Bilgisayar ve Mobil Cihazlarda Bluetooth Üzerinden Güvenli Veri İletimi

Mehmet Ali ÖZÇELİK[1], M.Kemal KIYMIK[2]

[1]Gaziantep Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Elektrik Programı, Gaziantep, Türkiye
[2]Kahramanmaraş Sütçü İmam Üniversitesi, Elektrik Elektronik Mühendisliği, Kahramanmaraş, Türkiye

ÖZET: Bluetooth kablosuz teknolojisi kısa mesafede 2.4 GHz endüstriyel-bilimsel-tıbbi (ISM) radyo frekans bandını kullanan bir teknolojidir. Bluetooth teknolojisi düşük güç tüketimli, ucuz ve tüm elektronik cihazlara entegre edilmeye olanak veren bir teknikle kablosuz veri ve ses iletişimi sağlamaktadır. Bluetooth sistemi, taşınabilir bilgisayarlar, modemler, kameralar, LAN (Local Area Network) erişim cihazları, ev aletleri, araç teknolojileri 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 açıklıkları araştırılmış, bluetooth güvenlik yapısının geliştirilmesi üzerinde durulmuş, cep telefonu ve bilgisayar üzerinden bluetooth güvenlik yapısını güçlendiren veri iletimi uygulaması gerçekleştirilmiştir.

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

Secure Data Transmission in Computer and Mobile Device over Bluetooth

ABSTRACT: 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 being cheap. That the environment 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 beendeveloped.
In this paper, 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. Also two applications of these method is realized on mobile phones and computer.

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

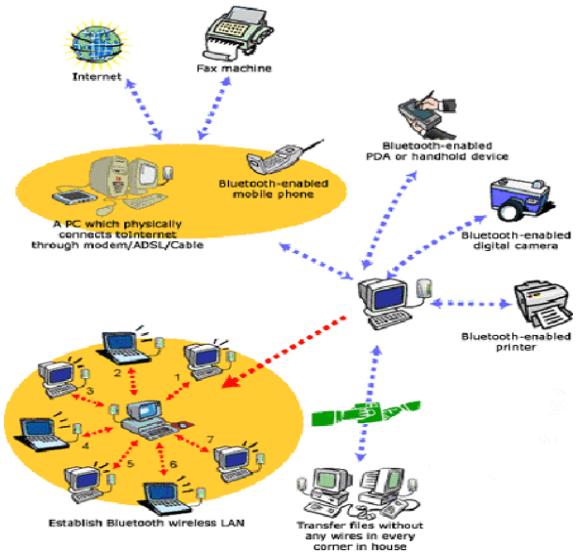
1. GİRİŞ

Son yıllarda bilişim teknolojileri alanında meydana gelen hızlı gelişmeler mobil haberleşme ve kablosuz teknolojiler sahasına yansımış ve kablosuz iletilimin en popüler teknolojilerden biri haline gelmesini sağlamıştır. 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 modulüne gönderilen tüm komutlar ve modulün ana birime verdiği cevaplar HCI vasıtasıyla iletilir. Bluetooth haberleşmesi, 2.4 GHz'de ve lisans gerektirmeyen ISM bandında (endüstriyel, bilimsel ve tıp uygulamalarına ayrılmış frekans bandı) gerçekleşmektedir[1]. Maksimum veri akış hızı 3 MB/sn'dir. Şekil 1' de Bluetooth sistemi yapısı görülmektedir.

Şekil 1. Bluetooth Sistemi Yapısı

Bağlantıyı sağlamak için iki adet Bluetooth ile donatılmış cihazın birbirlerine 20 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 2' de Bluetooth kullanım alanları verilmektedir.

*Sorumlu Yazar: Mehmet Ali ÖZÇELİK, ozcelik@gantep.edu.tr

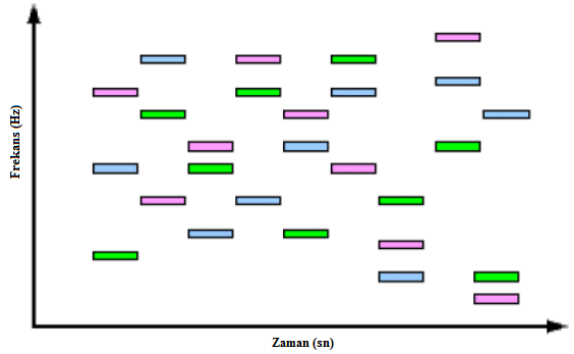


Şekil 2. Bluetooth kullanım alanları

Bluetooth vasıtasıyla özel amaçlı haberleşme ağlarının kurulması, tüm kişisel cihazların arasında senkronizasyonun kablosuz olarak sağlanması çok kolaydır. 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 aberleşmesinde kullanılmalıdır. Girişim etkisi uygun bir şekilde yürütülmelidir.

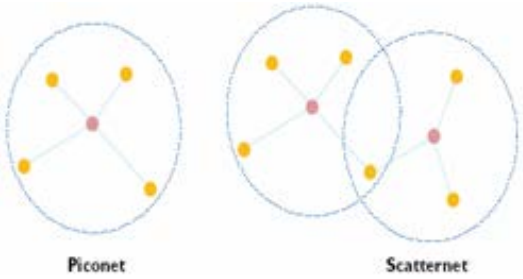


Şekil 3. Bluetooth frekans atlama durumu

Bluetooth radyo frekans işlemleri 2.402 GHz den başlar; 2.480 GHz de son bulur.1 MHz'lik aralıklara ayrılmış 79 frekans atlaması sayesinde frekans spektrumu genişletilir. Saniyede ortalama 1600 atlamaya izin veren full-duplex sinyal iletişim tekniği kullanılır.

1.1. 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 bluetooh 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[2]. Bütün bluetooth cihazları eşdeğer olmalarına rağmen, piconet oluştururken piconet bağlantısı süresince bir birim master, diğerleri slave olarak rol alır. Bu durum Şekil 4 'de verilmektedir.



Şekil 4. Bir piconet'in ve scatternet'in şematik gösterimi

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. 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.

Bluetooth teknolojisi hem zamanın önemli olduğu veri haberleşmesine, hem de zaman duyarlılığı olmayan fakat yüksek hızlı paket veri haberleşmesine imkan tanır. Bu verileri taşımak üzere, cihazlar arasında iki farklı tipte link tanımlanmıştır[3]. 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.

1.2. 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 [4]:

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

Karşıla-yanıtla prosedurü; 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 prosedurü ile öğrenilebilir. Bu durum bir güvenlik açığı meydana getirmektedir.

1.3. 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 olaral görülür. Kriptoloji ise hem kriptografi, hem de kripto analizinin bir birleşimi olarak tanımlanır.

1.4. Kriptolojinin Hedefleri

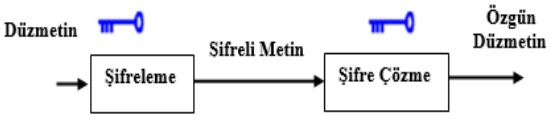
Bilgi güvenliğinin sağlanabilmesi için çok sayıda kavram ve servisten söz etmek mümkündür. Temel olarak kriptografi için birbirinin içerisine geçmiş dört farklı güvenlik servisi önem kazanmaktadır. Kriptolojinin hedefi de, bu dört servisi hem teoride hem pratikte işlevsel hale getirmektir.

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

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 5). 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 [5].



Şekil 5. Gizli (Simetrik) Anahtarlı 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, davetsiz şahıs iletilerinizi okuyamaz. Simetrik algoritmalar diğer tür simetrik olmayan türlere göre daha hızlıdır ve donanımla gerçekleşmesi daha kolaydır. Bluetooth güvenliğinde kullanılan safer algoritması dışında DES, Blowfish, RC4, AES gibi algoritmalar simetrik tür algoritmalara örnek verilebilir.

3. BULGULAR VE TARTIŞMA

3.1. Geliştirilen Uygulamanın Mobil 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 veya telefondan bilgisayara aktarılır (Şekil .6) kullanılır.

Şekil 6. Geliştirilen uygulamanın PC veya telefona aktarılması

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

Şekil 7. Mobil telefon emülatörü

Uygulamada Şekil 7'de verilen mobil 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 8'de verilmektedir.

Şekil 8. Bluetooth cihaz arama sorgulamasında bulunan cihaz

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

Şekil 9. Gönderilecek verinin ve anahtar şifresisinin girilmesi

Şekil 9'da 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 10'da ise anahtar değerinin girilerek orjinal kelimenin elde edilmesi görülmektedir.

Şekil 10. Şifreli verinin alınması ve aynı anahtar değerinin girilerek verinin deşifrelenmesi

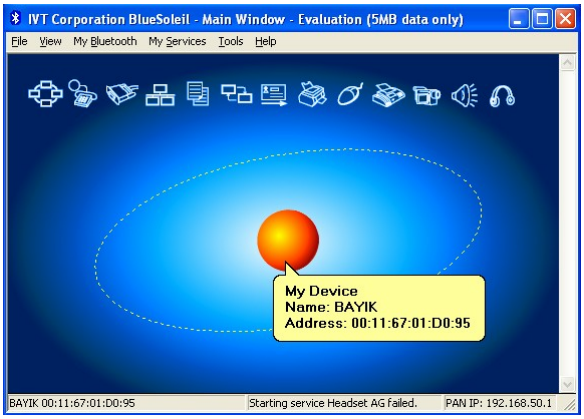
İki mobil telefon arasında yapılan bu uygulama, iki Bluetooth API destekli mobil telefon arasında yapıldığında aynı görüntüler meydana gelir. Borland JBuilder yazılım ortamında kullanılan algoritmanın simetrik olması şifrelemenin daha hızlı olmasına meydan vermektedir.

3.2. İki Bilgisayar (PC) Arasında Bluetooth Üzerinden Güvenli Veri İletimi

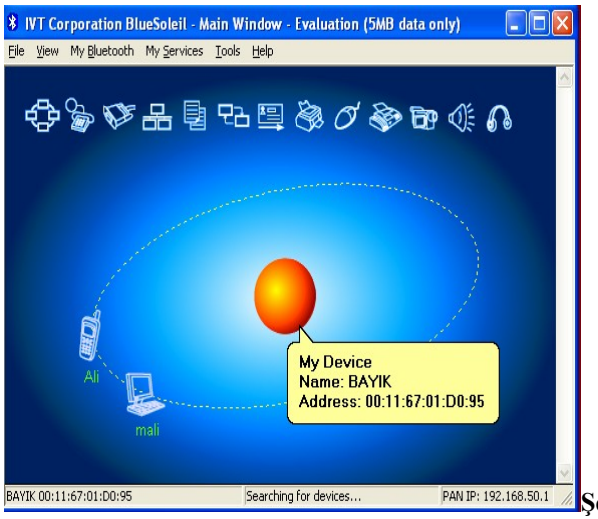
İki bilgisayar arasında bluetooth üzerinden güvenli veri iletimi uygulamasında kullanılan PC'lerde bluetooth özelliği olmadığından, PC'lere bluetooth özelliği kazandırmak için iki adet bluetooth

USB aparatı kullanılmıştır. Kullanılan aparatların algılama mesafesi 20 metre olup, bütün bluetooth cihazlarını desteklemektedir.

Şekil 11'de Bluesoleil yazılımın display görüntüsü görülmektedir. Görüntü orta kısmında bulunan dairesel şekil mouse'la tıklandığında cihaz keşif araması başlatılmış olur.



Şekil 11. Bluesoleil Display görüntüsü

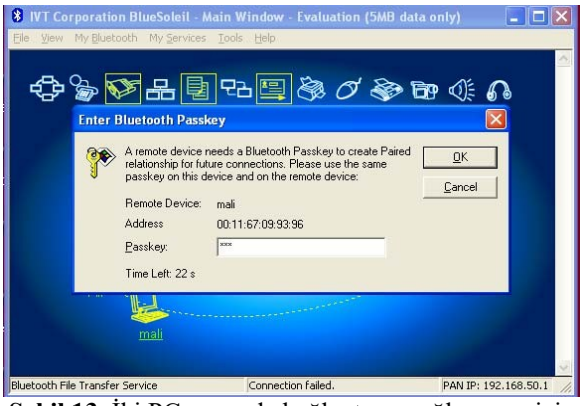


Şekil 12. Cihaz keşif tarama sonucu

Şekil 12'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 ınformation 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.

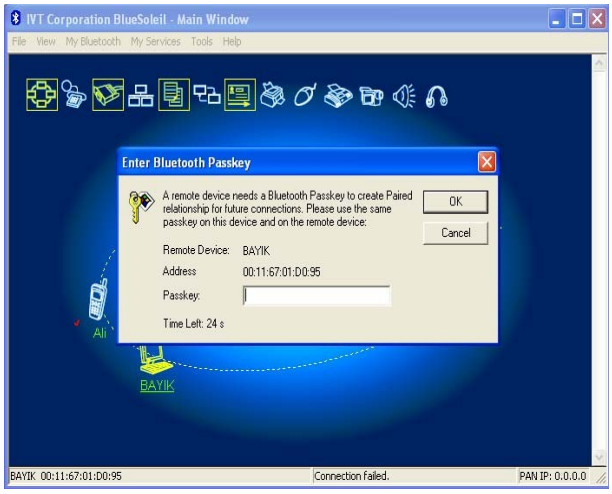
Yapılan uygulamada Bluetooth file transfer service kullanılarak şifreli veri iletimi sağlanmıştır.



Şekil 13. İki PC arasında bağlantının sağlanması için giriş anahtar değerlerinin girilmesi

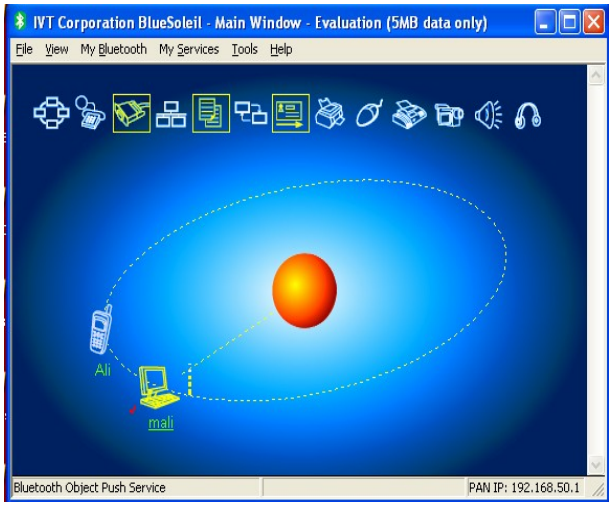
Veri iletiminin sağlanabilmesi için her iki PC'den girilen giriş anahtar değerlerininaynı olması gerekmektedir. Aksi takdirde iletim sağlanmaz, aynı değerlerin girilmesi sonucu yapılan bağlantıda, dosya transferi yapılacak seviyeye gelmektedir. Bluesoleil software'in kurulması sonucunda Bluetooth adında 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 14'de iki bilgisayar arasında bluetooth bağlantısının sağlanabilmesi için anahtar değeri talebi görülmektedir.



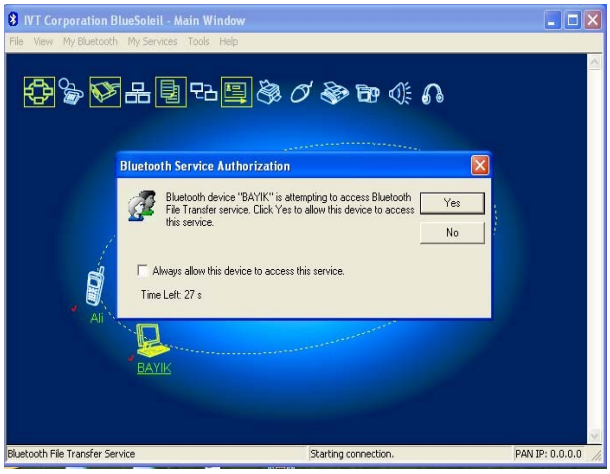
Şekil 14. Anahtar değerinin diğer bilgisayarda girilmesi

Şekil 15'te anahtar değerlerinin girilmesi sonucu bağlantının kurulumu görülmektedir.



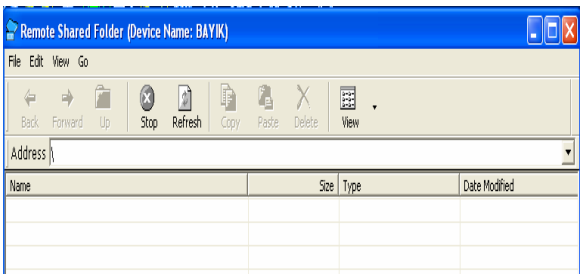
Şekil 15. Aynı anahtar değerlerinin girilmesi sonucu bağlantının yapılması

Şekil 16'da dosya veri transferinin kabul edilme onay penceresi görülmektedir.



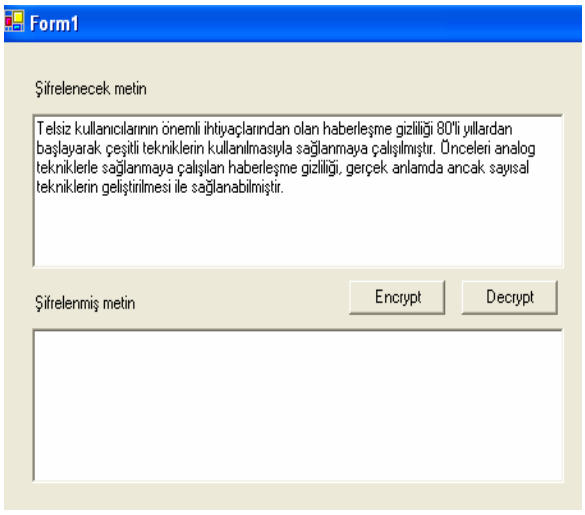
Şekil 16. Dosya transferinin kabul etmesi

Şekil 17'de dosya transferi kabul edilmesi sonucu klasörün açılmış durumu görülmektedir.

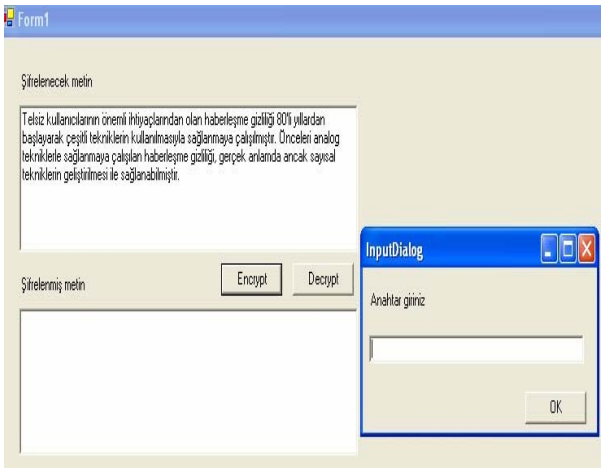


Şekil 17. Veri paylaşımını sağlayacak "Remote Shared Folder "in açılması

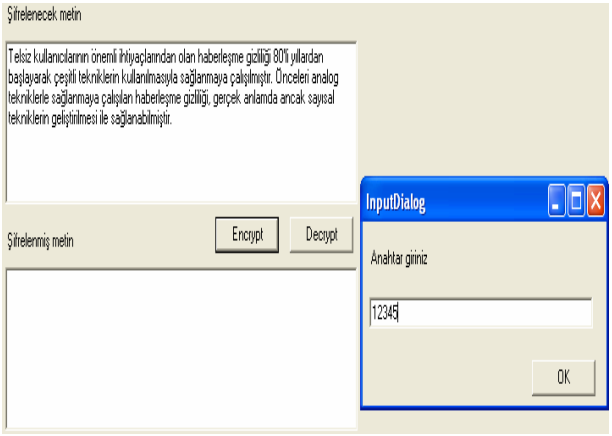
Remote Shared Folder'in açılması işleminden sonra iletilecek verinin şifrelenmesi aşamasına geçilir. Verinin şifrelemesinde Rijndael (AES) simetrik algoritması kullanılmıştır. Şifreleme yazılımın ara yüzünde iki kısım bulunmaktadır. Şifrelenecek metin birinci kısma yazıldıktan veya kopyalandıktan sonra Encrypt butonuna tıklandığında giriş anahtar değeri istenir, giriş anahtar değerinin girilmesiyle metin şifreli hale getirilir (Şekil. 21), şifrelenen metin kopyalanarak oluşturulan word belgesinin içine atılarak "Gönderilecek şifreli metin adı" verilir, şifrelenmiş word belgesi "Remote Shared Folder" içerisine aktarıldığında şifreli metin diğer alıcı cihaza bluetooth üzerinden aktarılmış olur. Bilgisayar tarafından alınan şifreli veri, shared klasörü altında kendine yer bulur, buradan tekrar alınacak şifreli doküman, Bayık adlı PC'de bulunan şifreleme yazılımının ara yüzü "şifrelenmiş metin" kısmına aktarılır (Şekil 23), bu kısımda "decrypt" butonuna tıklandığın da şifrelemeyi sağlayan aynı zamanda deşifre işlemini de sağlayan şifreleme anahtarı istenir (Şekil 24), bu değer tekrar girildiğinde (Şekil 25), karşı cihazdan bluetooth üzerinden alınan şifreli metin çözülmüş hale gelir(decrypt).



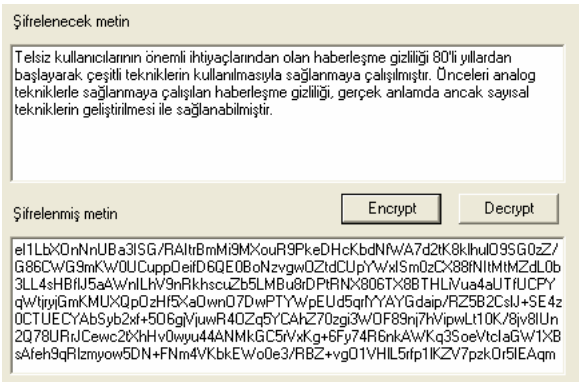
Şekil 18. Şifrelenecek metinin girilmesi



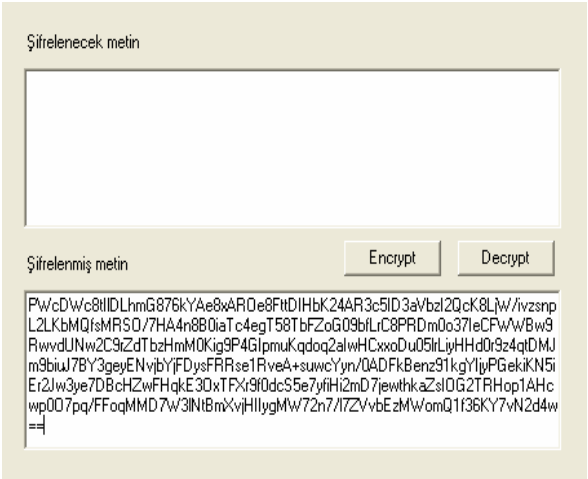
Şekil 19. Şifreleme (encrypt) anahtarının belirlenmesi



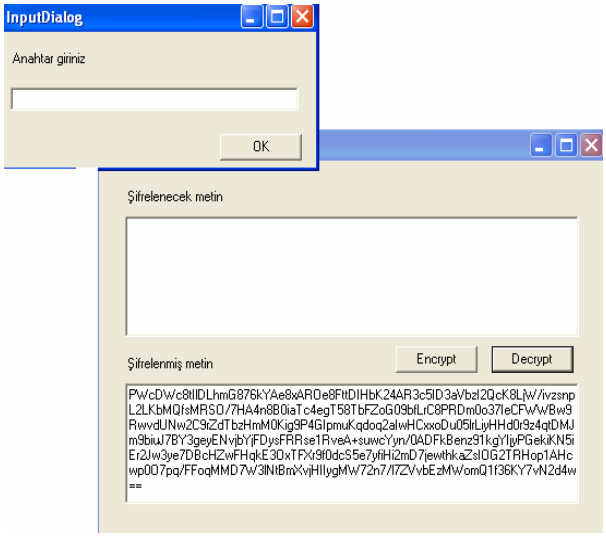
Şekil 20. Şifreleme (encrypt) anahtarının girilmesi



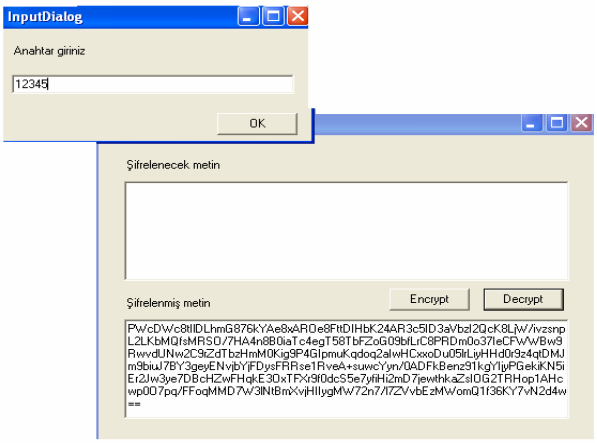
Şekil 21. Girilen metnin şifrelenmesi işlemi



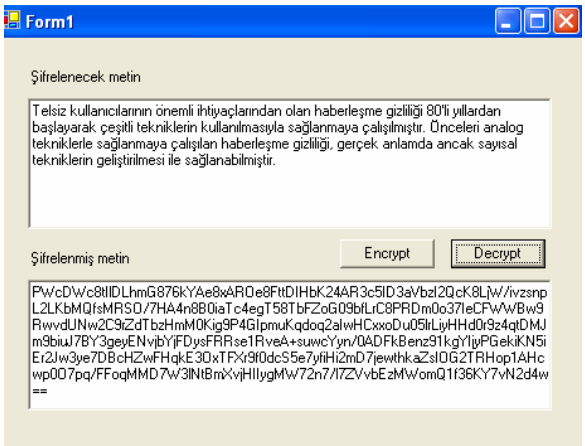
Şekil 22. Alınan şifreli metnin Şifreleme/Deşifreleme ara yüzüne aktarılması



Şekil 23. Şifreli metnin çözülmesi (decrypt) için anahtar değerinin istenmesi



Şekil 24. Şifre çözme (decrypt) işlemi için anahtar değerinin girilmesi



Şekil 25. Alınan şifreli metnin tekrar orijinal haline gelmesi (decrypt)

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.

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 mobil telefonar arası ve bilgisayarlar arası 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]. Pieterse H., Olivier M.S., 2014, Bluetooth Command and Control channel, Computers&Security, 45(2014), pp. 75-83

[2]. Sriskanthan N., Tan F., Karande A., 2002, Bluetooth based home automation system, Microprocessors and Microsystems, 26(2002), pp. 281-289.

[3]. Kaouthar S., Afifi H.,(2006), A new solution for micro-mobility management in next generation networks, Computers and Electrical Engineering, 32(2006), pp. 22-36.

[4]. Özçelik, M.A., (2006), " Bluetooth üzerinden güvenli veri iletimi" Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

[5]. Menezes, J.A., Vanstone V.O., Oorschot P.C.,(1996), Handbook of Applied Cryptography, CRC Press, ISBN:0-8493-8523-7.