Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 23, No 3, 531-538, 2008

J. Fac. Eng. Arch. Gazi Univ.
Vol 23, No 3, 531-538, 2008

KABLOSUZ TAŞINABİLİR UZAKTAN SAĞLIK İZLEME SİSTEMLERİNDE SAYISAL İMZA KULLANIMI

Veysel ASLANTAŞ, Rifat KURBAN ve Tuba ÇAĞLIKANTAR*
Bilgisayar Müh. Bölümü, Mühendislik Fakültesi, Erciyes Üniversitesi, 38039, Kayseri, aslantas@erciyes.edu.tr, rkurban@erciyes.edu.tr
* Jeodezi ve Fotogrametri Müh. Bölümü, Mühendislik Fakültesi, Erciyes Üniversitesi, 38039, Kayseri, tubac@erciyes.edu.tr

(Geliş/Received: 06.02.2007 ; Kabul/Accepted: 29.04.2008)

ÖZET

Tıbbi verilerin uzun dönemli veya gerçek-zamanlı uzaktan takip edilmesi ve acil durumlarda ilgili kurumların haberdar edilmesi oldukça önemlidir. Özellikle yaşlanan toplumlar için alınacak önlemler birçok sağlık problemini azaltacaktır. Bu çalışmada, üzerinde üç-elektrotlu bir elektrokardiyogram (EKG) ve ısı algılayıcısı bulunan bir taşınabilir sistem ile tıbbi verilerin kişi üzerinden alınması ve bu verilerin boylamsal artıklık denetimi (BAD) ve RSA tabanlı bir sayısal imza yöntemiyle imzalanması gerçekleştirilmiştir. Verilerin, IEEE 802.15.1 Bluetooth kablosuz iletişim teknolojisi ile bir kişisel sayısal asistan (KSA) cep bilgisayara iletilmesi, orada görüntülenmesi ve depolanması ve acil bir durum olduğunda kablosuz yerel alan ağı üzerinden veya GSM/GPRS teknolojisi ile merkezi sunucuya iletilmesi sağlanmıştır. Böylece kişinin günlük hayatını etkilemeden, sağlık durumunun hastane dışından izlenmesi mümkün hale gelmiştir. İzleme birimi ve cep bilgisayarı arasındaki Bluetooth iletiminde veriler sayısal olarak imzalanarak veri güvenliği ve bütünlüğü sağlanmıştır.

Anahtar Kelimeler: Uzaktan sağlık İzleme, sayısal imza.

USING DIGITAL SIGNATURES IN WIRELESS PORTABLE REMOTE HEALTH MONITORING SYSTEMS

ABSTRACT

Real-time monitoring of medical records and informing the units in emergency situations are very important. Especially in aging societies, taking precautions will reduce a lot of health problems. A portable monitoring unit that contain three-electrode electrocardiogram (ECG) and body temperature sensor is designed. The acquired data is digitally signed with longitudinal redundancy check and RSA algorithms and send to the personal digital assistant (PDA) pocket pc using Bluetooth wireless communication technology. PDA displays and stores the medical records and forwards them to the central server in emergency situations using wireless local area network or GSM/GPRS. Therefore, the developed system enables to monitor patients outside of hospitals without restricting the daily activities of them. The data transferred between portable monitoring unit and PDA is digitally signed. Thus, data security and integrity are achieved.

Keywords: Remote health monitoring, digital signature.

1. GİRİŞ (INTRODUCTION)

Dünya nüfusunun artmasıyla beraber, sağlık bakımı birçok ülkede büyük bir problem haline gelmiş ve yaşlanan toplumlarda kronik hastalıkların evde tedavileri ve bakımları zorunlu bir hal almıştır. [1]. Sağlık uzmanları ekonomik ve akıllı sistemler üreterek kalp rahatsızlıkları ve Alzheimer hastalığı gibi kronik rahatsızlık yaşayan insanların hayatlarını kolaylaştırmayı hedef edinmişlerdir. Koroner kalp rahatsızlıkları, dünya genelindeki ölümlerin sebepleri arasında ilk sırada gelmekte ve her yıl yaklaşık 7.2 milyon insan çeşitli kalp rahatsızlıklarından dolayı yaşamını yitirmektedir [2].

Kablosuz haberleşme ve gömülü hesaplama teknolojisindeki gelişmelerle birlikte uzaktan sağlık izleme ve teletıp konusu son yıllarda önemli

gelişmeler göstermiş ve böylece düşük maliyetli ve taşınabilir uzaktan sağlık izleme sistemlerinin gerçekleştirilmesi mümkün hale gelmiştir [3-5].

Tipik uzaktan sağlık izleme sistemleri, çeşitli biyopotansiyellerin ve vücut işaretlerinin kişi üzerine takılan kablosuz algılayıcılar ile elde edilmesi,bu verilerin yakın veya uzaktaki bir istasyona aktarılarak orada işlenmesi esasına dayanmaktadır. Elektrokardiyogram (EKG) [6-9], kandaki oksijen saturasyonu (darbe oksimetresi) ve fotoplestimograf (PPG) [6,10], kan basıncı [7,11], ivmelenme tabanlı x-y-z vücut hareketi ve elektromiyografi (EMG) [6] gibi tıbbi parametreler taşınabilir sistemlerce elde edilmiş ve özel tasarlanmış RF sistemleri [6,7], GSM/GPRS [8], Bluetooth [10] gibi tekniklerle uzak bilgisayarlara veya cep bilgisayarlarına [6,7] aktarılmıştır. Diğer taraftan, kablosuz algılayıcı ağları kullanan uzaktan sağlık izleme sistemleri de geliştirilmiştir [12,13].

Eğer basit kablosuz bir EKG algılayıcısı tasarlanır ve hasta bu cihazı kolayca kullanabilirse, taşınabilir bir bilgisayar ile entegre edilip kritik kardiyak durumları tespit edilebilir ve kalp ritim bozukluğu gibi rahatsızlıklar teşhis edilerek erken alarm sistemleri oluşturulabilir. Bu şekilde çalışan bir sistem, ticari olarak satılan cihazların aksine kolay kullanılabilir, ekonomik ve 24 saat sürekli olarak uzaktan EKG izlemeyi gerçekleştirilebilir. Bu çözüm hastanın hareket özgürlüğünü kısıtlamayacağı gibi gelişmiş alarm özellikleriyle de pek çok kardiyak rahatsızlığın önceden teşhis edilebilmesini mümkün kılacaktır [14,15].

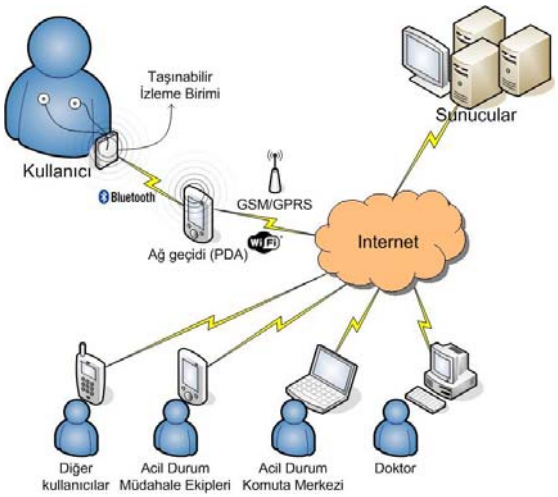
Diğer taraftan, kişilerin sağlık verilerinin iletilmesinde kişisel bilgilerin gizliliği büyük önem taşımaktadır [16]. Veri toplama merkezi, gezgin istemcilerden gelen verilerin gerçekten izlenen kişiden geldiğine emin olmalıdır. Üçüncü şahıslar tarafından gönderilebilecek sahte veriler sisteme kabul edilmemelidir. Ayrıca istemcilerden gelen verilerin bütünlüğü yani verilerin iletim esnasında bozulmadığının garanti edilmesi gerekmektedir.

Bu çalışmada, oldukça basit ve yeni bir sayısal imza yaklaşımı kullanan taşınabilir bir uzaktan sağlık izleme sistemi tasarımı sunulmuştur.

2. TAŞINABİLİR UZAKTAN SAĞLIK İZLEME SİSTEMİ (PORTABLE REMOTE HEALTH MONITORING SYSTEM)

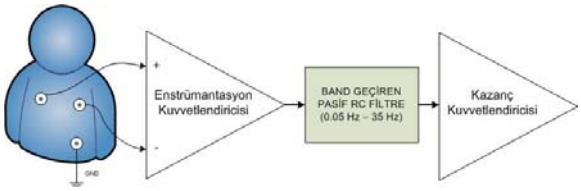
Kişinin EKG, vücut ısısı ve nabız gibi sağlık parametrelerinin Taşınabilir İzleme Birimi (TİB) adı verilen bir gömülü sistem vasıtasıyla elde edilerek, IEEE 802.15.1 Bluetooth kablosuz haberleşme protokolü ile ağ geçidi olarak ayarlanmış bir cep bilgisayarına aktarılması, bilgilerin cihaz üzerinde görüntülenmesi ve uzun dönemli olarak depolanması, acil durum söz konusu olduğunda bilgilerin merkezi sunucuya IEEE 802.11 kablosuz yerel alan ağı veya GSM/GPRS teknolojisi ile kablosuz olarak İnternet üzerinden gönderilmesi işlemi gerçekleştirilmiştir.

Bunun sonucunda, kişi önemli ölçüde hareket özgürlüğü elde ederken, kişinin günlük yaşamını aksatmadan tıbbi verilerin uzun dönemli olarak depolanması, bu verilerin merkezi bir sunucuya gerçek-zamanlı olarak aktarılması, olası acil durumlarda çeşitli alarmların tetiklenmesi ve ilgili kurumların harekete geçirilmesi sağlanmıştır. Önerilen yaklaşımın genel işleyişi Şekil 1'de verilmiştir. Sistemin donanım kısmı öncelikle bilgisayar ortamında Proteus ISIS simülasyon yazılımı ile tasarlanmış ve test edilmiş, daha sonra fiziksel olarak gerçekleştirilmiştir.



Şekil 1. Sistemin genel işleyiş şeması (Basic diagram of the proposed system)

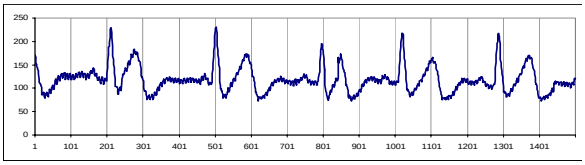
EKG işaretleri, insan vücudu üzerinden algılanan, kalbin bir elektriksel aktivitesi sonucu ortaya çıkan belli tipteki işaretlerdir [17]. 0.05 mV - 10 mV genliğinde olan bu işaretler bir enstrümantasyon kuvvetlendiricisi ile kuvvetlendirilirken, çevresel faktörlerden meydana gelen 50 Hz şebeke gürültüsü, biyolojik gürültü, devredeki elemanların kendisinden kaynaklanan gürültüler, pasif alçak geçiren ve yüksek geçiren RC süzgeçlerle giderilmeye çalışılmıştır. Bu çalışmada, üç-elektrotlu sağ-bacak sürücülü bir kuvvetlendirici tasarlanmıştır.



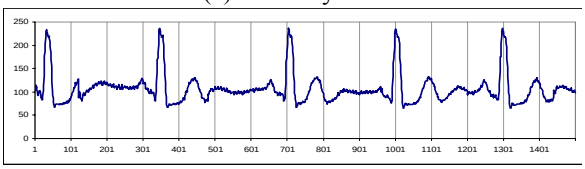
Şekil 2. EKG algılayıcısı blok diyagramı (Block diagram of ECG sensor)

Ag-Cl elektrotlardan alınan işaretler, enstrümantasyon kuvvetlendiricisi olarak kullanılan Analog Devices'a ait AD620 işlemsel yükselteci ile yükseltilmiş ve 0.05

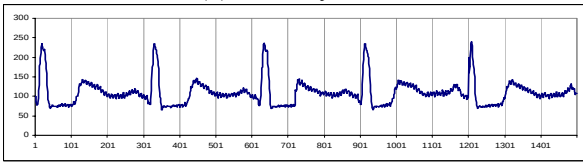
Hz – 35 Hz frekans aralığında bant geçiren pasif RC süzgecinden geçirilmiştir. Son adımda, üretilen işaret mikrodenetleyicinin analog örnekleme aralığına çekilmek için National Semiconductor'a ait LF353 işlemsel yükselteci ile tekrar yükseltilmiştir. Şekil 2'de algılayıcının blok diyagramı, Şekil 3'de ise tasarlanan algılayıcıdan edilen EKG grafikleri verilmiştir.



(a) Derivasyon I



(b) Derivasyon II



(c) Derivasyon III

Şekil 3. Tasarlanan devreden elde edilen EKG grafikleri. (ECG graphics acquired from designed circuit)

EKG verilerini örneklemek, analiz etmek ve cep bilgisayarına iletmek için Taşınabilir izleme birimi (TİB) adı verilen bir gömülü sistem geliştirilmiştir. TİB'nin üzerinde çalışan yazılımın kod çatısı Tablo 1'de verilmiştir. TİB vasıtasıyla, EKG kuvvetlendiricisinin çıkışındaki analog işaret, 512 Hz ile 8-bit çözünürlükte örneklenmektedir. Ayrıca, elektrik şebekelerinden kaynaklanan 50 Hz girişim gürültülerini tamamen bastırmak için 3. dereceden bir 50 Hz bant-durduran sayısal IIR Butterworth süzgeç uygulanmıştır.

Tablo 1. TİB üzerinde çalışan yazılımın kod çatısı (Software framework of the Portable Monitoring Unit)

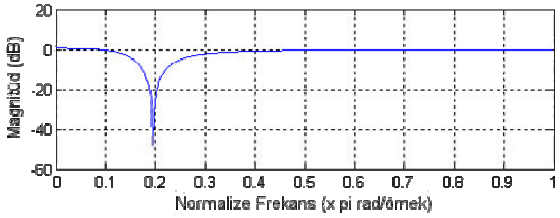
```
#include <PIC16F877.h>
#int_rtcc  // RTCC interrupt service routine
clock_isr(){//2.048 ms'de bir tetiklenir(500 Hz)
   ekg_ornekle();
   IIR_suzgec();
   ekg_nabiz_bul();
   isi_oku();  //6 sn'de bir tetiklenir
   BAD_hesapla();
   sayisal_imza_hazirla();
   paketle_ve_gonder();
}
#int_rda  //USART  interrupt  service  routine
usart_isr(){
   paket_mod_degisimi_yap(); //mod=0 veya mod=1
}
main(){
  set_timer0();
  set_adc();
  enable_interrupts(INT_RTCC|INT_RDA);
  while (true){
  //NOP
  }
}
```

IIR süzgeçlerin genel ifadesi denklem (1)'de verilmiştir. Tasarlanan IIR süzgecin katsayıları kayar noktalı yani gerçek sayılardır. Mikrodenetleyicinin kısıtlı bir hafızaya sahip olması ve de işlem yeteneği göz önünde bulundurulursa katsayıların gerçek sayılar olarak kullanılması çok zor ve maliyetli olacaktır. Bu yüzden üretilen süzgeç katsayıları bir sabit ile çarpılıp yuvarlanarak tam sayı haline getirilmiştir. Kullanılan süzgeç katsayıları Tablo 2'de, tasarlanan süzgecin frekans cevabı ise Şekil 4'de verilmiştir.

$$H(z) = \frac{B(z)}{A(z)} = \frac{b(1) + b(2)z^{-1} + ... + b(n+1)z^{-n}}{1 + a(1)z^{-1} + ... + a(n+1)z^{-n}} \quad (1)$$

Tablo 2. Tam sayılara çevrilmiş süzgeç katsayıları (Filter coefficents converted to integer values)

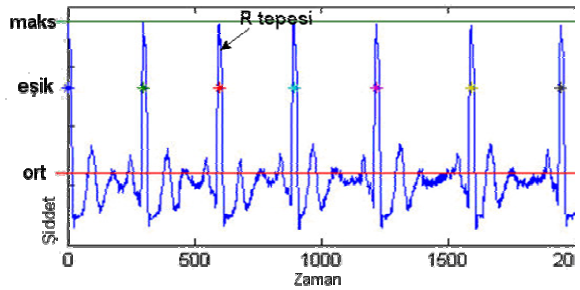
B(1) = 133	B(2) = -219	B(3) = 133
A(1) = 150	A(2) = -219	A(3) = 117



Şekil 4. Tasarlanan IIR süzgecin frekans tepkisi (Frequency response of the designed IIR filter)

Bu işlemlerden sonraki adım, EKG verilerinin analizi ederek kişinin nabız bilgisini hesaplamaktır. Nabız bulma işleminde, EKG verisindeki R tepeleri arasındaki uzaklık bulunmakta ve enterpolasyon ile bir dakika içerisindeki frekansı hesaplanmaktadır. Nabız bulma algoritması 6 sn'lik veri üzerinde çalışmaktadır. Algoritma, bu verinin ilk 1 saniyesini öğrenmek için diğer 5 sn'lik kısmını ise R tepelerini bulmak için kullanmaktadır. Her bir tepe arasındaki uzaklığı hesaba katarak, yaklaşık nabız oranlarını hesaplamakta ve elde ettiği değerlerin ortalamasını alıp, nabız değeri olarak cep bilgisayarına göndermektedir. Nabız bulma algoritmasının akışı şu şekildedir:

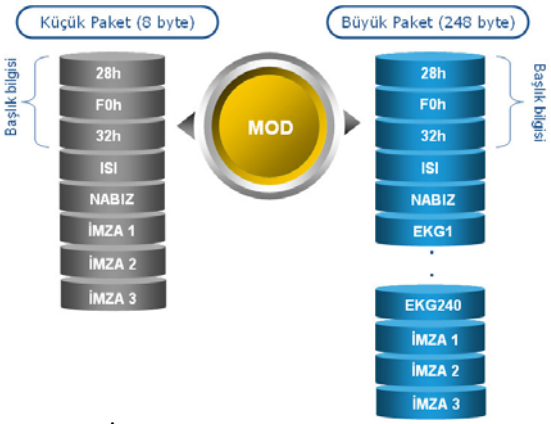
- *1 sn'lik EKG verisinin ortalama değerini bul (ort)*
- *1 sn'lik EKG verisinin maksimum değerini bul (maks)*
- *Eşik seviyesini belirle, Esik=(ort+maks)/2*
- *5 sn'lik kısım için eşik seviyesini geçen tepelerin yerlerini bul*
- *Tepeler arası mesafelerden nabızı hesapla*
- *Eğer nabız 40 -130 arasında değilse o değeri yoksay*
- *Elde ettiğin nabız değerlerinin ortalamasını al*
- *Bu işlemleri 6 sn'de bir tekrarla*



Şekil 5. Nabız Bulma Algoritması (Heart rate detection algorithm)

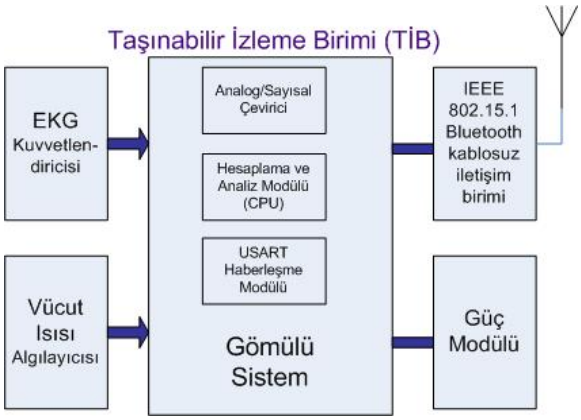
Şekil 5'de algoritmanın EKG verileri üzerinde bulduğu R tepeleri ve adaptif eşik seviyesi * karakterleri ile gösterilmiştir.

Diğer bir yandan TİB, Maxim-Dallas'a ait DS1621 sayısal ısı algılayıcısından vücut ısısı bilgisini I^2C protokolü üzerinden okumaktadır. Elde ettiği bu verileri (EKG, nabız ve ısı) Şekil 6'de belirtilen biçimde paketlemektedir. Sistemde iki farklı veri paketi bulunmaktadır. Küçük paket olarak adlandırılan paket toplam 8 byte uzunlukta olup, bunun ilk 3 byte'ı başlık bilgisini içermekte, sonraki 1 byte'lık kısmı ısı, 1 bytelık kısmı da hesaplanan nabız bilgisinden oluşmaktadır. Verinin kalan son 3 byte'ında da imza bilgisi bulunmaktadır. Büyük paket olarak adlandırılan diğer paketin ilk 5 byte'ı küçük paketle aynı olup devamında 240 byte EKG işareti bulunmaktadır. Yine verinin sonunda 3 byte imza bilgisi bulunmaktadır. Önerilen sayısal imza yaklaşımı bir sonraki bölümde anlatılmıştır. Kullanıcı hangi paketi istediğini TİB'e bildirebilmektedir.

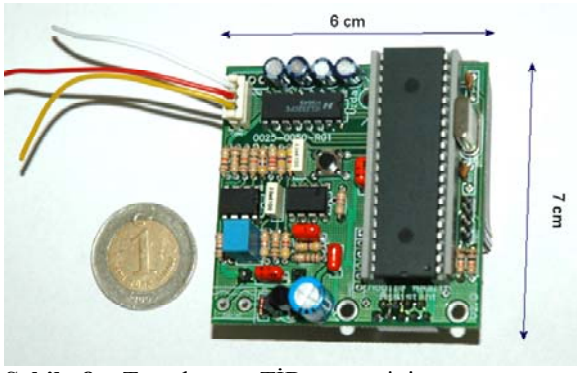


Şekil 6. TİB veri paketleri (PMU data packet frames)

Bu veriler, Bluetooth modülü sayesinde cep bilgisayarına gönderilmekte ve orada depolanmaktadır. Mikrodenetleyici tabanlı tasarlanan bu sistemde Microchip'e ait PIC16F877 entegresi kullanılmıştır. Tasarlanan TİB'in blok şeması Şekil 7'de, oluşturulan prototipi ise Şekil 8'de verilmiştir. Bluetooth kablosuz haberleşme için Free2Move firmasına ait F2M01C1 modelli seri port konektörlü modül kullanılmıştır. Bu modül TİB ile seri olarak haberleşmekte ve aldığı verileri cep bilgisayarının Bluetooth modülü ile yine seri olarak iletmektedir.



Şekil 7. Taşınabilir izleme birimi blok şeması (Portable Monitoring Unit block diagram)



Şekil 8. Tasarlanan TİB prototipi (Designed PMU prototype)

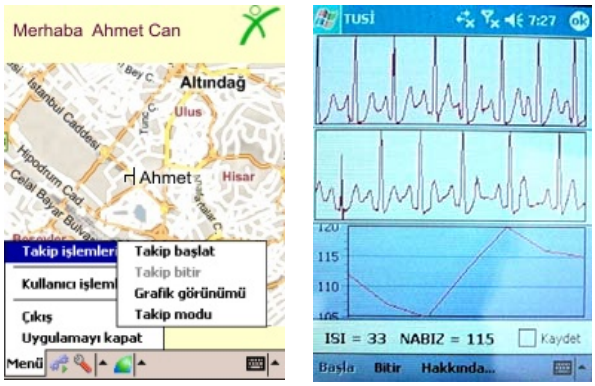
Sistemde HP firmasına ait iPAQ h6300 model cep bilgisayarı kullanılmıştır. Bu cihazın üzerinde; dâhili kablosuz yerel alan ağı kartı ve GSM/GPRS telefon entegresi bulunmaktadır. Üzerinde pek çok farklı teknolojiyi barındırıyor olmasından dolayı, bu cihaz tercih edilmiştir.

Sistemde Web servisleri, Mobil kullanıcı yazılımı, Acil durum müdahale operatörü yazılımı, Acil durum ambulans ekibi yazılımı ve Web uygulaması olmak üzere 4 farklı yazılım bulunmaktadır. Ayrıca veritabanı yönetim sistemi de saklı yordamlar ve tetikleyiciler içermektedir. Tüm yazılımların birbirleri ve veritabanı ile haberleşmeleri de XML Web servisleri vasıtasıyla sağlanmaktadır. Bütün yazılım mimarisi Microsoft Visual Studio 2005 ortamında Windows Uygulamaları, ASP.NET Web Uygulamaları, XML Web Servisleri, Cep Bilgisayarı Uygulamaları, ASP.NET Atlas Sunucu Kütüphaneleri ve Akıllı İstemci gibi .NET teknolojileri kullanılarak gerçekleştirilmiştir. Yazılım mimarisinin kullandığı veritabanı Microsoft SQL Server 2005'tir.

Web servisleri, sistemi meydana getiren yazılımların, endüstri standardı olmuş haberleşme protokolleri üzerinde iletişim kurmasını sağlar. Web servislerini HTTP üzerinden hizmet vermesi de kullanılabilirliği

en üst seviyeye çıkarmakta yardımcı olur. Güvenlik, yetkilendirme, kimliklendirme gibi işlemlerin tek bir merkez üzerinden yürütülmesi, takip sisteminin güvenliğinin sağlanmasında önemli bir rol oynar.

Mobil kullanıcı yazılımı, takip edilen kullanıcının taşınabilir cihazında koşan bir uygulamadır. Sistem için çok büyük önem arz etmektedir. Çünkü sistemin acil durum senaryolarını başlatan tüm analizler bu uygulamada meydana getirilir. TİB, kullanıcıdan elde ettiği sağlık verilerini Bluetooth seri port profilini (SPP) kullanarak belli periyotlarda cep bilgisayarına iletir. Önerilen sayısal imza yaklaşımı ile üçüncü şahısların verilere müdahale etmesi olasılığı ortadan kaldırılmış olur. Mobil kullanıcı yazılımındaki analiz motoru verilerin tanımlanan limitleri aşıp aşmadığına bakarak verilerin kritiklik derecesini belirler. Kritiklik derecesine göre, ya kullanıcıya bir uyarı mesajı gönderilir ya da bir alarm tetiklenip ilgili tüm acil sağlık istasyonlarına ve doktora bilgi verilir. Ayrıca cep bilgisayarı yazılımı yine Bluetooth teknolojisi ile taşınabilir bir GPS alıcısıyla haberleşerek kişinin konum bilgisini elde eder ve Microsoft Mappoint servislerini kullanarak bu bilgiyi ekranda gösterir. Mobil kullanıcı yazılımı ekran görüntüleri Şekil 9'da verilmiştir.



(a) Ana ekran ve hasta konumu (Main screen and patients location) (b) EKG, ısı ve nabız bilgileri (ECG, temperature and heart rate information)

Şekil 9. Mobil kullanıcı yazılımı (Mobile user software)

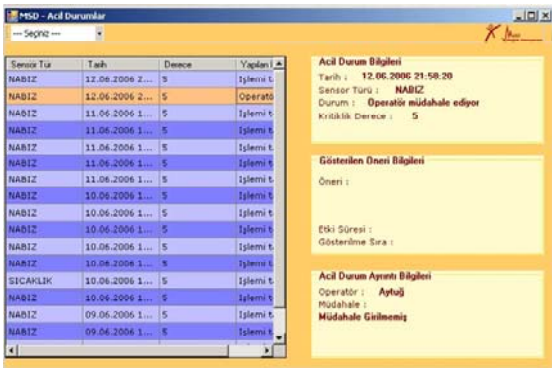
Alınan veriler cep bilgisayarı ekranında gösterilirken acil bir durum oluştuğu anda kablosuz yerel alan ağı vasıtasıyla veya kapsama alanında bir kablosuz erişim noktası yoksa cep bilgisayarı üzerindeki GSM/GPRS teknolojileri kullanılarak merkezi sunucuya Web servisleri aracılığıyla İnternet üzerinden gönderilir. Eğer kapsama alanında bir GSM şebekesi de yoksa veriler cep bilgisayarı üzerinde depolanır ve ilk bağlantı gerçekleştiği zaman veriler yine merkezi sunucuya gönderilir. Veri trafiğini azaltmak ve verimi artırmak için veriler gönderilmeden Gzip algoritması ile yüksek oranda sıkıştırılır.

Acil durum ambulans ekibi yazılımı, kritik durumdaki hastaya müdahale edecek ekibin kullandığı yazılımdır. Takip edilen kişilerin sağlık değerleri kritik bir durum oluşturduğunda bir alarm meydana gelir ve acil durum ambulans müdahale ekip yazılımına iletilir. Bu yazılım ekip ile hastanın konumunu cep bilgisayarı ekranında gösterir ve aradaki en kısa yolu işaretleyerek hastaya çok hızlı bir şekilde ulaşılmasını sağlar.

Acil durum müdahale operatör yazılımı ise 112 acil servis komuta merkezindeki operatörlerin kullandığı bir yazılımdır ve Win32 mimarisinde tasarlanmıştır. Bu program sayesinde operatör, takibi yapılan kişinin ölçülen parametrelerini (EKG, nabız ve ısı) gerçek-zamanlı olarak görür, sesli iletişime geçerek durumunu daha iyi analiz eder ve kişiyi yönlendirir. Böylece kişinin durumu daha da kötüleşmeden, etkin bir müdahale yapılarak sağlık kurumlarına iletilmesi sağlanır. Aynı zamanda operatör, acil durumları sayısal harita üzerinde ayrıntılı şekilde görebilir.

Şekil 10. Acil durum müdahale operatör yazılımı (Emergency situation intervention operator software interface)

Yazılım üzerinden, takip edilen kişinin harita üzerinde konumu, takip edilen kişinin bulunduğu yere en yakın sağlık kuruluşları, kişinin sisteme kayıtlı bilgileri, EKG, sıcaklık ve nabız verileri grafiksel olarak, acil yardım ekiplerinin durumu, takip edilen kişinin periyodik önerileri ve yapılmışlık durumları, takip edilen kişinin oluşan acil durumları gibi bilgilere ulaşılabilir. Acil durum müdahale operatör yazılımının ana ekranı Şekil 10'da, hastaya ait geçmiş acil durumlar ise Şekil 11'de verilmiştir.



Şekil 11. Hastaya ait önceki acil durumlar. (Past emergency situation records of the patient)

Diğer taraftan, Şekil 12'de görülen Web uygulaması ile kişinin genel sağlık bilgileri, acil durumları, acil durum önerileri, periyodik önerileri, algılayıcı parametreleri, takip işlemleri, mesaj gönderme ve rapor görüntüleme işlemleri web üzerinden gerçekleştirilebilmektedir. Güvenlik, kullanıcı tabanlı yetkilendirme işlemiyle sağlanmaktadır. Bu uygulamanın web tabanlı olmasının kazandırdığı en büyük avantaj, doktorun nerede olursa olsun kişiye ve kişinin bilgilerine kolayca erişebilmesidir. Bunun sonucunda, hasta ve doktor için mekândan tamamen bağımsız bir izleme sistemi gerçekleştirilmiş olmaktadır.

Şekil 12. Web uygulaması ve raporlama sayfası. (Web application and reporting page)

3. SAYISAL İMZALAMA (DIGITAL SIGNATURING)

Sayısal imza terimi genelde elektronik imza ile aynı anlamda kullanılmaktadır. Elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmaktadır. Sayısal imza, imzalanan veriye göre çeşitlilik gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Yani kişilerin, elle atılan imzada olduğu şekilde tek imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır [18].

Sayısal imza, mesaj bütünlüğü ve doğrulamayı garanti eder. Kriptografik imzalar, hata denetim veya kontrol toplamı (checksum) algoritmalarından oldukça farklıdır. Bu algoritmalar sadece veri bütünlüğü ile ilgilenirken doğrulama ile ilgili bir işlevleri yoktur. Popüler elektronik imza yöntemleri OpenPGP, DSA ve bazı S/MIME IETF standartlarıdır. Tüm mevcut kriptografik sayısal imza metotları, alıcının, gönderenin açık-anahtarını elinde bulundurmasıyla, mesajı gönderenin gerçekten ilgili gönderici olduğunu teyit etmesi ve diğer bir yandan mesaj bütünlüğünün de ölçülmesini sağlar. Böylece imzalanmış veri inkâr edilemez ve veride ya da açık anahtarda hile ile değişiklik yapılmadığı belirlenmiş olur. Bu tip imzaların iletiminde genelde güvenli bir kanala ihtiyaç duyulmaz.

Önerilen sayısal imza yaklaşımında gönderilecek verinin önce boylamsal artıklık denetimi (BAD) toplamı hesaplanmıştır. Mikrodenetleyicilerin çeşitli hafıza ve performans kısıtlamalarından dolayı MD5 ve SHA gibi karıştırma algoritmaları kullanılmamıştır. Kontrol toplamı algoritmaları arasından BAD tercih edilmiştir. Böylece, gerçek-zamanlı olarak yapılan sayısal imzalama işleminin hesaplamasındaki zaman karmaşıklığı kısalmıştır. Daha sonra elde edilen BAD verisi 24-bit RSA açık-anahtar şifreleme algoritması ile şifrelenmekte ve elde edilen sayısal imza veriye eklenerek cep bilgisayarına iletilmektedir. Cep bilgisayarı veriyi ve imzayı aldıktan sonra özel-anahtar ile imzadaki kodlanmış BAD bilgisini çözerek çıkarmaktadır. Aynı zamanda kendisi de veri üzerinde BAD hesaplayarak imzadan çıkartılan BAD ile karşılaştırmaktadır. Böylece veri bütünlüğü ve şifreleme sağlanmış olmaktadır. Önerilen sayısal imza algoritmasının genel yapısı aşağıdaki gibidir:

Sayısal imza = RSA(BAD(veri))

BAD kontrol toplamı algoritmasının temel adımları ise şu şekildedir:

BAD = 0 olarak ata
Döngü: mesajdaki tüm karakterler boyunca
Başla
Bir sonraki karakteri c olarak ata
BAD= BAD XOR c
Bitir

Burada XOR terimi, BAD ve c değişkenin eşleşen bit'lerinin bire-bir XOR işlemine tabi tutulması anlamına gelmektedir. Diğer bir ifade ile, karakter dizisindeki tüm elemanların ASCII değerleri toplandıktan sonra ikiye göre komplementi alınarak da BAD hesaplanabilir.

RSA algoritması kriptolojide açık-anahtar şifrelemede kullanılır. İmzalama için en uygun algoritmalardan birisidir. RSA halen e-ticaret uygulamalarında yeterli uzunlukta anahtarlar seçildiği takdirde güvenli olarak görülmekte ve kullanılmaktadır. RSA'da açık-anahtar ve özel-anahtar olmak üzere iki tip anahtar vardır. Kullanıcıya ait açık-anahtar herkeste bulunur ve mesajın kodlanmasında kullanılır. Ancak kodlanmış mesajlar sadece özel-anahtar ile çözülebilir. Diğer bir ifadeyle, herkes mesajı şifreleyebilir ancak özel-anahtara sahip olan kişi mesajı çözebilir. Açık ve özel anahtarlar aşağıdaki algoritma ile elde edilebilir:

1. p ve q olmak üzere iki tane büyük asal sayı seç, ancak $p \neq q$ olmak şartıyla.
2. $n = pq$ hesapla.
3. $\phi(n) = (p-1)(q-1)$ hesapla.

4. $\phi(n)$ ile aralarında asal olan ve 1'den büyük bir e sayısı seç.
5. $de \equiv 1(\mathrm{mod}\,\phi(n))$ olmak üzere d 'yi hesapla.

Bu durumda, açık-anahtar; *n*: modül ve *e*: açık üsden oluşmakta ve özel-anahtar ise *n*: modül ve *d*: özel üsten oluşmaktadır. Mesajlar kodlanırken $c = m^e \bmod n$ eşitliğinden yararlanılır. Burada *m* kodlanmak istenen mesajı, *c* ise mesajın kodlanmış halini göstermektedir. Kodlanmış mesajlar ise $m = c^d \bmod n$ eşitliği ile tekrar çözülebilir. RSA algoritmasının güvenilir olabilmesi için *e*, *n* ve *d* değerleri yeterince büyük seçilmelidir. Ancak sayılar büyüdükçe algoritmanın hesaplama yükü ve hafıza ihtiyacı artmaktadır. Mod işlemlerini daha az hafıza ile çözmek için aşağıdaki modüler üs alma algoritması kullanılmaktadır:

1. $c = 1$ ve $e' = 0$ olarak ata.
2. e' 'yi 1 artır.
3. $c \equiv mc(\mathrm{mod}\,n)$ olarak ata.
4. $e' < e$ ise 2. adıma git, değilse *c* değişkeni $c \equiv m^e(\mathrm{mod}\,n)$ işleminin sonucunu içermektedir.

BAD ve RSA algoritmaları birleştirilerek bir sayısal imza tekniği oluşturulmuştur. Taşınabilir izleme biriminin elde ettiği veriler açık-anahtar kullanılarak imzalanmakta ve cep bilgisayarına gönderilmektedir. Cep bilgisayarı üzerindeki yazılım gelen veriden elde ettiği BAD ile özel-anahtarını kullanarak imzadan çözdüğü BAD ile eşleştirmekte ve verinin güvenli ve tutarlı olup olmadığını kontrol etmektedir. Önerilen sayısal imza algoritmasının C dilindeki kodu Tablo 3'de verilmiştir.

Tablo 3. Sayısal imza algoritmasının C kodu (C codes of the proposed digital signature)

```
c=1;
ee=0;
bad=0;
for(i=0;i<veriuzunluk;i++){
   bad=(bad+veri[i]) % 256;
}

m=bad;
while (ee<e){
   ee=ee+1;
   c=(m * c) % n;
}
imza=c;
```

4. SONUÇ (CONCLUSION)

Bu çalışmada taşınabilir bir uzaktan sağlık izleme sistemi sunulmuş ve taşınabilir izleme birimi ile PDA arasındaki kablosuz Bluetooth haberleşmesi sırasında veri bütünlüğü ve yetkilendirilmenin sağlanması için BAD ve RSA tabanlı bir sayısal imza yaklaşımı önerilmiştir.

Önerilen sistem kardiyak arrest, kalp çarpıntısı (ventricular tachycardia) veya aritmi gibi rahatsızlıklar için hastane içinden veya dışından sürekli olay kaydedici olarak kullanılabilmektedir. Diğer bir yandan TİB ve cep bilgisayarının ayrık olması ve bunların kablosuz haberleşebilmeleri, cep bilgisayarının merkezi sunucu ile kablosuz haberleşebilmesi ile sistem dağıtık bir mimari oluşturmakta, kişinin yaşamını zorlaştırmadan hareket kabiliyetini artırmaktadır. Ayrıca Bluetooth, kablosuz yerel alan ağı ve GSM/GPRS gibi cep bilgisayarlarında standart olarak bulunan teknolojilerin kullanılmasıyla harici ek haberleşme donanımlarının tasarlanmasına gerek kalmamış ve dolayısıyla sistem boyutları da küçültülmüştür. Cep bilgisayarından merkezi sunucuya iletilen veriler sıkıştırılarak sistemin verimliliği artırılmış ve kullanım maliyetleri de düşürülmüştür. Kolay kullanılabilirliği, taşınabilirliği ve alarm özellikleri de göz önüne alındığında, sistem pek çok kardiyak rahatsızlığını teşhisi ve tedavisi için önemli bir rol oynamakta ve kişinin hayat kalitesinin yükseltilmesine de yardımcı olmaktadır. Diğer taraftan, TİB'in Bluetooth haberleşme yapabilme kabiliyeti sayesinde sistem sadece cep bilgisayarları ile değil, Bluetooth modülü olan dizüstü, masaüstü hatta cep telefonları ile de haberleşebilmekte, verileri bu cihazlar üzerinde gösterebilmekte ve bu cihazları ağ geçidi olarak kullanarak bilgileri internet üzerinden merkezi sunucuya aktarabilmektedir.

Sayısal imzalama algoritmasının oldukça basit olması ve fazla hafıza ihtiyacına ihtiyaç duymaması nedeniyle donanımsal olarak gerçekleştirilebilmesi mümkün olmuştur. Endüstri standardı olmuş mevcut sayısal imza algoritmalarını bu tür kısıtlı donanımlar üzerinde gerçekleştirmek pratikte pek de mümkün değildir. İmzanın kırılamaması için oldukça büyük asal sayılar seçilmesi gerekmektedir. Ancak sayıların yükselmesi ile birlikte algoritmanın hafıza ihtiyacı ve işlem zamanı artmaktadır. Bu çalışmada 24-bit RSA işlemleri başarıyla gerçekleştirilmiştir. Daha yüksek değerlerde mikrodenetleyicinin değişkenleri yeterli gelmemekte ve üstten taşma meydana gelmektedir. *e*'nin büyük bir değer olması durumunda ise işlem zamanı oldukça uzamakta, algoritmanın çalışma süresi *e*'nin değeri kadar katlanmaktadır.

Gerçekleştirilen prototiplerin güç tüketimi yaklaşık 80 mA ve boyutları 3cm x 6cm x 7cm olup bu değerler daha da küçültülebilir. Ayrıca daha kapsamlı bir sağlık izleme için EKG, nabız ve ısı bilgilerinin yanı sıra tansiyon, darbe oksimetresi ve PPG, x-y-z vücut hareketi gibi algılayıcılar da sisteme entegre edilebilir. Diğer bir yandan sistemden elde edilen veriler yapay zekâ teknikleri ile otomatik olarak yorumlanabilir ve detaylı analizler yapılabilir.

KAYNAKLAR (REFERENCES)

1. Ross P.E., "Managing Care Through the Air", **IEEE Spectrum**, 14-19, 2004.
2. World Health Organisation (WHO), **"The Atlas of Heart Disease and Stroke",** http://www.who.int/cardiovascular_diseases/resources/atlas/en/index.html, 2002.
3. Binkley P.F., "Predicting the potential of wearable technology", **IEEE Engineering in Medicine and Biology Magazine,** Cilt 22, No 3, 2003.
4. Jovanov E., Raskovic D., **Wireless Intelligent Sensors**, Springer, 2006.
5. Priddy B., Jovanov E., **Wireless LAN Technologies for Healthcare Applications**, Springer, 2006.
6. Lorincz K., Malan D.J., Fulford-Jones T.R.F., Nawoj A., Clavel A., Shnayder V., Mainland G., Welsh, M., Moulton S., "Sensor networks for emergency response: challenges and opportunities", **IEEE Pervasive Computing,** Cilt 3, No 4, 16 - 23, 2004.
7. Bolanos M., Nazeran H., Gonzalez I., Parra R., Martinez C., "A PDA-based electrocardiogram/ blood pressure telemonitor for telemedicine", **IEEE Enginnering in Medicine and Biology (EMBC),** San Francisco, 2004.
8. Fensli R., Gunnarson E., Hejlesen O., "A wireless ECG system for continuous event recording and communication to a clinical alarm station", **IEEE Enginnering in Medicine and Biology (EMBC),** San Francisco, 2004.
9. Fulford-Jones T. R. F., Wei G., Welsh M., "A Portable, Low-Power, Wireless Two-Lead EKG System", **IEEE Enginnering in Medicine and Biology (EMBC),** San Francisco, 2004.
10. Hung K., Zhang Y.T., Tai B., "Wearable medical devices for tele-home healthcare", **IEEE Enginnering in Medicine and Biology (EMBC),** San Francisco, 2004.
11. Lee R.G., Chen K.C., Hsiao C.C., "A mobile care system with alert mechanism", **IEEE Transactions on Information Technology in Biomedicine**, Cilt 11, No 5, 507-517, 2007.
12. Malan D., Fulford-Jones T., Welsh M., Moulton. S, "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", **International Workshop on Wearable and Implantable Body Sensor Networks**, 2004
13. Otto C., Milenkovic A., Sanders C., Jovanov E., "System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring," **Journal of Mobile Multimedia**, Cilt 1, No 4, 307-326, 2006.
14. Kurban R., **"Kablosuz Taşınabilir Uzaktan Sağlık İzleme Sistemi: Mobil Sağlık Danışmanı"**, Yüksek Lisans Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, 2006.
15. Aslantas V., Kurban R., Caglikantar T., "A Low-Cost Wireless Healthcare Monitoring System And Communication to a Clinical Alarm Station", **ELECO 2007, 5th International Conference on Electrical and Electronics Engineering**, Bursa, 2007.
16. Hu F., Jiang M., Wagner M., "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign", **IEEE Transactions on Information Technology in Biomedicine,** Cilt 11, 619-627, 2007.
17. Rodriguez J., Goni A., Illarramendi A., "Real-time classification of ECGs on a PDA", **IEEE Transactions on Information Technology in Biomedicine,** Cilt 9, No 1, sf. 23-34, 2005.
18. Sağıroğlu Ş., Alkan M., **Her Yönüyle Elektronik İmza e-İMZA**, Grafiker, 2005.