T.C.
İSTANBUL TEKNİK ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

AĞ GÜVENLİĞİ
Prof. Dr. Bülent ÖRENCİK

BLUETOOH GÜVENLİĞİ

ESRA GÜNEY
504061513

İÇİNDEKİLER

1. Giriş----------3
2. Telsiz Teknolojiler----------3
2.1. WWAN, WLAN Ve WPAN----------3
3.Bluetooth----------4
3.1. Tarihi----------5
3.2. Radyo Belirtimi----------5
3.2.1. Frekans Bantları----------5
3.2.2. Verici Karakteristikleri----------6
3.2.3. Alıcı Karakteristikleri----------6
3.3. Temelbant Belirtimi----------6
3.3.1. Bluetooth Saati----------6
3.3.2. Bluetooth Cihaz Adresi----------7
3.4. Bluetooth Protokolleri----------7
3.4.1. Bağ Yöneticisi Protokolü (LMP) ----------7
3.4.2. Mantıksal Bağ Kontrol Ve Uyarlama Protokolü (L2CAP) ----------7
3.4.3. Servis Keşif Protokolü (SDP) ----------8
3.5. Güvenlik----------8
3.5.1. Anahtar Tipleri Ve Yönetimi----------8
3.5.2. Anahtaların Üretilmesi Ve İlklendirme Yordamı----------10
3.5.2.1. İlklendirme Anahtarının Üretilmesi, Kınıt----------10
3.5.2.2. Cihaz Anahtarının Üretilmesi, Ka----------10
3.5.2.3. Birleşim Anahtarının Üretilmesi, Kab----------11
3.5.2.4. Şifreleme Anahtarının Üretilmesi, Kc----------12
3.5.3. Kimlik Doğrulama----------12
3.5.3.1. Kimlik Doğrulama İçin Anahtar Üretim Fonksiyonları----------13
3.5.4. Şifreleme----------13
3.5.4.1. Şifreleme Kavramı----------14
3.5.4.2. Şifreleme İçin Anahtar Üretim Fonksiyonu----------14
3.5.5. Güvenlik Mimarisi----------15
3.5.5.1. Güvenlik Yöneticisi----------15
3.5.5.1. Akış Şemaları----------17
3.5.6.Güvenlik Açıkları----------20
3.5.6.1.Bluejacking----------20
3.5.6.2.Bluebugging----------20
3.5.6.3.Bluesnarfing----------20

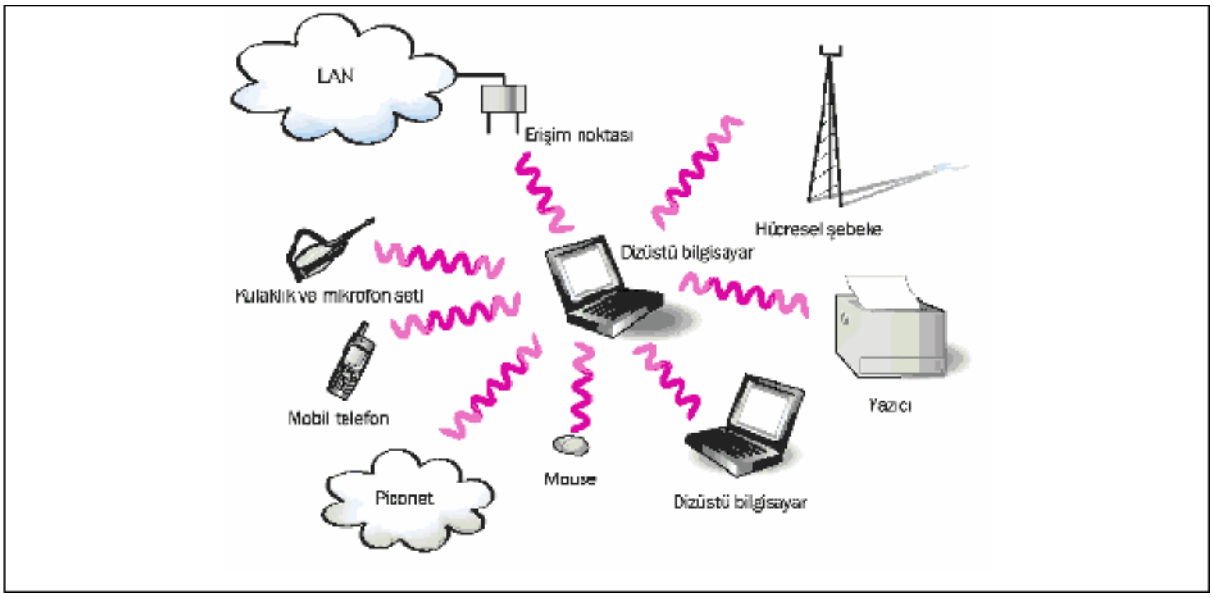
3.5.6.4.Cabir Virüsü----------20
3.5.6.5.Car Whisperer----------20
3.5.6.6.Anahtarların Güvenilirsizliği----------20
3.5.6.7.Safer+ Algoritması Yetersizliği----------20
3.5.6.8.Aradaki Adam Problemi. ----------20
3.5.6.9.Tekrarlama Saldırısı----------20
3.5.6.10.Hizmet Engelleme Saldırısı----------21
3.5.7. Bluetooth Güvenliği Artırmaya Yönelik İpuçları----------21
Kynaklar----------22

ŞEKİLLER

Şekil-1 Bluetooth Kablosuz İletişim Teknolojisine Sahip Bir Kullanıcı Modeli
Şekil-2 Kablosuz İletişim Teknolojileri
Şekil-3 Bluetooth Çalışma Frekansı Bantları
Şekil-4 Güç Sınıfları
Şekil-5 Tek Bağımlı Cihazlı Piconet(a), Çok-Bağımlı Cihaza Sahip Piconet(b),Scatternet(c)
Şekil-6 OSI – Bluetooth Karşılaştırması
Şekil-7 Kimlik Doğrulama Ve Şifreleme Yordamlarında Kullanılan Öğeler
Şekil-8 Cihaz Anahtarının Üretilmesi
Şekil-9 İlklendirme Anahtarının(Kinit), Bağ Anahtarının(Kunıt) Üretilmesi,Değişimi
Şekil-10 İlklendirme Anahtarının(Kinit), Bağ Anahtarının(K) Üretilmesi,Değişimi
Şekil-11 Bluetooth İçin Meydana - Okuma Yanıt Sistemi(Kimlik Dogrulama)
Şekil-12 Kimlik Doğrulama Anahtarları Üretimi
Şekil-13 Şifreleme Yordamının Fonksiyonel Yapısı
Şekil-14 Şifreleme Anahtarı Üretimi
Şekil-15 Geçiş İznine Sahip Güvenli Bir Servis İçin Bil
Şekil-16 Güvenlik Yöneticisi Tarafından Uygulanan Geçiş Kontrol Akış Çizeneği
Şekil-17 Kimlik Doğrulama Yordamı Akış Çizeneği
Şekil-18 İzin Verme Yordamı Akış Çizeneği

1. GİRİŞ

Bluetooth, kablo bağlantısını ortadan kaldırarak hemen hemen tüm taşınabilir cihazların telsiz bağlantısını sağlayıp, birbirleri ile sorunsuzca haberleşmesini gerçekleştirmek için tasarlanan bir standarttır. Radyo frekans işlemleri 2.400 GHz'de, *lisansız* ISM bandında yer alır. İspanya, Fransa ve Japonya'da 83,5 MHz'lik bu bandın 37 MHz'i (2.4465-2.4835) yani 23 RF kanalı kullanılırken; Fransa ve İspanya hariç tüm Avrupa ülkeleriyle, Amerika ve diğer ülkelerde bu bandın tamamı, yani 79 RF kanalı kullanılır. Her kanal 1Mhz band genişliğine sahiptir. Frekans sıçrama spektrumu ve saniyede azami 1.600 sıçramaya müsaade eden tam çift yönlü sinyal iletişimi kullanılır. Mesaj bitleri Gaussian Frekans Kaydırmalı Kiplenim tekniği kullanılarak modüle edilirler ve bu sayede kanal başına 1 Mbps'lık bir hıza ulaşılır. Bu hız veri için maximum 720 kbps olabilmektedir.

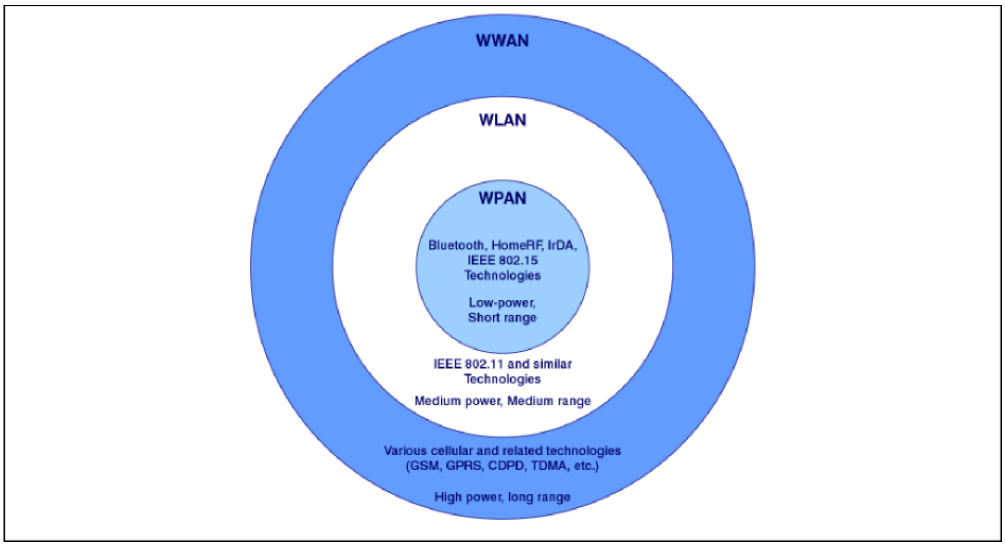


Şekil-1Bluetooth kablosuz iletişim teknolojisine sahip bir kullanıcı modeli

2. TELSİZ TEKNOLOJİLER

En basit anlamıyla telsiz teknolojileri, bir veya daha fazla cihazın aralarında fiziksel bir bağlantı (ağ kablosu) olmaksızın birbirleriyle haberleşebilmesi için geliştirilmiş sistemler olarak tanımlayabiliriz. Bu teknolojiler temelde, kullanıcıların bilgiye her yerden ve her koşulda (sabit veya hareketli durumlarda) ulaşabilmelerini sağlarlar.

2.1. WWAN, WLAN Ve WPAN



Şekil-2 Kablosuz İletişim Teknolojileri

Telsiz teknolojileri, iletişim kurdukları kapsama alanlarına göre, telsiz geniş alan ağları (WWANs), telsiz yerel alan ağları (WLANs) ve telsiz kişisel alan ağları (WPANs) olarak üç grupta kategorize edebiliriz.

WWAN'ların tipik olarak kapsama alanları, kilometreler veya bir kaç yüz metreler ile tanımlanabilir. Bu uzaklıklarda haberleşebilmek için de, yüksek güçle iletişime ve dolayısıyla da uygun frekans bantları için özel lisanslara ihtiyaç duyulur. Ayrıca bu güçlerle iletişim yapmak, sizi güç tüketimi ve veri hızı arasında da bire bir seçim yapmaya zorlar. Popüler olarak günümüzde kullanılan en önemli WWAN teknolojisi, sayısal hücre haberleşmesinde standartlaşmış GSM'dir.

WLAN'ların ise kapsama alanları bir kilometre ile yüz metreler arasında değişmektedir. Bu dar kapsama alanı da bizim daha düşük güçlerle iletişim yapabilmemize ve lisansız frekans bantlarını da kullanabilmemize imkan sunmaktadır. IEEE 802.11 ve HIPERLAN en önemli WLAN örneklerindendir.

WPAN'lar ise cep telefonları, PDA'lar, tablet bilgisayarlar, taşınabilir müzik çalarlar, dijital kameralar gibi daha çok "kişisel elektronik cihazlar" olarak adlandırabileceğimiz bu cihazların, kendileriyle ve birbirleriyle haberleşebilmesi için tasarlanmış bir teknolojidir. WLAN'ın aksine hareketli cihazlar için daha uygun ve daha pratiktir. Genel olarak on ve yüzmetre arasında değişen bir kapsama alanında haberleşirler. En önemli örnekleri HomeRF, IrDa, IEEE 802.15 teknolojileridir.Bluetooth da, şu anda dünyada kullanılan en popüler WPAN standartıdır.

Telsiz ağların elbetteki en önemli üstünlüğü, iletişim yapılırken kabloların yerine hava dalgalarının kullanılmasıdır. Kanalın herkes tarafından kolayca dinlenebilmesi de bu teknolojilerin ne kadar güvenli olduğu sorusunu akla getirmiştir.

3.BLUETOOTH

Adını, 10.yüzyılda Danimarka ve Norveç'i birleştiren Harald Blatand (İngilizce okunuşu Bluetooth) ismindeki bir Danimarka Kral'ından almıştır.

Bluetooth kablosuz teknolojisi, hareketli ve/veya sabit elektronik cihazların birbirleriyle iletişimi için gerekli kablo bağlantısını ortadan kaldırmak amacıyla geliştirilmiş, kısa-mesafeli bir iletişim sistemidir. En önemli özellikleri, düşük maliyetli, düşük güç tüketimli ve kararlı bir iletişime olanak sağlamasıdır.

Bluetooth fiziksel katmanı 2,4GHz. deki lisanssız ISM bandında çalışır. Sistem girişim ve sönümlenmeleri engellemek için frekans sıçramalı bir alıcı-verici ünitesi kullanır. İletişim çok sayıdaki FHSS taşıyıcısı ile sağlanır. Alıcı ve verici ünitelerin karmaşıklığının azaltılabilmesi için ikili FM modülasyonu kullanılır. Sembol oranı saniyede 1 Megasembol 'dür. (Ms/s) .

Tipik bir Bluetooth iletişimi sırasında fiziksel radyo kanalı, ortak saat ve frekans sıçrama örüntüsünde eşzamanlı olarak çalışan bir grup cihaz tarafından paylaşılır. Bu eşzamanlılığı ana (master) olarak tanımlanan cihaz sağlar. Diğer cihazlar ise bağımlı (slave) olarak tanımlanır. Bu biçim içerisindeki cihazların oluşturduğu yapı da piconet olarak adlandırılır. Bluetooth teknolojisinin temel iletişimi piconet üzerinden sağlanmaktadır.

İletişim sırasında piconet içerisindeki cihazlar, ISM bandındaki 79 frekansa, özel frekans sıçrama örüntüsü sayesinde sözde-rastlantısal bir sırayla atlarlar. Bu örüntü, iletişimin başında, ana cihazın saati ve cihaz adresi kullanılarak üretilir. Aynı zamanda bu frekans sıçrama örüntüsü, girişime neden olan başka cihazların kullandığı frekansları çıkararak, kendini yeni ortama adapte edilebilecek şekilde de dizayn edilmiştir.

İletişim, fiziksel kanal üzerinde ayrılan belli zaman dilimleri üzerinden yapılır. Bluetooth cihazları arasında veri, bu zaman dilimleri içerisinde konumlandırılmış paketler yoluyla gönderilir. Zaman bölmeli çoğullama yönetimi kullanılarak da, cihazlar arasında tam çift yönlü bir iletişim sağlanır.

3.1. Tarihi

Bilindiği gibi IEEE, elektrik ve elektronik alanında yüzlerce standart geliştiren uluslararası bir kuruluştur. 802 komitesi de yerel ve geniş alan ağları için standartlar geliştirir. Örneğin IEEE 802.3 ethernet tabanlı tek bağlantılı ağlar için geliştirilen bir standartken, IEEE 802.11 telsiz yerel alan ağları için kullanılan bir standarttır. Yine 802.15 grubu da telsiz kişisel alan ağları için standart geliştirmektedir.

Bluetooth projesi ise ilk olarak, 1994 yılında Ericsson'un bu alandaki standartların yaygınlaşması için, rakiplerinin de içinde olduğu diğer iletişim ve bilişim firmalarını, Bluetooth'a dahil olmaları için teşvik etmesiyle başlar. Bu alandaki diğer öncüler, Nokia, Toshiba, IBM ve Intel'dir. Böylece, 1998 yılı Mayıs ayında Bluetooth SIG adında bir endüstri platformu oluşturularak, bu projenin kapsamı genişletilir. Yapılan çalışmalar neticesinde 1999 Temmuz ayında ilk Bluetooth belirtimi yayınlanır.

1 Aralık 1999'da da, 3Com, Lucent Technologies, Microsoft ve Motorola'nın da katılımıyla, toplam dokuz üyeye ulaşan SIG Endüstri Gurubu'nun, bundan sonraki genel koordinasyonu sağlayacağı duyurulur. 2000 yılında IEEE ile görüşmeler tamamlanarak Bluetooth'un bir IEEE 802.15 standartı olması kararlaştırılır. Nisan 2002'de de Bluetooth, IEEE Std 802.15.1-2002 adıyla tüm dünyaya duyurulur. IEEE ile Bluetooth SIG arasında yapılan sözleşmeye göre IEEE bu standartı değiştirme, yayınlama, tek başına veya diğer IEEE standartları ile birlikte dağıtma iznine sahiptir.

Yine ilk olarak 1999'da piyasaya sürülen ve bir WLAN standartı olan IEEE 802.11 b de, Blutooth gibi 2,4Ghz'lik lisansız ISM bandında çalışan bir başka telsiz ağ teknolojisidir. Bluetooth ile birlikte adı oldukça çok anılan bu teknolojiyle, bir erişim noktası yardımıyla önce var olan yerel ağlara, sonra da geniş ağlara bağlanılabilmektedir. Pazarda daha çok Bluetooth'a karşı bir teknoloji olarak algılanan IEEE 802.11 b, aslında Bluetooth ile birlikte birbirlerinin tamamlayıcısı iki teknolojidir.

Bunun yanında Bluetooth ile birlikte iletişim için aynı temel frekans bandını kullanmaları, özellikle taşınabilir bilgisayarlarda olduğu gibi, aynı cihazın içerisinde beraber kullanılmaya başlanıldığında, göz ardı edilemez bir girişime neden olmaktadır. Bu girişimin önlenebilmesi veya azaltılabilmesi için de yine 2000 yılında IEEE 802.15.2 çalışma gurubu oluşturulmuş ve bu konu üzerinde bir model geliştirmek üzere çalışmalara başlamıştır. Her iki teknoloji için de ağ topolojilerinin değişken yapısı, bu girişimi engelleme işini oldukça zorlaştırmıştır. Fakat IEEE 802.15.2 grubu ve SIG endüstri platformunun beraber çalışmaları sonucunda Bluetooth için Uyarlanabilen Frekans Hoplama Tekniği geliştirilmiştir. Bu yöntemi tanımlayan en yeni Bluetooth belirtimi de Kasım 2003'de yayınlanmıştır.Şu anda kullanılan sürüm ise 2004 – V2.0+EDR isimli tanımlamadır. Yakın zamanda versiyon 2.1 in çıkması bekleniyor.

3.2. Radyo Belirtimi

3.2.1. Frekans bantları

Bluetooth sistemi 2400 – 2483,5 MHz 'lik bir frekans bandında çalışır. 79 RF kanalı1MHz'lik aralıklarla ile dizilir.

Frekans Aralığı	RF Kanalları
2.400 – 2.4835 GHz.	f=2402+k MHz, k=0,...,78

Şekil-3 Bluetooth çalışma frekansı bantları

3.2.2. Verici karakteristikleri

Verici anten çıkışındaki güçler baz alındığında, Bluetooth cihazlarını üç sınıfa ayırmak mümkündür. Bu sınıflar ve minimum, maksimum güç değerlerini gösteren çizelge aşağıda verilmektedir.

Güç Sınıfı	Maksimum Çıkış Gücü (P_{max})	Mesafe
1	100 mW (20dbm)	100 metre
2	2,5 mW (4dbm)	35 metre
3	1 mW (0dbm)	10 metre

Şekil-4 Güç sınıfları

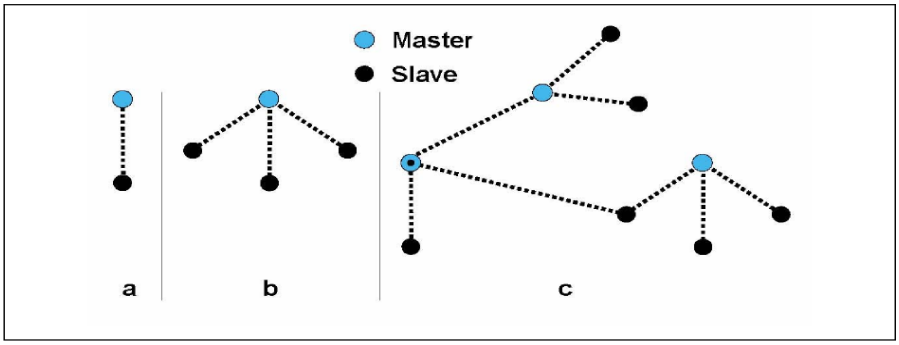
3.2.3. Alıcı karakteristikleri

Bir Bluetooth alıcısının hassaslığının en azından -70dBm olması gerektiği belirtilmektedir. Fakat haberleşme sistemlerinde iletişimin geçerliliği için önemli olan asıl parametre bit hata oranı olmaktadır. Bluetooth için de kabul edilebilir bit hata oranı (BER) maksimum %0,1'dir.

3.3. Temelbant Belirtimi

Bluetooth sistemi hem noktadan noktaya, hem de noktadan çoklu noktaya bağlantı imkanı sağlar. Noktadan noktaya bağlantıda fiziksel kanal iki Bluetooth cihazı tarafından paylaşılırken, noktadan çoklu noktaya bağlantıda fiziksel kanal bir çok Bluetooth cihazı tarafından paylaşılır. İki veya daha fazla cihazın aynı kanalı paylaştığı yapı piconet olarak adlandırılır. Piconet yapısı içerisindeki cihazların biri ana cihaz olurken, diğer cihazlar bağımlı cihaz olarak davranır. Piconet içerisinde yedi bağımlı cihaz aktif olarak iletişim yapabilir. Fakat çok daha fazla bağımlı cihaz park modunu kullanarak piconette birbilerine bağlı kalabilirler. Park modundaki bu bağımlı cihazlar kanal içerisinde aktif değil, fakat ana cihaz ile eşzamanlı durumdadırlar.

Ortak cihaza sahip olan piconetler de scatternet olarak adlandırılır. Her piconette sadece bir ana cihaz bulunurken, bağımlı cihazlar farklı piconetler içerisinde yer alabilir. Ayrıca bir piconet içerisindeki ana cihaz, diğer piconetler içerisinde bağımlı cihaz olarak da yer alabilir. Piconetlerin birbirleriyle eşzamanlı olmasına gerek yoktur; her piconet kendi frekans sıçrama dizisine sahiptir.



Şekil-5 Tek bağımlı cihaza sahip piconet (a),

çok-bağımlı cihaza sahip piconet (b), scatternet (c)

3.3.1. Bluetooth saati

Her Bluetooth cihazı kendi kiristal salınıcısından elde edilen doğal bir saate sahiptir. Bleutooth cihazları piconet yapısında birbirleriyle eşzamanlı hale gelebilmek için kendi doğal saatlerine bazı sapma değerleri eklerler. Bu şekilde tüm cihazların saatleri ana cihazın saatine eşitlenmiş olur. Bluetooth saatinin günü belirten saat ile bir bağlantısı yoktur. Bu saati oluşturmak için 28 bitlik bir sayaç kullanılır.

3.3.2. Bluetooth cihaz adresi

Bluetooth cihaz adresi (BD_ADDR) her cihaza özel olarak verilen, eşsiz 48 bitlik bir adrestir.

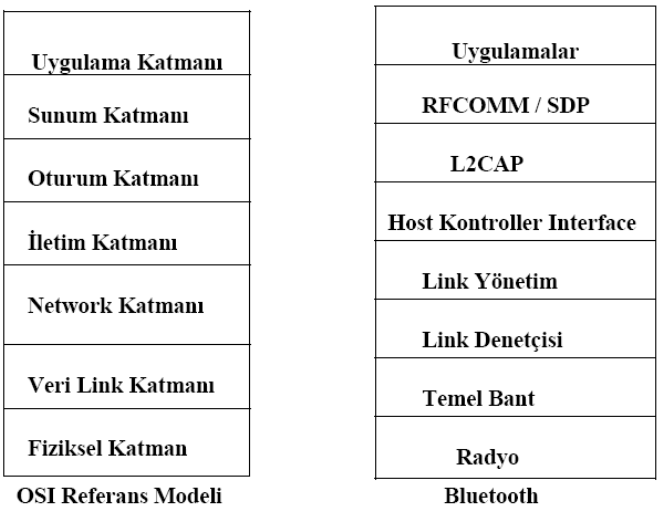
3.3.3. Ses ve Veri İletimi

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.

- ses haberleşmesi için eş zamanlı bağlantı hattı (SCO-Synchronous Connection Oriented)
- veri haberleşmesi için eş zamanlı olmayan bağlantı (ACL- Asynchronous Connectionless) hattıdır.

3.4. Bluetooth Protokolleri

Bluetooth çekirdek protocolleri kullanım amaçları ve yerlerine göre Bağ Yöneticisi Protokolü, Mantıksal Bağ Kontrol ve Uyarlama Protokolü ve Servis Keşif Protokolü olarak üçe ayrılır. Bu protokoller aşağıda kısaca açıklanmaktadır. Ayrıca Bluetooth V1.2 belirtiminde tanımlanmış ve daha üst katmanlarda kullanılan farklı protokoller de mevcuttur.,



Şekil-6 OSI – BLUETOOTH karşılaştırması

3.4.1. Bağ yöneticisi protokolü (LMP)

Bağlantının kurulması ve kontrolü aşamasındaki tüm işlemler bu protokol yardımıyla başarılır. Sorgu, çağrı yordamlarının çağırılması, piconet, scatternet yapılarının oluşturulması, frekans sıçrama dizilerinin seçilmesi, uygun güç seviyesinin belirlenmesi, ağ güvenliği için gerekli tüm paremetrelerin kontrolü, kimlik doğrulama, izin verme, şifreleme algoritmaların çalıştırılması, PIN kodunun her iki tarafta da uygun şekilde girilmesinin sağlanması bu protokol yoluyla sağlanır.

3.4.2. Mantıksal bağ kontrol ve uyarlama protokolü (L2CAP)

L2CAP, Bluetooth bağ katmanın veri düzlemi olarak görülebilir. Temel band paket büyüklükleri, yüksek katman paketlerin taşınabilmesi için çok küçük olduğundan, L2CAP katmanı tanımlanarak, yüksek katmanlara daha büyük ve işlevsel paketlerin iletilmesi sağlanabilmektedir.

Dolayısıyla yüksek katmanlar için paket bölütlenmesi ve yeniden oluşturulması, her kanal için akış kontrolü ve hata kontrolünün yapılması ve servis kalitesi bilgilerinin taşınması bu protokol sayesinde başarılmış olmaktadır.

3.4.3. Servis keşif protokolü (SDP)

Cihazlarda varolan servislerin keşfedilmesi için çeşitli uygulamalar tanımlayarak ve bu uygulamaların karakteristiklerinin belirlenmesini sağlar. SDP aslında bir istemci-sunucu protokolüdür. Haberleşmesini sorgu-yanıt prensibine göre yapar. Sunucu, cihazda bulunan servislerin kaydını tutarken, istemci de bu cihazda varolan tüm servisleri araştırır. Bir Bluetooth cihazında maksimum bir adet SDP sunucusu bulunur. Eğer cihaz sadece istemci olarak kullanılacaksa bu sunucuya da ihtiyaç yoktur.

3.5. Güvenlik

Bluetooth, görevdeşler arası iletişime sahip bir teknolojidir. Kullanıcı koruması ve bilgi gizliliğini sağlayabilmek için, hem uygulama katmanında (application layer) hem de bağ katmanında (link layer) işlev gören güvenlik önemleri düşünülmüştür. Bu önlemler de, eşdüzey ortamlara uygun olacak şekilde, yani her bir cihazda kimlik doğrulama (authentication) ve şifreleme (encryption) işlemleri aynı yolla gerçekleşecek şekilde dizay edilmiştir.Bağ katmanında güvenliği sağlayabilmek için dört farklı öğe kullanılır: Bluetooth cihaz adresi, iki gizli anahtar ve her yeni hareket için tekrar üretilen sözde rastlantısal sayıdır.

ÖĞE	BÜYÜKLÜĞÜ
BD_ADDR	48 bit
Kimlik Doğrulama için Gizli Kullanıcı	128 bit
Şifreleme için Gizli KullanıcıAnahtarı, ayarlanabilir uzunlukta (8 bit katları)	8 – 128 bit
RAND	128 bit

Şekil-7 Kimlik doğrulama ve şifreleme yordamlarında kullanılan öğeler

Bluetooth cihaz adresi BD_ADDR, iletişim sırasında kullanıcı etkileşimi veya Bluetooth'un çalışma kiplerinden sorgu yordamı yoluyla kolayca öğrenilebilen bir adrrestir.

Gizli anahtarlar Bluetooth cihazlarının birbirleri ile ilk iletişimi sırasındaki, ilklendirme yordamı içerisinde üretilirler. Bluetooth çalışma kipleri veya yordamları yoluyla kesinlikle açığa çıkarılamazlar. Şifreleme anahtarı, kimlik doğrulama işlemi sırasında, kimlik doğrulama anahtarından elde edilir. Kimlik doğrulaması için kullanılan anahtarın uzunluğu sabit 128 bit iken, şifreleme algoritması için kullanılan anahtarın uzunluğu 1 ve 16 bayt (8 – 128 bit) arasında değişir. Şifreleme anahtarının uzunluğu iki nedenden dolayı değişken olarak düzenlenmiştir. Birincisi, farklı ülkelerde bir çok farklı nedenden dolayı uygulamaya koyulan kriptografi algoritmaları üzerindeki ihracat düzenlemeleri; ikincisi de gelecekteki ihtiyaçlar söz konusu olduğunda, şifreleme algoritmasının hem yazılım hem de donanım olarak değiştirilmeden kolayca tekrar kullanılabilmesidir.

Şifreleme anahtarı, hem kullanış amacı, hem de Bluetooth algoritmaları içerisinde değişmeden kaldığı yaşam süresi bakımından, kimlik doğrulama için kullanılan anahtardan oldukça farklıdır. Kullanılan her şifreleme algoritması için yeni bir şifreleme anahtarı üretilirken, kimlik doğrulama anahtarı sadece iki cihazın birbirleriyle ilk iletişime geçme aşamasında üretilir. Bu özelliğinden dolayı da kimlik doğrulama için kullanılan bu anahtar, bağ anahtarı olarak adlandırılmıştır.

RAND ise cihazdaki 128 bitlik sözde rastlantısal veya rastlantısal işlemler sonucunda elde edilen sözde rastlantısal bir sayıdır. Durağan bir parametre değildir, iki cihazın haberleşmesi sırasında çok sık değiştirilir.

3.5.1. Anahtar tipleri ve yönetimi

Güvenlik için en önemli paremetrelerden biri, elbetteki algoritmalarda kullanılan anahtarlar ve bunların işlevsel ve etkin bir şekilde üretilip yönetilmesidir. Bu konunun daha iyi

anlaşılabilmesi için önce anahtar tiplerinden ve niye farklı anahtarlara ihtiyaç duyulduğundan bahsedilecek, sonra da nasıl üretildikleri üzerinde durulacaktır.

Bundan önce, şifreleme anahtarı ile ilgili olarak önemli bir ayrıntıya da burada yer vermek istiyorum. Daha önce de bahsedildiği gibi, şifreleme anahtar uzunlığu diğer anahtarlardan farklı olarak değişebilen bir yapıya sahip. Fakat bu anahtar uzunluğu, sonradan kullanıcı tarafından hiçbir şekilde belirlenememekte ve buna sadece cihazın üretilmesi aşamasında karar verilmektedir. Ayrıca bluetooth temelbant (baseband) sevisinde de, kullanıcının izin verilen anahtar uzunluğundan farklı bir anahtar seçemesi engellenmektedir.

Bağ anahtarı iki veya daha fazla cihaz arasında paylaşılan ve algoritmalarda kullanılan tüm güvenlik hareketlerinin de aslında temelini oluşturan, 128 bitlik rastlantısal bir sayıdır. Bağ anahtarının kendisi, kimlik doğrulama yordamına direk katılırken, şifreleme anahtarının üretilmesi aşamasında dolaylı yoldan, bir parametre olarak yer alır.

Bağ anahtarı, yarı kalıcı bir anahtardır. Bluetooth çipinde yer alan uçucu olmayan bellekte saklanır.Yarıkalıcılığı,istenildiğinde değiştirilmesinin mümkün olmasından kaynaklanır. Bir kere üretildiğinde, bunu paylaşan Bluetooth cihazları arasındaki bir çok kimlik doğrulama alt bağlantılarında değiştirilmeden kullanılır.

Farklı uygulamalara cevap verebilmek için dört tip bağ anahtarı tanımlanmıştır.

- Birleşim anahtarı (the combination key) K_{AB}
- Cihaz anahtarı (the unit key) K_A
- Geçici anahtar (the temporary key) K_{MASTER}
- İlklendirme anahtarı (the initialization key) K_{INIT}

Bu anahtarlara ek olarak, daha önce de bahsedildiği gibi, bir de şifreleme anahtarı vardır. K_C olarak ifade edilen bu anahtar, bağ anahtarının da kullanıldığı bir algoritma sonucunda elde edilir. Şifreleme algoritmasının her çağırılışında şifreleme anahtarı otomatik olarak değiştirilir.

Bluetooth cihazı için birleşim anahtarı ile cihaz anahtarı arasında fonksiyonel olarak bir fark yoktur. Çünkü ikisi de iletişim süresince bağ anahtarı olarak kullanılır. Farkı elde edilme yolundan kaynaklanır. Cihaz anahtarı tek bir Bluetooth cihazı tarafından elde edilir. Cihazın kurulumu aşamasında bir kere üretilir ve kolay kolay değiştirilmez. Birleşim anahtarı ise iki yeni cihazın ilk defa iletişim kurmaya çalışması aşamasında elde edilir; bu yüzden de iki cihaza da bağımlıdır.

Cihaz anahtarının mı yoksa birleşim anahtarının mı kullanılacağı, iletişim yapmak isteyen cihazlara ya da uygulamaya bağlıdır. Anahtarları saklamak için daha az hafızaya sahip veya çok kullanıcılı ortamlar için tasarlanan cihazlarda cihaz adresini kullanmak daha etkin olurken, daha yüksek güvenlik seviyeleri gerektiren uygulamalarda birleşim anahtarını kullanmak daha uygun olacaktır.

Geçici anahtar ise adından da anlaşıldığı üzere sadece bazı özel durumlarda, geçici olarak kullanılır. Mesela ana ünite, aynı şifreleme anahtarını kullanarak,birden fazla cihazla iletişim yapmak istediğinde, geçici olarak bağ anahtarının yerine geçer ve iletişimi sağlarlar.

İlklendirme anahtarı da sadece ilklendirme yordamı süresince, yani ne birleşim ne de cihaz adresinin henüz tanımlanmadığı ve bu anahtarların cihazlar arasında değişiminin yapılmadığı ya da bağ anahtarının herhangi bir şekilde kaybedildiği durumlarda bağ anahtarı olarak kullanılır. Amacı, cihaz veya birleşim anahtarının üretilmesi aşamasında anahtarın, Bluetooth cihazları arasında güvenli olarak değişimini sağlamaktır. Bu anahtarın üretilmesi aşamasında PIN olarak adlandırdığımız bir güvenlik kodu da kullanılır.

PIN kodu kullanıcı yüzü olmayan Bluetooth cihazlarında sabit olabildiği gibi, kullanıcının kodu girebileceği tuş takımı olan cihazlarda, iletişim yapmak isteyen her iki cihazda da aynı

olacak şekilde, isteğe bağlı olarak da seçilebilir. PIN kodunun telefon, laptop gibi cihazlarda isteğe bağlı olarak girilmesi, elbette iletişimi daha güvenli hale getirmektedir. Fakat kullanım amacına göre tuştakımı gerektirmeyen cihazlarda zorunlu olarak sabit PIN seçeneği kullanılmaktadır. Eğer cihazda bir PIN kodu tanımlanmamışsa da sıfır varsayılan değeri kullanılır.

Bir çok uygulamada PIN kodu sadece dört onlu basamaklı sayı içerir. Bu güvenliğin çok önemli olmadığı, çok kullanıcılı bazı ortamlar için kabul edilebilir gibi görünse de, daha hassas ve özel uygulamalar için yeterince güvenilir gözükmemektedir. Aslında bu kod, dahil olduğu algoritmalar açısından bakıldığında 1 ile 16 bayt arasındaki herhangi bir uzunlukta seçilebilir. Fakat büyük uzunluklar için, PIN değişimi sırasında insan etkileşimi söz konusu olduğundan, bu işin, cihazın uygulama katmanda yazılım ile desteklenerek yapılması önerilmektedir. (Diffie-Hellman Anahtar Dağıtım Yöntemi)

3.5.2. Anahtaların üretilmesi ve ilklendirme yordamı

Bağ anahtarının kimlik doğrulama yordamında kullanılabilmesi için üretilmesi ve Bluetooth cihazları arasında dağıtılması gerekmektedir. Çünkü bağ anahtarı gizli bir anahtardır ve bluetooth adresi gibi sorgu yordamıyla öğrenilemez. Bu anahtarın üretimi ve değişimi de ilklendirme yordamı içerisinde yapılır. Bu yordam beş ana kısımdan oluşur.

- ilklendirme anahtarının üretilmesi
- bağ anahtarının üretilmesi
- bağ anahtarının değişimi
- kimlik doğrulama
- her bir cihaz için şifreleme anahtarının üretilmesi (isteğe bağlı)

İlklendirme yordamından sonra bluetooth cihazları iletişim yapmaya başlayabilecek ya da bağlantı koparılacaktır. Eğer şifreleme gerçekleşecekse, bağ anahtarından üretilen uygun şifreleme anahtarı ile E_0 algoritması işleme konulacaktır.

3.5.2.1. İlklendirme anahtarının üretilmesi, K_{INIT}

BD_ADDR, PIN kodu, PIN kodunun bayt olarak uzunluğu ve IN_RAND rastlantısal sayısının kullanıldığı E_{22} algoritması sonucunda elde edilir.128 bitlik bir anahtardır ve bağ anahtarının oluşturulması için gereken anahtar değişimi için düşünülmüştür. Cihazlar uygun anahtar değişimini tamamladıktan sonra, bu anahtar hafızadan silinir. E_{22} algoritmasında 16 baytlık PIN kodu kullanıldığı için, uzunlukları 16 bayttan daha az seçilmiş PIN kodları algoritmaya girmeden önce BD_ADDR ile birleştirilip (~), yeni bir 16 baytlık PIN kodu oluşturulur. Eğer cihazlardan birisi sabit PIN koduna sahipse, bu işlem için diğer cihazın BD_ADDR değeri kullanılırken ; her iki cihaz da değişken PIN koduna sahipse, IN_RAND rastlantısal sayı gönderilen cihazın BD_ADDR'i kullanılır. Bu yordam , K_{INIT} *a*nahtarının, değişken PIN koduna bağlı cihazın kimliğine bağımlı bir yapıya sahip olması için uygulanır. Eğer her iki cihaz da sabit PIN koduna sahipse bu iki cihaz iletişim kuramazlar.

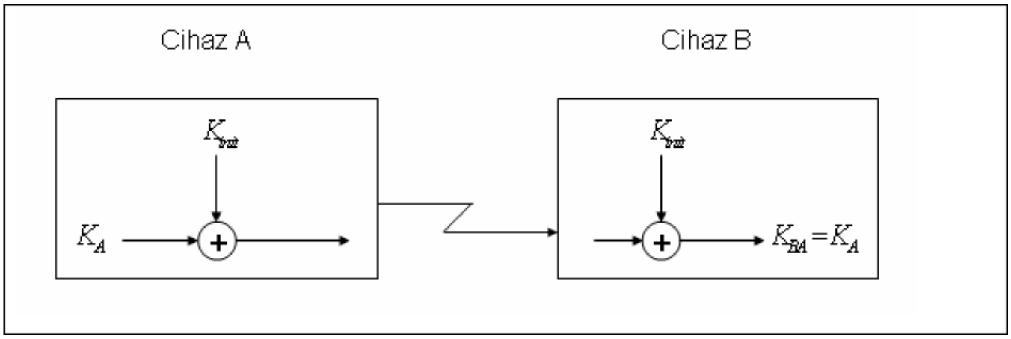
Kötü niyetli kullanıcıların, farklı BD_ADDR deneyerek, çok uzun PIN kodlarını test edip bulmaları bu şekilde mümkün olabilmektedir. Dolayısıyla buna karşı farklı uygulamalar için farklı önlemler alınması gerekmektedir. Fakat aynı şekilde BD_ADDR'i sabit tutularak değişik PIN kodları denenirse, buna sistem otomatik olartak müdahale edecek ve bir sonraki deneme için izin verilen bekleme zamanı üstel (exponential) olarak artırılacaktır.

3.5.2.2. Cihaz anahtarının üretilmesi, K_A

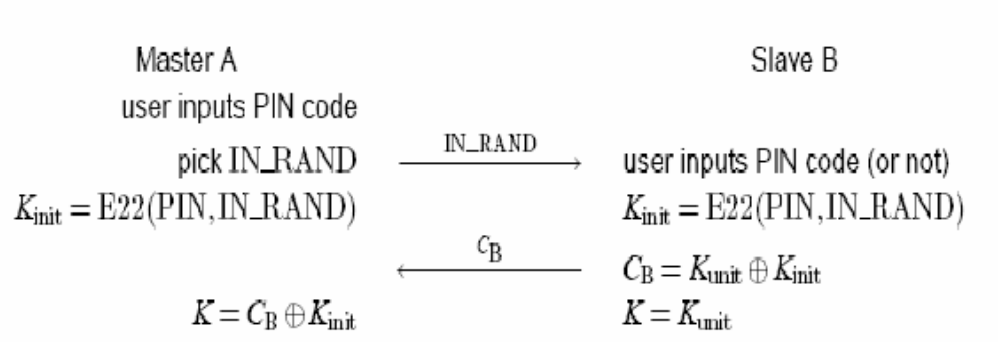
Bluetooth cihazının fabrikadan sonra ilk defa çalışmaya başlamasıyla birlikte, E_{21} algoritması kullanılarak üretilir. Bir kere üretildikten sonra uçucu olmayan bellekte saklanır ve kolay kolay değiştirilmez.,İletişim kurmak isteyen iki cihazdan hangisinin cihaz anahtarının, bağ

anahtarı olarak kullanılacağına ilklendirme yordamında karar verilir. Tipik olarak daha sınırlı hafızaya sahip cihazın anahtarı kullanılır. Çünkü bağ anahtarının oluşturulması için cihazın sadece kendi anahtarını hatırlaması yeterli olacaktır.

Aşağıdaki şekildeki gibi, A ile B cihazları arasında A cihazının cihaz anahtarı, K_A, bağ anahtarı olarak kullanılmaktadır. A cihazı K_A cihaz anahtarını B cihazına göndermekte, B cihazı da K_A anahtarını K_{BA} bağ anahtarı olarak hafızasına kaydetmektedir. Başka bir C cihazı ile A cihazının olduğu bir örnekte de, bağ anahtarı yine K_A olarak seçilirse, bu anahtar C cihazının hafızasına K_{CA} bağ anahtarı olarak kaydedilir.



Şekil-8 Cihaz anahtarının üretilmesi



Şekil-9 İlklendirme anahtarının($K_{İNİT}$), Bağ anahtarının(K_{UNIT}) üretilmesi,değişimi

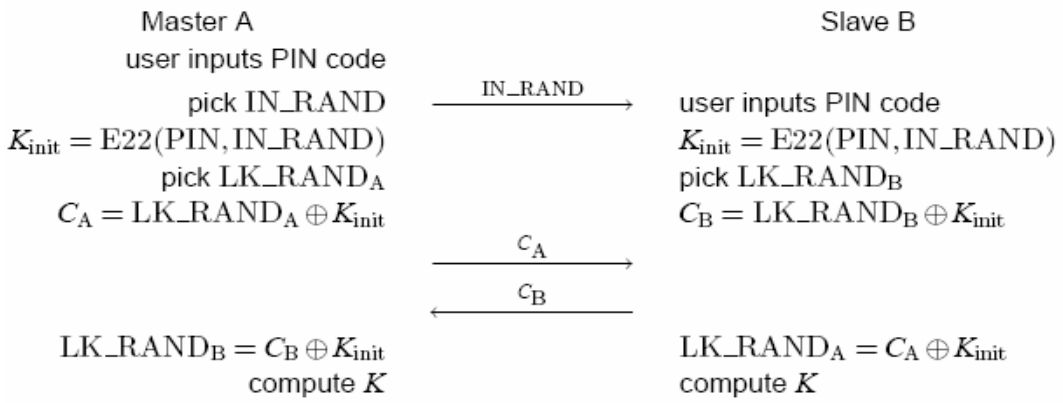
3.5.2.3. Birleşim anahtarının üretilmesi, K_{AB}

A ve B cihaz anahtarlarının birleşiminden oluşan bu anahtar, yine ilklendirme yordamı içerisinde üretilir. İlk önce her bir cihaz LA_RAND_A ve LA_RAND_B rastlantısal sayılarını üretirler. E_{21} algoritması kullanılarak da yine farklı iki rastlantısal sayı üretilir.

$LK_K_A = E_{21}(LK_RAND_A, BD_ADDR_A)$ ve $LK_K_B = E_{21}(LK_RAND_B, BD_ADDR_B)$

LK_RAND_A ve LK_RAND_B rastlantısal sayıları, o an aktif olan bağ anahtarı K_{INIT} ile mod 2 toplama işlemine tabi tutularak güvenli bir şekilde cihazlar arasında değiştirilir.Yani A cihazı $C_A = K_{INIT} \sim LK_RAND_A$, B cihazı $C_B = K_{INIT} \sim LK_RAND_B$ sayılarını gönderirler. Değişim tamamlandıktan sonra her bir cihaz, aldığı bu sayıyı K_{INIT} bağ anahtarı ile tekrar mod 2 toplama işlemine tabi tutularak, diğer cihazın rastlantısal sayısını elde eder. Böylelikle LK_RAND_A ve LK_RAND_B sayıları her iki cihazda da bulunmuş olup, bu sayılar XOR'lanarak da birleşim anahtarı üretilir.

$$K_{BA} = LK_K_A \sim LK_K_B$$



$$K = E21(LK_RAND_A, BD_ADDR_A) \oplus E21(LK_RAND_B, BD_ADDR_B)$$

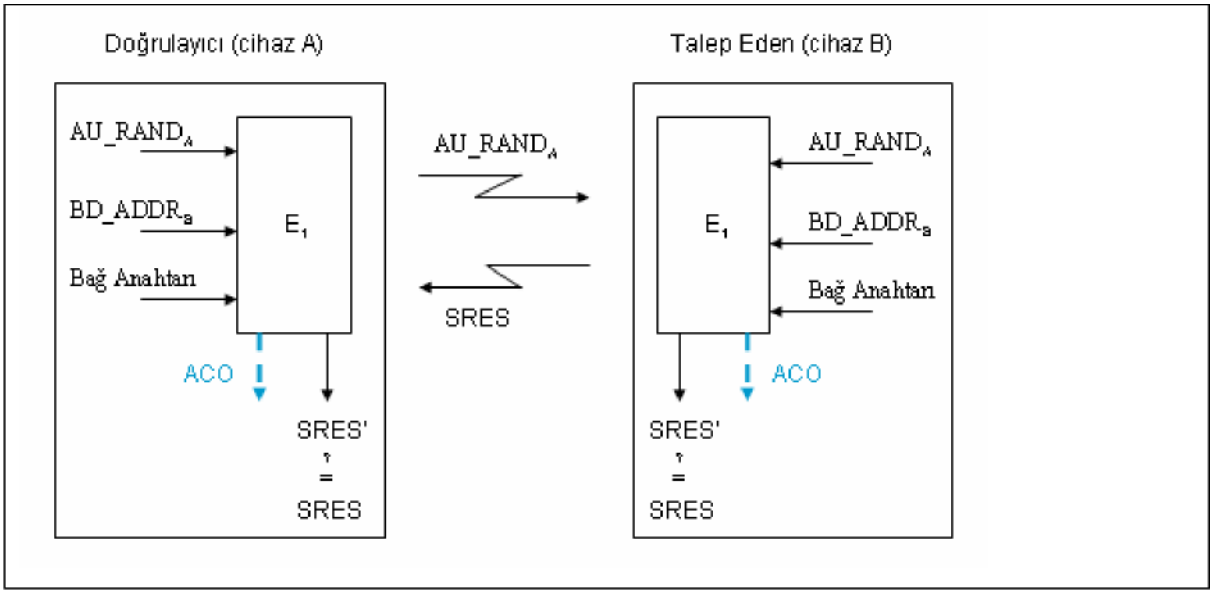
Şekil-10 İlklendirme anahtarının(K_{INIT}), Bağ anahtarının(K) üretilmesi,değişimi

3.5.2.4. Şifreleme anahtarının üretilmesi, K_C

E_3 algoritması yoluyla, bağ anahtarı, 96-bitlik şifreleme sapması (COF) sayısı ve 128-bitlik rastlantısal sayı kullanılarak üretilir. COF değeri duruma göre iki farklı değerden birini alabilir. Şöyleki eğer bağ anahtarı, ana (master) cihazın anahtarı ise COF, ana cihazın BD_ADDR kullanılarak elde edilirken; diğer durumlarda kimlik doğrulama şifreleme sapması (ACO) değerine eşit olur.

$$(K, RAND, COF) \rightarrow Hash(K, RAND, COF, 12)$$

3.5.3. KİMLİK DOĞRULAMA



Şekil-11 Bluetooth için meydana - okuma yanıt sistemi(Kimlik Dogrulama)

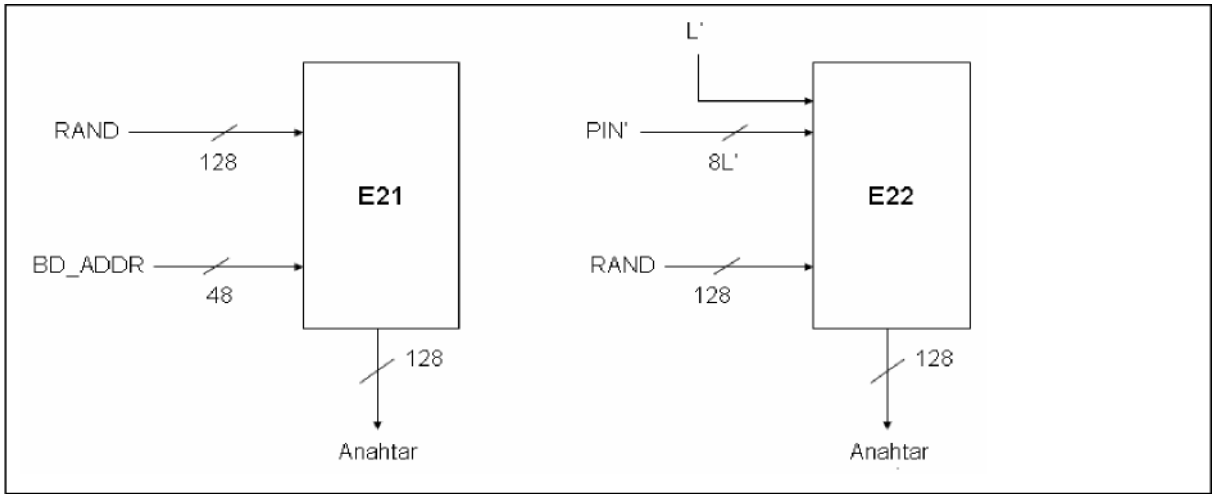
Bluetooth'da kullanılan kimlik doğrulama yordamı, kimliğinin doğrulanması talep edilen cihazın gizli anahtar bilgisinin, simetrik gizli anahtarlar kullanılarak kontrol edildiği bir meydan okuma – yanıt prensibini dayanır. Bu prensibe göre doğrulayıcı cihaz, kimliğinin doğrulanması talep edilen cihaza rastlantısal bir sayı,AU_RANDA gönderir. Rastlantısal sayıyı alan bu cihaz, kendi cihaz adresini BD_ADDR_B ve kontrol edilmesi istenilen bağ anahtarını da kullanarak, *E_1* kimlik doğrulama algoritması ile yoluyla bir yanıt üretir. SRES

olarak adlandırılan bu 32 bitlik imzalanmış yanıt, doğrulayıcı cihaza tekrar gönderilir. Doğrulayıcı cihaz da, diğer cihazın adresi BD_ADDR_B ürettiği AU_RAND_A rastlantısal sayısı ortak bağ anahtarını kullanarak kendi yanıtını SRES üretir. Bluetooth da, doğrulayıcı cihazın ana cihaz olmasına gerek yoktur. Bağımlı cihaz da uygulamaya göre ana cihazdan kimlik doğrulamayı talep edebilir. Genelde Bluetooth uygulamalarının çoğunda tek taraflı kimlik doğrulama istenir. Fakat bazı özel uygulamalar için karşılıklı kimlik doğrulama yordamı da gerekebilmektedir.

3.5.3.1. Kimlik doğrulama için anahtar üretim fonksiyonları

Kimlik doğrulama yordamı içerisinde kullanılacak tüm anahtarlar iki moda sahip E_2 algoritması ile üretilirler. E_{21} olarak adlandırılan bu algoritmanın ilk modunda 128-bitlik RAND rastlantısal sayısı ve 48 bitlik Bluetooth cihaz adresi kullanılarak, 128-bitlik bir anahtar üretilir. Bu algoritma cihaz anahtarının ve birleşim anahtarının üretilmesi için kullanılır. E_{22} olarak adlandırılan bu algoritmanın ikinci modunda da 128-bitlik RAND rastlantısal sayısı ve L-bayt uzunluğundaki kullanıcı PIN kodu kullanılarak, 128-bitlik bir anahtar üretilir. Bu algoritma da ilklendirme anahtarı ve geçici anahtarın üretilmesi için kullanılır.

Bu algoritmaların temelinde şifreleme için kullanılan ve SAFER+ algoritmasının değiştirilmiş versiyonu olan A_R fonksiyonu kullanılmıştır. A_2 algoritmasının iki modunun da detayları aşağıda verilmektedir.



Şekil-12 Kimlik doğrulama anahtarları üretimi

3.5.4. ŞİFRELEME

Bluetooth'un paket yapısını oluşturan yararlı yük, giriş kodu ve paket başlığı bölümlerinden, sadece kullanıcı mesajının yer aldığı yararlı yük kısmı şifrelenir. Diğer kısımlar kesinlikle şifrelenmez. Bu şifreleme her yararlı yük paketi için tekrar senkronize edilerek,akışkan şifre algoritmasıyla başarılır.

E_0 akışkan şifre sistemi üç ana kısımdan oluşur.

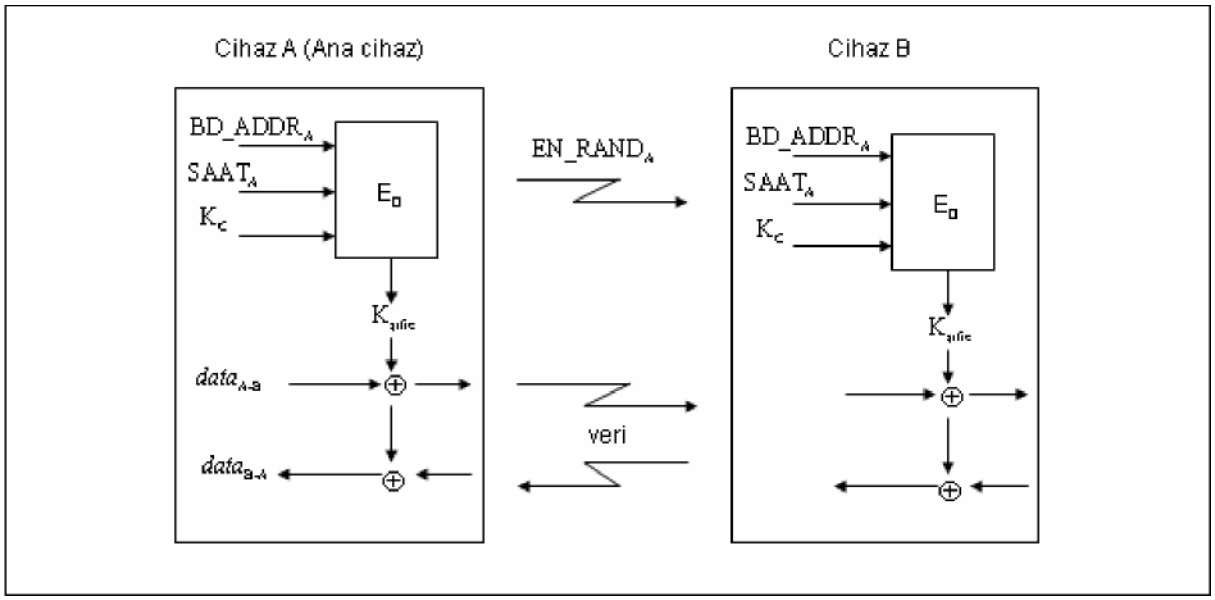
- Birinci kısım, ilklendirme aşaması (yararlı yük anahtar üreteci). Algoritmanın girdilerini belli kurallara göre alıp, bunları yararlı yük anahtar üreteci içerisindeki dört adet Doğrusal Geribesleme Kaydıran Yazmaça yerleştirir.
- İkinci kısım akışkan anahtar bitlerinin üretilmesi aşaması. Bu bitler temel olarak Massey ve Rueppel'a ait toplama akışkan şifre üretecinden elde edilir. Toplama üreteci, ilinti saldırılarına karşı zayıf olmakla beraber, iletişimdeki yüksek senkronizasyon frekansları sayesinde bu tip saldırılar engellenmektedir.
- Üçüncü kısım şifreleme ve şifre çözme aşaması.

3.5.4.1. Şifreleme kavramı

Bluetooth temelband da, şifreleme ile ilgili üç ana seçenekten bahsedebiliriz.

- Hiçbir mesaj şifrelenmez. Varsayılan değerdir.
- Sadece noktadan noktaya iletişimde şifreleme yapılır. Tümegönderim mesajları şifrelenmez.
- Tümegönderim veya noktadan noktaya tüm mesajlar şifrelenir.

İletişim kurmak isteyen cihazlar bağlantıyı gerçekleştirdiklerinde bu seçenekten birini seçerler ve şifreleme yordamı buna göre gerçekleşir veya gerçekleşmez.Şifreleme için daha öncede bahsedildiği gibi akışkan şifre algoritması kullanılır. Şifrelenmesini istediğimiz veriler, bu algoritma sonucunda oluşan $K_{ŞİFRE}$ akışkan anahtarı bitleri ile modulo-2 toplamı yapılarak diğer cihaza gönderilirler.



Şekil-13 Şifreleme yordamının fonksiyonel yapısı

Mesajın yer aldığı her yararlı yük paketi ayrı ayrı şifrelenir.E_0 algoritması, K_C şifreleme anahtarını, ana cihazın BD_ADDR_A adresini ve yine ana cihazın gerçek-zamanlı (real-time) saatini kullanır. K_C şifreleme anahtarı, ayrıca E_0 algoritması içerisinde $K_{C'}$ anahtarına dönüştürülerek E_0 algoritmasına katılır.

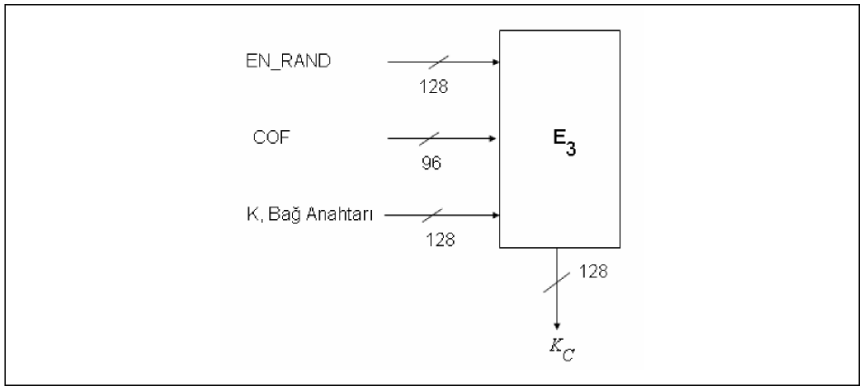
26-bitlik Bluetooth saati her bir zaman diliminde bir (1) artırılır. Saatdeki en az bir bitlik bu değişimden dolayı da her bir paket için, aynı veriye bile sahip olsa, farklı bir $K_{ŞİFRE}$ akışkan anahtarı bitleri oluşturulmuş olur.

3.5.4.2. Şifreleme için anahtar üretim fonksiyonu

E_0 şifreleme algoritmasının girdilerinden biri olan K_C anahtarının üretilmesi için, E_3 olarak adlandırdığımız bir algoritma kullanırız. Temelde bu algoritma da diğer anahtar üretim fonksiyonlarında kullandığımız A_R fonksiyonun bir uygulamasıdır.

$$(K, RAND, COF) \rightarrow Hash(K, RAND, COF, 12)$$

Dikkat edilirse bu algoritmanın çıktısı olan K_C anahtarı 128-bit uzunluğundadır.Dolayısıyla E_0 şifreleme algoritmasında kullanılmadan önce, anahtar uzunluğunun istenilen boyuta getirilmesi gerekmektedir.



Şekil-14 Şifrelema anahtarı üretimi

3.5.5. Güvenlik mimarisi

Bluetooth Genel Geçiş Profil'i, cihazlar için üç güvenlik modu önermiştir. Bluetooth cihazı aynı anda bu modlardan yalnızca biri üzerinden çalışabilir. Bu modlar aşağıda kısaca açıklanmaktadır.

- **Güvenlik modu 1** (güvenli-olmayan)Cihaz güvenlik ile ilgili hiç bir yordamı işleme sokmaz.
- **Güvenlik modu 2** (servis seviyesinde uygulanan güvenlik)Cihaz bağlantı kurulmadan önce güvenlik ile ilgili hiç bir yordamı işleme sokmaz. Tüm güvenlik mekanizmaları iki cihaz arasında bağlantı kurulduktan sonra başlatılır. Bu mod ile her uygulama için farklı ve esnek güvenlik yapılarının oluşturulmasına izin vermektedir.
- **Güvenlik modu 3** (bağ katmanı seviyesinde uygulanan güvenlik)Cihaz henüz bağlantı kurulmadan önce güvenlik mekanizmalarını işleme sokar.

Ayrıca Bluetooth güvenlik mimarisinde hem cihazlar hem de verilen servisler için farklı güvenlik seviyeleri tanımlanmıştır.

Cihazlar için iki güvenlik seviyesi tanımlanır.

- ***Güvenli cihaz :*** Genel olarak daha önceden kalıcı bir bağlantı kurulup, iletişim yapılmış cihazdır. Uygulama katmanından bazı sınırlamalar getirilmediği sürece tüm servislere sınırsız olarak giriş iznine sahiptir.
- ***Güvensiz cihaz :*** Daha önce sabit ve kalıcı bir bağlantı kurulamamış veya da bir bağlantı kurulsa da, çeşitli nedenlerle güvensiz olarak kabul edilmiş ci hazd ı r.

Servisler için ise üç güvenlik seviyesi tanımlanır.

- Hem izin verme, hem de kimlik doğrulama yordamları istenen servisler. Otomatik geçişe sadece *güvenli cihazlar için* izin verilir.
- Sadece kimlik doğrulama yordamı istenen servisler. İzin verme yordamına gerek duymazlar.
- Tüm cihazlara açık servisler. Ne izin verme, ne de kimlik doğrulama yordamları işleme koyulur.

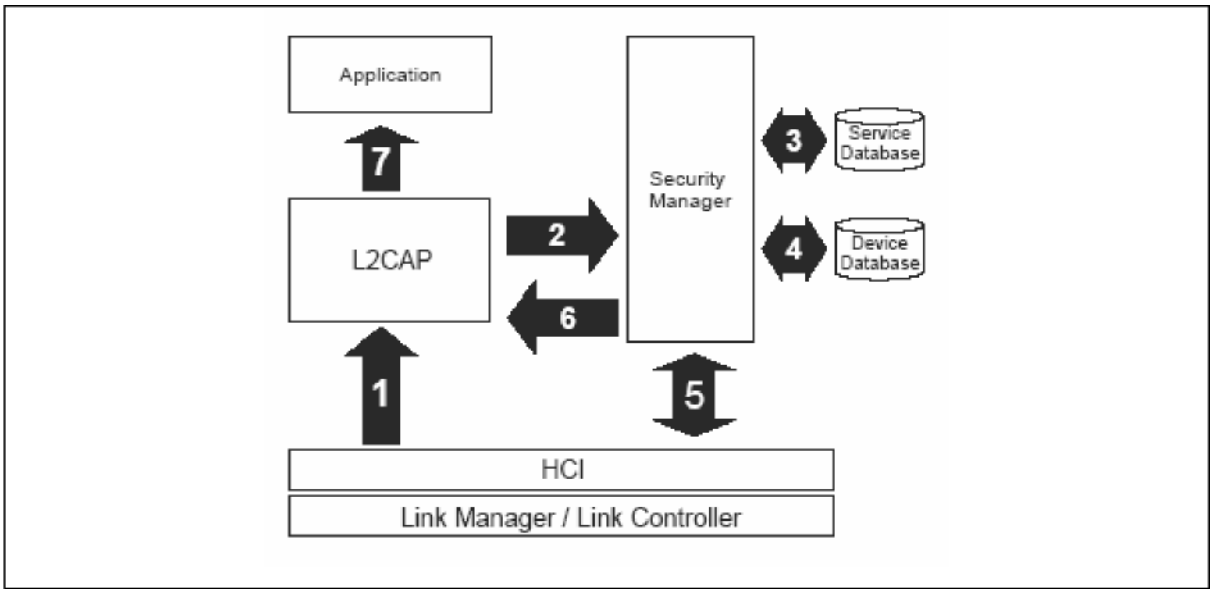
3.5.5.1. Güvenlik yöneticisi

Bluetooth güvenlik mimarisinin merkezinde güvenlik yöneticisi bulunur. Güvenlik yöneticisinin diğer protokol ve arayüzler ile ilişkisi basit bir sorgu-yanıt ve kayıt yordamlarıyla düzenlenir. Güvenlik yöneticisi içerisinde her servis için ayrı bir veritabanı tablosu tutulur. Bu tablo ile istenilen veritabanına ulaşılıp, istenilen servis veya cihaz için geçiş izni sorgulanır. Bluetooth güvenlik yöneticisinin fonksiyonları aşağıdaki gibidir.

- Servislerin güvenlik ile ilgili veritabanı bilgilerini tutmak
- Cihazların güvenlik ile ilgili veritabanı bilgilerini tutmak
- İlgili protokollerden veya uygulamalardan gelecek geçiş izni talebini cevaplandırmak
- Uygulamaya bağlanmadan önce gerekiyorsa kimlik doğrulama ve şifreleme yordamlarının kullanılmasını zorunlu kılmak.
- Cihazların eşleşmeleri için gerekli PIN girişlerinin yapılmasını sağlar.

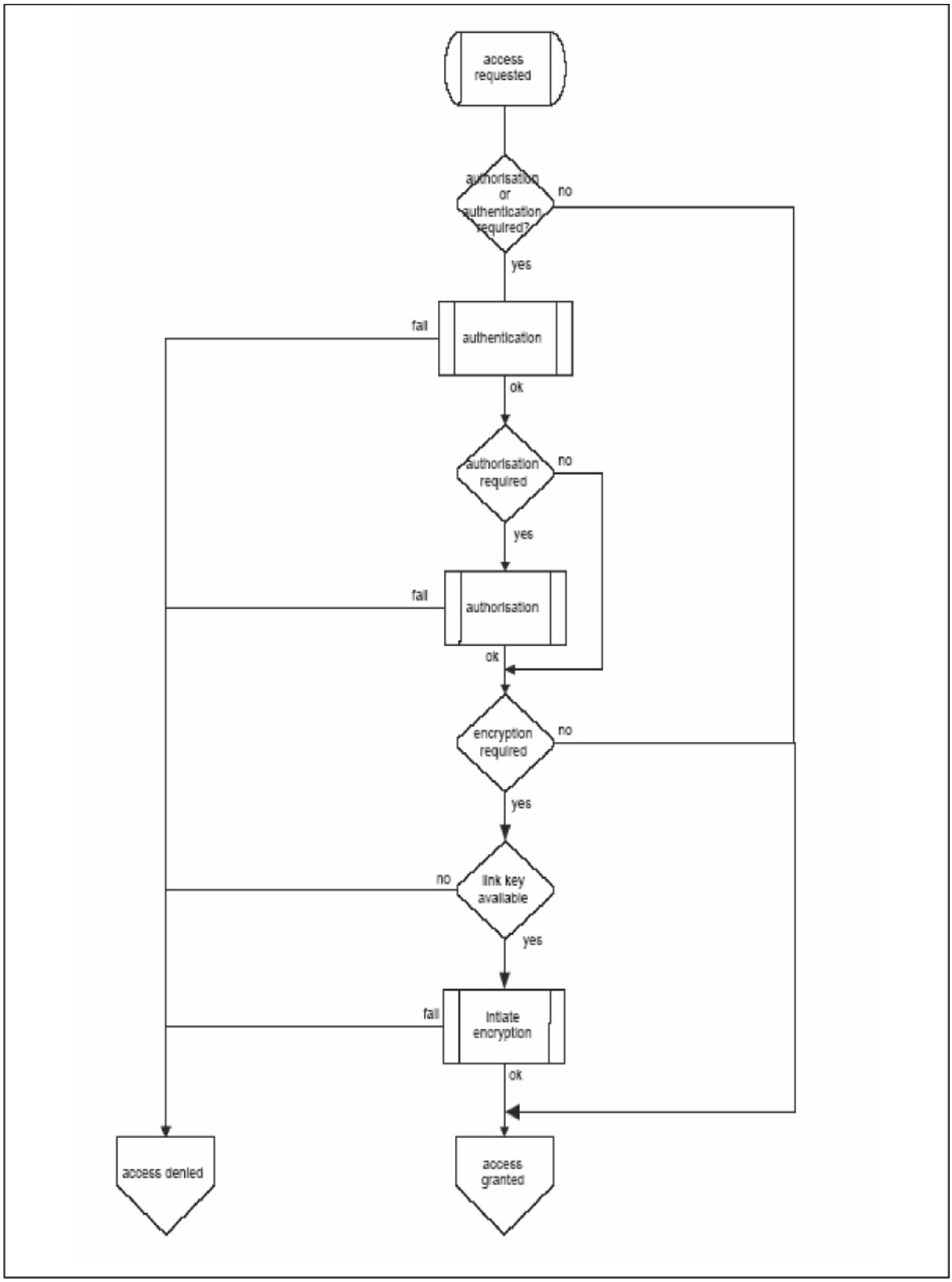
Bir örnek vermek gerekirse, güvenli bir cihaz için bu mimari içerisindeki bilgi akışı da aşağıdaki gibi özetlenebilir.

1. L2CAP'den bağlantı için izin istenir.
2. L2CAP, güvenlik yöneticisine başvurararak geçiş için izninin olup olmadığını sorgular.
3. Güvenlik yöneticisi, sahip olduğu veritabanı tablosuna göre istenilen servise geçiş için servis veritabanını tarar.
4. Güvenlik yöneticisi, yine veritabanı tablosuna göre istenilen cihazın güvenlik durumu için cihaz veritabanını tarar.
5. Güvenlik yöneticisinin denetiminde, iletişim yapılmaya çalışılan cihaz ile uygulamaya konulacak servise bağlı olarak kimlik doğrulama ve şifreleme yordamları işleme sokulur.
6. Güvenlik yöneticisi geçişi onaylar
7. L2CAP, bağlantının kurulmasına devam eder.

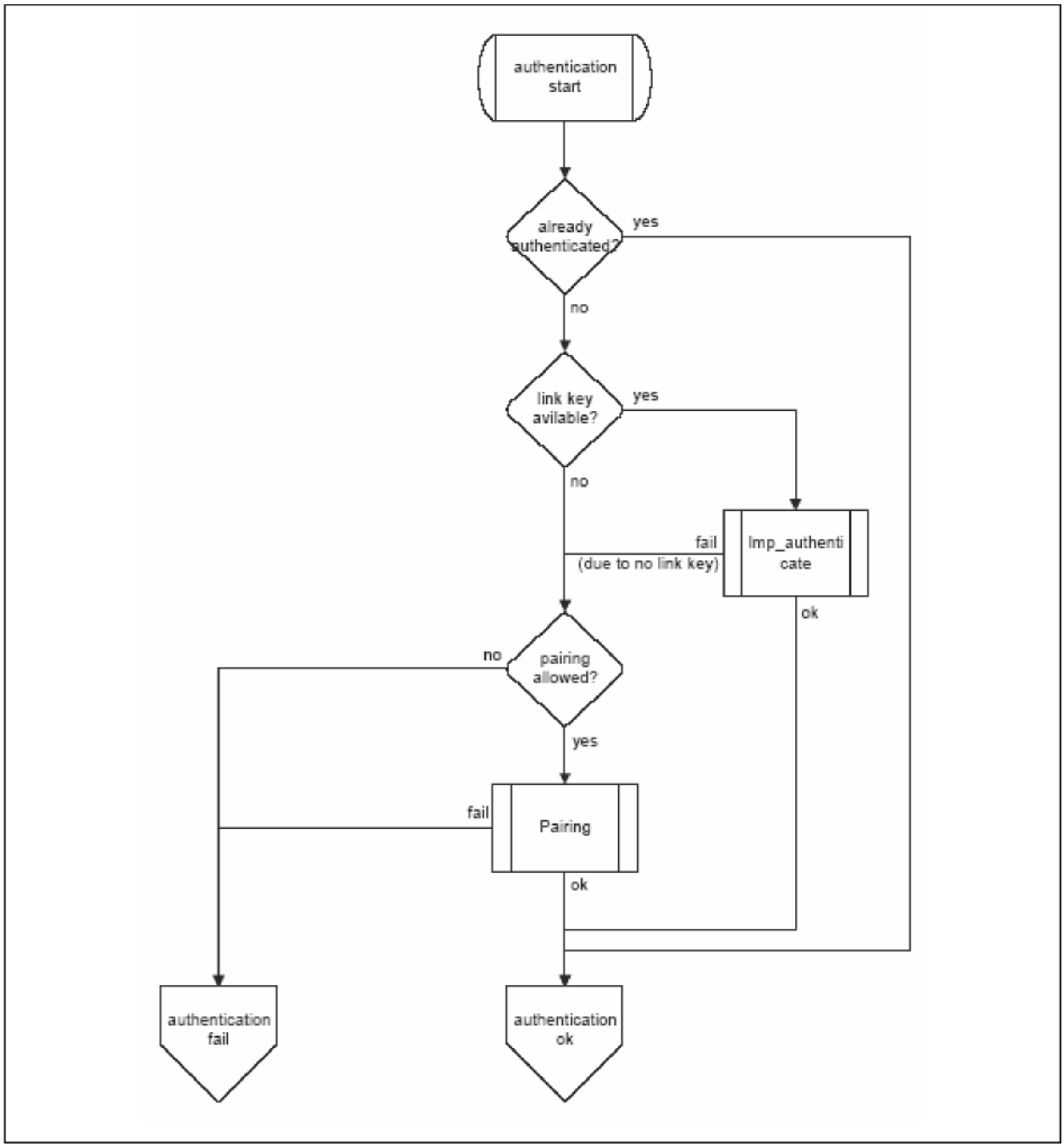


Şekil-15 Geçiş iznine sahip güvenli bir servis için bilgi akışı

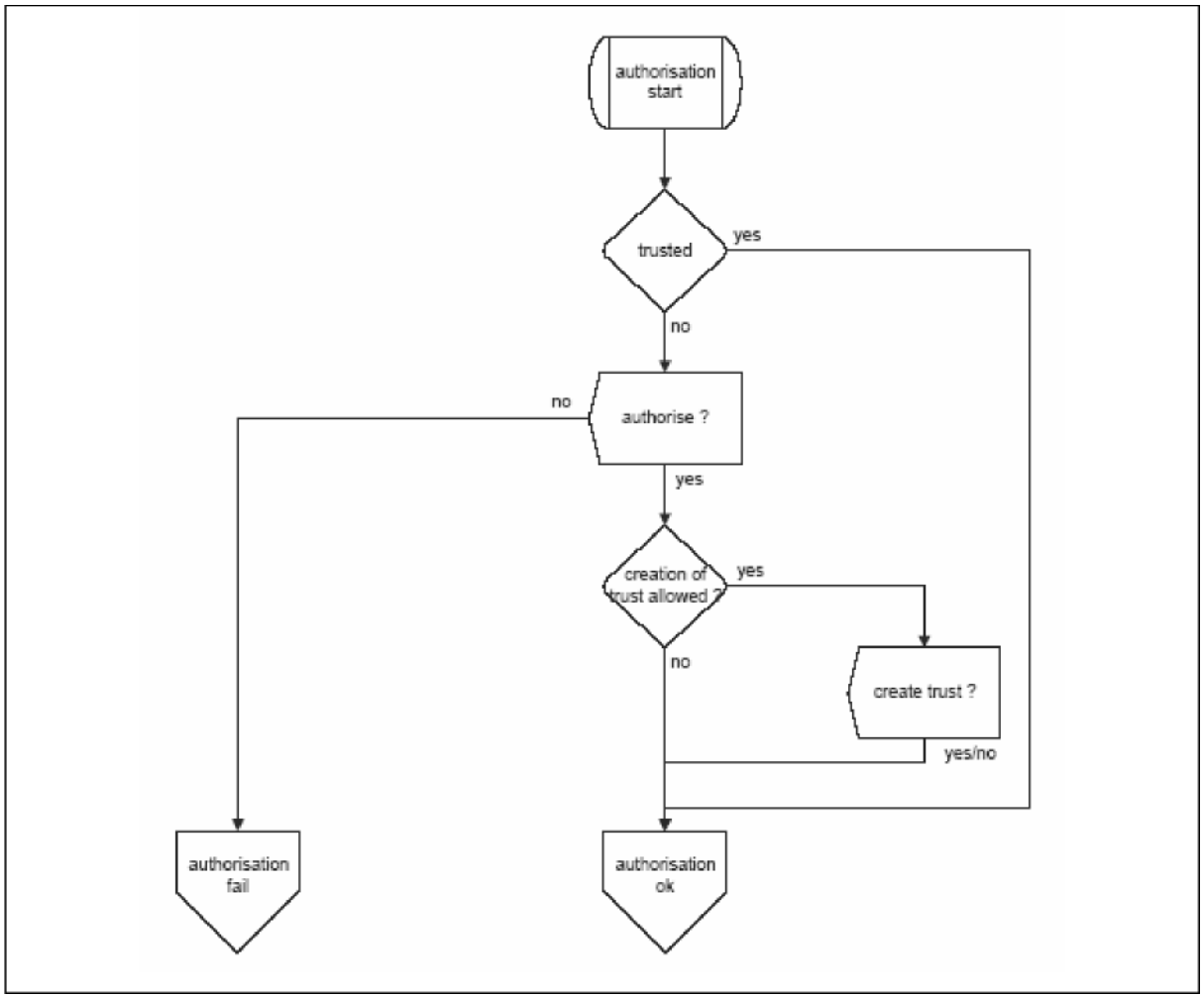
3.5.5.1. Akış Şemaları



Şekil-16 Güvenlik yöneticisi tarafından uygulanan geçiş kontrol akış çizeneği



Şekil-17 Kimlik doğrulama yordamı akış çizeneği



Şekil-18 İzin verme yordamı akış çizeneği

3.5.6.GÜVENLİK AÇIKLARI

3.5.6.1.Bluejacking

Bluejacking bir kullanıcının menzil dahilindeki başka bir kullanıcıya isimsiz olarak kartvizit göndermesidir.

Telefonunuzun verilerinde herhangi bir değişiklik İÇERMEZ. Genellikle kartvizitler mesaj veya fıkradan oluşurlar ve bluejacker'lar, sadece alıcıdan yaratıcı bir yanıt beklerler.

Bluejackerların cesaretini kırmak için, basitçe kartviziti reddedin ya da tamamen kurtulmak için, telefonunuzu keşfedilemez konumuna ayarlayın

3.5.6.2.Bluebugging

Bluebugging, yetenekli bir kişinin, sahibinin bilgisi veya onayı olmadan bir cep telefonunun komutlarına ulaşmasını içerir. Bu, hackerın, çağrı yapmasına veya mesaj göndermesine, takvim veya telefon rehberini okumasına ve not yazmasına, telefon konuşmalarını dinlemesine ve İnternete bağlanmasına imkan verir.

3.5.6.3.Bluesnarfing

Bluesnarfing, yetenekli bir hackerın, kullanıcısının izni veya bilgisi olmadan cep telefonu üzerindeki telefon rehberi, resimler, takvim ve EMEI (Uluslararası Mobil Ekipman Kimliği) gibi verilere ulaşmasını içerir.

3.5.6.4.Cabir virüsü

Cabir virüsü, zararlı kodların bir örneğidir.

Virüs, kullanıcının eklenmiş dosyayı kabul edip kurması şartıyla telefonu etkiliyor. Bir kez kurulduktan sonra Bluetooth teknolojisinden yararlanarak kendini saldırıya açık diğer aygıtlara gönderiyor. Bu niteliğinden ötürü, Cabir bilgisayar solucanı kapsamına sokuluyor.

Bu solucan, Symbian 60 platformunu kullanan ve Bluetooth özelliğine sahip telefonları tehdit ediyor

3.5.6.5.Car Whisperer

Bluetooth destekli araba ses sistemlerinden ses verisi çalma.

3.5.6.6.Anahtarların güvenilirsizliği

Aynı cihaz adını alan kullanıcılar içinde geçerli olup yerine geçme durumunda yetkisiz erişim ortaya çıkmaktadır.

Giriş anahtar kodunun 1-16 bayt arasında herhangi bir değer alabilmesi, giriş anahtar kodunun seçiminde zayıf anahtar üretimi için bir etken oluşturmaktadır.

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

3.5.6.7.Safer+ algoritması yetersizliği

Kimlik doğrulama ve tüm anahtarların üretilmesi aşamasında kullanılan Safer + Bluetooth algoritması, günümüz şartlarında artık yeterince güvenli sayılmamaktadır.

3.5.6.8.Aradaki adam problemi

Açık anahtar algoritması kullanılmadığından aradaki adam saldırısına karsı savunmasızdır.

3.5.6.9.Tekrarlama saldırısı

79 kanalı birden dinlenirse tekrarlama saldırısı olabilir.

3.5.6.10.Hizmet engelleme saldırısı

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

3.5.7. BLUETOOTH GÜVENLİĞİ ARTIRMAYA YÖNELİK İPUÇLARI

1. Bluetooth ayarınızı "keşfedilemez" modunda tutun.(iletim devre dışı bırakılır) ve yalnızca kullandığınız zamanlarda "keşfedilebilir" moda geçin. Cep telefonunuzu veya PDA'nızı keşfedilebilir modda bırakmak, aygıtı tehlikeli biçimde Bluetooth iletimine açık bırakır — yürüyüşe çıktığınız sırada, araba kullanırken ve hatta işyerinizde dolaşırken 10 metre uzaktaki herhangi bir Bluetooth kullanıcısı sinyalinizi alabilir ve bu sinyali kullanarak aygıtınıza erişebilir

2. Güçlü bir PIN kodu kullanın. Beş basamak veya daha uzun kodlar daha zor cozulur.

3. Kablosuz aygıtlarınızda önemli verilerinizi saklamaktan kaçının;Sosyal güvenlik numaranız, kredi kartı numaralarınız ve parolalarınız gibi bilgileri saklamayın.

4. Bluetooth gelişmeleri ve güvenlik sorunları konusunda güncel bilgileri edinin.Yazılım güncelleştirmeleri veya belirli güvenlik açıkları için aygıt üreticinize düzenli olarak başvurun.

5. Bağ anahtarı için cihaz anahtarının kullanımından kaçınınız. Bunun yerine birleşim anahtarını kullanınız.

6. İzinsiz dinleyicilere karşı, iki cihazın ilk iletişiminin mümkün olduğunca güvenli bir ortamda yapılmasını sağlayın.

KAYNAKLAR

[1] Bluetooth 1.2 Specifications

https://www.bluetooth.com/

[2] Bluetooth 1.2 Specifications

https://www.bluetooth.org/

[3] SIG, Bluetooth Specification Version 2.0 + EDR, [2004]

[4] SIG, Specification of the Bluetooth System, [10-Nov-2004], http://bluetooth.com/Bluetooth/Learn/Technology/Specifications/

[5] Mikkola Lauri,Bluetooth Security,[2006]

[6] Serge Vaudenay ,Bluetooth Security,[2006]

[7] Özçelik, Mehmet Ali , ,Bluetooth Üzerinden Veri İletimi,2005