Bluetooth üzerinden güvenli veri iletimi*

Secure data transmission over bluetooth

Mehmet Ali Özçelik[1], Mustafa Karabulut[1], Abdulhamit Subaşı[2]

Gaziantep Meslek Yüksekokulu[1], International Burch University[2]
ozcelik@gantep.edu.tr,mkarabulut@gantep.edu.tr,asubasi@ibu.edu.ba

Özetçe

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, taşınabilir bilgisayarlar, modemler, kameralar, LAN (Local Area Network) erişim cihazları, ev aletleri ve PDA'lar (Personal Digital Assistant) gibi sayısal cihazlar arasında veri aktarımı sağlamak gayesiyle kullanılmaktadır.

Bluetooth iletişim ortamının kablosuz olması ve ortamın tüm kullanıcılara açık olması sistemde güvenlik açıklıkları meydana getirmektedir. Bu nedenden dolayı kablosuz ağ ortamı olan bluetooth'a özgü güvenlik uygulamaları geliştirilmektedir. Bu çalışmada bluetooth teknolojisi ve veri güvenliği açıkları araştırılmış, bluetooth güvenlik yapısının geliştirilmesi üzerinden durulmuş, cep telefonu üzerinden yeni güvenli veri iletimi uygulaması gerçekleştirilmiştir.

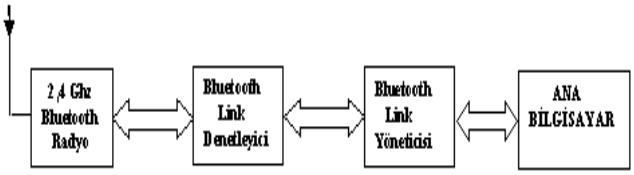
Abstract

Bluetooth is a technology that provides wireless communication in short distance and that uses 2.4 Ghz (ISM) radio-frequency band. Bluetooth technology supplies wireless data and voice communication with the technique enabling to be integrated to all equipments and having low power consumption and being cheap. Bluetooth is used to provide data transmission between the digital equipments such as laptops, modems, cameras, local area networks (LAN) access equipments, phones, home apparatus and personal digital assistant (PDA).

Since bluetooth communication environment is wireless and open for all users, it may cause some security problems. Because of these reasons, security protocols and methods that are peculiar to Bluetooth were investigated. In this paper, the data security structure of bluetooth technology was explained and new methods were applied to improve the security of bluetooth wireless communication. Also one application of these methods is realized on mobile phones.

1.Giriş

Bluetooth sistemi yapısı radyo birimi, link kontrol birimi, link yönetimi ve kullanıcı uç ara yüz fonksiyonlarına destek veren bir birimden oluşmaktadır. Ana bilgisayar kontrol arayüzü (HCI-Host Controller Interface) ana birimin bluetooth donanımına erişmesi için bir araç vazifesi görür. Bluetooth sistem yapısı şekil 1'de görülmektedir. Bluetooth vasıtasıyla özel amaçlı haberleşme ağlarının kurulması, tüm kişisel cihazların arasında senkronizyonun sağlanması çok kolaydır..



Şekil 1: Bluetooth sistemi yapısı

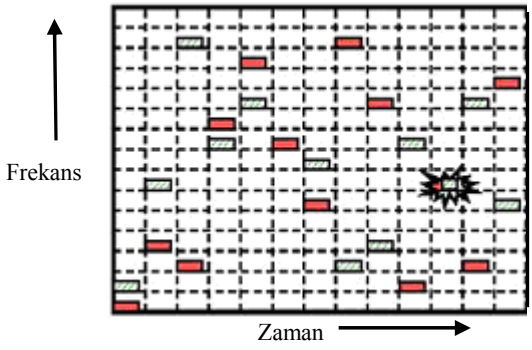
Örneğin, ana birim bir dizüstü bilgisayar ve kişisel bilgisayarın içine yerleştirilmiş elektronik kartta bluetooth cihazı olabilir. Ana birimden bluetooth modülüne gönderilen tüm komutlar ve modülün ana birime verdiği cevaplar HCI vasıtasıyla iletilir.

Bağlantıyı sağlamak için iki adet bluetooth ile donatılmış cihazın birbirlerine 10 metrelik bir mesafede yaklaşmaları gerekmektedir. Bluetooth telsiz tabanlı bir bağlantı kullandığından, iletişim kurmak için görüş hattı bağlantısına ihtiyaç duymaz. Ofisinizde kullandığınız bilgisayarınız, bilgiyi yan odadaki yazıcıya gönderebilir ya da evinizin alarm sistemini cep telefonuyla kontrol edebilirsiniz. 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 lisansız 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) [1]
- Her kanal için bant genişliği 1 Mhz ile sınırlandırılmıştır.
- Frekans atlama tekniği, yaygın spektrum haberleşmesinde kullanılmalıdır.

* Bu çalışma 2003K120730 no.lu DPT projesi tarafından desteklenmiştir.

- Girişim etkisi uygun bir şekilde yürütülmelidir.



Şekil 2: Bluetooth frekans atlama durumu .

Bluetooth teknolojisinde, daha güvenilir ve daha etkili haberleşme için frekans atlama mekanizması kullanılmaktadır. Şekil 2'de iki cihazın frekans atlama metodunu kullanarak veri paketlerini iletmesi ve iki cihazın paketleri aynı frekansta kullanmak isteme durumu görülmektedir [2]. 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 Şebeke Yapısı

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.

Bluetooth cihazları, her bir paketten sonra yeni bir frekansa atladıkları zaman mutlaka kullanacakları frekans sırası ile uyuşmak 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.

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.

Bluetooth Güvenliği

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

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. Bu durum bir güvenlik açığı meydana getirmektedir.

Bilgi güvenliği ve kriptoloji

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 .

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.

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 değişiklerin yetkisiz yapılmamasını ve eğer yapıldıysa bu değişiklerin ortaya çıkarılmasını amaçlayan bir servistir. Ayrıca bu

değişikliğe yetkili veya yetkisiz kimin neden olduğunun tesbit edilmesi de yine bu servisin kapsamına girmektedir.

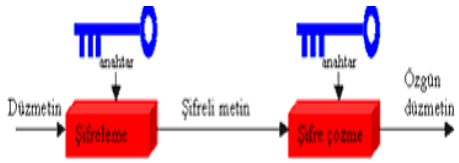
Kimlik doğrulama**:** Güvenli bir iletişim yapmak isteyen her kullanıcı, öncelikle karşısındakinin doğru kişi olup olmadığından emin olmak ister. Bunun için tarafların birbirlerine uyguladıkları ve karşısındakinin kimliğini teyit etme amacına yönelik tüm yöntemler bu servisin görevleri arasındadır.

İnkar edememe**:** Olayı gerçekleştiren kişinin daha sonra bunu inkar edememesi için tasarlanan çeşitli yöntemleri tanımlar [3].

2. Materyal ve Metod

2.1. 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) [4]. Kriptografi dünyasında daha geleneksel olarak bilinen bir yöntemdir. Hem şifreleme hem de şifre çözme için aynı gizli anahtar kullanılır. Gizli anahtar kripto 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 sağlamaktadır.



Şekil 3: Gizli (Simetrik) anahtar şifreleme

Algoritmalardaki bütün güvenlik anahtara (veya anahtarlara) dayalıdır, hiçbiri algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenebildiği anlamına gelir. Bu algoritmayı kullanan ürünler seri üretilebilir. Bir davetsiz misafirin sizin algoritmanızı bilmesi önemli değildir; sizin özel anahtarınızı bilmedikçe, o şahıs iletilerinizi okuyamaz. Simetrik anahtarlamalı algoritmalar diğer tür simetrik olmayan algoritmalara göre daha hızlıdır ve donanımla gerçeklemesi daha kolaydır. Bluetooth güvenliğinde kullanılan safer algoritması bunun dışında DES, Blowfish, RC4, Rijndael gibi algoritmalar simetrik tür algoritmalara örnek verilebilir.

2.2. J2ME (Java 2 Micro Edition)

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. Bluetooth güvenli veri iletiminde simetrik şifreleme sağlayan java mıdlet uygulaması bilgisayar Jbuilder ortamından jad ve jar uzantılı iki mıdlet in java ve bluetooth destekli gezgin telefona veya gezgin telefon emülatörüne aktarılmasıyla yapılmıştır. Bir gezgin aygıtta Java denildiğinde kastedilen MİDlet'tir [5].

Midlet, aygıta değişik yollarla indirilir ve çalıştırılır, uygulamada kullanılan simetrik algoritma ise en yaygın kullanılan simetrik algoritma DES'tir (Data Encryption Standard).

3. Bulgular ve tartışma

3.1. 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 4) kullanılır.

Şekil 4: Geliştirilen uygulamanın gezgin telefona aktarılması

Oluşturulan şifreleme programı Nokia'nın 6600, 6630, 6230i, 6620, 6680 ve 7610 modellerinde, Sony-Ericsson'un P900 ve P910 modellerinde çalıştırılmıştır. Belirtilen cihaz modelleri Java ve Bluetooth API desteklidir. Daha sonra uygulama iki mobil telefon üzerinde yapılmıştır. Bluetooth üzerinden güvenli veri uygulamasının görüntüleri aşağıdaki şekillerde verilmiştir.

Şekil 5: Gezgin telefon emülatörü

Uygulamada Şekil 5'de verilen gezgin telefonlardan 2 adet kullanılmıştır. Cihaz bluetooth üzerinden güvenli veri iletiminin sağlanabilmesi için bluetooth modlarının açık olması gerekir bu durum gezgin telefonlarda

bağlantılar–bluetooth açık sekmesi işaretlenerek yapılır. Cihazlardan birisi (E_1) mesaj gönderici, diğeri (E_2) ise mesaj alıcı konumları verilir. Daha sonra E_1 aygıt arama moduna geçerek bluetooth kapsama alanı içerisinde aktif durumda olan E_2 yi bulur.

Bu durum Şekil 6'da verilmektedir.

Şekil 6: Bluetooth cihaz arama sorgulamasında E_1 mesaj gönderici emülatörü tarafından bulunan bt_000033127B35 adresli E_2 cihazı,cihaz arama sonucunda şifreli veri gönderilecek E_2 seçilir.

Şekil 7: Gönderilecek verinin ve anahtar şifresisinin girilmesi

Şekil 7'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 8: Şifreli verinin alınması ve aynı anahtar değerinin girilerek verinin deşifrelenmesi [6].

İki mobil telefon 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 bütünlüğüde sağlanabilmektedir. Bu şekilde de hem bu işlemler için harcanan zaman, hem de anahtar yönetimi için gereken ek yük azaltılmış olmaktadır.

4. Sonuçlar

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.Veri iletimi bluetooth yapısı ile bağlantılı olarak sağlanmıştır. Bu şekilde yerine geçme ve yetkisiz erişim durumu önlenmiş, Bluetooth mevcut güvenlik yapısı daha güçlenmiş yerine geçme açıklığı kapatılmıştır.

5. Kaynaklar

[1] Subramani , M.and Ilyas, M., "Simulation Based Analysis of Bluetooth Networks" College of Engineering Florida Atlantic University, ISBN : 1- 56555-269-5, Florida, 2003.
[2] Bluetooth-Lower Layer Approach www.holtman.org
[3] Menezes, J.A., Vanstone V.O., "Handbook of Applied Cryptography, CRC Pres, 1996.
[4] Akben, S.B., and Subaşı A., "RSA ve Eliptik Eğri Algoritmasının Performans Karşılaştırması" Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi 8(1), 35-40, 2005.
[5] Flanagan, D., *Java in a Nutshell A Desktop Quick Reference, 4th ed.*, O'Reilly & Associates, 2002.
[6] Özçelik, M.A.," Bluetooth üzerinden güvenli veri iletimi" Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2006.