrıca, paket tipi alanı paketin kaç tane bölmeden oluştuğu bilgisi de taşır. Bu şekilde, alıcı konumda olmayan birimlerin, artan zaman dilimlerinde kanalı meşgul etmesi engellenir.

**3.1.11.9. Akış Kontrol Alanı (Flow)**

Bu bit ACL link üzerindeki paketlerin akış kontrolü için kullanılır. Alıcıdaki ACL link için ayrılmış tampon bellek dolu ise ve boşaltılmazsa, verinin geçici olarak iletimini durdurmak için, alıcı geriye bir Dur bit'i (Flow=0) gönderir. Dur işareti sadece ACL tipi paketler için geçerlidir. Alıcı sadece kontrol bilgisini taşıyan paketleri (ID, POLL, NULL paketleri) ya da SCO paketlerini alamaya devam eder. Tampon bellek boşaldığı zaman, geriye bir Git bit'i (Flow=1) gönderilir. Eğer hiçbir paket alınmaz ya da alınan başlık hatalı olursa, alıcı taraf bunu Git bit'i olarak yorumlayacaktır.

**3.1.11.10. Doğrulama Alanı (ARQN)**

Alıcı taraf CRC alanını da kapsayan, kullanıcı verisini başarılı bir şekilde aldığı zaman bunu kaynağa bildirmek amacıyla geriye bir doğrulama biti göndermektedir. ARQN bit'i negatif veya pozitif doğrulama bilgisini içerebilir. Paket iletimi başarılı oldu ise geriye pozitif ACK (ARQN=1), eğer başarısız oldu ise geriye negatif NAK (ARQN=0) gönderilir. Burada ACK ve NAK sırasıyla pozitif bilgi ve negatif bilgi anlamını taşır. Verici bir doğrulama mesajı almaz ise paket iletiminin başarısız olduğunu düşünür ve NAK olarak yorumlar. İletimin başarısı CRC (Cyclic Redundancy Check) kodu ile kontrol edilir.

**3.1.11.11. Sıralama Alanı (SEQN)**

SEQN bit'i veri paketlerini sıralamak için, sıralama numarası şeması hazırlar. Veriyi CRC kodu ile birlikte içeren her yeni gönderilen pakette SEQN bit'inin evriği alınır. Bu yöntem hedef alıcıya giden paketleri bir filtreden geçirmek için kullanılmaktadır. Bir paket sadece bir kez gönderilmektedir; eğer başarısız ACK bildiriminden dolayı bir paket tekrar gönderilmiş ise alıcı aynı paketten iki tane alır. Bu durumda alıcı ardışık iki paket karşılaştırılır ve fazla olanı atar.

**3.1.11.12. Hata Kontrol Alanı (HEC)**

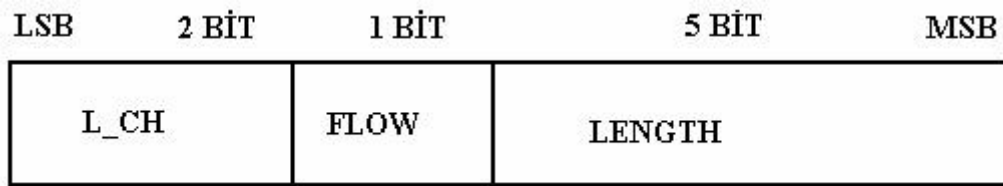
Her bir başlık alanı kendi içerisinde başlığın bütünlüğünü test etmek amacıyla bir başlık hata kontrol alanı (HEC) içerir. 8 bit'ten oluşan HEC (Header Error Check) alanı özel bir polinom olan polinom 647 tarafından üretilmiştir. HEC üretici HEC alanı üretilmeden önce 8 bit bir değer ile koşullandırılır. Daha sonra, HEC 10 bit'lik başlık için hesaplanır. Alıcı HEC alanını kontrol etmeden önce, HEC kontrol devresini hazırlamalıdır.

**3.1.11.13. Kullanıcı Verisi (Payload)**

Kullanıcı verisi alanı için ses ve veri paketleri birbirinden farklılık göstermektedir. SCO paketleri sadece ses alanı, ACL paketleri sadece veri alanı içerirken, DV paketleri hem ses hem de veri alanı içermektedir. Ses alanı sabit uzunluktadır. Veri alanı (ACL paketleri) üç kısımdan oluşmaktadır: Kullanıcı verisi başlığı, veri gövdesi ve CRC alanı.

**3.1.11.14. Kullanıcı Verisi Başlığı (Payload Header)**

Bu alan sadece ACL paketlerinde bulunmaktadır. Kullanıcı verisi başlık alanı 8 bit uzunluğundadır ve Şekil 3.19’da görüldüğü gibi üç kısımdan oluşur.



Şekil 3.19. Kullanıcı verisi başlık formatı (Tek Zaman Bölmeli)

**L-CH:** Bluetooth şebekelerinde kullanılan lojik kanalları sınıflandırmak için kullanılan 2 bit uzunluğunda bir alandır. Bu 2 bit ile 4 adet farklı lojik kanal tanımlanabilir.

**FLOW:** Veri akışını gösteren bir bittir. LMP PDU’larını taşıyan DM1 paketleri için her zaman 1 değerindedir.

**LENGTH:** Kullanıcı verisinin büyüklüğünü gösteren 5 bit uzunluğunda bir kısımdır.

**3.1.11.15. Veri Gövdesi (Payload Body)**

Kullanıcı verisini taşıyan ve gerçek veri hızını tanımlayan kısımdır. Bu alan büyüklüğü length alanında belirtilmektedir.

**3.1.11.16. CRC Alanı**

CRC alanı hata kontrolü için kullanılır ve özel bir polinomdan hesaplanır. Verinin doğru iletilip iletilmediği alıcı tarafından doğrulanır.

**3.1.11.17. Paket Tipleri**

Piconet içerisinde kullanılan paketler kullanılan fiziksel link (SCO, ACL) tipine bağlıdır. Bu SCO ve ACL linklerinin her biri için 12 adet farklı paket tipi tanımlanmıştır. 4 adet kontrol paketi iki link tipi için ortaktır. Paket tipi (TYPE) ise link tipine bakmaksızın her bir paket için taktır. Link’teki farklı paketleri belirlemek için 4 bit’lik tip kodu (TYPE code) kullanılmaktadır. Paket tipleri 4 bölüme ayrılmıştır. İlk bölüm tüm fiziksel link tiplerinde ortak olan 4 kontrol paketi için rezerve edilmiştir. İkinci bölüm, tek zaman bölmeli 6 adet paket tipi için ayrılmıştır. Üçüncü bölümde, 4 adet üç zaman bölmeli paket bulunur. Son olarak dördüncü bölüm, beş zaman bölmeli 2 adet paket için rezerve

edilmiştir. Paket tipinden kaç adet zaman bölmesi içerdiği anlaşılabilir.

Çizelge 3.5’de SCO ve ACL linkleri için tanımlanmış Bluetooth paket tipleri özetlenmektedir.

Çizelge 3.5. Bluetooth paket tipleri.

| BÖLÜM | TİP KODU<br>$b_3b_2b_1b_0$ | ZAMAN<br>BÖLMESİ | SCO link | ACL link |
|-------|----------------------------|------------------|----------|----------|
| 1     | 0000                       | 1                | NULL     | NULL     |
|       | 0001                       | 1                | POLL     | POLL     |
|       | 0010                       | 1                | FHS      | FHS      |
|       | 0011                       | 1                | DM1      | DM1      |
| 2     | 0100                       | 1                | tanımsız | DH1      |
|       | 0101                       | 1                | HV1      | tanımsız |
|       | 0110                       | 1                | HV2      | tanımsız |
|       | 0111                       | 1                | HV3      | tanımsız |
|       | 1000                       | 1                | DV       | tanımsız |
|       | 1001                       | 1                | tanımsız | AUX1     |
| 3     | 1010                       | 3                | tanımsız | DM3      |
|       | 1011                       | 3                | tanımsız | DH3      |
|       | 1100                       | 3                | tanımsız | tanımsız |
|       | 1101                       | 3                | tanımsız | tanımsız |
| 4     | 1110                       | 5                | tanımsız | DM5      |
|       | 1111                       | 5                | tanımsız | DH5      |

### 3.1.11.18. Ortak Paket Tipleri

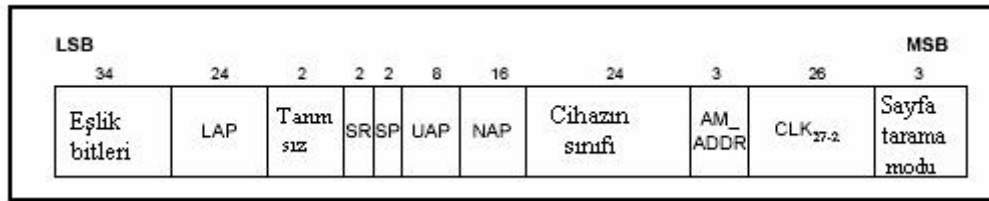
Toplam 5 çeşit ortak paket tipi bulunur. Çizelge 3.5’de bölüm 1 deki paketlere ek olarak listelenmemiş bir de ID paket tipi vardır.

**ID Paketi:** ID paketi cihaz erişim kodu (DAC) ya da sorgu erişim kodu (IAC) taşımaktadır. Sabit paket uzunluğu 68 bit’tir. Bu paket tipi çağrı (paging), sorgu (inquiry) ve cevap (response) işlemlerinde kullanılmaktadır.

**NULL Paketi:** Null paketi kullanıcı verisi (payload data) içermez. Dolayısıyla, sadece kanal erişim kodu ve paket başlığından oluşmaktadır. Toplam uzunluğu 126 bit’tir. NULL paket kaynağa link bilgisini geri iletmek için kullanılır. Bu bilgiler, önceki iletimin başarısı yani doğrulama bilgisi (ARQN) ya da alıcı taraftaki tampon belleğin statü bilgisi (FLOW) olabilir. NULL paket için doğrulama gerekmez.

**POLL Paketi:** Bu paket yapı olarak NULL paketine büyük ölçüde benzemektedir. POLL pakette kullanıcı verisi içermez. NULL paketinden farklı olarak bu paket alıcıdan kendisi için doğrulama mesajı istemektedir. POLL paketi ARQN ve SEQN alanlarını etkilememektedir. Alıcı durumundaki slave birim bu paketten aldığı zaman master'a cevap göndermek zorundadır. Böylece master bu paketi piconet içerisindeki slave birimleri yoklamak amacı ile kullanabilir. Çünkü slave birimler iletecek verisi olmazsa bile cevap vermek yani doğrulama mesajı yollamak zorundadır.

**FHS Paketi:** FHS paketi göndericinin Bluetooth cihaz adresini ve saat bilgisini taşıyan bir kontrol paketidir. Bu paket, 144 bilgi bit'inden oluşan kullanıcı verisi (payload) ve 16 bit CRC kodundan oluşur. Kullanıcı verisi 2/3 oranındaki FEC algoritmasıyla kodlanır ve 144 olan bit sayısı 240 değerine ulaşır. FHS paketi tek zaman bölmelidir. FHS kullanıcı verisinin formatı ve içeriği Şekil 3.20'de görüldüğü biçimdedir. Kullanıcı verisi 11 farklı kısım içermektedir. FHS paketleri master çağrı yanıtında, sorguya yanıtta ve master slave anahtarlama sırasında kullanılmaktadır. Çağrı yanıtında ve master slave anahtarlama sırasında FHS paketine doğrulama bilgisi gönderilmesine rağmen sorgu yanıtında doğrulama bilgisi gönderilmemektedir. FHS paketleri gerçek zaman saat bilgisini içermektedir ve her yeni iletimden önce bu saat bilgisi güncellenir.



Şekil 3.20. FHS kullanıcı verisi formatı

**DM1 Paketi:** DM1 paketi her link tipi için kontrol mesajlarını destekleyen özelliği dolayısıyla, Çizelge 3.5'te birinci bölümde yer almaktadır. DM1 paketi ayrıca düzenli kullanıcı verisini de taşımaktadır. SCO linki üzerinden DM1 paketi gönderildiği zaman verici eşzamanlı bilgiyi, kontrol bilgisi göndermek için kesebilir.

Çizelge 3.6' da link kontrol paketlerinin karakteristikleri özetlenmiştir. Burada kullanıcı verisi kısmı; FEC, CRC ve kullanıcı verisi başlığı hariç paket kullanıcı verisini (payload) göstermektedir.

Çizelge 3.6. Link kontrol paketleri

| Tip  | Kullanıcı verisi (byte) | FEC | CRC | Maksimum simetrik hız | Maksimum asimetrik hız |
|------|-------------------------|-----|-----|-----------------------|------------------------|
| ID   | yok                     | yok | yok | yok                   | yok                    |
| NULL | yok                     | yok | yok | yok                   | yok                    |
| POLL | yok                     | yok | yok | yok                   | yok                    |
| FHS  | 18                      | 2/3 | var | yok                   | yok                    |

**3.1.11.19. SCO Paketleri**

SCO Paketleri senkron SCO linki üzerinde taşınırlar. Bu paketler CRC kod alanını içermezler; bu yüzden, hiçbir zaman tekrar gönderilmezler. SCO paketleri verici tarafından eşzamanlı giriş/çıkış ses port'una yönlendirilir. SCO paketleri 64 Kbit/sn hızda konuşma (ses) iletimi için kullanılmaktadır.

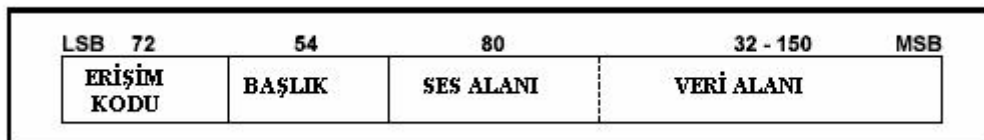
**HV1 Paketi:** HV1 paketi 10 byte'lık bilgi taşımaktadır. Paket içindeki bilgi 1/3 oranındaki FEC algoritmasıyla korunur. HV1 paketleri CRC alanı içermezler. Sabit kullanıcı verisi uzunluğu 240 bit'tir. Bu paket tipi, kullanıcı verisi başlığı da içermez. HV paketleri yüksek kalitede ses iletimini desteklemektedir. Ses paketleri asla tekrar iletilmezler dolayısıyla CRC alanına ihtiyaç duymazlar. HV1 paketleri 64 Kbit/sn hızıyla 1.25 ms konuşma taşırlar bu yüzden HV1 paketlerinin her iki zaman bölmesinde bir gönderilmeleri gerekir. Yani, Tscs değeri 2'dir.

**HV2 Paketi:** HV2 paketleri 20 byte'lık bilgi taşırlar. Bu bilgi 2/3 oranındaki FEC algoritmasıyla korunmaktadır. CRC alanı içermezler. Kullanıcı verisinin uzunluğu sabittir ve 240 bit'tir. Kullanıcı verisi başlık alanı da HV2 paketlerinde bulunmamaktadır. Ses iletimi için kullanılan HV2 paketleri, 64 Kbit/sn hızla 2.5 ms konuşma taşıyabilir. Dolayısıyla, HV2 paketleri her 4 zaman bölmesinde bir iletilmelidir. Yani, Tscs parametresinin değeri 4'tür.

**HV3 Paketi:** HV3 paketleri 30 byte uzunluğunda bilgi taşımaktadır. Bu bilgi FEC algoritmasıyla korunmaz ve CRC alanı içermezler. Kullanıcı verisinin uzunluğu 240 bit'tir. Kullanıcı verisi başlığı yoktur. HV3 paketleri 64 Kbit/sn hız ile 3.75 ms konuşma taşıyabilmektedir; bu yüzden her 6 zaman bölmesinde bir iletilmelidir. Yani, Tscs değeri 6'dır.

**DV Paketi:** DV paketi hem ses hem de veri alanı içeren bir pakettir. DV paketi kullanıcı verisi 80 bit ses alanı ve 150 bit veri alanı olarak Şekil 3.21'de görüldüğü gibi bölünmüştür.

Ses alanı FEC algoritmasıyla korunmamaktadır. Veri kısmı ise 1 byte kullanıcı verisi başlığını da içeren, 10 byte bilgi ve 16 bit CRC kodu taşımaktadır. Veri alanı 2/3 oranında FEC algoritmasıyla kodlanmıştır. DV paketleri, senkron ses içeriklerinden dolayı düzenli aralıklarla alıcıya gönderilmek zorunda olduğu için, SCO paket tiplerinin içerisinde yer alırlar. Alıcıda, DV paketinin ses ve veri alanlarına tamamen birbirinden bağımsız davranılır. Ses alanı normal SCO verisi gibi ele alınır ve asla yeniden iletilmez; yani ses alanı her zaman yenidir. Veri alanı ise hatalara karşı kontrol edilir ve eğer gerekli ise tekrar iletilir.



Şekil 3.21. DV paket formatı

SCO paketlerinin karakteristikleri Çizelge 3.7’ de özetlenmiştir. Burada kullanıcı verisi kısmı; FEC, CRC ve kullanıcı verisi başlığı hariç paket kullanıcı verisini (payload) göstermektedir. “v” harfi sadece veri kısmını simgelemektedir.

Çizelge 3.7. SCO paket tipleri

| PAKET TİPİ | KULLANICI VERİSİ BAŞLIĞI (BYTE) | KULLANICI VERİSİ (BYTE) | FEC     | CRC | MAKSİMUM SİMETRİK HIZ (KBİT/SN) |
|------------|---------------------------------|-------------------------|---------|-----|---------------------------------|
| HV1        | yok                             | 10                      | 1 / 3   | yok | 64.0                            |
| HV2        | yok                             | 20                      | 2 / 3   | yok | 64.0                            |
| HV3        | yok                             | 30                      | yok     | yok | 64.0                            |
| DV         | 1 V                             | 10+(0-9) V              | 2 / 3 V | var | 64.0+57.6 V                     |

### 3.1.11.20. ACL Paketleri

ACL paketleri eş zamanlı olamayan link’ler üzerinden taşınırlar. Taşınan veri kullanıcı verisi ya da kontrol verisi olabilir. DM1 paketi de dahil toplam yedi tane ACL paketi tanımlanmıştır. ACL paket tiplerinin altı tanesi CRC kod alanı içerir ve vericiye paketin hatalı olarak iletildiği bilgisi geri döner ise bu paket tekrar gönderilir. Yedinci ACL paketi çeşidi AUX1 ise CRC alanı içermez, bu yüzden bu paketin tekrar iletilmesi söz konusu değildir.

**DM1 Paketi:** DM1 paketi sadece veri bilgisi taşıyan bir pakettir. 1 byte kullanıcı verisi başlığı da dahil olmak üzere kullanıcı verisi (payload) toplam 18 byte bilgi ve 16 bit (2 byte) CRC kod alanı içerir. DM1 paketi tek zaman bölmelidir. Taşınan bilgi ve CRC alanının toplamı 2/3 oranında FEC algoritması ile kodlandığı zaman, her 10 bit’lik bölmeye 5 tane eşlik (parity) bit’i eklenir. Kullanıcı verisi başlığı sadece 1 byte uzunluğundadır ve yapısındaki Length kısmı sayesinde kullanıcı verisinin uzunluğu byte cinsinden belirlenebilir.

**DH1 Paketi:** DH1 paketi DM1 paket tipine büyük oranda benzemektedir. Ancak, DH1 paketinin kullanıcı verisi FEC algoritmasıyla kodlanmaz. Bu yüzden bu paket 16 bit’lik CRC koduna ek olarak 28 byte’lık bilgi taşıyabilmektedir. DH1 paketi de tek zaman bölmelidir.

**DM3 Paketi:** DM3 kullanıcı veri alanı genişletilmiş DM1 paketi gibi düşünülebilir. DM3 paketi üç zaman bölmelidir. Kullanıcı verisi başlık alanını da dahil olmak üzere kullanıcı verisi toplam 123 byte bilgi ve 16 bit CRC kodu içerir. DM3 paketinde kullanıcı verisi başlık alanı 2 byte’dır. Kullanıcı alanı başlığı yapısındaki Length kısmı, kullanıcı verisinin uzunluğunu belirlemektedir. DM3 paketi alınıp verilirken, RF sıçrama frekansı, 3 zaman bölmesi boyunca değişmemelidir. İlk zaman bölmesinde kanal erişim kodu kanala verilmektedir.

**DH3 Paketi:** Bu paket DM3 paketi ile benzer yapıdadır. Fakat DH3 paketinde kullanıcı verisindeki bilgi FEC algoritmasıyla kodlanmaz. Bu yüzden, DH3 paketi 185

byte kullanıcı bilgisi ve 16 bit CRC kod alanı taşıyabilir. DH3 paketi de üç zaman bölmelidir. DH3 paketi alınıp verilir iken de, RF sıçrama frekansı, 3 zaman bölmesi boyunca değişmemelidir. İlk zaman bölmesinde kanal erişim kodu kanala verilmektedir.

**DM5 Paketi:** DM5 paketi de DM1 paketinin kullanıcı verisi alanı genişletilmiş şekli gibi düşünülebilir. DM5 paketi 5 zaman bölmelidir. Kullanıcı verisi başlığı da dahil kullanıcı verisi alanı (payload), 226 byte bilgi ve 16 bit CRC kodu içerir. Bu pakette kullanıcı verisi başlık alanı 2 byte uzunluğundadır. DM5 paketi alınıp verilirken, RF sıçrama frekansı, 5 zaman bölmesi boyunca değişmemelidir. İlk zaman bölmesinde kanal erişim kodu kanala verilmektedir.

**DH5 Paketi:** DH5 paketi DM5 paketi ile benzer yapıdadır. Fakat DH5 paketinde kullanıcı verisindeki bilgi FEC algoritmasıyla kodlanmaz. Bu yüzden, bu paket 341 byte kullanıcı bilgisi ve 16 bit CRC kod alanı taşıyabilir. DH5 paketi de 5 zaman bölmelidir. H5 paketi alınıp verilirken, RF sıçrama frekansı, 5 zaman bölmesi boyunca değişmemelidir. İlk zaman bölmesinde kanal erişim kodu kanala verilmektedir.

**AUX1 Paketi:** AUX1 paketi DH1 paket yapısı ile benzerlik göstermektedir; fakat CRC kod alanı içermez. Bu paket 1 byte kullanıcı verisi başlığı da dahil olmak üzere, 30 byte bilgi taşır. Tek zaman bölmelidir.

ACL paketlerinin karakteristikleri Çizelge 3.8’de özetlenmiştir. Burada kullanıcı verisi kısmı; FEC, CRC ve kullanıcı verisi başlığı hariç paket kullanıcı verisini (payload) göstermektedir.

Çizelge 3.8. ACL paket çeşitleri

| Paket<br>Tipi | Kullanıcı<br>Verisi<br>Başlığı (Byte) | Kullanıcı<br>Verisi<br>(Byte) | FEC   | CRC | Maksimum<br>Simetrik Hız<br>(Kbit/Sn) | Maksimum<br>Asimetrik Hız<br>(Kbit / Sn) |       |
|---------------|---------------------------------------|-------------------------------|-------|-----|---------------------------------------|------------------------------------------|-------|
|               |                                       |                               |       |     |                                       | İleri                                    | Geri  |
| DM1           | 1                                     | 0 - 17                        | 2 / 3 | Var | 108.8                                 | 108.8                                    | 108.8 |
| DH1           | 1                                     | 0 - 27                        | Yok   | Yok | 172.8                                 | 172.8                                    | 172.8 |
| DM3           | 2                                     | 0 - 121                       | 2 / 3 | Var | 258.1                                 | 387.2                                    | 54.4  |
| DH3           | 2                                     | 0 - 183                       | Yok   | Var | 390.4                                 | 585.6                                    | 86.4  |
| DM5           | 2                                     | 0 - 224                       | 2 / 3 | Var | 286.7                                 | 477.8                                    | 36.3  |
| DH5           | 2                                     | 0 - 339                       | Yok   | Var | 433.9                                 | 723.2                                    | 57.6  |
| AUX1          | 1                                     | 0 - 29                        | Yok   | Yok | 185.6                                 | 185.6                                    | 185.6 |

### 3.1.11.21. Lojik Kanallar

Bluetooth teknolojisi SCO ve ACL fiziksel link’leri üzerinden taşınan 5 farklı lojik kanal tanımlamaktadır. Değişik paket tiplerinin içeriğini ayırt etmede bu kanallar önemlidir.

**LC (Link Control) Kanalı :** Link Kontrol kanalı, paket başlığında taşınmaktadır. ARQ, SEQ ve ilgili kontrol verisini içerir. Bu veri, link’in denetlenmesi ve korunması açısından çok önemlidir.

**LM (Link Manager) Kanalı :** Link Yöneticisi kanalı, atanmış ACL kullanıcı

verisinde taşınmaktadır. Bu kanal, alıcı taraftaki ve verici taraftaki link yöneticileri arasında alınıp verilen paketleri içermektedir. Tipik olarak, DM tipi paketlerle taşınır. LM kanalı, ikili sistemde L\_CH=11 kodu ile belirlenir. DM1 paketi hem SCO hem ACL link'lerinde ortak olduğu için, LMP mesajları aktif SCO linki üzerinden taşınabilir.

**UA/UI (User Asynchronous or User Isochronous data) Kanalı :** Bu kanal, ACL kullanıcı verisinde bulunur ve L2CAP kullanıcı verisini taşır. Parçalama işlemi (fragmentation) uygun L\_CH değeri ile yapılır; başlangıç paketleri için 10, devam eden paketler için ise 01 değeri kullanılır. Eş süreli veri Temel bantın etki alanı dışında olmasına rağmen, yığının üst seviyelerindeki zaman başlangıç paketleri tarafından desteklenir ve doğru bir şekilde iletilir.

**US (User Synchronous data) :** Bu kanal açık eşzamanlı kullanıcı bilgilerini içerir. SCO linki üzerinden taşınır.

### 3.1.11.22. Bluetooth Link Denetleyici Durumları

Bluetooth Link denetleyicileri (LC), başlıca iki temel işlemi gerçekleştirmektedir. Bunlar; askıya alma ya da bekleme durumu (standby) ve bağlantı (connection) durumudur. Bu iki temel durum (state) dışında yedi tane de alt durum mevcuttur: Çağrı (paging), çağrı tarama (page scan), sorgu (inquiry), sorgu tarama (inquiry scan), master yanıtı (master response), slave yanıtı (slave response) ve sorgu yanıtı (inquiry response) olmak üzere. Bu durumlar, piconet'e yeni üye kabul etmek, yeni bağlantılar kurmak ve kapsama alanında hangi birimlerin bulunduğu sorusuna yanıt aramak amacıyla kullanılmaktadır.

### 3.1.12. Şifreleme

Bluetooth teknolojisinde iki tip şifreleme algoritması kullanılmaktadır. Her iki algoritmada simetrik anahtar tabanlı kriptolojik algoritmalar vardır. Şifreleme için blok şifrelere göre daha hızlı olan Eo akışkan şifre yöntemi, kimlik doğrulama ve tüm anahtar üretim fonksiyonları içinse SAFER+ blok şifre yöntemi tercih edilmiştir.

Şifreleme işlemi için iki uç birimden en az biri tasdik (authentication) edilmelidir. Eğer master birim piconet şebekesi içindeki tüm slave birimlerin kendisi gibi aynı şifreleme parametrelerini kullanmasını isterse bunu için geçici bir anahtar (temporary key) kullanacağını duyurulmalıdır. Bu geçici anahtar (master key) tüm slave birimler için artık bir link anahtarı (link key ) yerine kullanılır. Tüm bu işlemler bittikten sonra, şifreleme başlatılır. Çizelge 3.9'de şifreleme için kullanılan PDU türleri gösterilmiştir.

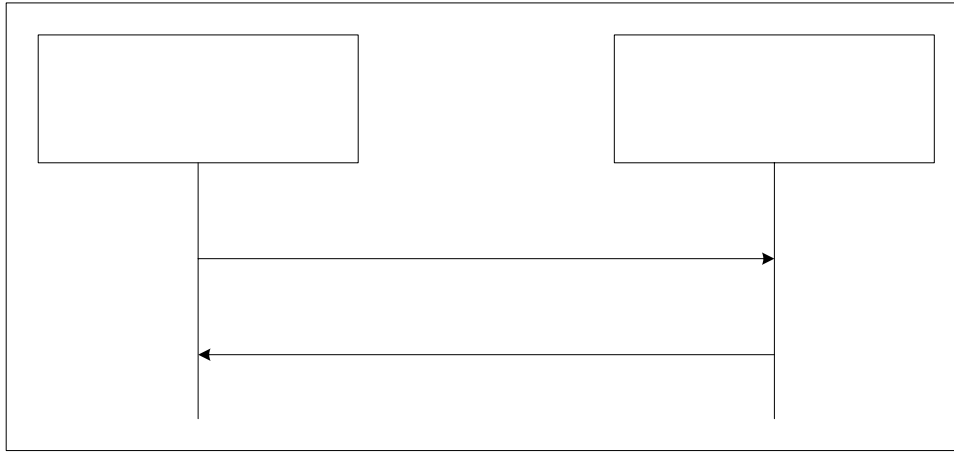
Çizelge 3.9. Şifreleme işlemi için PDU türleri (O:opsiyonel,M:zorunlu)

| M / O | PDU                         | İÇERİK         |
|-------|-----------------------------|----------------|
| O     | LMP_encryption_mode_req     | Şifreleme Modu |
| O     | LMP_encryption_key_size_req | Anahtar Boyu   |
| O     | LMP_start_encryption_req    | Rasgele Sayı   |
| O     | LMP_stop_encryption_req     | -              |

### 3.1.12.1. Şifreleme Modları

#### 3.1.12.2.

Öncelikle master ve slave birimler şifreleme mekanizmasını kullanma veya kullanmama konusunda anlaşmaya varmaları gerekir. Bu anlaşmanın sonucu: "şifreleme mekanizmasını kullanalım" olursa bu durumda yapılacak tek şey şifreleme modunun seçilmesidir. Birinci mod; şifreleme mekanizmasını noktadan noktaya iletecek paketlere veya bir noktadan birden çok noktaya iletilecek paketlere (broadcast paketleri) uygulanmasıdır. Master ve slave birimler şifreleme modunu seçtikten sonra master birim şifreleme hakkında daha fazla bilgiyi slave birime sağlar. Şekil 3.22’de master ve slave birimlerin şifreleme mekanizması için anlaşmaya varma prosedürleri verilmiştir.

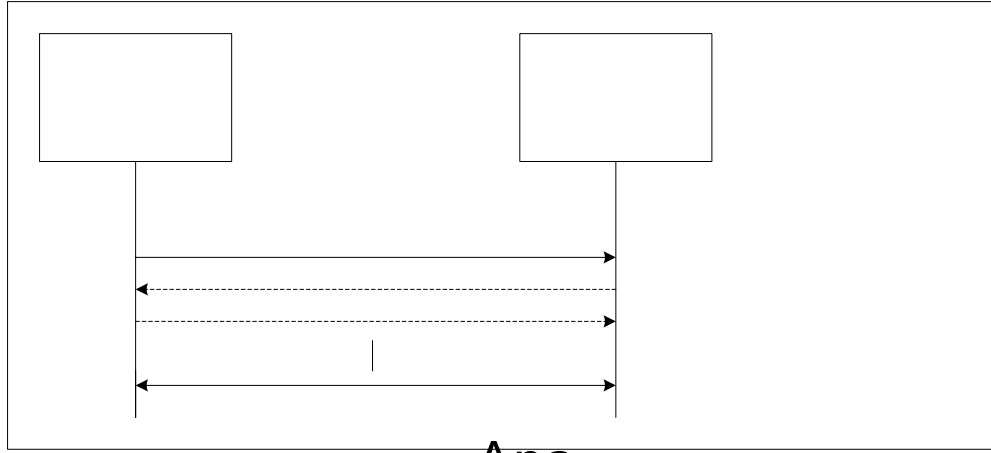


Şekil 3.22. Şifreleme modu için anlaşmaya varma

#### 3.1.12.2. Şifreleme Anahtar Boyu

Şifreleme modu seçildikten sonra bir sonraki adım şifreleme mekanizması için şifreleme anahtar boyunu tesbit etmektir. Burada anahtar boyutu  $L$  sembolü ile gösterilecektir. Master birim kendi seçtiği bir anahtar boyutunu slave birime LMP\_key\_size\_req PDU su ile gönderir .Master birimin önerdiği bu değer,  $L_{sug,m}$  başlangıçta  $L_{max}$  değerine eşitlenir. Eğer slave birime ait,  $L_{min,s}$  değeri,  $L_{min,s} \leq L_{sug,m}$  koşulunu desteklerse bu durumda master birim LMP\_accepted PDU ile geri yanıt verir. Artık  $L_{sug,m}$  değeri şifreleme anahtar boyutu olarak kabul edilir. Slave birim önerilen değeri kabul etmeyebilir. O zaman kendisi LMP\_encryption\_key\_size\_req PDU’su ile önerdiği anahtar boyutunu,  $L_{sug,s}$  master birime gönderir. Bu değer slave birimin desteklediği en büyük anahtar boyutu değeridir. Ve bu değer master birim tarafından önerilen  $L_{sug,m}$  değerinden daha küçüktür. Master birim bu mesajı aldıktan sonra önerilen şifreleme anahtar boyutu üzerinde gerekli işlemleri yapar. Bu süreç müşterek bir anahtar boyutu üzerinde gerekli işlemleri yapar. Bu süreç müşterek bir anahtar boyutu seçilinceye kadar devam eder veya şifreleme mekanizması başarısızlıkla sonuçlandırılır. Eğer anahtar boyutu konusunda bir anlaşmaya varıldıysa birimler den biri LMP\_accepted PDU’yu gönderir ve son transfer edilen LMP\_encryption\_key\_size\_req PDU su içindeki değer anahtar boyutu olarak seçilir. Bu basamaktan sonra şifreleme mekanizması çalıştırılıp paketlere uygulanır. Eğer anahtar boyutu üzerinde bir anlaşma sağlanamıyorsa birimlerden birisi LMP\_not\_accepted mesajını göndererek birimlerin Bluetooth keşifmeleri engellenir. Böyle bir durumda hiçbir paket şifrlenmemiş olduğu için güvenli bir haberleşme

sağlanamaz. Şekil 3.23’de şifreleme anahtar boyutunun nasıl belirlendiği gösterilmiştir.

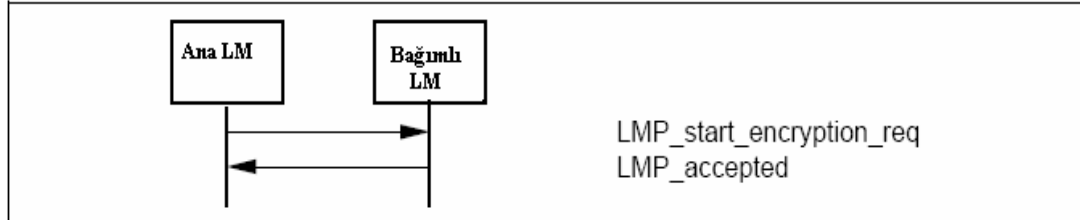


Ana  
LM

Şekil 3.23. Şifreleme anahtar boyutunun belirlenmesi

### 3.1.12.3. Şifreleme Mekanizmasını Başlatma

Bu basamakta şifreleme mekanizması başlatılır. Master birim önce rasgele bir sayı (EN\_RANDOM) üretir ve daha sonra şifreleme anahtarını E3 (current link key, EN\_RANDOM, COF) algoritmasını kullanarak hesaplar. Slave birim bu mesajı aldıktan sonra anlaşmalı şifreleme anahtarı, Kc, değerini hesaplar. Sonra master birime LMP\_accepted mesajını gönderir. Her iki uç birimde de Kc ve EN\_RANDOM parametreleri, şifreleme algoritması için giriş olarak kullanılır. Şekil 3.24’de şifreleme mekanizmasının başlama prosedürleri verilmiştir.



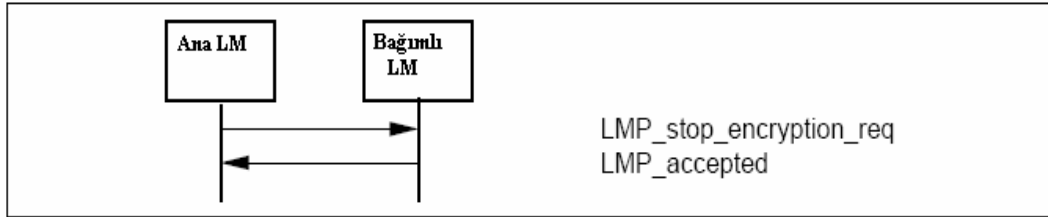
Şekil 3.24 Şifreleme mekanizmasını başlama

### Şifreleme İşlemini Başlatma Üç Basamakta Gerçekleşir.

- Master birim şifrelenmemiş paketleri göndermek ve şifrelenmiş paketleri alacak biçimde konfigüre edilmiştir.
- Slave birim ise hem alma ve hem de gönderme işlemlerinde şifrelenmiş paketler kullanır.
- Master birim şifrelenmiş paketleri hem alma ve hemde göndermek için konfigüre edilmiştir.

Basamak<sub>1</sub> ve basamak<sub>2</sub> arasında master birimden slave birime iletim mümkündür. Bu süreç LMP\_start\_encryption\_req mesajının iletilmesini kapsar. Basamak<sub>2</sub> ise bu mesajın alınmasıyla tetiklenir. Basamak<sub>2</sub> ile basamak<sub>3</sub> arasında ise slave birimden master birime iletim mümkündür. Bu süreç ise LMP\_accepted mesajının iletilmesi sürecini kapsar. Basamak<sub>3</sub> ise bu mesaj alındığı zaman tetiklenir.

#### 3.1.12.4. Şifreleme Mekanizmasını Sonlandırma (Stop Encryption)



Şekil 3.25. Şifreleme anahtar mekanizmasının sonlandırılması

Şifreleme başlama işlemine benzer biçimde şifreleme sonlandırma işlemide üç basamakta gerçekleşir. Şekil 3.25’de şifreleme sonlandırma işlemi verilmiştir.

- Master birim şifrelenmiş paketleri gönderecek ve şifrelenmiş paketleri alacak biçimde konfigüre edilmiştir.
- Slave birim ise şifrelenmemiş paketleri alabilme ve gönderebilme biçiminde konfigüre edilmiştir.
- Son basamakta ise master birim şifrelenmiş paketleri alabilme ve gönderebilme biçiminde konfigüre edilmiştir.

#### 3.1.13. Bluetooth Fonksiyonlarının Bluetooth Güvenliğinde Kullanılması

Güvenlik için kullanılan yöntemler dört değer kullanılır: cihaz adresi (genel), doğrulama anahtarı (özel), şifreleme anahtarı (özel) ve rasgele bir sayı. Anahtarların gizli olması gerekir. Belirli bir cihaza erişebilmek için güvenlik yöntemi kullanıcı tarafından bilinen gizli bir PIN kodu gerektirir. Cihazlar arasındaki değiş-tokuş yöntemleri aşağıda belirtilmiştir.

- Kullanıcı PIN’i başlama anahtarı oluşturulur.
- Doğrulama yöntemi meydan okuma (challenge) ve cevap verme planı yerine getirilir. Sağlayıcı (verifier) cihaz belirli bir işlemle üretilen rasgele bir sayıyı talep sayıyı işleterek bir cevap hazırlar ve sağlayıcı birime gönderir. Sağlayıcı birim ise aynı girişleri kullanarak elde ettiği çıkışı, gelen cevapla karşılaştırır. Eğer sonuçlar birbirine eşit ise her iki cihaz arasında bir doğrulanma kurulmuş olur, aksi halde bağlantı sağlayıcı bağlantıyı keser.
- Her bluetooth cihazı, üretim sırasında hafızasına yüklenmiş olan bir birim anahtara sahiptir. Bluetooth birimi cihaz başlama anahtarını kullanarak birim anahtarı

şifrelemektedir. Şifrelenmiş bu birim anahtar ikinci cihaza gönderilir ve ikinci cihazda başlama anahtarını kullanarak şifrelenmiş anahtarı deşifre edip birim anahtarı öğrenir. Başlama anahtarı bu işlem yapılmadan önce iki cihaz arasında meydana gelen değiş-tokuş yöntemi ile elde edilmektedir.

- İkinci cihaz, birim anahtarını birinci cihazın birim anahtarına ekleyerek birleşim anahtarını oluşturabilir. Eğer her iki cihaz da bu anahtarı tutabilecek seviyede ise bunu link anahtarı olarak cihazlardan birinin birim anahtarı olarak kullanılır. Link anahtarı belirlendikten sonra başlama anahtarı diskalifiye edilir.

Aynı iki cihaz arasında başka zaman kurulacak link için aynı link anahtarı kullanılabilir. Bu da kanal üzerinden tekrar anahtar gönderme gereksinimini ortadan kaldırır. Böylece iki cihaz arasında iletilen veri minimum kullanıcı etkileşimi ile iletilmiş olur.

### **3.1.14. Bilgi Güvenliği ve Kriptoloji**

Diffie ve Hellman'ın, bundan yaklaşık otuz yıl önce kaleme aldığı "şifreleme biliminde yeni yönelimler" adlı makalesi şöyle başlar: "We stand today on the brink of a revolution in cryptography" (Biz bugün kriptografi alanında yaşanan bir devrimin eşiğinde durmaktayız) (Diffie ve ark.; 1976).

Bundan on yıl sonra da yine ünlü bir matematikçi ve şifreleme uzmanı olan Ronald L.Rivest, Diffie-Hellman'a atıfta bulunarak, "Kriptografi " adlı makalesinde bu devrimden şöyle bahseder: "Today we are in the midst of that revolution"(Bugün biz bu devrimin tam ortasındayız) (Rivest, 1986).

Güvenlik kavramının her alanda çok önem kazandığı bugünlerde ise bu devrimin neresinde olduğumuzu kestirmek çok kolay olmasa gerek.

Kripto sistemleri, güvenli bir iletişim sağlamak amacıyla, kötü niyetli kişilerin amaçlarını boşa çıkarmak için tasarlanan sistemler bütünü olarak tanımlanır. Şifre bilimi kriptografi, kripto sistemleri tasarlayan bir araştırma dalı; kripto analizi ise bu sistemlerin kırılması, çökertilmesi amacına yönelik çalışmalar yapan bir alan olarak görülür. Kriptoloji ise hem kriptografi , hem de kripto analizinin bir birleşimi olarak tanımlanır (Rivest, 1986).

Kriptografi, 1960'lara kadar ulusal sırları ve stratejileri koruyan bir araç olarak kalmıştır (D.Kahn,The Codebreakers, 1996). Özellikle ikinci dünya savaşında bir çok ülke gizli haberleşmelerini şifreleme makinaları kullanarak sağlamıştır. Nazi Almanyası'nın "Enigma"sı Japonya'nın "Purple"ı, Amerika'nın "Hebern"i bu şifreleme makinalarına verilebilecek en önemli örneklerdendir. 1960'lı yıllardan sonra,bilgisayar ve iletişim sistemlerindeki büyüme, bilgilerin dijital olarak korunması ihtiyacını, beraberinde de ilgili güvenlik servislerinin sağlanmasının zorunluluğunu ortaya çıkarmıştır. 1970'li yılların başında IBM'in Feistel algoritmasını önermesiyle başlayan bu değişim, DEA algoritmasının 1977 yılında Amerika FIPS'de DES adıyla standartlaşmasıyla doruğa yükselmiştir .DES, tarihte en çok bilinen kriptolama algoritmasıdır (Engin Çomakçı, 2004).

**3.1.14.1. Kriptolojinin Hedefleri**

Bilgi güvenliğinin sağlanabilmesi için çok sayıda kavram ve servisten söz etmek mümkündür. Temel olarak kriptografi için birbirinin içerisine geçmiş dört farklı güvenlik servisi önem kazanmaktadır. Kriptolojinin hedefi de, bu dört servisi hem teoride hem pratikte işlevsel hale getirmektir (Menezes ve ark.; 1996).

- **Gizlilik:** Bilginin içeriğinin yetkisiz olarak açığa çıkmasını engellemek için kullanılan bir servistir. Gizlilik kavramına, fiziksel ortamın özelliklerinden, matematiksel düzlemde önerilen algoritmik yapıya kadar bir çok farklı açıdan bakılmalıdır.

- **Bütünlük:** Bilgi üzerinde silme, değiştirme gibi değişikliklerin yetkisiz yapılmamasını ve eğer yapıldıysa bu değişikliklerin ortaya çıkarılmasını amaçlayan bir servistir. Ayrıca bu değişikliğe yetkili veya yetkisiz kimin neden olduğunun tesbit edilmesi de yine bu servisin kapsamına girmektedir.

- **Kimlik doğrulama:** Güvenli bir iletişim yapmak isteyen her kullanıcı, öncelikle karşısındakinin doğru kişi olup olmadığından emin olmak ister. Bunun için tarafların birbirlerine uyguladıkları ve karşısındakinin kimliğini teyit etme amacına yönelik tüm yöntemler bu servisin görevleri arasındadır.

- **İnkâr edememe:** Olayı gerçekleştiren kişinin daha sonra bunu inkâr edememesi için tasarlanan çeşitli yöntemleri tanımlar.

**3.1.14.2. Şifreleme**

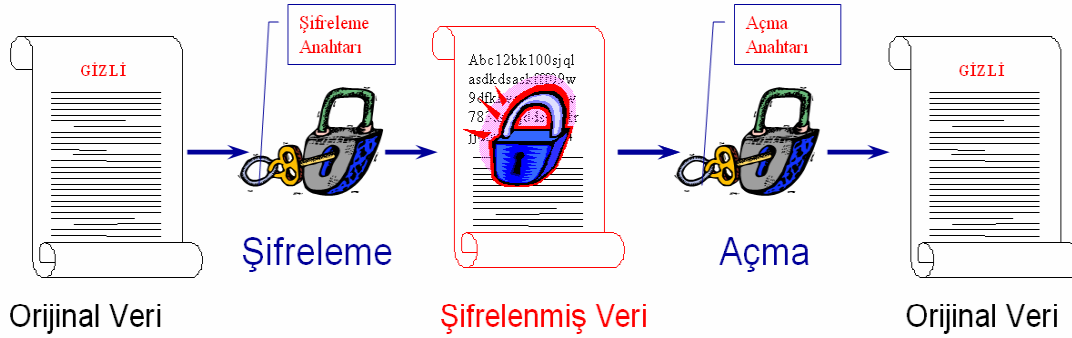
Şifre bilimin amacı ileti güvenliğini sağlamaktır. Şifreleme ilk olarak M.Ö. 1900'lü yıllarda Mısırlılar tarafından kullanılmıştır. Tüm şifreleme işlemleri aynı temel prensibe dayanmaktadır: Bilgi içeriğinin bir algoritma ya da formül kullanılarak uygun anahtar olmadan okunamayacak hale getirilmesi işlemidir. Şifreleme iki temel kategoride incelenmektedir: Tek anahtar şifreleme, şifreleme ve şifre çözme için aynı gizli anahtarın kullanıldığı bir yöntemdir. Açık anahtar şifreleme de ise şifreleme ve şifre çözme için biri özel diğeri açık olmak üzere iki anahtar kullanılır.

Bu çalışma içerisinde, daha çok Bluetooth güvenlik mekanizmalarıyla doğrudan ilgili olduğu düşündüğümüz şifreleme, kimlik doğrulama yöntemleri üzerinde durulmaktadır. Dijital imza, dijital zarf gibi günümüzde uygulama alanı bulan diğer önemli kriptolojik yöntemler bu tez kapsamı dışında bırakılmıştır.

**3.1.14.3. Şifrelemenin Temel Elemanları**

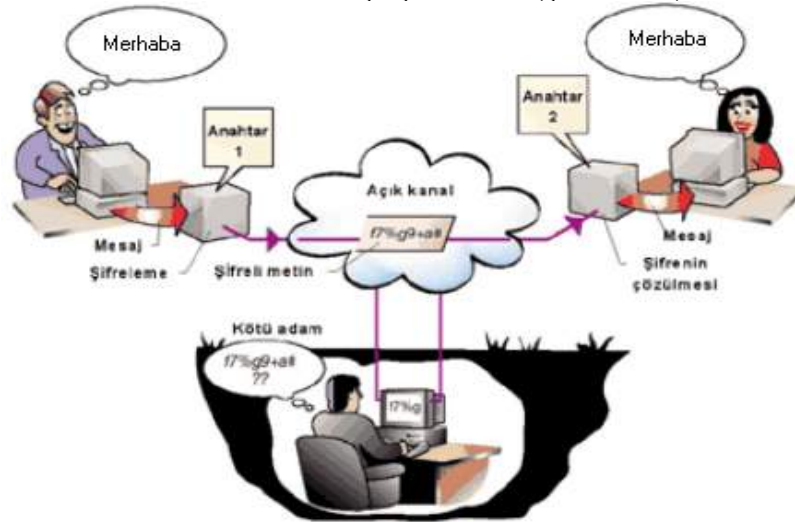
Bir göndericinin bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar. Burada söz konusu ileti düz metindir. Bazı kullanımlarda "plaintext" adı da verilir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (encryption). Bu işlem düz metni şifreli metine dönüştürür. Bilginin içeriğinin başkalarının anlamayacağı hale gelir. Bu bilgi bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir bilgi olabilir. Şifrelenmiş bir ileti şifreli

metindir (ciphertext). Şifreli metni düzmetine geri çevirme işlemi şifre çözümüdür (decrypt). Bu işlemler Şekil 3.26'da gösterilmektedir.



Şekil 3.26. Kriptolojik şifreleme işlemi

Eğer bir algoritmanın güvenliği bu algoritmanın çalışma biçimini gizlemeye dayalıysa, bu bir sınırlandırılmış algoritmadır. Sınırlandırılmış algoritmalar günümüzün şartlarına pek uymamaktadır; bir gruba ait kullanıcılar bunları kullanamamaktadır, çünkü gruptan bir kullanıcının her çıkışında geri kalan herkesin başka bir algoritmaya geçmesi gerekmektedir. İçlerinden birisi yanlışlıkla gizleneni açığa vurduğunda, diğer herkesin algoritmalarını değiştirmeleri gerekmektedir. Daha da kötüsü, sınırlandırılmış algoritmalar kalite kontrolüne ve standardizasyona olanak tanımamaktadır. Her bir grup kullanıcının kendisine ait bir algoritması olmalıdır. Bu tür bir grup hazır şifre çözüm anahtarının yazılım veya donanım ürünlerini kullanamaz; davetsiz bir misafir aynı ürünü alıp algoritmayı öğrenebilir. Kendi algoritmalarını ve gerçekleştirmelerini kendileri yazmaları gerekir. Günümüz kriptografisi bu sorunu bir anahtar ile çözmektedir. Bu anahtar çok çeşitli değerler alabilen herhangi bir anahtar olabilir. Günümüzde kullanılmakta olan modern ve güçlü şifreleme algoritmaları artık gizli değildir. Bu algoritmalar güvenliklerini kullandıkları farklı uzunluk ve yapılarıdaki anahtarlarla sağlarlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanır. Bir anahtar ile şifrelenmiş bilgi, kullanılan algoritmaya bağlı olarak, ilgili anahtar ile çözülebilir. Genel olarak anahtarın kullanımı şu şekildedir (Şekil 3.27).



Şekil 3.27. Bir mesajın dinlenmesini önlemek için anahtar ile şifreleme.

Kullanıcı bir mesajı ( $m$ ) göndermeden önce bir anahtar ( $k_1$ ) kullanarak şifreler. Şifreli metin ( $c$ ) yasadışı dinleyicilere açık olan bir kanaldan gönderilir. Mesajı okumak için alıcı bir anahtar ( $k_2$ ) kullanarak şifreyi çözer ve  $m$  mesajını elde eder. Aktif düşmanlar araya girip iletişimi dinleyebilir. Eğer  $k_1$  ve  $k_2$  eşitse, sistem simetrik. Aksi takdirde bu sistem asimetrik olarak nitelenir. Güvenliğin garantilenmesi için  $k_2$  her zaman gizli olmalıdır, ancak  $k_1$ 'i kullanarak  $k_2$ 'yi elde etmek mümkün olmadığı sürece  $k_1$  açıklanabilir. Bu durumda sisteme açık anahtarlı sistem (public key system) adı verilir.

Açık anahtarlı sistemlerin güvenliği her zaman belirli matematiksel problemleri çözmenin zorluğuna dayanır, simetrik sistemler daha çok tek kullanımlık, geçici yapıdadırlar. Açık anahtarlı sistemlerin en büyük dezavantajı matematiksel yapıları nedeniyle simetrik sistemlerden daha yavaş olmalarıdır; özellikle açık anahtarlı sistemlerdeki anahtarların boyutları simetrik sistemlerin anahtarlarının boyutlarından çok daha büyüktür. Kısaca, kullanılacak şifreleme yöntemi gerçekleştirilecek uygulamaya bağlı olarak seçilir. Şekil 3.28 ve Şekil 3.29'da tek ve iki anahtarlı şifreleme yapısı verilmiştir.



Şekil 3.28. Tek anahtar şifreleme



Şekil 3.29. İki farklı anahtar ile şifreleme ve şifre çözme (Subaşı, ve ark., 2005)

Algoritmalarındaki bütün güvenlik anahtara (veya anahtarlara) dayalıdır, hiçbir algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenabildiği anlamına gelir. Bu algoritmayı kullanan ürünler seri üretilebilir. Bir davetsiz misafirin sizin algoritmanızı bilmesi önemli değildir; sizin özel anahtarınızı bilmedikçe, o şahıs iletilerinizi okuyamaz.

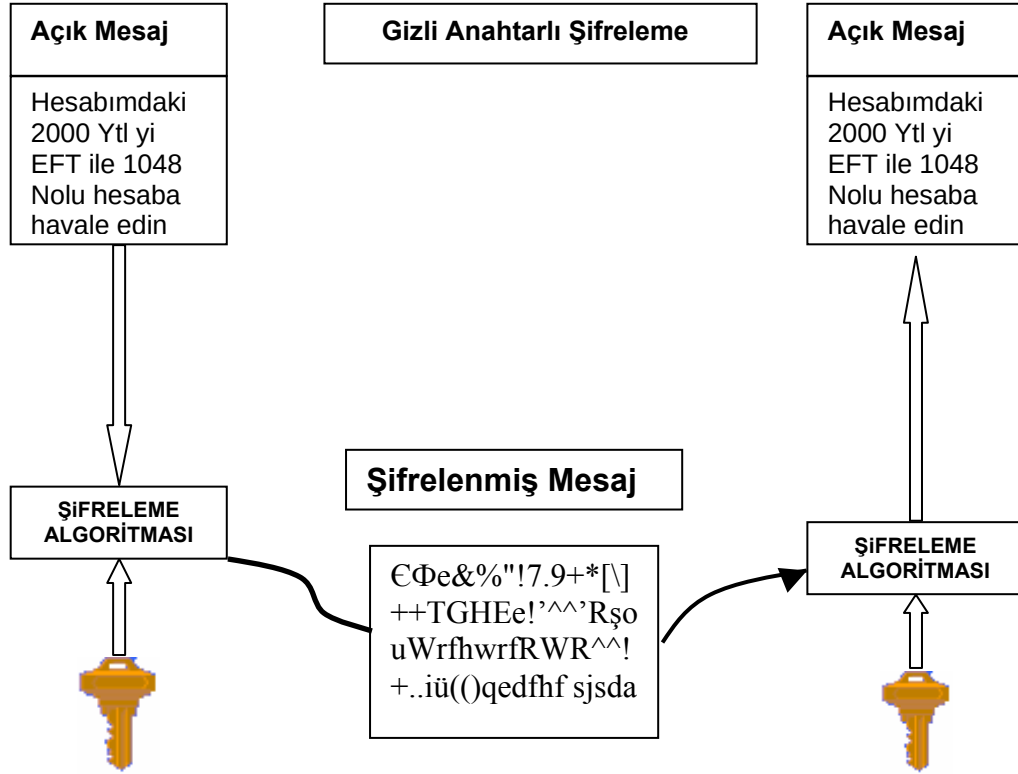
Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki kategoriye ayrılmaktadır. Bu yöntemler:

- Gizli-Anahtar (Simetrik) yöntemleri (Geleneksel kriptolama sistemleri)
- Açık-Anahtar (Asimetrik) yöntemleri (Açık anahtar kriptolama sistemleri)

#### 3.1.14.4. Gizli-Anahtar (Simetrik) Yöntemleri (Geleneksel Kriptolama Sistemleri)

Gizli anahtar ile şifrelemede, her iki tarafta da kullanılan anahtarların aynı olması nedeniyle, simetrik anahtar olarak da adlandırılır (Şekil 3.30). Kriptografi dünyasında daha geleneksel olarak bilinen bir yöntemdir. Hem şifreleme hem de şifre çözme için aynı gizli anahtar kullanılır. Gizli anahtar kriptolama sistemlerinin en büyük problemi, alıcı ve verici

tarafların, yetkisiz kişilerin ortak gizli anahtarı öğrenmesine izin vermeden bir anahtar üzerinde anlaşabilmeleridir. Bunun için öncelikle mümkün olduğu kadar gizli anahtarların üretilmesi sırasında ortamda gizli dinleme olmasını engellemek gerekir. Anahtar değişimi için kullanılan en basit yöntem ise, gizli anahtarın kurye kullanarak değişimini sağlamaktır.



Şekil 3.30. Gizli (Simetrik) Anahtarlı şifreleme

#### Simetrik Anahtarlamanın Artıları

- Algoritmalar hızlıdır
- Algoritmaların donanımla gerçekleştirilmesi kolaydır
- "Gizlilik" güvenlik hizmetini yerine getirir.

#### Simetrik Anahtarlamanın Eksileri

- Ölçeklenebilir değil
- Emniyetli anahtar dağıtımı zor
- "Bütünlük" ve "Kimlik Doğrulama" güvenlik hizmetlerini gerçekleştirmek zor

#### Simetrik Şifreleme Anahtarları

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)

- Skipjack
- RC5
- RC2
- RC4
- Safer
- Cast-128
- Cast-256
- Twofish
- Blowfish
- Seal

### **3.1.14.5. Safer Algoritması**

Safer blok şifreleme algoritması ilk olarak 1993 yılında Cylink Corporation adına James L.Massey tarafından tasarlanmıştır. İlk uyarlaması Safer K-64, 64 bit blok uzunluğuna ve 64 bit anahtar uzunluğuna sahiptir. Daha önce bahsedilen bir çok blok şifrenin aksine, şifreleme ve şifre çözme algoritmaları birbirinden farklıdır. Şu ana kadar cylink tarafından bir çok Safer algoritması tasarlanmıştır. Safer K-128, Safer SK-64, Safer SK-128, Safer SK-40, Safer+ ve son olarak da Safer++ diğer safer algoritmalarıdır (Massey, 1993).

Bluetooth teknolojisinin kimlik doğrulama yordamı içerisinde de Safer + blok şifresi kullanılmıştır (Massey, 1998).

Ayrıca Safer +, 1997 yılındaki AES seçmelerinde katılan onbeş aday arasına kalmış bir algoritmadır. Safer K-128, 64 bit anahtar uzunluğuna sahip safer K-64'ün 128 bitlik versiyonudur. 64 bitlik Safer SK-64 ve 128 bitlik Safer SK-128 ise Knudsen'un tesbit ettiği, safer algoritmalarının anahtar üretim aşamasındaki zayıflığını gidermek için tasarlanan algoritmalarıdır .Daha hızlı olması için anahtar uzunluğu ve tur sayısı düşürülen 40 bitlik Safer SK-40 ile Avrupa Komisyonu (EC), Bilgi Toplumu Teknolojileri (IST) programı içerisinde NESSIE projesine aday olarak katılan Safer++ ise Cyclink'in günümüzde kullanılan son tasarımlarıdır (Knudsen, 1995).

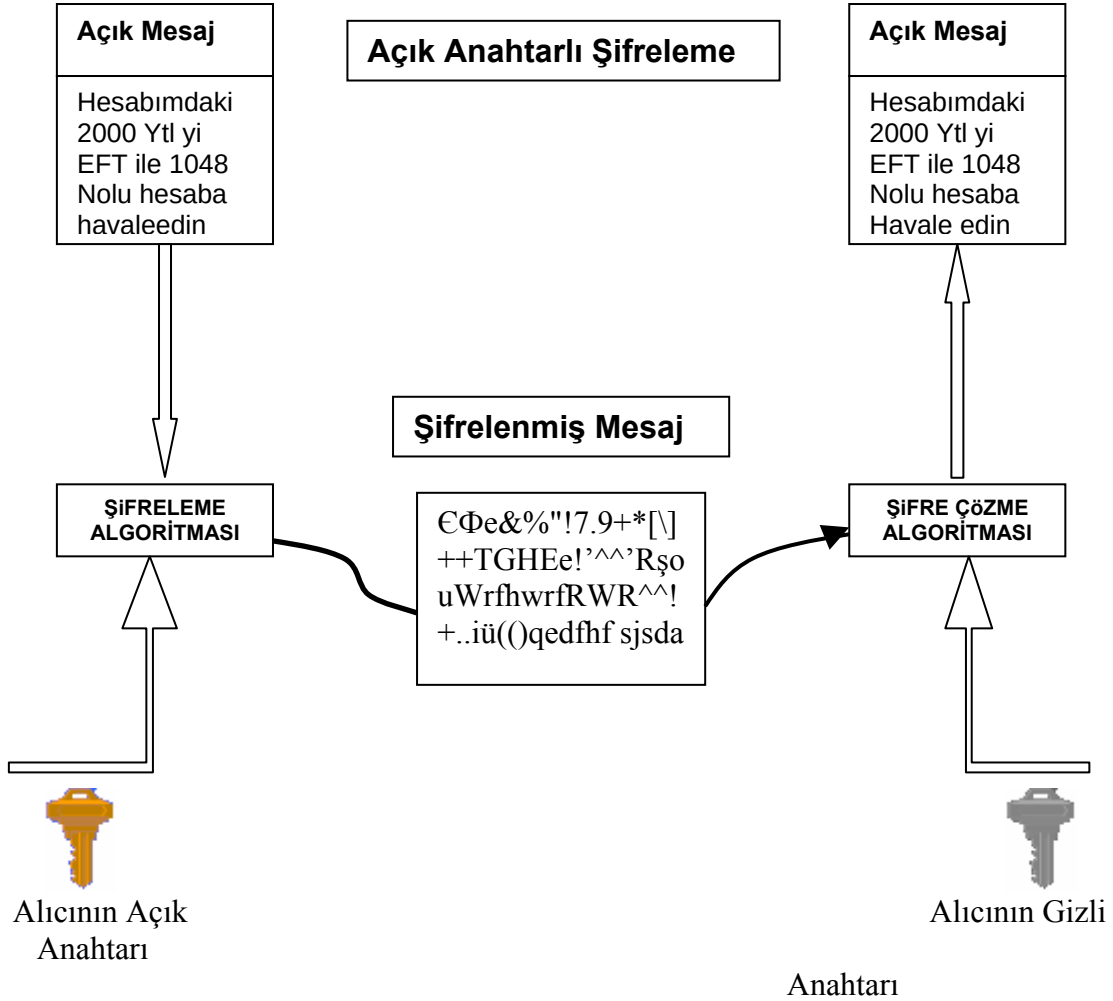
Safer ++, bazı yapısal özelliklerinden ve kırılabilen maksimum tur sayısı ile toplam tur sayısı arasındaki farkın (güvenlik payı) düşük olmasından dolayı, NESSIE'nin güvenli blok şifreleri önerdiği algoritmalar arasında yer alamamıştır (Preneel, 2003).

### **3.1.14.6. Açık (Asimetrik) Anahtar Şifreleme**

Açık Anahtar krypto sistemi, kavram olarak ilk defa Diffie ve Hellman tarafından tanımlanmıştır (Diffie ve ark.; 1976).

Bu sistemde, gizli anahtar sisteminde kullanılan tek anahtar yerine, hem şifreleme hem de şifre çözme için birbirinden farklı iki anahtar kullanılır. Bu anahtarlardan birisi sadece o kişiye özel, gizli anahtar; diğeri ise herkes tarafından bilinmesinde sakınca olmayan açık anahtardır. Bu anahtarların özelliği, açık anahtarlar ile şifrelenen mesajın gizli anahtar ile çözülebilmesi, gizli anahtar ile şifrelenen mesajın ise sadece açık anahtar ile doğrulanabilmesidir. Ayrıca anahtarlar arasında birinin bilinmesiyle diğerrinin tahmin

edilmesi mümkün olmayan matematiksel bir bağlantı bulunmaktadır. Şekil 3.31’de bu anahtarların birbirleriyle ilişkisi verilmektedir.



Şekil 3.31. Açık (Asimetrik) anahtar şifreleme

#### Açık (Asimetrik) Anahtar Şifrelemenin Artıları

- Anahtar yönetimi ölçeklenebilir
- Kripto-analize karşı dirençli (Kırılması zor)
- Bütünlük, Kimlik doğrulama ve İnkâr edememezlik güvenlik hizmetleri sağlanabilir.

#### Açık (Asimetrik) Anahtar Şifrelemenin Eksileri

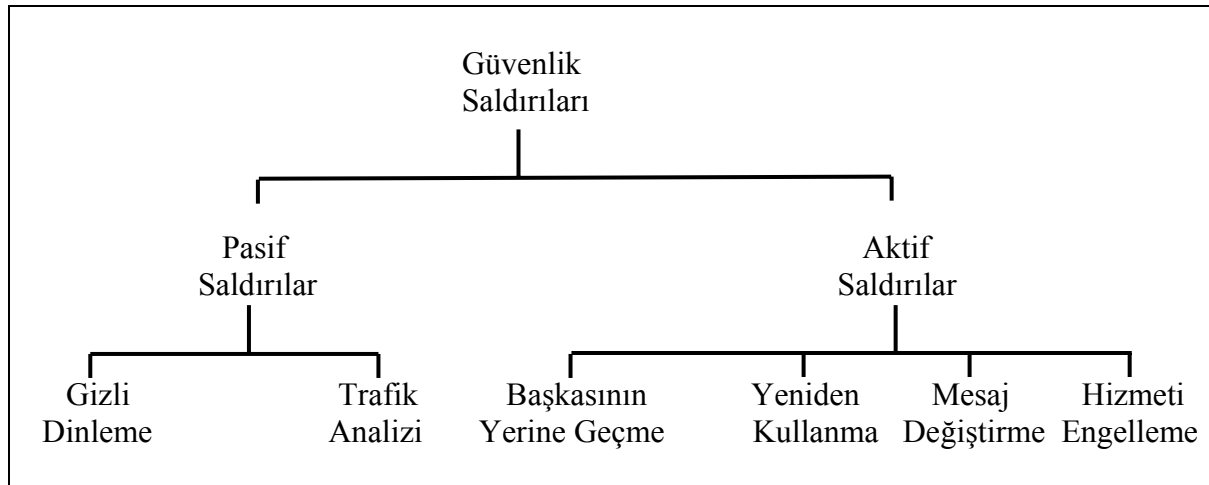
- Algoritmalar genel olarak yavaş (Simetrik kriptografi algoritmalarına göre ~1500 kat!)
- Anahtar uzunluğu bazı durumlar için kullanışlı değil

### Açık (Asimetrik) Şifreleme Algoritmaları

- RSA (Rivest-Shamir-Adleman)
- El Gamal
- PGP (Pretty Good Privacy)
- Diffie-Hellman anahtar belirleme
- DSA (Digital Signature Algorithm)
- Eliptik Eğri

### 3.1.15. Ağ Sistemlerine Yapılabilecek Güvenlik Saldırıları

Bluetooth teknolojisini tehdit eden saldırıların daha iyi anlaşılabilmesi için öncelikle telli veya telsiz ağ sistemlerine yapılan güvenlik saldırılarının açıklanması gerekir. Genel olarak ağ sistemlerini tehdit eden güvenlik saldırıları Şekil 3.32’de gösterildiği gibi sınıflandırılır (Karygiannis ve ark.; 2000).



Şekil 3.32. Güvenlik saldırılarının sınıflandırılması

#### 3.1.15.1. Pasif Saldırılar

Kötü niyetli kişinin iletişim kanalını izinsiz olarak dinlemesi ile yapılabilecek saldırıları kapsar. Bu tip saldırılar sadece mesajın gizliliğini tehdit ederler. Gizli dinleme ve trafik analizi olarak iki gruba ayrılır.

- **Gizli dinleme:** Gönderilen mesajın içeriğini tesbit etmek için kanalı dinleyerek yapılan saldırılardır. Şifreleri metinden orijinal mesaj elde edilmeye çalışılır. Bunun için bir çok yöntem geliştirilmiştir. Bilinen veri yöntemi, sadece şifreli metin yöntemi, seçilen veri yöntemi, uyarlanmış seçilen veri yöntemi ve seçilen şifreli metin yöntemi, bilinen en önemli gizli dinleme yöntemlerindendir (Menezes ve ark.; 1996).

- **Trafik analizi:** İletişim sırasındaki mesaj trafiğinin incelenmesiyle, orijinal mesajın içeriği ile ilgili olarak çok sayıda bilgi elde edilebilir. Çünkü iletişim başlangıcında veya standart mesajlaşmaların olduğu bazı iletişim safhalarında, orijinal mesajı tahmin etmek daha kolay olmaktadır. Bu sayede de şifreleme anahtarı tesbit edilip gizli mesaja ulaşmak

mümkün olabilmektedir.

Ayrıca deneme yanılma-kaba kuvvet saldırısı, blok şifrelere karşı uygulanan doğrusal, ayrımsal saldırılar, akışkan şifrelere karşı geliştirilen cebirsel saldırılar, yine son yıllarda ortaya çıkarılan bumerang saldırısı ve saydam saldırısı da şifreleme algoritmalarına karşı kullanılan diğer pasif saldırılardır.

### **3.1.15.2. Aktif Saldırılar**

Mesaj üzerinde yetkisiz değişiklik yapılması veya aktif olarak mesajı kullanarak gizli bilgiye ulaşılması amacını taşıyan saldırılardır. Bu tip aktif saldırıların tesbit edilmesi mümkün olsa bile bunların tamamen engellenmesi oldukça zor olmaktadır. Genelde dört farklı şekilde ortaya çıkarlar;

- Başkasının yerine geçme: Yetkili bir kullanıcıyı taklit ederek yetkisi olmayan servisleri kullanıp, gizli bilgiye ulaşma amacını taşıyan saldırılardır.
- Yeniden kullanma: Pasif saldırı ile elde ettiği verilerin (meydan okuma-yanıt değerleri, orijinal mesaj ve şifreli mesaj çiftleri, vs) biriktirilerek yeniden kullanılmasına dayanan bir güvenlik saldırısıdır.
- Mesaj değiştirme: Orijinal mesajın ekleme, silme, sırasını bozma gibi yöntemlerle değiştirilmesini amaçlayan saldırılardır.
- Hizmeti engelleme: İletişim olanaklarının kullanımı veya yönetimini sınırlandırarak, sağlıklı bir iletişim yapılmasını engelleyen saldırılardır.

Doğum günü saldırısı ve sözlük saldırısı da yine aktif yöntemler kullanarak yapılan diğer saldırılara verilebilecek diğer örneklerdir.

Ayrıca son beş altı yıldır, yukarıda örnekleri verilen klasik saldırılar dışında, yan kanal saldırıları da oldukça önem kazanmıştır .Bu çalışmalar, veri olarak şifrelenen mesaj dışında şifreleme süresi, güç tüketimi, yayılan elektromanyetik radyasyon gibi diğer bilgileri de kullanarak şifreyi çözmeyi amaçlamaktadır.

Yine son yıllarda önemi artan ve şifreleme çipindeki olası donanımsal hataları kullanarak şifre çözmeyi amaçlayan bazı yöntemler de geliştirilmektedir. Bu tip saldırıların klasik yöntemlere karşı en büyük dezavantajı uygulamaya bağımlı olmasıdır (Çomakçı, 2004).

### **3.1.16. J2ME ( Java 2 Micro Edition )**

Java dili birçok farklı yazılım ve donanım platformunda çalışma özelliği olan ve etkili ağ uygulamaları ile yüksek kullanıcı ara yüzü kapasitesine sahiptir. Java programlama dili bilgisayar dünyasında önemli bir yer teşkil etmektedir. Nesne tabanlı programlama özelliği, yazılan programın değişikliğe uğraması yada yeniden derlenmesi gerekmeden farklı yapıdaki bilgisayar sistemlerinde kullanılması gibi özellikler Java dilinin popülerliğini sağlayan önemli özelliklerin sadece bir kaçıdır ( Flanagan, D., 2002).

İlk geliştirilme amacı SUN Microsystem şirketinin içinde ortak bir dil kullanılması için tasarlanan ve o zamanki adı OAK olan Java dili, kısa zamanda dünya çapında yoğun olarak kullanıma girmiştir. Javanın kullanıldığı yerler, basit bir ev bilgisayarlarından, en kompleks sistem sunuculara kadar değişen bir yelpazede yer almıştır. Java'nın yakaladığı bu şöhreti gören SUN Microsystems, bu dilin avantajlarını kablosuz cihazlara da taşımaya karar vermiş ve haziran 1999 tarihindeki JavaOne konferansında hazırladığı Java 2 Micro Edition (J2ME) sürümünü duyurmuştur ( Mahmoud, Q. H., 2002).

J2ME (Java 2 Micro Edition) javanın küçük cihazlar için geliştirmiş olduğu bir sürümdür. Bu cihazlar cep telefonları, palm, tv kutu'ları gibi cihazlardır. Bu cihazlar PC'lere göre sınırlı kaynakları olan cihazlardır. Bu yüzden bu cihazlara yönelik değişik bir sürüm yaratılmıştır.

J2ME'nin amacı bütün bu sayılan, değişik yeteneklere ve olanaklara sahip aygıt türlerinde ortak işlevler sağlamaktır. Bunun için modüler bir yapı kurulmuş, çeşitli konfigürasyon (configuration)'lar ve profil (profile)'ler belirlenmiştir.

### **Konfigürasyon (Configuration)'lar ve Profil (Profile)'ler**

J2ME konfigürasyonu bir aygıt ailesi için minimum Java platformunu tanımlar. Bu aileye ait aygıtlar benzer bellek ve işlemci yeteneklerine sahiptir. Bir konfigürasyon, sistem düzeyinde programcının o aygıtın desteklediğini bildiği bazı dil ve platform özelliklerinin tanımlamasıdır. Belli bir konfigürasyona giren aygıtlarda hangi Java kütüphanelerinin olduğunu bilir ve ona göre program yazabilir. Özet olarak, bir konfigürasyon şu maddeleri içerir:

- Belli Java programlama dili özellikleri
- Belli Java sanal makinesi özellikleri
- Belli Java kütüphaneleri

J2ME profili (profile) uygulama düzeyinde verilen servislerden oluşur. Verilen servis herhangi bir konuda olabilir. Ancak belli konulardaki profiller standarttır, o profili destekleyen bütün aygıtlarda aynı servis aynı şekilde bulunur. Profiller bir konfigürasyon üzerinde çalışırlar. Ayrıca bir profil bir başka profil üzerinde çalışabilir. Bir aygıtı birden fazla profili destekleyebilir ancak sadece tek bir konfigürasyona sahip olur. Örneğin SMS Mesajlaşması bir profil konusudur. Bu, gezgin telefon konfigürasyonu için çok yaygın bir profile'dir

### **J2ME'de Tanımlanmış Konfigürasyonlar**

Konfigürasyonlar Java 2 Standart Edition (J2SE)'deki bazı sınıfları (class) içerebilirler. Ancak hepsini içermeleri, bu cihazların bilgisayara göre daha az teknik özellik içermesi nedeniyle mümkün değildir. J2SE'deki bir sınıf belli bir konfigürasyonda tanımlıysa mutlaka aynı şekilde tanımlı olmak zorundadır. Farklı bir metot ekleyemez. Buna karşın eski metotları tanımlamak zorunda değildirler.

J2ME iki konfigürasyon tanımlar:

- **CLDC (Connected, Limited Device Configuration):** Kişisel, kesikli bağlantılı gezgin aygıtlar için.

- **CDC (Connected Device Configuration):** Sürekli bağlantılı ağ aygıtları için.

CDC daha gelişmiş (örneğin 2 MB'tan fazla belleğe sahip aygıtlar) için tanımlanmışken CLDC daha az gelişmiş (örneğin 160 KB kadar düşük bellekli) aygıtlar için tanımlanmıştır. CDC tanımlaması CLDC'yi tümüyle kapsar. Yani CLDC'de tanımlanmış bütün servis ve kütüphaneler CDC'de de bulunur.

### **CDC (Connected Device Configuration)**

CDC, J2SE'de bulunan birçok özelliği barındırmaktadır. CDC için CVM (Compact Virtual Machine) sanal makinesi geliştirilmiştir. JVM (Java Virtual Machine)'de olan hemen hemen bütün özellikleri içermektedir. Ancak sınırlı kaynağa sahip aygıtlar için tasarlanmıştır.

CDC'de tanımlanmış paketler:

- java.lang, java.lang.ref, java.lang.reflect
- java.util, java.util.zip, java.util.jar
- java.net
- java.io
- java.text
- java.security, java.security.cert
- java.math
- javax.microedition.io

CDC konfigürasyonu çeşitli profillerle tamamlanmıştır. İlk olarak tanımlanan profil Foundation Profile'dır. Bu profil java.lang, java.util, java.net, java.io ve java.security'deki eksiklikleri (J2SE'de bulunup, CDC'de bulunmayan nesneleri) eklemektedir. Bu profille birlikte CDC bir programlama ortamı sağlamış olmaktadır. Ancak bu ortamda AWR veya Swing gibi bir ara yüz yoktur. Bir programda ara yüz kullanmak için Personal Profile gibi bir profili desteklemelidir. Personal Profile'i bütün AWT (Abstract Windows Toolkit) paketlerini desteklemektedir. Ayrıca java.beans ve javax.microedition.xlet paketleri bulunmaktadır. Personal Profile'la birlikte Personal Java adlı Java sisteminde J2ME'a bir geçiş yolu sağlamış olur. Bir başka profil de RMI (Remote Method Invocation - Uzaktan Yöntem Çağırma) Profile'dır. Bir nesnenin ağda başka bir aygıtta çalışan bir nesnenin herhangi bir metodunu doğrudan çağırmasını sağlayan RMI nesnelerinin hemem hemen tamamını desteklemektedir.

### **CLDC (Connected, Limited Device Configuration)**

Java 2 Micro Edition'da tanımlanmış ikinci konfigürasyon CLDC (Connected, Limited Device Configuration) düşük bellekli, şarj gibi zayıf güç kaynakları olan, kablosuz bağlantılı aygıtlar için tanımlanmıştır.

CLDC'de Java dili desteği olarak bazı özellikler eksik bırakılmıştır: Float (kesirli) tipi Object Serialization ve Error class'ı gibi. Float'ı desteklememesinin nedeni söz konusu düşük yetenekli aygıtların kesirli sayıları destekleyen donanım birimlerinin olmamasıdır.

CLDC'yi destekleyen KVM (Kilobyte Virtual Machine) adlı bir VM (Virtual Machine) bulunmaktadır (Bir kaç KB'lık hafızaya sığıdığı için bu ismi almıştır). Bu konfigürasyon şu paketlerden sınıflar içerir:

- java.lang
- java.util
- java.io
- javax.microedition.io

### 3.1.16.1. J2ME'de Tanımlanmış Profiller (Profile)

#### MIDP Profili

MIDP (Mobile Information Device Profile) mevcut profiller arasında ilk ve en yaygın olanıdır ve uygulamanın yaşam döngüsü, kullanıcı grafik arabirimleri, iletişim ağı ve kalıcı veri depolama ile ilgili kütüphanelerini içerir. MIDP, CLDC konfigürasyonunun üzerine kurulmuştur ve günümüzde Motorola, Nokia, Ericsson ve RIM (Blackberry) gibi sektörün devleri tarafından desteklenmektedir.

MIDP 1.0'ın desteklediği paketler:

- java.io
- java.lang, java.util
- javax.microedition.io
- javax.microedition.lcdui
- javax.microedition.midlet
- javax.microedition.rms

MIDP 2.0'ın desteklediği paketler:

- java.io
- java.lang
- java.util
- javax.microedition.io
- javax.microedition.lcdui
- javax.microedition.lcdui.game
- javax.microedition.media
- javax.microedition.media.control
- javax.microedition.midlet, javax.microedition.pki
- javax.microedition.rms

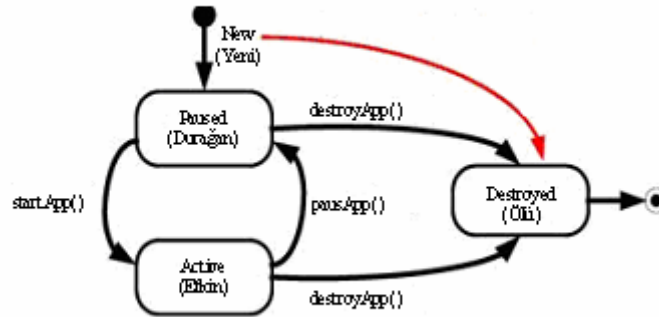
### MIDP Programlama ve MIDlet'ler

CLDC üzerinde, MIDP profili için yazılan Java uygulamaları MIDlet olarak adlandırılır. Yaygın bir şekilde desteklenen bir profil olduğunda J2ME uygulaması ve bir gezgin aygıtta Java denildiğinde kastedilen MIDlet'tir. Midlet, aygıtta değişik yollarla indirilir ve çalıştırılır. Bir MIDP uygulaması geliştirmek için bazı temel bilgileri edinmek gerekir. Bunlardan bazıları: MIDlet'lerin yaşam döngüsü, kullanıcı arabirimleri, komut işleme, konuşlandırma ve uygulama yönetimi olarak sayılabilir.

### MID'let Yaşam Döngüsü

AMS (Application Management Software - Uygulama Yönetim Yazılımı) MIDlet'in kurulumu, başlaması, durdurulması ve kaldırılması ile ilgili işlemlerin yapıldığı ortamdır. AMS, JAM (Java Application Manager - Java Uygulama Yöneticisi) olarak da bilinir.

MIDlet'ler 3 durumda bulunabilir (Şekil 3.33) : durağan (paused), etkin (active) ve ölü (destroy). Bir MIDlet oluşturulduğu ve başlatıldığı zaman durağan kiptedir. Eğer MIDlet yapılandırıcısında kural dışı bir durum oluşursa MIDlet ölü durumuna geçer. MIDlet'ler etkin durumdan durağan duruma pauseApp() metodunu tamamladıktan sonra geçebilirler. Veya etkin konumdan durağan duruma startApp() metodunu tamamladıktan sonra geçebilirler. MIDlet'ler ölü konumuna destroyApp() metodunun tamamlanmasından sonra geçerler. Bu metot MIDlet'in kullandığı kaynakları serbest bırakır ve gerekli temizleme işlemlerini yapar.

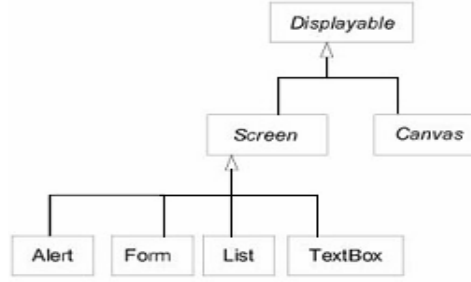


Şekil 3.33. MIDlet yaşam döngüsü

Bir MIDlet yazılımcısı yazılımını etkin kipte çalıştırır ve gerektiği zaman diğer durumlar arasında geçişleri sağlar.

### MIDP Kullanıcı Arabirimi

MIDP kullanıcı arabirimi düşük ve yüksek düzey olmak üzere iki ana kategoriye ayrılır. Düşük düzey kullanıcı arabirimi Canvas isimli nesneye dayanır. Yüksek düzey kullanıcı arabirim nesneleri ise Alert, Form, List ve TextBox olarak sıralanabilir (Şekil 3.34). Bu nesnelerin görünüş biçimleri profilin gerçekleştirildiği cihazların kullanıcı arabirimlerine göre değişebilir.



Şekil 3.34. MIDP kullanıcı arabirimi nesneleri (Efe, 2003)

Canvas nesnesi ile kullanıcı arabirimine daha direkt kontrol sağlanır. Mesela ekranda nelerin çizileceği ve klavye olayları hakkında daha geniş bir kontrol sağlanır. Kullanıcı arabirimlerini kullanırken en önemli, dikkat edilmesi gereken nokta yazacağımız MIDlet'lerin değişik kapasiteli cihazlarda çalışabiliyor olmasıdır. Dolayısı ile ekran genişliği, ekranın renkli veya siyah-beyaz oluşuna göre bir takım kontroller yaptırılarak MIDlet'ler bu değişik ortamlara uyum sağlayabilecek şekilde yazılabilir.

### Midlet Geliştirme ve Kurulum

Cep telefonları MIDP profile'ni desteklerler. Cep telefonunda çalışan bir program yapmanız için MIDlet class'ını extend etmelisiniz. Yaptığınız programın cep telefona kurulması için jar ve jad dosyalarının oluşturulması gerekmektedir. jar ve jad dosyalarını kullandığınız editor'ler sizin için oluşturmaktadırlar. jar dosyası class dosyalarının bulunduğu sıkıştırılmış dosyadır. jad dosyası ise midlet ve jar hakkında bilgi tutan bir dosyadır, jar ve jad dosyası kablo yoluyla telefona kurulabilir. PC'de bulunan bir jad veya jar kablo ile telefona kurulabilir. Kablo dışında bluetooth usb dongle kullanılarak da bu dosyalar cep telefonlarında kurulabilir. Tüm java destekli telefonlar bunu desteklerler.

### Basit Bir Örnek

Cep telefonunda çalışan programlara midlet denir. Midlet yaratmak için javax.microedition.midlet paketindeki MIDlet class'ını extend etmeniz gerekir. MIDlet class'ı abstract bir class'tır. Aşağıdaki üç method implement edilmelidir.

```

public void startApp() {}
protected void pauseApp() {}
protected void destroyApp(boolean boolean0) {}

```

Aşağıda ekrana HelloWorld yazdıran bir MID'let örneği görülmektedir.

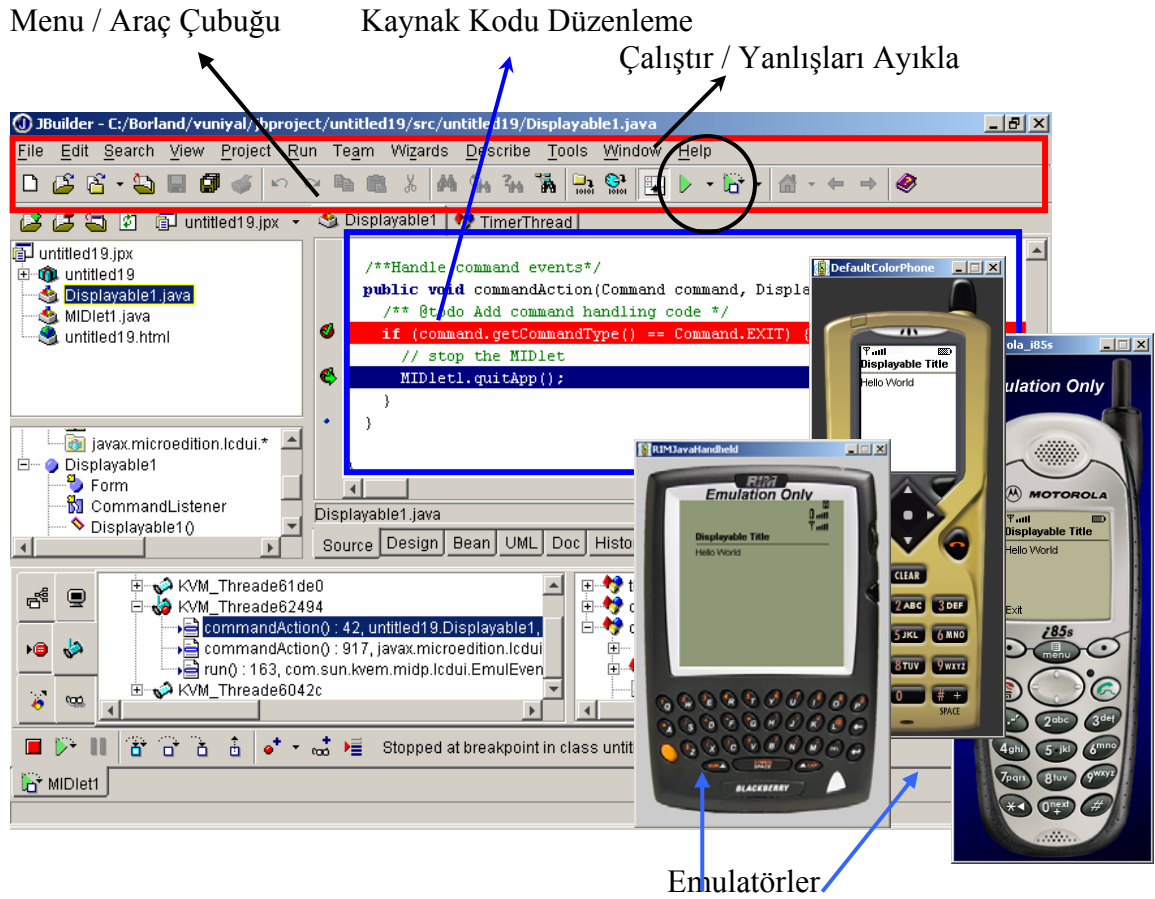
```

import javax.microedition.midlet. *;
import javax.microedition.midlet. *;
public class Hello World extends MIDlet{
    protected void startApp(){
        TextBox box=new TextBox("Hello","Hello World",100,TextField.ANY);
        Display.getDisplay(this).setCurrent(box);
    }
    protected void pauseApp(){}
    protected void destroyApp(boolean boolean0){}
}

```

## 3.1.16.2. Borland J Builder 9/X (MobileSet 3.0)

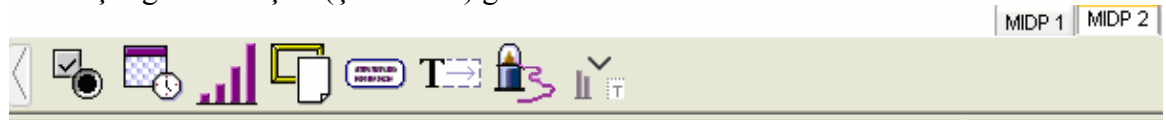
Borland JBuilder içerisinde J2ME araçları bütünleşik haldedir. JBuilder ile geliştirilen gezgin uygulamalar aslında J2ME araçları kullanılarak geliştirilmektedir. Java desteği olan tüm aygıtlarda JBuilder (Şekil 3.35) ile geliştirilen uygulamalar çalıştırılabilir.



Şekil 3.35. JBuilder uygulama geliştirme ortamı ve emulatorlar (Aksu, 2005).

MIDP/CLDC platformları, J2ME uygulamaları geliştirmek için Borland J Builder ile tam bütünleşmiş bir haldedir.

Borland J Builder, Java geliştirme özelliklerinden daha fazlasını sağlar. Bunlar hata ayıklama, yerleştirme araçları (deployment), emulasyon aygıtı, gezgin uygulamalar oluşturmak için görsel araçlar (Şekil 3.39) gibi önemli özelliklerdir.



Şekil 3.36. J Builder (MobileSet 3.0)'in kullanıcı arabirimi oluşturma araçları.(Aksu, 2005)

### 3.2. METOD

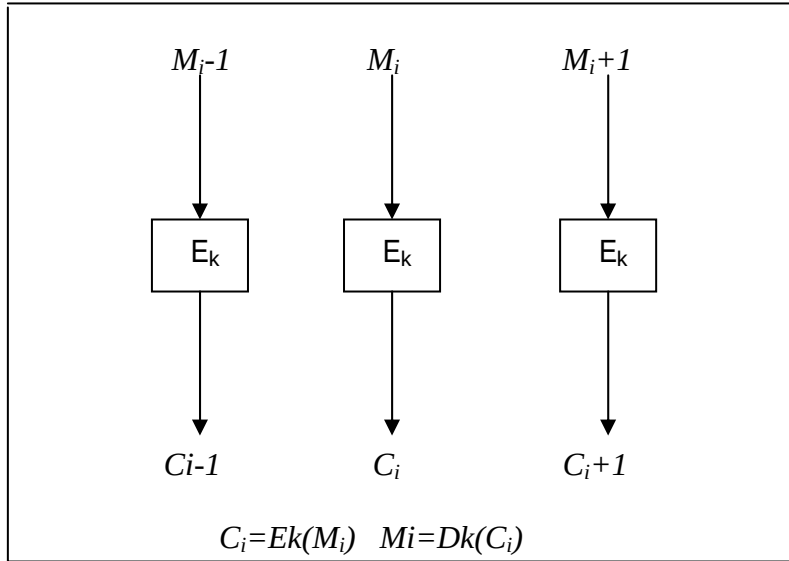
#### 3.2.1. DES Algoritması

1970’li yılların başında IBM’in Lucifer algoritmasını geliştirmesiyle ortaya çıkardığı, o zamanlar DEA olarak adlandırılan bir blok şifre algoritmasıdır. Bu algoritma 1977 yılında Amerika FIPS’de standartlaşırken DES olarak adlandırılmıştır. Yayımlandıktan sonra tüm dünyada en çok bilinen ve üzerinde an çok çalışılan simetrik anahtar algoritması olmuştur.

DES algoritması 64 bitlik blok uzunluğunda ve 56 bitlik anahtar boyutuna sahip bir blok şifresidir. Donanımsal olarak kolayca üretilebilmesi için geliştirilmiş bir Feistel yapısı içerir. Hem şifreleme ve şifre çözme algoritmalarında, hem de mesaj kimlik doğrulama kodu (MAC) üretilmesi ve doğrulanması algoritmalarında, hem de mesaj kimlik doğrulama kodu (MAC) üretilmesi ve doğrulanması algoritmalarında kullanılmaktadır.

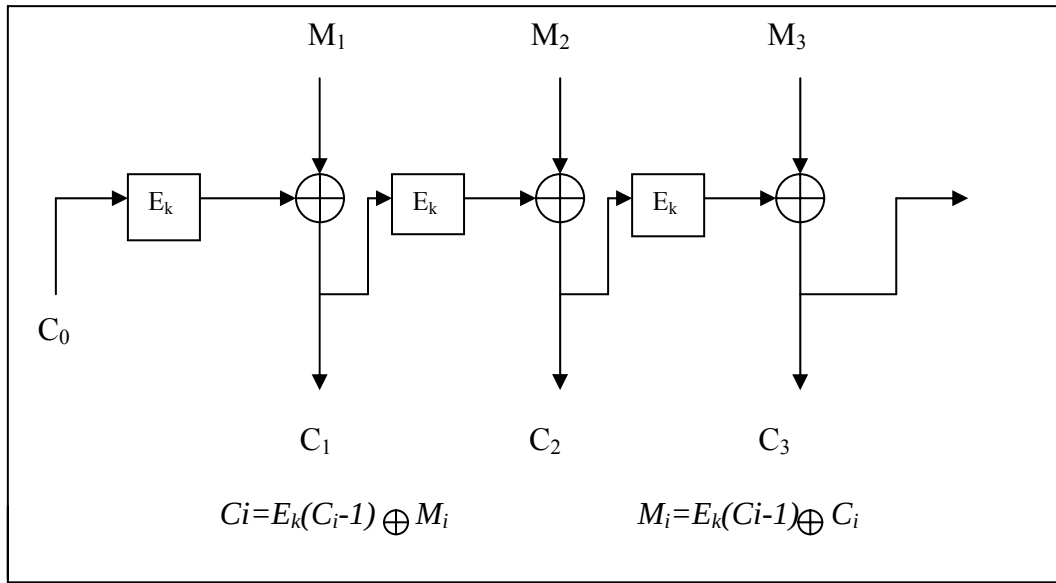
DES algoritmasının FIPS’te şifreleme için tanımlanmış, farklı özelliklere sahip dört çalışma modu bulunmaktadır. Bu modlar ECB, CBC, CFB ve OFB modlarıdır (National Institute of standards and Technologies (NIST, 1980).

ECB modu 56 bitlik bir anahtar kullanarak, birbiri ardına 64 bitlik şifresiz veri bloklarını şifreler (Şekil 3.37).



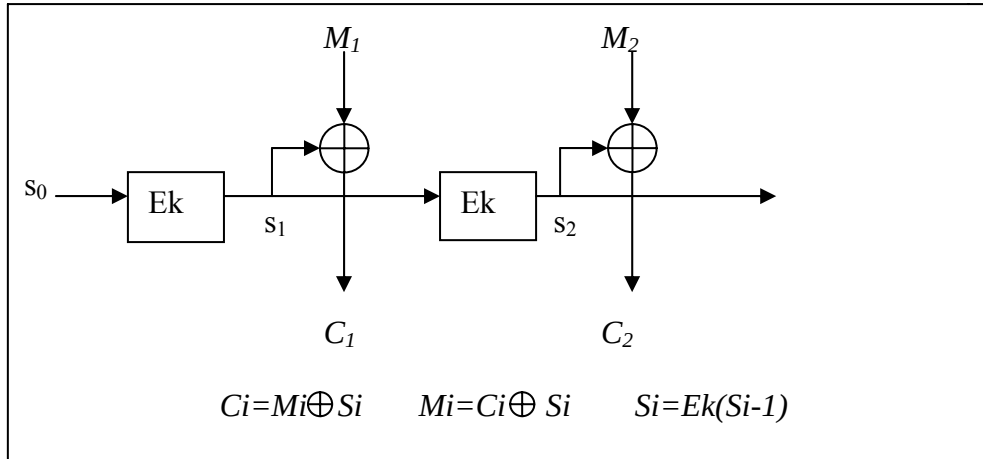
Şekil 3.37. ECB modu

CFB de (Şekil 3.38) ise şifrelenmiş bir önceki metin bloğu tekrar şifrelenip, şifresiz metin bloğuyla mod 2 toplama işlemine tabi tutularak yeni şifrelenecek metin bloğunu oluşturur. Şifreli metnin şifrelenmesi, şifresiz metnin şifrelenmesinden daha rastlantısal bir çıktı oluşturduğu için diğer modlara göre daha güçlüdür.



Şekil 3.38. CFB modu

OFB modu (Şekil 3.39) ise CFB moduna çok benzer. Her bir şifresiz metin bloğuyla mod 2 toplama işlemine sokulan değer, şifresiz metin bloğundan da şifreli metin bloğundan da bağımsız olarak, sadece bir önceki değerın şifrenmesiyle üretilir. Dolayısıyla şifrelemeye ilk olarak katılacak bir ilklendirme vektörüne ihtiyaç duyar. Bu modun CFB moduna göre en önemli avantajı, iletişim sırasında oluşan bit hatalarının diğer blokların şifre çözümünü etkilememesinden dolayı, hatanın sadece bilginin kaybolduğu blokta kalmasıdır.



Şekil 3.39. OFB modu

**Triple DES**

İlk olarak Diffie ve Hellman tarafından 1997 yılında önerilmiştir. DES algoritmasının üç defa kullanılmasıyla elde edilir. Daha çok bankacılık sektöründe uygulama alanı bulmuştur.  $k_1$ ,  $k_2$  ve  $k_3$  şifreleme anahtarları,  $M$  şifresiz metin,  $E_k$  DES şifreleme algoritması ise, şifreli metin:

$$C=E_{k_3}(D_{k_2}(E_{k_1}(M)))$$

Yukarıda açıklanan şifreleme modu bazı kaynaklarda DES-EDE olarak da adlandırılır. Ayrıca şifreleme algoritması  $E_k$ 'nın üç defa arka arkaya kullanılmasıyla oluşan DES-EEE modu da yine triple DES için kullanılan çalışma modlarından biridir.

ANSI X9.52 standartlarına göre de Triple DES algoritmasında üç anahtar seçeneği kullanılabilmektedir. Buna göre;

- $k$ ,  $k_2$  ve  $k_3$  şifreleme anahtarların her biri birbirinden farklı ve bağımsız,
- $k$  ve  $k_2$  bağımsız,  $k_3=k$
- $k=k_2=k_3$

Triple DES, standart DES algoritmasından daha iyi performans gösterir. Fakat yavaş olduğu için günümüz ihtiyaçlarını karşılayabilecek bir algoritma olarak görülmemektedir (Hellman ve ark.; 1981 ; Oorschot ve ark.;1991 ; Kaliski , 1994).

**3.2.2. Rijndael (AES) Algoritması**

Şifreleme alanında oluşturulan algoritmaların gün geçtikçe daha kolay çözülmeye başlaması, NIST'i de yeni bir güvenlik algoritması arayışına sokmuştur. NIST'in asıl amacı FIPS'de yer alacak ve gizli devlet bilgilerinin korunmasını sağlayacak bir şifreleme algoritması gerçekleştirmektir.

NIST, 2 Ocak 1997 tarihinde tüm dünyayı kapsayan bir çağrı yaparak, adaylardan yeni oluşturulacak AES için bir algoritma önermeleri istenmiştir. Bu algoritmaların DES gibi simetrik blok şifresi olması ve en az 128 bit blok uzunluğunda işlem yaparak, 128, 192 ve 256 bitlik anahtarlar ile şifrenmesi gerekmektedir.

20 Ağustos 1998 tarihinde on iki ülkeden gelen başvurular değerlendirilmiş ve onbeş AES algoritmasının ilk turu geçtiğini açıklanmıştır. Bu algoritmalar: CAST-256 (Kanada), Deal (Kanada ve Norveç), MARS (ABD), RC6 (ABD), Twofish (ABD), Safer + (ABD), HPC (ABD) , Frog (Kosta Rika), Magenta (Almanya), Rijndael (Belçika), DFC (Fransa), Serpent (İngiltere, İsrail, Norveç), Crypton (Güney Kore), E2 (Japonya) ve LOK197 (Avustralya).

15 Nisan 1999 tarihinde tüm dünyadan gelen yorum ve incelemeler baz alınarak ikinci tur ile bu sayı beşe düşürülmüştür. Buna göre finale kalan algoritmalar: MARS, RC6, Serpent, Twofish ve Rijndael olmuştur. Bluetooth'un şifreleme algoritması olan Safer+ ise elenerek ikinci tura geçememiştir.

2 Ekim 2000 tarihine kadar da hem NIST hem de ilgili diğer kuruluşlar tarafından yapılan incelemeler ve analizler sonucunda, AES'in bir Rijndael algoritması olması gerektiğine karar verilmiştir. Kasım 2001 tarihinde de Rijndael algoritması FIPS 197'de yayınlanarak kullanılmaya başlanmıştır (Overview of the AES Development Effort, 2001).

Rijndael, John Daemen ve Vincent tarafından geliştirilen bir gizli anahtar blok şifre algoritmasıdır. Değişken blok ve anahtar uzunluğuna sahiptir. 128, 192 veya 256 bit uzunluklarındaki bloklar, yine 128, 192 ve 256 bit uzunluğundaki anahtarlar ile şifrelenebilmektedir (Daemen ve ark.; 2003).

FIPS 197'de AES olarak 128 bit uzunluğundaki bloklar için kullanılan uyarlaması standartlaştırılmıştır (FIPS PUB 197, 2001).

Temel olarak J.Daemen, L.Knudsen ve V.Rijmen tarafından geliştirilen Square blok şifre algoritmasına dayanır. Bu algoritma bir çok blok şifre algoritmasının temelini oluşturan Feistel şifre yapısından tamamen farklı bir tasarıma sahiptir. Algoritma içerisinde blok anahtar uzunluğuna göre farklı tur işlemi yapılır (Daemen ve ark.; 1997).

Buna göre:

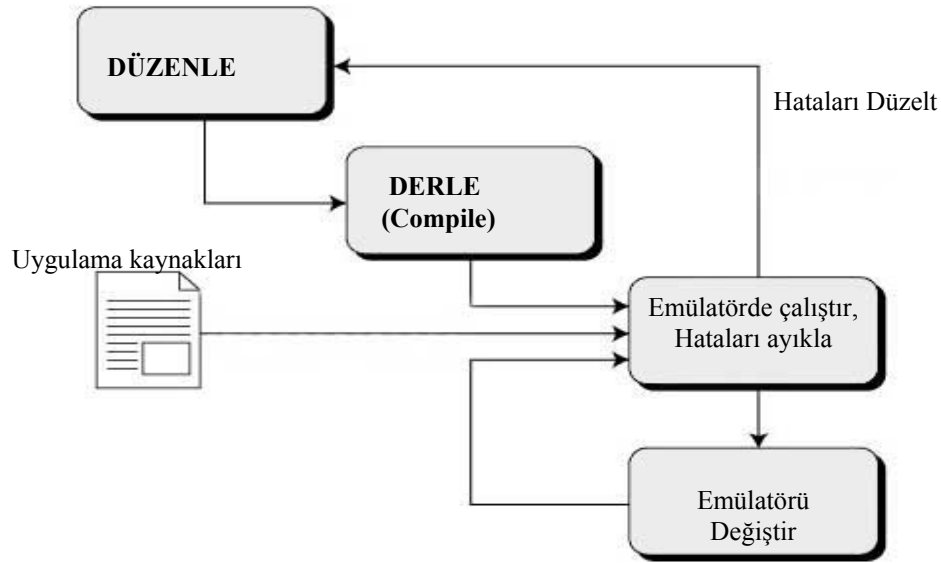
- Eğer hem blok hem de blok uzunluğu 128 bit ise 9 tur,
- Blok veya anahtar uzunluklarından birisi 192 bit, diğeri 128 veya 192 bit uzunluğunda ise 11 tur,
- Blok veya anahtar uzunluğundan herhangi birisi 256 bit ise 13 tur kullanılır.

Günümüzde bilinen en güvenilir blok şifre algoritmasıdır. Hem donanım hem de yazılım olarak kolayca uygulanabilen, basit, hızlı, az yer kaplayan ve çok yönlü bir yapısı vardır.

Rijndael algoritmasının AES olarak standartlaşmasıyla beraber, simetrik anahtar blok şifre algoritmaları için yeni bir çalışma modu daha önerilmiştir. CTR olarak adlandırılan bu mod FIPS tarafından kabul edilerek Kasım 2001 yılında yayınlanmıştır (National Institute of Standards and Technologies (NIST), 2001).

### **3.2.3. Uygulama Geliştirmede Emülatörlerin Kullanımı**

Uygulama geliştirmede bir problemin nihai sonucunu hemen ulaşılamaz. Sonuca ulaşma birçok denemeyi gerektiren öteleme işlemleridir. Şekil 3.40 akış şeması biçiminde bu deneme işlemlerini (emülatör kullanım döngüsü) göstermektedir. Bu şema yazılımı kullanarak fiziksel cihazların karakteristiklerini benzetip programlayarak aygıt emülatörleri ile ilgili genel düşünceyi ortaya koyar. Başarılı bir ürün elde etmek için gerekli olan ilk yapılacak şey prototipin geliştirilmesidir. Geliştirilmiş gezgin ve kablosuz uygulamalar çoğu uygulama geliştiricileri için yeni bir deneme olacaktır (çünkü onlar genellikle sınırlı bellek ve ekran boyutları ile çalışma tecrübesine sahip değillerdir). Üstelik çoğu uygulama geliştiriciler güvenli ağlar üzerinde çalışmaktadır (Aksu, 2005)



Şekil 3.40. Uygulama geliştirmede emülatörlerin kullanım döngüsü.

Gezgin aygıtlar biçim ve boyut olarak farklıdır. Çünkü yeni yönetim kaynakları, kullanıcı ara yüzleri için karmaşık yapılar ilave edilmiştir.

Gezgin cihazlar için uygulama geliştirirken geliştirme ve test döngüsü için gezgin cihazların karakteristiklerini simüle eden emülatörler kullanılırlar. Geliştirilen uygulamanın son hali yani hatalardan ayıklanmış hedeflenen çözüm gezgin cihaza yüklenir. Gerçekten emülatörler gezgin uygulamalar geliştirmek için iyi çözümdür. Yoksa çok pahalı gezgin cihazları temin etmek kolay değildir.

### 3.2.4. Geliştirilen Uygulamanın Gezgin Telefona Aktarılması

PC veya dizüstü bilgisayarlarda geliştirilen gezgin telefon uygulamaları ya da doğrudan USB, seri, paralel bağlantılarla veya cep telefonundan internete bağlanarak internet üzerinden ya da kablosuz bağlantılarla (Bluetooth,) gezgin telefon cihazına aktarılır (Şekil 3.41) kullanılır.



Şekil 3.41. Geliştirilen uygulamanın gezgin telefona aktarılması (Aksu, 2005).

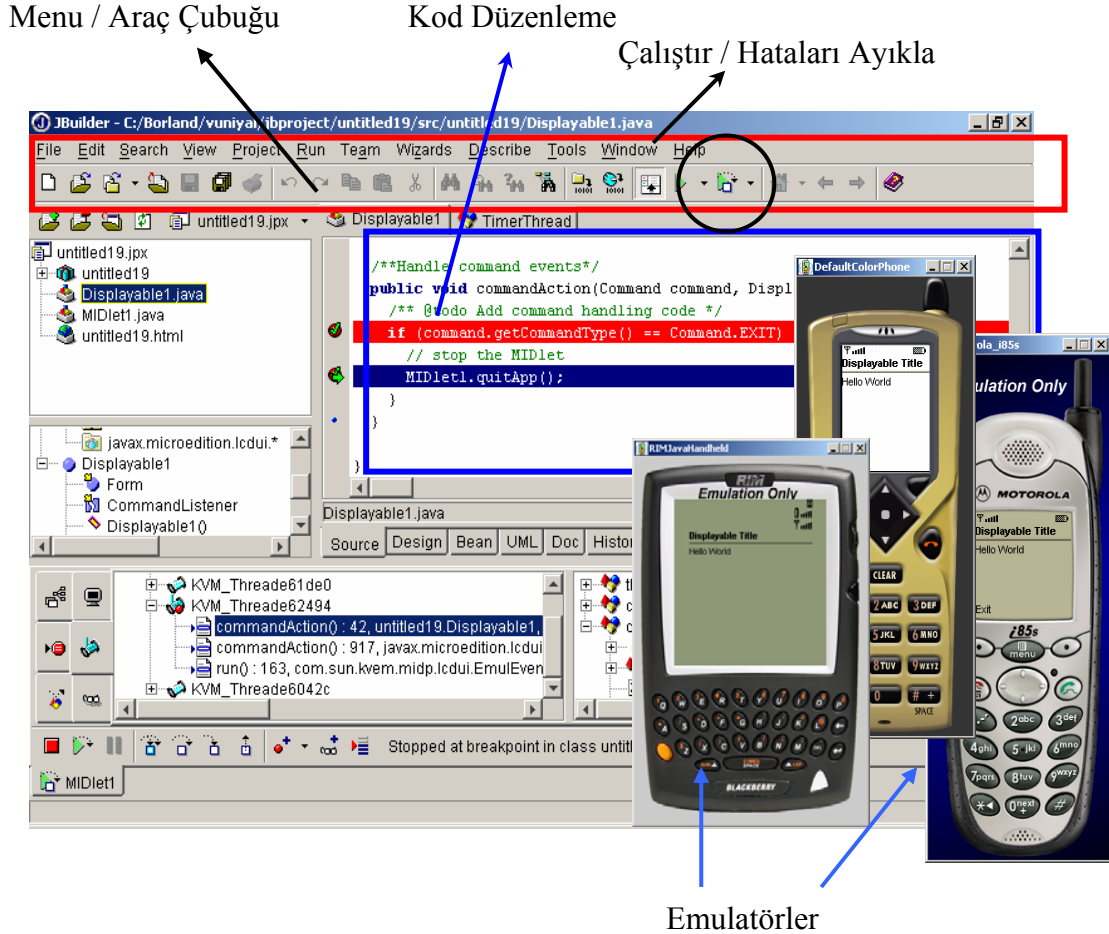
PC üzerinden doğrudan aktarma yapılabilir. Bunun için USB, seri v.b. bağlantılarda kullanılmak üzere telefonla birlikte verilen özel veri kablosu gerekmektedir.

PC üzerinden göndermede başka bir metot ise PC'ye kızıl ötesi ya da Bluetooth cihazları takılarak PC'lere kızıl ötesi veya Bluetooth özelliği kazandırılabilir. PC üzerinden Borland JBuilder ortamında oluşturulan midlet uygulaması, gezgin telefona belirtilen bluetooth usb dongle veya PC-Gezgin telefon bağlantısı sağlayan kablo vasıtasıyla aktarılacaktır. İki PC arasında Bluetooth USB Dongle kullanılarak güvenli iletim metodu uygulanacaktır.

#### 4. BULGULAR VE TARTIŞMA

##### 4.1. İki Gezgin Telefon Arasında Bluetooth Üzerinden Güvenli Veri İletimi

Uygulama geliştirmek için dil olarak Borland J Builder 9 kullanılmıştır. Borland J Builder içerisinde J2ME araçları bütünleşik haldedir. Borland J Builder ile geliştirilen gezgin uygulamalar aslında J2ME araçları kullanılarak geliştirilmektedir. Java desteği olan tüm aygıtlarda J Builder (Şekil 4.1) ile geliştirilen uygulamalar çalıştırılabilir.



Şekil 4.1. JBuilder uygulama geliştirme ortamı ve emulatörler (Aksu, 2005).

CLDC üzerinde, MIDP profili için yazılan Java uygulamaları MIDlet olarak adlandırılır. Yaygın bir şekilde desteklenen bir profil olduğunda J2ME uygulaması ve bir gezgin aygıtta Java denildiğinde kastedilen MIDlet'tir. Midlet, aygıtta değişik yollarla indirilir ve çalıştırılır. Bir MIDP uygulaması geliştirmek için bazı temel bilgileri edinmek gerekir. Bunlardan bazıları: MIDlet'lerin yaşam döngüsü, kullanıcı arabirimleri, komut işleme, konuşlandırma ve uygulama yönetimi olarak sayılabilir.

MIDlet'ler üç durumda bulunabilirler: durağan (paused), etkin (active) ve ölü (destroy). Bir MIDlet oluşturulduğu ve başlatıldığı zaman durağan kiptedir. Eğer MIDlet yapılandırıcısında kural dışı bir durum oluşursa MIDlet ölü durumuna geçer. MIDlet'ler etkin durumdan durağan durumuna pauseApp() metodunu tamamladıktan sonra

geçebilirler. Veya etkin konumdan durağan duruma startApp() metodunu tamamladıktan sonra geçebilirler. MIDlet'ler ölü konumuna destroyApp() metodunun tamamlanmasından sonra geçerler. Bu metot MIDlet'in kullandığı kaynakları serbest bırakır ve gerekli temizleme işlemlerini yapar.

MIDP/CLDC platformları, J2ME uygulamaları geliştirmek için Borland J Builder ile tam bütünleşik bir haldedir.

Borland J Builder, Java geliştirme özelliklerinden daha fazlasını sağlar. Bunlar hata ayıklama, yerleştirme araçları (deployment), emulasyon aygıtı, gezgin uygulamalar oluşturmak için görsel araçları (Şekil 4.2) içerir. Bu gezgin görsel araçlar form üzerine eklenerek uygulama geliştirilebilir.

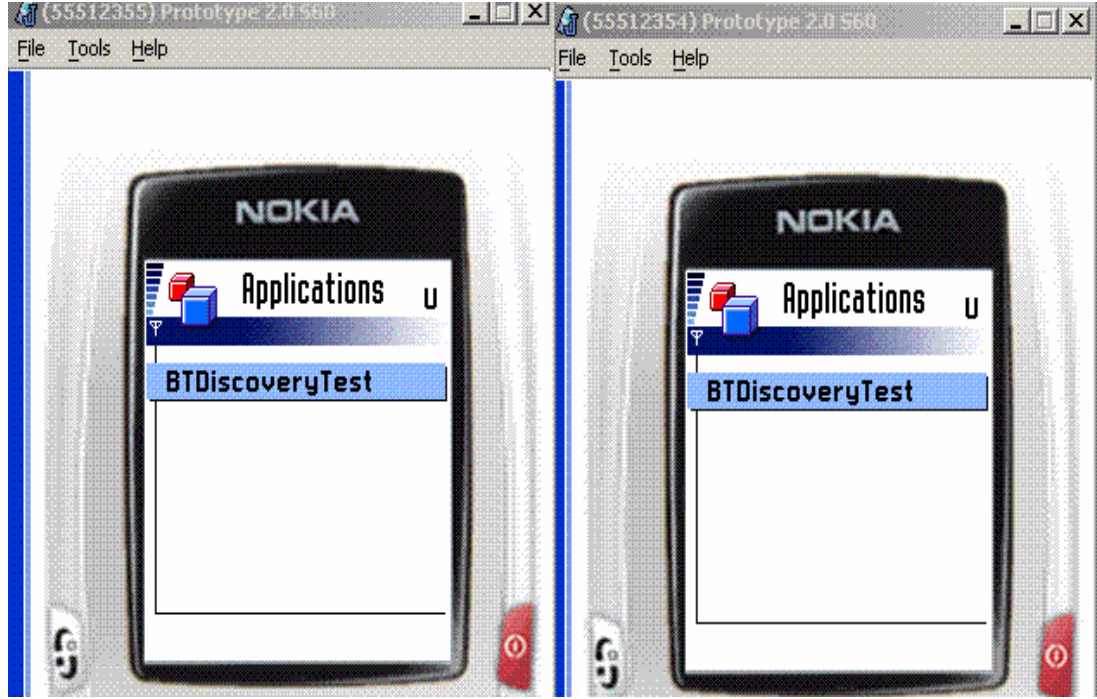


Şekil 4.2. JBuilder'in kullanıcı arabirimi oluşturma araçları.

Bluetooth üzerinden güvenli veri iletimi sağlayan JBuilder ortamında oluşturulan yazılım çalışması jad ve jar uzantılı iki tane MIDlet'ten oluşmaktadır. Yazılım çalışmasında simetrik algoritma türü olan DES algoritması kullanılmıştır. Uygulamanın gezgin telefonda çalışabilmesi için gezgin telefonun Java ve Bluetooth API destekli olması gerekmektedir.

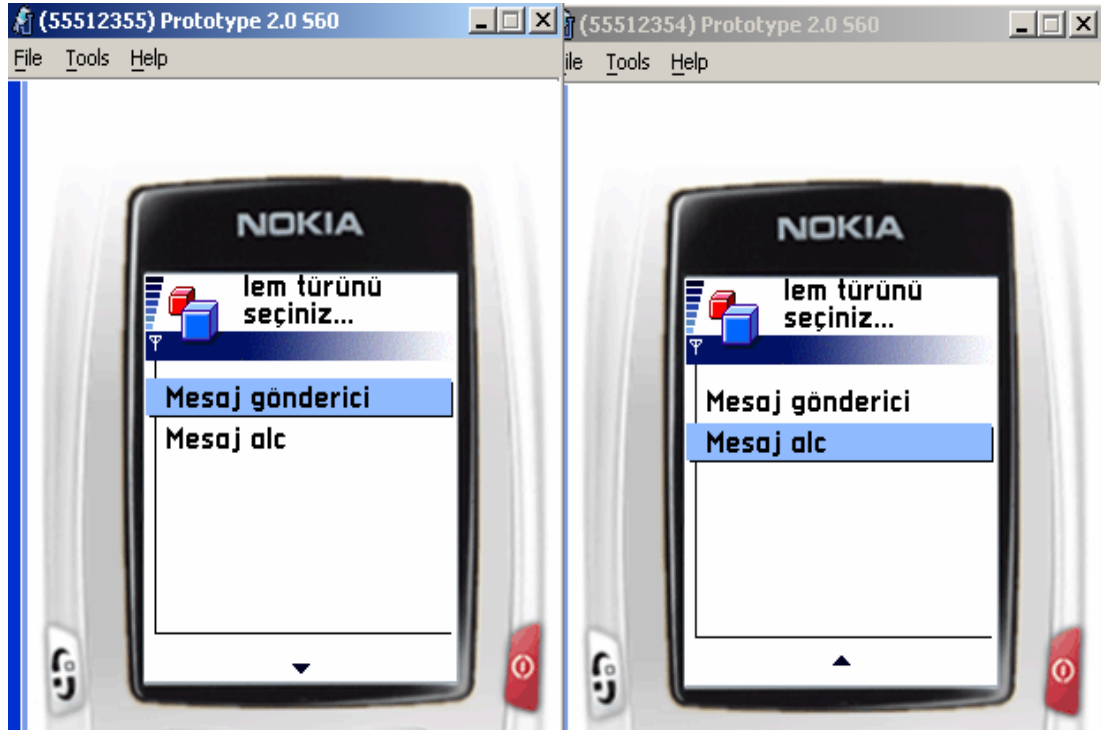
Oluşturulan şifreleme programı Nokia'nın 6600, 6630, 6230i, 6680 ve 6620 modellerinde, Sony-Ericsson'un P900 ve P910 modellerinde çalıştırılmıştır. Belirtilen cihaz modelleri Java ve Bluetooth API desteklidir.

Daha sonra uygulama iki emülatör arasında yapılmıştır. Bluetooth üzerinden güvenli veri uygulamasının emülatör görüntüleri sırasıyla aşağıdaki şekillerde verilmiştir.



Şekil 4.3. Emülatör görüntüleri

Şekil 4.3’de gezgin telefon emülatör görüntüleri verilmiştir. İşlem seçimi Şekil 4.4’de verilmiştir. Cihazlardan biri mesaj gönderici diğeri mesaj alıcı konumunu alır.



Şekil 4.4. Mesaj Gönderici ve Mesaj Alıcı Konumları seçimi



Şekil 4.5. Cihaz keşif

Bluetooth cihaz keşif sorgulaması sonucunda kapsam alanı içerisinde aktif bluetooth cihaz bulunarak seçilir. Mesaj gönderici cihaz, mesaj alıcı cihaz konumları alınır.



Şekil 4.6. Mesaj gönderici emülatörün cihaz keşif araması.

Bluetooth destekli cihazların aranması durumunda 10 m ortam içerisinde bluetooth bağlantı modu açık olan cihazlar aranır. Bu durum gezgin telefonlarında bağlantı-bluetooth açık seçimi yapılarak sağlanır.



Şekil 4.7. Bluetooth cihaz arama sorgulamasında bulunan cihaz.

Cihaz arama sonucunda şifreli veri gönderilecek emülatör seçilir.



Şekil 4.8. Gönderilecek verinin ve veri anahtar şifresinin girilmesi

Şekil 4.8’de gönderilecek veri yazılarak, veri şifre anahtarı girilir. Yazılımda kullanılan DES algoritması simetrik tür algoritma olduğundan veri şifre anahtarı mesajı çözmede önemlidir. Şifreleme ve şifre çözülmesinde aynı anahtar kullanılır.



Şekil 4.9. Mesaj gönderici emülatörün veriyi gönderme istemi.

Mesaj gönderici emülatörün veriyi gönderme isteği onaylandığında, Şekil 4.9'daki durum meydana gelir.



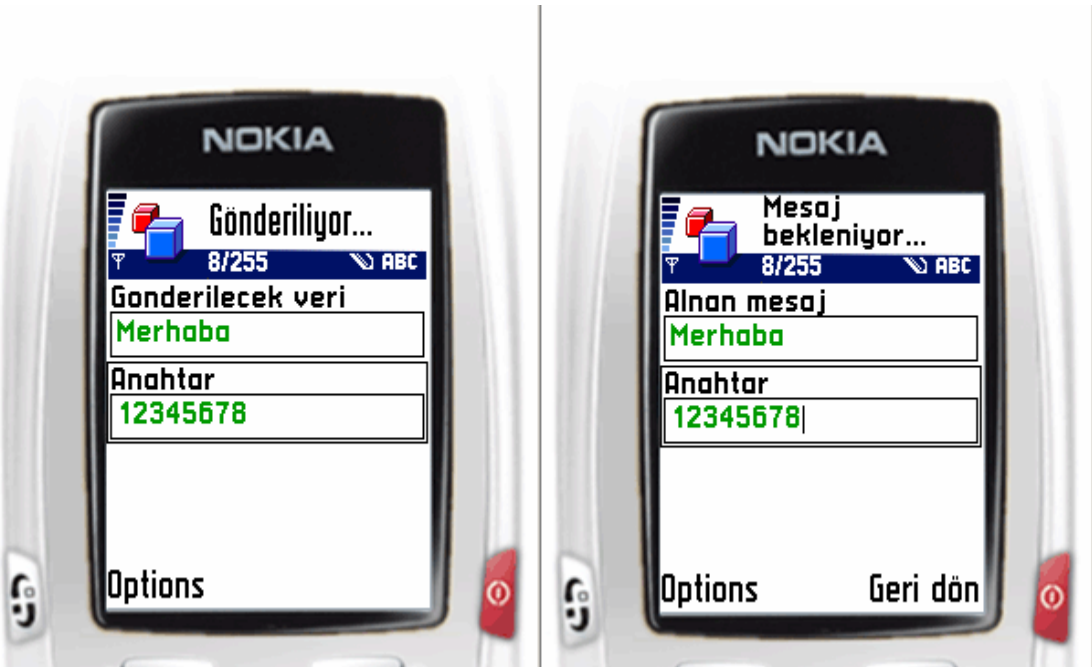
Şekil 4.10. Mesaj gönderici emülatörün veriyi şifreleyerek, mesaj alıcı emülatöre göndermesi

Mesaj göndericide yazılan ve 12345678 anahtarıyla şifrelenen "Merhaba" verisinin, Mesaj alıcıda şifrelenmiş görüntüsü (Şekil 4.10).



Şekil 4.11. Alınan şifreli verinin çözülmesi işlemi

Mesaj gönderici konumunda olan emülatörde şifreleme anahtarıyla şifrelenen verinin (Crypt), Master emülatörde çözülmesi (Decrypt) için aynı anahtarın girilmesi gerekir (Simetrik şifreleme). Aksi takdirde şifrelenen veri çözülemez (Decrypt).



Şekil 4.12. Mesaj gönderici emülatör tarafından gönderilen verinin, mesaj alıcı emülatörde çözülmesi.

İki emülatör arasında yapılan bu uygulama, iki Java ve Bluetooth API destekli gezgin telefon arasında yapıldığında aynı görüntüler meydana gelir. Borland JBuilder yazılım ortamında kullanılan algoritmanın simetrik olması şifrelemenin daha hızlı olmasına meydan vermektedir.

Aynı anahtar kullanılarak, mesaj gizliliğinin yanında veri bütünlüğünde sağlanabilmektedir. Bu şekilde de hem bu işlemler için harcanan zaman, hem de anahtar yönetimi için gereken ek yük azaltılmış olmaktadır.

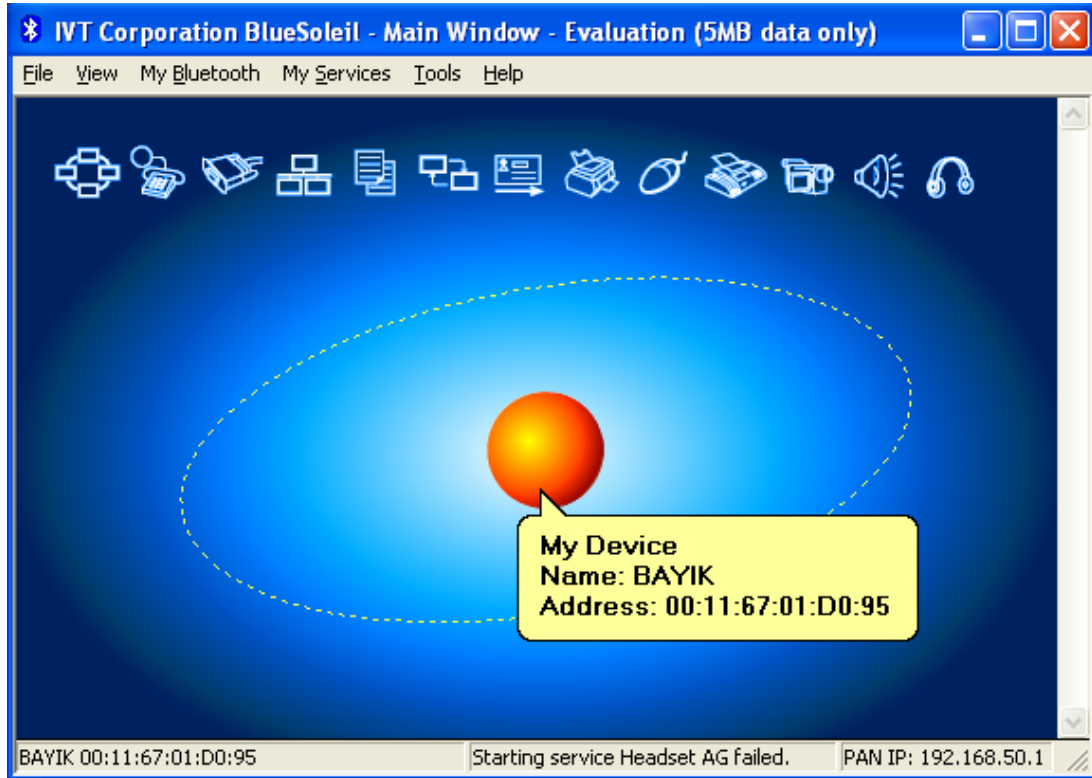
#### **4.2. İki Bilgisayar (PC) Arasında Bluetooth Üzerinden Güvenli Veri İletimi**

Bluetooth, hem yolculuk yapan notebook sahipleri için hem de masa üstü PC kullanıcıları için etkili bir seçenektir. Bir PDA'yı notebook ile senkronize etmek için olsun, bir PC'yi yazıcıya bağlamak için olsun , kabloları ortadan kaldırdığı bir gerçektir. Bununla birlikte, sadece az sayıda notebook ve daha az sayıda masaüstü PC, Bluetooth teknolojisi entegre edilmiş satılıyor. Bu yüzden kullanıcılar USB aparatlarına veya PC kartlarına yönelmek durumunda kalmaktadır.

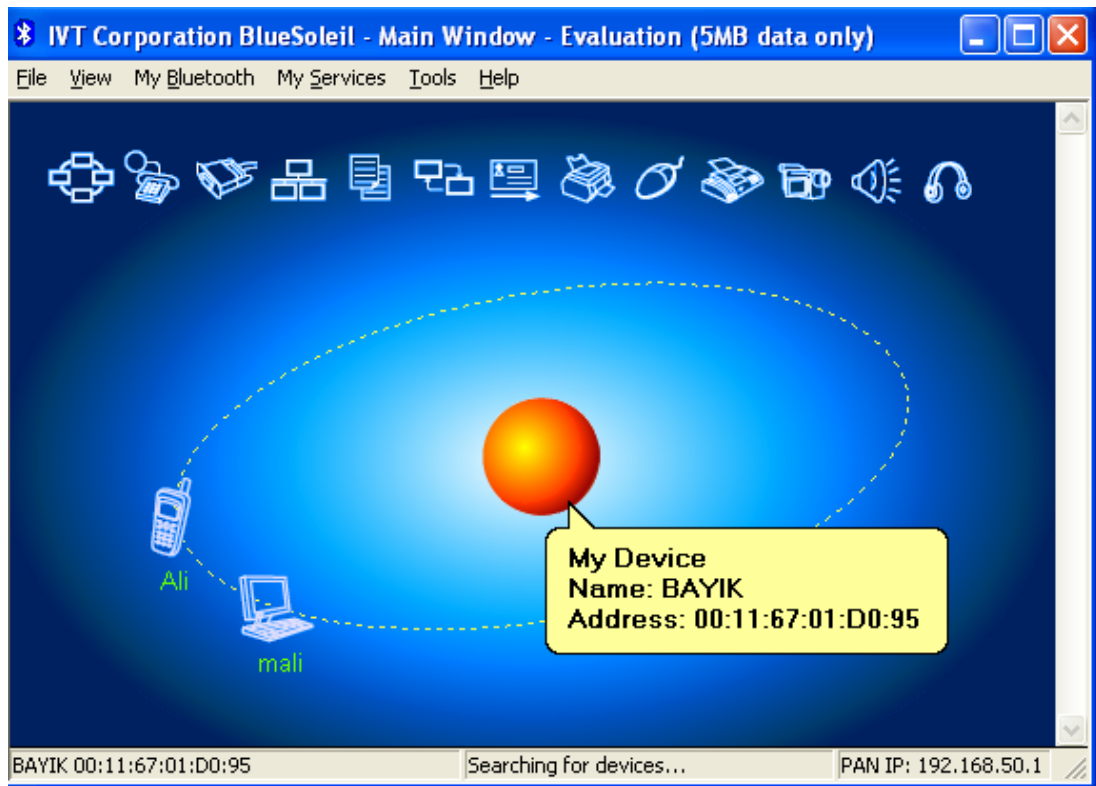
İki bilgisayar arasında bluetooth üzerinden güvenli veri iletimi uygulamasında kullanılan PC'lerde bluetooth özelliği olmadığından, PC'lere bluetooth özelliği kazandırmak için iki adet bluetooth USB aparatı kullanılmıştır.

Kullanılan aparatların algılama mesafesi 10 metre olup, bütün bluetooth cihazlarını desteklemektedir. Veri aktarım hızı ise yaklaşık 1 Mbit / Sn'dir. Bluetooth USB adapter, Bluesoleil Software ile kullanılmakta olup bu yazılım Windows 98 / 98 SE / ME / 2000 ve Windows XP desteklemektedir.

Şekil 4.13'te Bluesoleil yazılımının display görüntüsü görülmektedir. Görüntü orta kısmında bulunan dairesel şekil mouse'la tıklandığında cihaz keşif araması başlatılmış olur.



Şekil 4.13. Bluesoleil Display görüntüsü

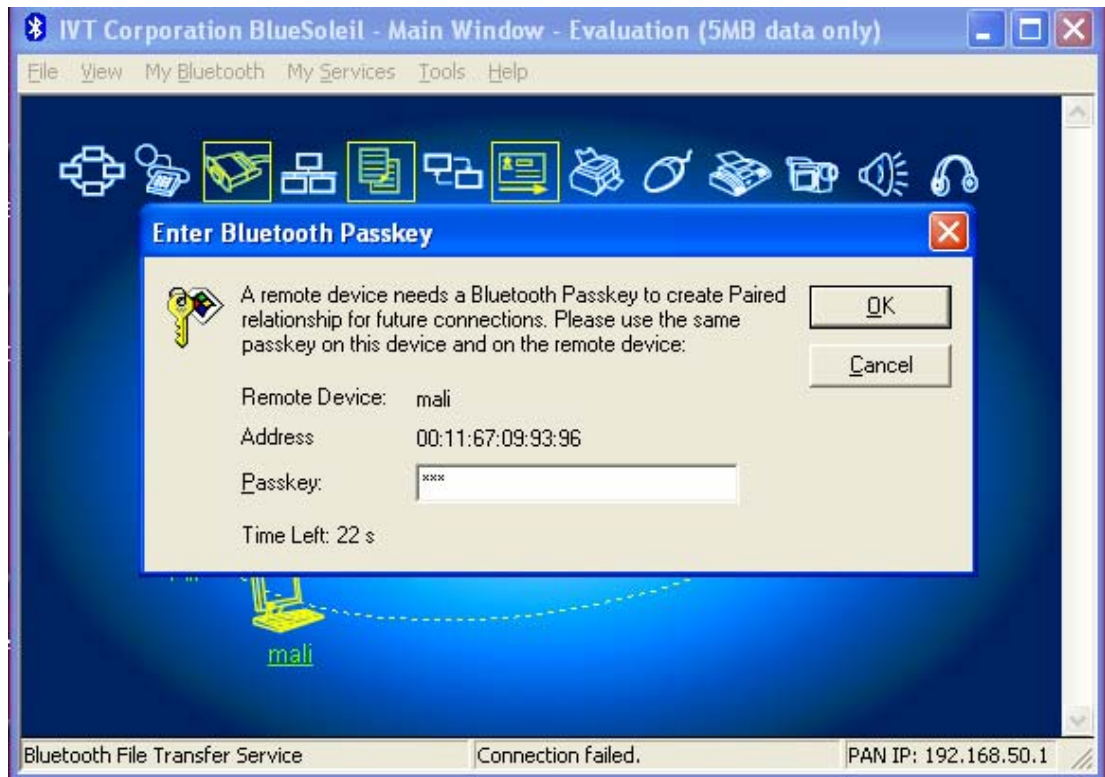


Şekil 4.14. Cihaz keşif tarama sonucu

Şekil 4.14’de görüldüğü gibi cihaz keşif tarama sonucunda kapsam alanı içerisinde bluetooth bağlantı durumu aktif PC ve Gezgin telefon piconet yapısı içerisinde görülmektedir. Görüntüleme piconet yapısı içerisinde cihaz adı ve adresi şeklindedir.

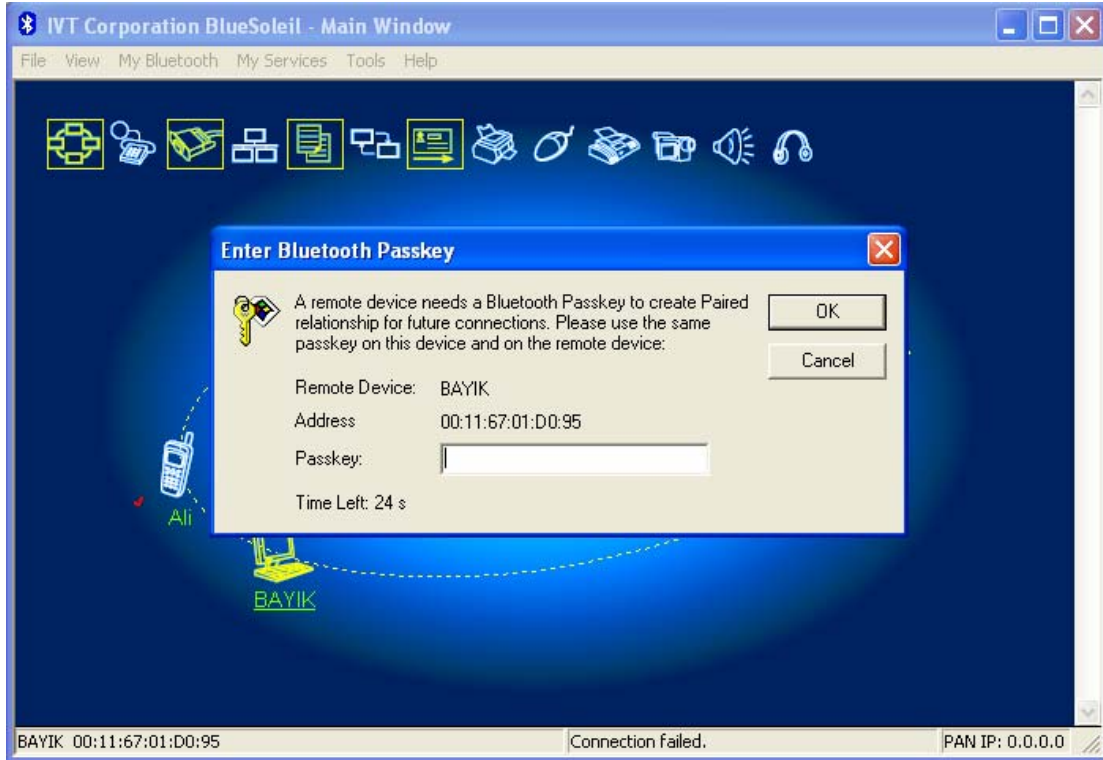
Bluesoleil yazılım seçenekleri, Bluetooth personal area networking service, Bluetooth dial-up networking service, Bluetooth serial port service, Bluetooth Lan access service, Bluetooth file transfer service, Bluetooth information synchronization service, Bluetooth object push service, Bluetooth printer service, Bluetooth human interface device, Bluetooth FAX service, Bluetooth basic imaging service, Bluetooth imaiging service, Bluetooth AV service, Bluetooth headset service şeklindedir.

Yapılan uygulamada Bluetooth file transfer service kullanılarak şifreli veri iletimi sağlanmıştır.

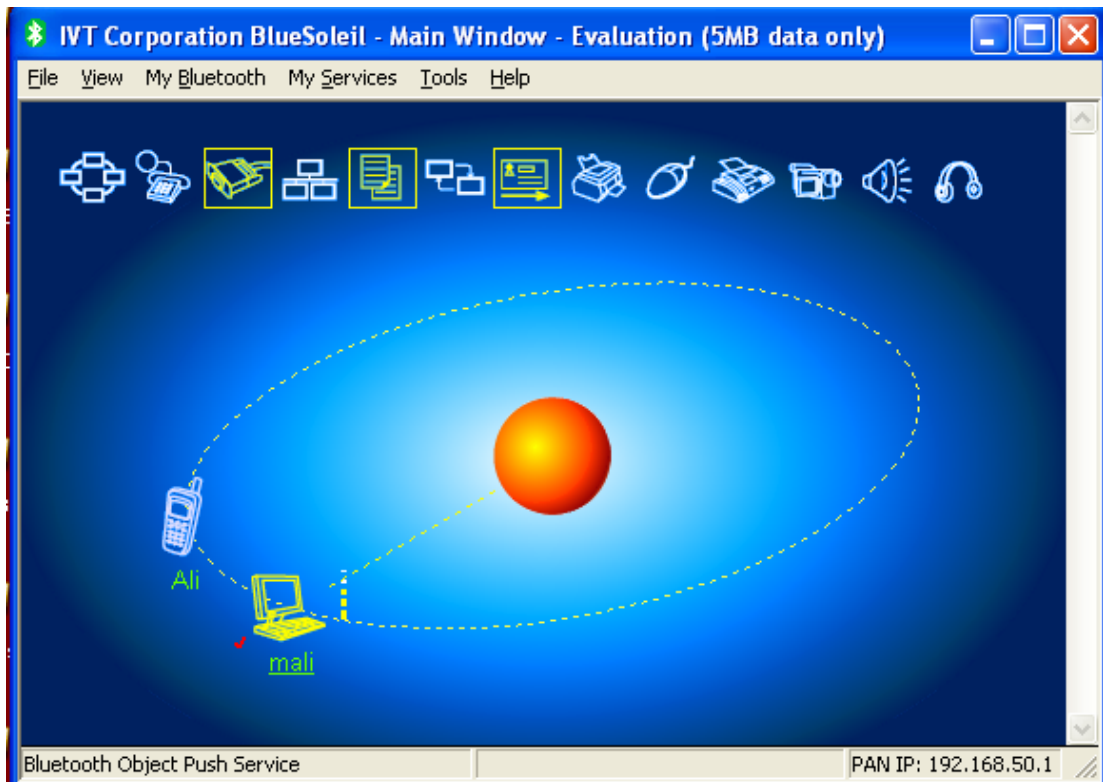


Şekil 4.15. İki PC arasında bağlantının sağlanması için giriş anahtar değerlerinin girilmesi

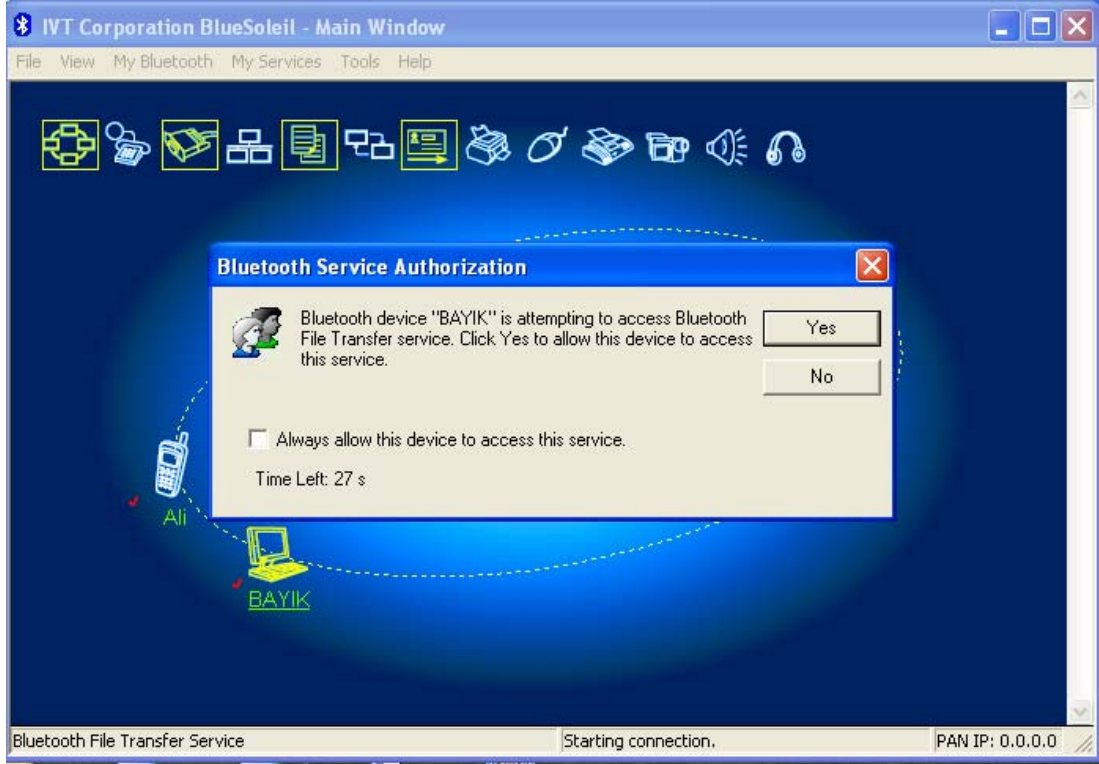
Veri iletiminin sağlanabilmesi için her iki PC’den girilen giriş anahtar değerlerinin aynı olması gerekmektedir. Aksi takdirde iletim sağlanmaz, aynı değerlerin girilmesi sonucu yapılan bağlantıda, dosya transferi yapılacak seviyeye gelmektedir. Bluesoleil software’in kurulması sonucunda Bluetooth adında bir klasör açılmaktadır. Bluetooth file transfer service ile gönderilen veriler alıcı konumdaki PC’de bulunan bluetooth klasörünün altında bulunan share klasörünün içerisine transfer edilmektedir.



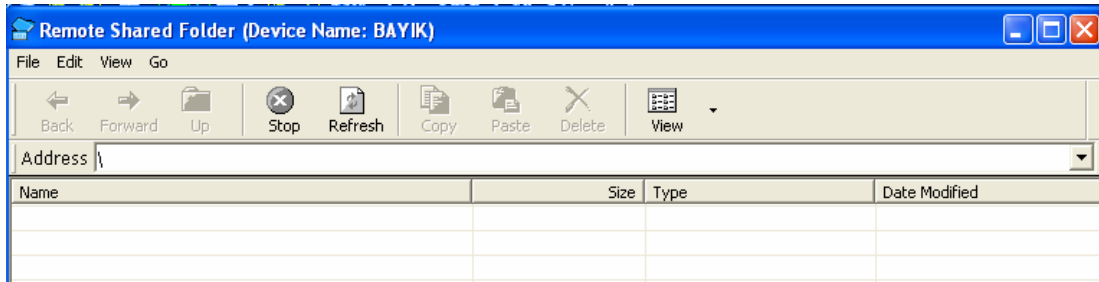
Şekil 4.16. Bayık PC'sinde girilen anahtar değerinin diğer PC'de girilmesi



Şekil 4.17. Aynı anahtar değerlerinin girilmesi sonucu bağlantının yapılması



Şekil 4.18. Bayık PC'sinin dosya transferini kabul etmesi



Şekil 4.19. Veri paylaşımını sağlayacak "Remote Shared Folder" in açılması

Remote Shared Folder'in açılması işleminden sonra iletilecek verinin şifrelenmesi aşamasına geçilir. Verinin şifrelemesinde Rijndael (AES) simetrik algoritması kullanılmıştır. Şifreleme yazılımın ara yüzünde iki kısım bulunmaktadır. Şifrelenecek metin birinci kısma yazıldıktan veya kopyalandıktan sonra Encrypt butonuna tıklandığında giriş anahtar değeri istenir, giriş anahtar değerinin girilmesiyle metin şifreli hale getirilir (Şekil 4.23), şifrelenen metin kopyalanarak oluşturulan word belgesinin içine atılarak "Gönderilecek şifreli metin adı" verilir (Şekil 4.24), şifrelenmiş word belgesi "Remote Shared Folder" içerisine aktarıldığında şifreli metin diğer alıcı cihaza bluetooth üzerinden aktarılmış olur. Bayık adlı PC tarafından alınan şifreli veri, shared klasörü altında kendine yer bulur, buradan tekrar alınacak şifreli doküman, Bayık PC'sinde de bulunan şifreleme yazılımının ara yüzü "şifrelenmiş metin" kısmına aktarılır (Şekil 4.27), bu kısımda "decrypt" butonuna tıklandığında şifrelemeyi sağlayan aynı zamanda deşifre işlemini de sağlayan şifreleme anahtarı istenir (Şekil 4.28), bu değer tekrar girildiğinde (Şekil 4.29), karşı cihazdan bluetooth üzerinden alınan şifreli metin çözülmüş hale gelir (decrypt).

Form1

Şifrelenecek metin

Telsiz kullanıcılarının önemli ihtiyaçlarından olan haberleşme gizliliği 80'li yıllardan başlayarak çeşitli tekniklerin kullanılmasıyla sağlanmaya çalışılmıştır. Önceleri analog tekniklerle sağlanmaya çalışılan haberleşme gizliliği, gerçek anlamda ancak sayısal tekniklerin geliştirilmesi ile sağlanabilmektedir.

Şifrenilmiş metin

Encrypt Decrypt

Şekil 4.20. Şifrelenecek metnin girilmesi

Form1

Şifrelenecek metin

Telsiz kullanıcılarının önemli ihtiyaçlarından olan haberleşme gizliliği 80'li yıllardan başlayarak çeşitli tekniklerin kullanılmasıyla sağlanmaya çalışılmıştır. Önceleri analog tekniklerle sağlanmaya çalışılan haberleşme gizliliği, gerçek anlamda ancak sayısal tekniklerin geliştirilmesi ile sağlanabilmektedir.

Şifrenilmiş metin

Encrypt Decrypt

InputDialog

Anahtar giriniz

OK

Şekil 4.21. Şifreleme (encrypt) anahtarının belirlenmesi

Şifrelenecek metin

Telsiz kullanıcılarının önemli ihtiyaçlarından olan haberleşme gizliliği 80'li yıllardan başlayarak çeşitli tekniklerin kullanılmasıyla sağlanmaya çalışılmıştır. Önceleri analog tekniklerle sağlanmaya çalışılan haberleşme gizliliği, gerçek anlamda ancak sayısal tekniklerin geliştirilmesi ile sağlanabilmektedir.

Şifrenilmiş metin

Encrypt Decrypt

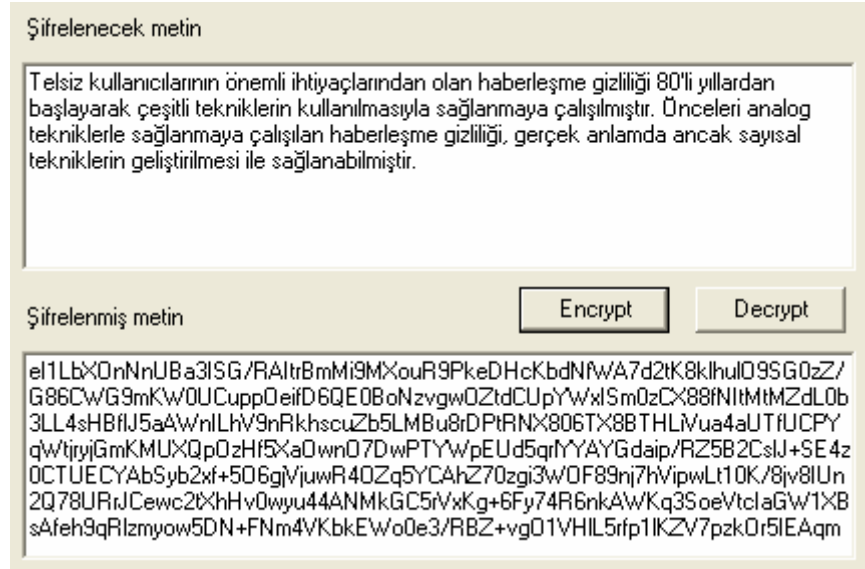
InputDialog

Anahtar giriniz

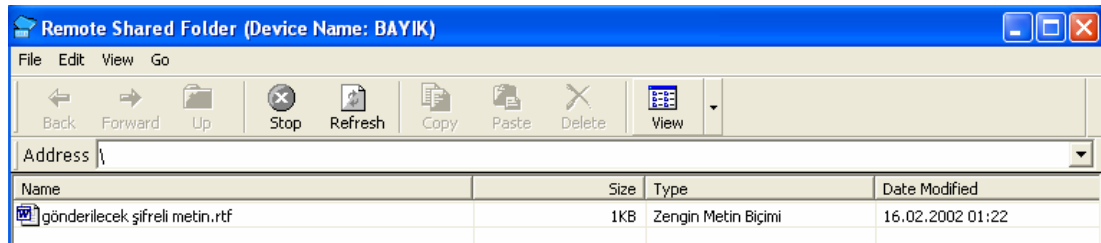
12345

OK

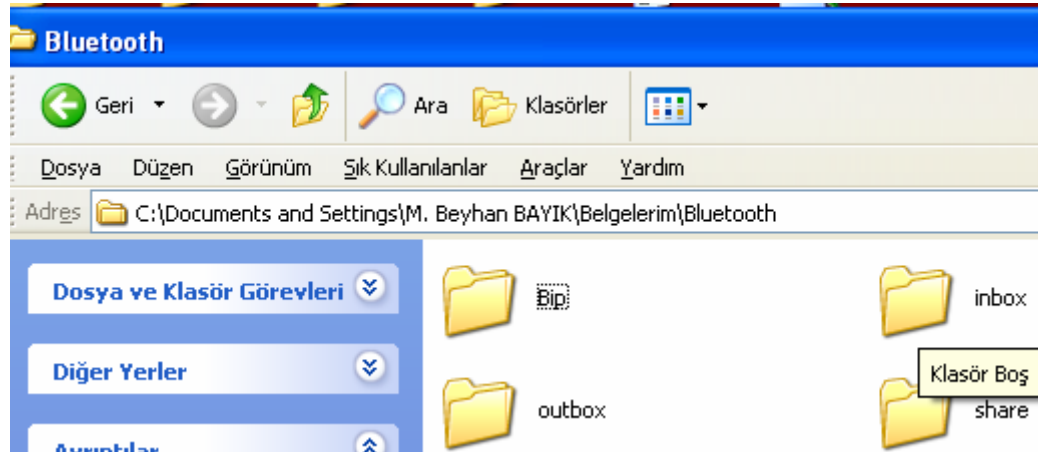
Şekil 4.22. Şifreleme (encrypt) anahtarının girilmesi



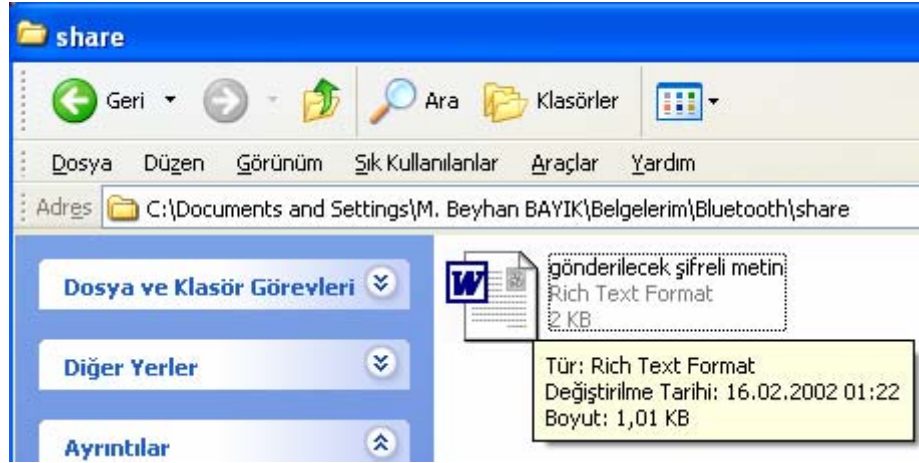
Şekil 4.23. Girilen metnin şifrlenmesi işlemi



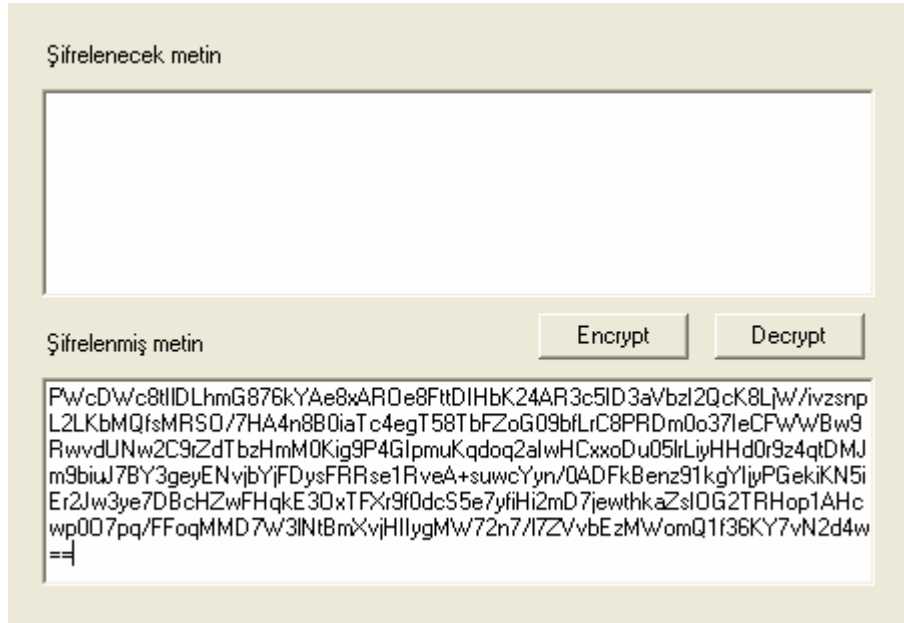
Şekil 4.24. Şifrelenen metnin word belgesi halinde Beyhan PC'sine aktarılması



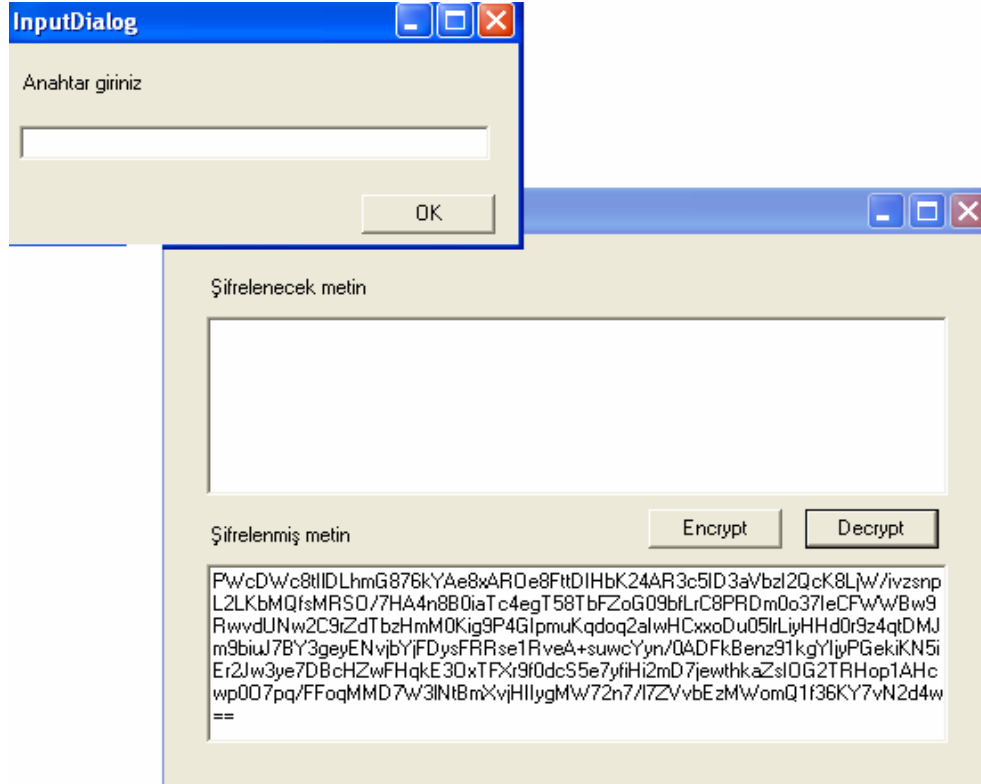
Şekil 4.25. Şifreli metnin alındığı share klasörü



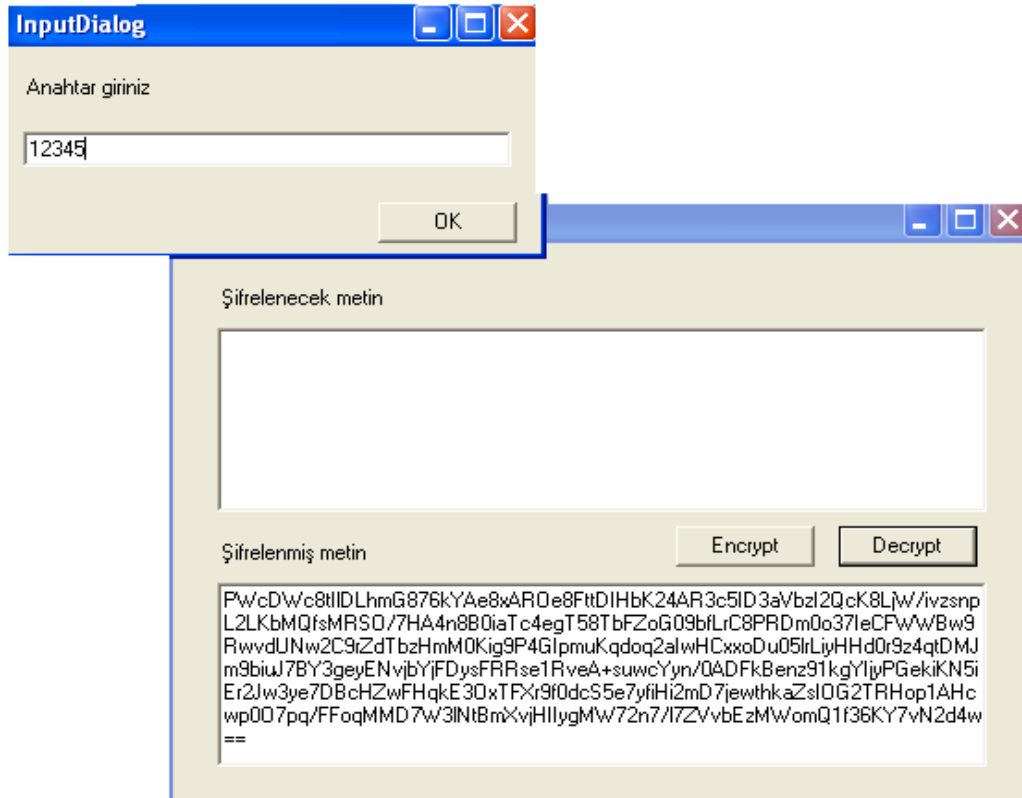
Şekil 4.26. Alınan şifreli metnin görüntüsü



Şekil 4.27. Alınan şifreli metnin Şifreleme/Deşifreleme ara yüzüne aktarılması



Şekil 4.28. Şifreli metnin çözülmesi (decrypt) için anahtar değerinin istenmesi



Şekil 4.29. Şifre çözme (decrypt) işlemi için anahtar değerinin girilmesi

Form1

Şifrelenecek metin

Telsiz kullanıcılarının önemli ihtiyaçlarından olan haberleşme gizliliği 80'li yıllardan başlayarak çeşitli tekniklerin kullanılmasıyla sağlanmaya çalışılmıştır. Önceleri analog tekniklerle sağlanmaya çalışılan haberleşme gizliliği, gerçek anlamda ancak sayısal tekniklerin geliştirilmesi ile sağlanabilmektedir.

Şifrelenmiş metin

Encrypt Decrypt

P'wcD'wc8tIIDLhmG876kYAe8xARDe8FttDIHbK24AR3c5ID3aVbzl2QcK8LjW/ivzsnpL2LKbMQfsMRSO/7HA4n8B0iaTc4egT58TbFZoG09bflrC8PRDm0o37leCFwWBw9RwvdUNw2C9rZdTbzHmMOKig9P4GlpmuKqdoq2alwHCxxoDu05lrLiyHHd0r9z4qtDMJm9biuJ7BY3geyENvjbYjFDysFRRse1RveA+suwcYyn/QADfkBenz91kgYIyPGekiKN5iEr2Jw3ye7DBcHZwFHqkE3DxTFxr9f0dcS5e7yfiHi2mD7jewthkaZsIOG2TRHop1AHcwp007pq/FFoqMMD7w3INtBmXvjHllygMw72n7/l7ZVvbEzMwomQ1f36KY7vN2d4w==

Şekil 4.30. Alınan şifreli metnin tekrar orijinal haline gelmesi (decrypt)

**5. SONUÇ VE ÖNERİLER**

Bluetooth sistem yapısı ve güvenliğini sağlayan yönetim mekanizmaları incelendiğinde kısa mesafede kablosuz iletişim ortamı sunan Bluetooth'un güvenlik eksiklerinin olduğu tesbit edilmiştir. Bu eksikleri özetleyecek olursak;

- Bluetooth destekli cihazlarda kullanılan cihaz adı, başka bir Bluetooth cihazı tarafından kullanılabilir, bu da kötü niyetli kişinin istediği saldırıyı gerçekleştirmesi için yeterli olmaktadır.

- Cihaz eşleşmesinde kullanılan giriş anahtar kodunun 1-16 bayt arasında herhangi bir değer alabilmesi, giriş anahtar kodunun seçiminde zayıf anahtar üretimi için bir etken oluşturmaktadır. Kullanıcı hafızada kolay tutabileceği doğum tarihi, plaka numarası, okul numarası gibi tahmin edilmesi kolay olabilen kodlar kullanabilmekte buna şifreleme anahtarının zayıflamasına neden olmaktadır.

- Kimlik doğrulamasında sadece cihazın kimliği doğrulanmakta, kullanıcı için herhangi bir kimlik doğrulaması yapılamamaktadır.

- Kimlik doğrulama ve tüm anahtarların üretilmesi aşamasında kullanılan Bluetooth Safer + algoritması, günümüz şartlarında artık yeterince güvenli sayılmamaktadır. (Jim Dray, 1999 ; Juan Soto, 1999).

- Bluetooth hizmeti engelleme saldırılarına karşı bir önlem alınmamıştır. Bu durum batarya ile çalışan cihazlar için güvenlik açığı meydana getirmektedir.

Bu tez çalışmasında kısa mesafede kablosuz iletişim ortamı sunan Bluetooth sistem ve güvenlik yapısı incelenmiş, mevcut güvenlik durumu ve eksikleri üzerinde durularak, yapı üzerinde ne gibi değişikliklerin yapılması gerektiği belirtilmiştir.

Tez çalışmasında; kablosuz iletişim ortamı teknolojilerin incelenmesi bu teknolojilerin avantaj ve dezavantajları belirtilerek kıyaslanması, daha önce yapılan çalışmalar hakkında bilgi verilmesi, Bluetooth sisteminin yapısı, bilgi güvenliği, kriptoloji, simetrik ve asimetrik şifreleme yapıları, şifreleme algoritmaları, J2ME , MIDlet konuları hakkında bilgi ve yapılan uygulama için kullanılan metodlardan bahsedilmiştir.

İki gezgin telefon arasında Bluetooth üzerinden güvenli veri iletimi için Borland J Builder ortamında oluşturulan DES algoritmik yapısı üzerindeki yazılım çalışması uygulaması gezgin telefon emülatörleri kullanılarak gerçekleştirilmiştir.

İki bilgisayar (PC) arasında yapılan uygulamada Bluetooth USB aparatları kullanılarak bilgisayarlara bluetooth özelliği kazandırılmış, bu aparatlar arasında haberleşme sağlayabilmek için Bluesoleil software kullanılmıştır. Bluetooth ortamında iletilecek verinin şifrelenmesi ve deşifrelenmesi için ise Rijndael (AES) algoritması kullanılmıştır.

Genel olarak; Bluetooth özelliği olan cihazlarda giriş kodu girilip kalıcı bir bağlantı kurulup iletişim yapıldıktan sonraki bağlantılarda giriş kod değeri istenmemektedir; bu

durumda aynı cihazı başka birinin kullanması durumunda mevcut Bluetooth sisteminde kullanıcı kimlik doğrulaması yapılamadığından ve master cihaz tarafından gönderilen veri slave durumunda olan cihaza ulaştığında veri açık hale gelmekte ve yetkisiz erişim sağlanması güvenli olmayan veri iletimi sonucunu oluşturmaktadır. Benzer olay aynı cihaz adını alan kullanıcılar içinde geçerli olup yerine geçme durumunda yetkisiz erişim ortaya çıkmaktadır.

Yapılan uygulamada veri gönderilmeden önce kullanıcı tarafından daha önceden kullanıcı ve alıcı tarafından seçilen ortak bir anahtar değeriyle şifrelenmektedir, şifrelenen veri master cihaz tarafından slave durumdaki cihaza gönderildiğinde alıcı durumda olan kullanıcı ancak belirlenen ortak anahtar değerini girmesiyle şifrelenen veriyi deşifre edebilir. Bu şekilde yerine geçme ve yetkisiz erişim durumu önlenmiş, Bluetooth mevcut güvenlik yapısı daha güçlenmiş bu açıklık kapatılmıştır.

Uygulamalarda simetrik algoritmik yapılar, asimetrik yapılara göre daha hızlı işlem gerçekleştirmekte olduğundan simetrik algoritmalar olan DES ve Rijndael (AES) kullanılmıştır.

Simetrik ve asimetrik algoritmalar üzerine yapılan araştırma sonucu Bluetooth kimlik doğrulama, anahtar üretimi aşamasında kullanılan safer+ algoritmasının günümüz geliştirilen algoritmalarına göre güvenlik ve performans yönünden yetersiz oluşu durumu ortaya çıkmaktadır, mevcut bluetooth sisteminde kullanılan algoritmik yapının güvenlik ve performans yönünden daha iyi bir yapıya sahip başka bir algoritmik yapıyla değişimi Bluetooth sistemini performans ve güvenlik yönünden geliştirecektir, önerilen değişiklik akademisyenler ve araştırmacılar için iyi bir çalışma materyali ve metodu olmaktadır.

**KAYNAKLAR**

- ANONİM, 2001. Overview of the AES Development Effort, <http://csrc.nist.gov/cryptokit/aes/>
- ANONİM, 2005. Bluetooth Information, [www.trust.com](http://www.trust.com)
- ANONİM, 2005. Bluetooth OEM modules, [www.kcwirefree.com](http://www.kcwirefree.com)
- ANONİM, 2002. Bluetooth-Lower Layer Approach, [www.holtmann.org/lecture/bluetooth](http://www.holtmann.org/lecture/bluetooth)
- AKSU, M., 2004. "3. Nesil Cep Telefonları İçin Symbian İşletim Sistemi Üzerinde Çalışabilen C++ Tabanlı Uygulama Geliştirilmesi", K.S.Ü. Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, s48-53.
- AKBEN S.B., SUBAŞI A., 2005. "RSA ve Eliptik Eğri Algoritmasının Performans Karşılaştırması" Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi 8(1)-2005, 35-40.
- BHAGWAT, 2001. Bluetooth: Tecnology for Short-Range Wireless Apps, Industry Report [www.winlab.rutgers.edu/~pravir/publications](http://www.winlab.rutgers.edu/~pravir/publications)
- ÇÖLKESEN, R., ÖRENCİK, B., 2002. "Bilgisayar Haberleşmesi ve Ağ Teknolojileri" kitabı, Papatya Yayıncılık, İstanbul, s235-237.
- ÇOMAKÇI, E., 2004. "Bluetooth Güvenlik Mimarisinin İncelenmesi ve Geliştirilmesi" Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Ana Bilim Dalı Yüksek Lisan Tezi, Ankara, s5-6, 15-18, 103-105.
- DAEMEN J., RIJMEN V., 2003. AES Proposal: Rijndael
- DAEMEN J., KNUDSEN L., RIJMEN V., 1997. The Block Cipher Square, Lecture Notes in Computer Science
- EFE, B., 2003. EST JAVA Projesi, İTÜ Bilişim Enstitüsü, s5-12, Maslak-İstanbul
- FIPS PUB 197, 2001. Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- Flanagan, D., *Java in a Nutshell A Desktop Quick Reference*, 4<sup>th</sup> ed., O'Reilly & Associates, March 2002.
- FLANAGAN D., 2002. Java in a Nutshell a Desktop quick Reference, 4<sup>th</sup> ed., O'Reilly & Associates

- FORMSAN, S. 2002. Reusable Bluetooth Networking Component for Symbian Operating System. Lappeenranta University, Master's Thesis, Finland, 84s.
- GUROVSKI I., KARADZIC V., 2002. "Self-configuring Bluetooth Networks, Lund Institute of Technology, Malmö, s7-37
- GEHRMANN, C., PERSSON, J., SMAEETS, B., 2004. "Bluetooth security" International Book Number: 1-58053-504-6, Artech House Boston, [www.artechhouse.com](http://www.artechhouse.com)
- HELLMAN, M.E., DIFFIE, W., 1976. New direction in cryptography. IEEE Trans. Inform. Theory, s644-654.
- KAHN, D., 1996. The Codebreakers: The Story of Secret Writing. New York: Scribner.
- KARYGIANNIS T., OWENS L., 2000. Wireless Network Security, 802.11, Bluetooth, Hanheld Devices, NIST Special Publication s800-48
- KALISKI B.S., 1994. On The Security and Performance of Several Triple DES Modes, RSA Laboratories
- KLINGSHEIM A.N., 2004. "J2ME Bluetooth Programming" Department of Informatics University of Bergen, Master's thesis
- KNUDSEN, L.R., 1995. A Key Schedule Weakness in safer K-64, Advances in Cryptology.
- LEO K., CHAI K., ALUKAIDEY T., JIMAA S., 2001. "Wireless Multi-Sharc, DSP Connectivity Using Bluetooth", Department of EC&EE, Universty of Hertfortshire. [www.mpdigest.com/Articles](http://www.mpdigest.com/Articles)
- MAHMOUD Q.H., 2002. Learning Wireless Java, O'Reilly & Associates
- MALLICK, M. 2003. Mobile and Wireless Design Essentials. Wiley Publishing, Indianapolis, Indiana, s454.
- MASSEY, J.L., 1993. Safer K-64: A Byte Oriented Block Cipherring Algorithm, Proceedings of 1st International Workshop on Fast Software Encryption, Springer-Verlag
- MASSEY, J.L., 1998. Safer+ Cylink Corporation's Submission for the Advanced Encryption Standart Candidate Conference, Ventura, CA.
- MENEZES, J.A., VANSTONE V.O., 1996. Handbook of Applied Cryptography, CRC Press.
- MERKLE R.C., HELLMAN M.E., 1981. On The Security of Multiple Encryption, Communication of ACM

NIST, 2001. Recommendation for Block Cipher Modes of Operations, FIPS publications 800-300A : National Institute of Technologies

NIST, 1980. National Institute of Standards and Technologies (NIST), FIPS publications 81: DES Modes of Operations

İLHAN, H., 2002. "Bluetooth Şifrelemesi ve Kanal Tasarımı" İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul, s32-35.

OORSCHOT P.C., WIENAR M.J., 1981. A Known Plaintext Attack on Two Key Triple Encryption, Volume 473 of Lecture Notes in Computer Science

PRENEEL, B., BİRYUKOV, A., OSWALD, E., ROMPAY, B.V., 2003. NESSIE Security Report Y4 M2 version 2.0, IST-1999-12324.

RİVEST, L.R., 1986. Cryptology.

SUBRAMANİ M., İLYAS M., 2003. "Simulation Based Analysis of Bluetooth Networks" College of Engineering Florida Atlantic University, ISBN : 1- 56555-269-5, Florida

**ÖZGEÇMİŞ**

Mehmet Ali ÖZÇELİK, HATAY'ın İSKENDERUN ilçesinde doğdu. İlk, orta öğrenimini GAZİANTEP'te ve yine Lise öğrenimini GAZİANTEP Mehmet Akif Ersoy Endüstri Meslek Lisesi Elektrik Bölümünde tamamladı, GAZİANTEP Üniversitesi Meslek Yüksek Okulu Elektrik Programını bitirdikten sonra, 1999 yılında Marmara Üniversitesi Teknik Eğitim Fakültesi Elektrik Eğitimi Bölümünden mezun oldu.