GU J Sci, Part C, 6(2): 250-258 (2018)

Gazi Üniversitesi

Fen Bilimleri Dergisi

PART C: TASARIM VE TEKNOLOJİ

dergipark.gov.tr/http-gujsc-gazi-edu-tr

Medikal İmplant Haberleşme Sistemleri için Bandgenişliği Verimli Örtüşmeli FSK Kodlamalı Güvenli Komut iletimi

Selman KULAÇ[1, *]

[1]*Düzce Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, 81620, Konuralp Yerleşkesi, DÜZCE*

Makale Bilgisi

Başvuru: 29/01/2017
Düzeltme: 28/03/2017
Kabul: 07/04/2017

Anahtar Kelimeler

Kablosuz İmplante Edilebilen Medikal Sistemler, Implant Telemetri Haberleşmesi, Fiziksel Katman Güvenliği, Güvenli Komut İletimi

Keywords

Wireless Implantable Medical Systems, Implant Telemetry Communications, Physical Layer Security, Secure Command Transmission

Öz

Günümüzde kablosuz iletişim çoğu sağlık sisteminde yer almaktadır. Implante edilebilen medikal sistemler de kablosuz iletişim yeteneğine sahiptirler. Fakat bu sistemlerde kablosuz iletişimin güvenli olması hem hasta hakları hem de hasta sağlığı açısından çok önemlidir. Bu nedenle kablosuz implante edilebilen medikal sistemlerinin iletimlerinin güvenli olması, aktif ve pasif saldırganlara karşı korunması gerekir. Bu çalışmada, özel bir örtüşmeli ve kodlamalı frekans kaydırmalı anahtarlama tekniği geliştirilmiş ve bu teknikle komut iletiminde karmaşıklığı düşük güvenlik sağlanmıştır. Önerilen yöntem karmaşıklığı düşük ve güvenlik yanında band genişliği verimliliği de sağladığından kablosuz implante edilebilen medikal sistemler için uygun durmaktadır.

Bandwidth Efficient Overlapped FSK Coded Secure Command Transmission for Medical Implant Communication Systems

Abstract

Nowadays, wireless communication systems are exploited in most health care systems. Implantable Medical Systems (IMS) also have wireless communication capability. However, it is very important that secure wireless communication should be provided in terms of both patient rights and patient health. Therefore, wireless transmission systems of IMS should also be robust against to eavesdroppers and adversaries. In this study, a specific overlapped and coded frequency shift keying (FSK) modulation technique is developed and security containing with low complexity is provided by this proposed technique. The developed method is suitable for wireless implantable medical systems since it provides low complexity and security as well as bandwidth efficiency.

1. GİRİŞ (INTRODUCTION)

Kablosuz iletişim insan hayatında son yıllarda daha da önem kazanmaktadır. Dolayısı ile kablosuz iletişimin yer aldığı farklı alanlar da türemiştir. Bunlardan biri de sağlık alanıdır. Sağlık alanında kablosuz implante edilebilen medikal cihaz (IMC) teknolojisi, kablosuzluk özelliği sayesinde daha da gelişmiş olarak karşımıza çıkmaktadır. Özellikle insan vücudunun içine yerleştirilmiş bir cihazla her an kablosuz olarak haberleşebiliyor olmak hasta takibi, cihaz durumu ve tedavi noktasında çok büyük faydalar sunmaktadır. Böylelikle, kablosuz implante edilebilen medikal cihazlar (IMC) gelecekte farklı hastalıkların tedavisinde de kullanılıyor olacaktır. Günümüzde halen kullanılan kablosuz implant cihazlarına örnek olarak; bazı hareket bozukluklarına karşı kullanılan derin beyin uyartıcılar (DBU), beyne ses sinyalleri sağlamak için iç kulağın hasarlı parçalarının (koklea) işini yapan koklear implantları, kalp pili olarak bilinen implante edilebilen kardiyoverter defibrilatörler (IKD /Pacemaker), gastrik uyartıcılar, insülin pompaları gösterilebilir. Örneğin DBU ele alınacak olursa; hekimin DBU sistemini kullanarak hastasının beyninin özel bir bölgesindeki nörokimyasal ve anatomik değişimleri

*İletişim yazarı, e-mail: selmankulac@duzce.edu.tr

DOI: 10.29109/http-gujsc-gazi-edu-tr.288622

gözlemleyebilmesi ve takip edebilmesi, uygun tedaviyi DBU'ya yükleyebilmesi mümkündür ve bu da tamamen kablosuz haberleşme ile gerçekleştirilmektedir. Burada özellikle belirtmek gerekir ki, DBU'nun uzaktan kontrolü ve hekim tarafından tedaviye uygun bir şekilde programlanarak uyartım sinyalleri üretmesi de düzgün bir telemetri ve komut iletimini gerektirir.

Kablosuz IMC'ler için bazı önemli gereksinimler veya talepler vardır. Bunlar biyolojik uyumlu olmaları, dirençli ve sağlam olmaları, düşük karmaşıklığa sahip olmaları, arıza yapma olasılıklarını düşürecek minimum sayıda parça içermeli, olabildiğince küçük boyutlara sahip olmaları, üstün ve hassas işlevselliğe sahip olmaları, çok uzun pil ve cihaz ömürlerine sahip olmaları, maksimum verimde çalışıyor olmaları, güncellenmeye ihtiyaç duymamaları, güvenlikli ve gizlilik hakkı veya mahremiyet duyarlı olmaları olarak sıralanabilir.

Güvenlik ve gizlilik hasta hakları olarak kabul edilmektedir. Dolayısı ile hastaya ait gizli ve hayati bilgiler, uygulanan tedavi, hastalık ve tedavi geçmişi gizli ve güvenli kalmalıdır. Bu nedenle Amerika Birleşik Devletlerindeki Gıda ve İlaç Yönetimi tarafından hazırlanan taslak rehber, piyasaya girdikten sonra tıbbi cihazlarda siber güvenlik açığı izleme, tanımlama ve bunlara yönelik tavsiyelerini anlatmaktadır [1]. Bu kapsamda değerlendirilirse, kablosuz IMC'ler için de güvenlik ve gizlilik önem arz etmektedir. Çünkü kablosuz IMC'ler için de hastaya, tedaviye, cihaz durumuna ait verilere ulaşmak olasıdır. Dahası, bu verilerde oynama yapmak, bu verileri yok etmek ve olağan veri iletişimini engellemek olasıdır. Hatta bu verilerle oynayarak implant cihazının hastaya öldürücü bir işlevde bulundurulması da mümkündür. Örneğin, geçmişte Amerika Birleşik Devletleri Başkan yardımcısı Dick Cheney'in kalp piline dışarıdan bir müdahale yapıldığı belirtilmektedir [2]. IMC'lerin kablosuz iletişimi esnasında hastaya, tedaviye, cihaz durumuna ilişkin kötü amaçlı dinlemeler olabilir ki, bu pasif saldırganlık olarak değerlendirilir. Bu dinlemeler çokça yapılarak, haberleşme protokolü çözüldükten sonra, cihazın aldatılarak cihaza anormal işlevler yaptırılması ise aktif saldırganlık olarak değerlendirilir. Burada aktif saldırganlık daha çabuk ve daha büyük kötü sonuçlar doğurabilir ki, bu da cihazın uzaktan kontrolünü sağlayabilmekle mümkündür.

Kablosuz iletişimde fiziksel katman güvenliği kriptografik yöntemlere uzak kalarak güvenli iletişim gerçekleştirmeyi hedeflemektedir [3]. Kablosuz IMC'ler için kriptografik işlemler, yukarıda bahsedilen taleplerin aksine karmaşıklığı artırma, parça sayısını artırma, boyutu artırma, güç tüketimini artırma vb. dezavantajlara sahiptir. Dolayısı ile implante edilmiş cihazların haberleşmesinde güvenliği sağlamak kriptografik yöntemlerin kullanımından ziyade, bu da fiziksel katman güvenliği ile sağlanabilir.

Kablosuz IMC'ler için fiziksel katman güvenliği ile ilişkili literatürde bazı çalışmalar mevcuttur. İlk olarak haberleşme pelerini (Communication Cloaker) olarak adlandırılan bir harici cihaz önerilmiştir [4]. Pelerin takıldığında veya giyildiğinde röle veya aktarıcı gibi davranır. Bu aktarma işlemi bir miktar kriptografik işlem içerir. Başka bir giyilebilir cihaz da IMDGuard veya Guardian olarak isimlendirilmiş olan ve güvenli iletim sağlayan harici bir cihazdır [5]. IMDGuard veya Guardian yöntemi, hastanın elektrokardiyogram işaretlerine dayalı kriptografik anahtar yönetim süreci odaklıdır. Bu iki önerilen yöntemde de, halihazırda var olan IMC'ler kriptografik donanımların yerleştirilmesi nedeni ile modifikasyona ihtiyaç duymakta ve istenmeyen karmaşıklık artışına neden olmaktadır. Anormallik algılama yöntemini barındıran ve MedMon olarak adlandırılan başka bir harici cihaz daha önerilmiştir [6]. MedMon aktarıcı veya röle olarak hareket etmez, aksine sadece iletilen sinyallerin fiziksel karakteristiklerine odaklanır. Anormal bir iletim durumu olursa, hastayı uyarır veya güçlü karıştırıcı sinyal yayarak anormal iletimi bastırır. MedMon aktif saldırganlara karşı iyi koruma sağlarken pasif dinleyicilere karşı herhangi bir tedbir sunmaz.

Önerilen başka bir harici cihaz da, Shield olarak adlandırılan ve IKD'leri aktif saldırganla karşı korumak üzere geliştirilmiş bir cihazdır [7]. Shield tüm IKD'den gelen tüm cevap sinyallerini ve aktif saldırgandan gelen tüm sinyalleri yüksek güçte sinyal yayarak bastırma (jamming) yaparken, kendi sorgu (uzaktan kontrol veya telemetri data) sinyallerini veya komutlarını (tedavi reçete verisi vs.) açık, güvensiz ve beraberinde bastırma sinyali olmadan iletir. Dolayısı ile sorgu ve komutlar herkese açık ve güvensiz bir şekilde kablosuz ortamda yayılırken, pasif dinleyiciler IKD'ye iletilen tüm bu komut verilerini rahatlıkla sürekli kaydedebilirler. Böylelikle pasif dinleyiciler bu sürekli açık verinin kaydı sayesinde yeni akıllı teknikler geliştirebilirler. Örneğin pasif dinleyiciler hekim tarafından uygulanan tedaviyi protokolü çözerek anlayabilirler, hastanın durumu ve IKD'nin durumu (pil ömrü, sağlıklı çalışıp çalışmadığı vs.)

hakkında çok güçlü tahminlerde bulunabilirler. Saldırganlar gönderilen komut yapısını tamamen anlayıp çözerlerse, IMC cihaz ayarlarını, IMC tedavi (elektriksel uyartım) parametrelerini değiştirme, cihazı devre dışı bırakma veya kapatma, tedaviyi sonlandırma, elektriksel şok uygulama komutu gönderme gibi yetenekleri elde edebilirler [7,8]. Literatürde, bazı araştırmacılar da fiziksel katman güvenlik açığının farkına varmışlar ve bu açık bazı makalelerde dile getirilmiştir [6,9].

Bu çalışmadaki amaç, kablosuz iletiminde güvenliğin çok önemli olduğu sorgu ve veya komut (uzaktan kontrol) sinyallerinin korunmasıdır. Bu komut sinyallerinin korunması hekim reçetesinin güvenli iletimi ve hasta mahremiyeti hakkına riayeti sağlayarak pasif dinleyicilere karşı önlem sunar. Pasif dinleyici hekim tarafından uygulanan tedaviyi ve IMC'nin yönetimi ve kontrolüne dair iletimleri kod çözemeyerek anlayamaz.

Bu çalışmada, aşağıdaki bazı önemli hususlar göz önünde bulundurulmuştur.

- Mevcut IMC'ler çok düşük hassasiyete sahip olabilir, fakat pasif dinleyiciler daha üstün hassasiyete sahip kabul edilmelidir.
- Sağlanacak güvenlik çözümünde gezgin pasif dinleyicilerin yerlerinin bilinmesine gerek olmamalıdır.
- Kriptografik yapı içeren güçlü sinyal işlemci veya karmaşıklık sadece programlayıcı tarafına yerleştirilebilir.

Amerika Birleşik Devletlerinde federal haberleşme komisyonu (FHK), medikal implant haberleşme servis (MİHS) bandı adında 3 MHz'lik bir frekans bandı tahsisi yapmıştır [10]. 402-405 MHz arası frekans bandını içeren bu bandda, IMC'ler ile kablosuz bağlantı kurabildikleri dış kontrol cihazlarının (hekim programlayıcı cihazı vs.) 25 μW'lık (16 dBm EIRP seviyesinde) iletim gücünü aşmayacak şekilde iletim yapmalarına izin verilmiştir. Bu bandaki iletimlerde, çoğunlukla tercih edilen modülasyon tipi frekans kaydırmalı anahtarlama (FSK) olmuştur [11]. Çünkü FSK modülasyonu IMC haberleşmesinde aşağıda verilen bazı avantajları sunar [12, 13].

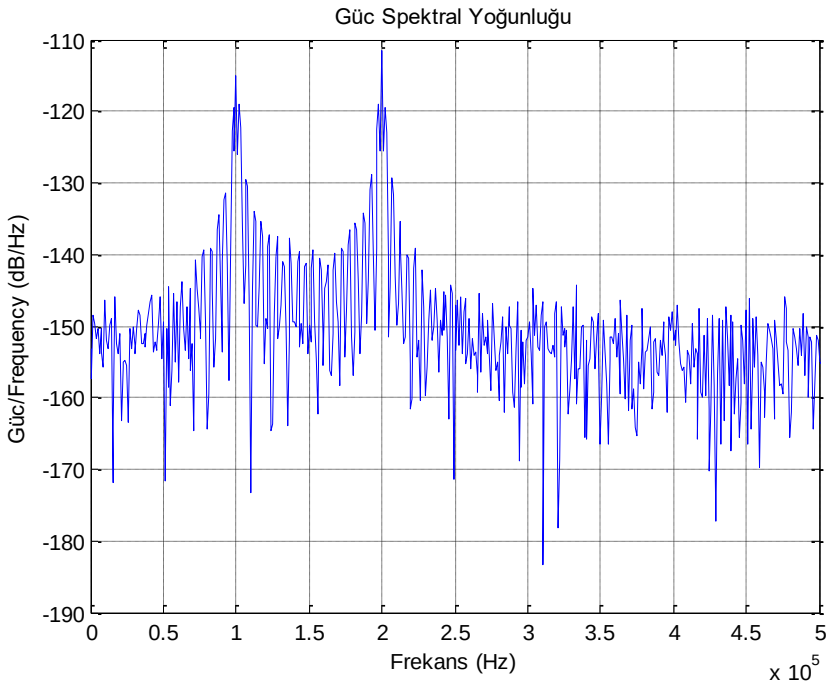
- Sabit genlik karakteristiği, güçlü gürültü bağışıklığı ve yükselteç eğriselliğine güçlü direnç sağlar.
- Modülator tasarımı basittir.
- Düşük güçlü vericiler için uygundur.

Bu çalışmada, hekim reçetesini barındıran verinin ve sorgu, komut veya uzaktan kontrol verilerinin iletiminde güvenlik koruması sağlayacak bir teknik geliştirilmiş ve önerilmiştir. Bu teknik, bir özel örtüşmeli çoklu ve kodlamalı FSK yapı kurularak geliştirilmiş ve bu teknikle komut iletiminde karmaşıklığı düşük güvenlik sağlanmıştır. Önerilen yöntem düşük karmaşıklık ve güvenlik yanında band genişliği verimliliği de sağlamaktadır. Bandgenişliği verimliliği implant haberleşmesinde çok önemlidir. Çünkü özellikle MİHS bandının meteoroloji ölçüm cihazları tarafından da kullanımı söz konusudur. Meteoroloji ölçüm cihazlarının kullanımı için tahsis edilen band MetAids bandı olarak isimlendirilmiş ve çakışan ortak kullanım bandı kullanıcı yoğunluğunu çokça artırmaktadır. Dolayısı ile [14]'teki çalışmada, daha büyük bellek gereksinimi ve bandgenişliği israfı ile birlikte güvenlik sunulması toplam verimliliği azaltmaktadır.

Çalışmanın kalanı aşağıdaki gibi sıralanmaktadır. Önerilen model Bölüm 2'de yer almaktadır. Bölüm 3 önerilen yönteme ilişkin başarım değerlendirmesini içermektedir. Son olarak, Bölüm 4'te sonuçlar yer almaktadır.

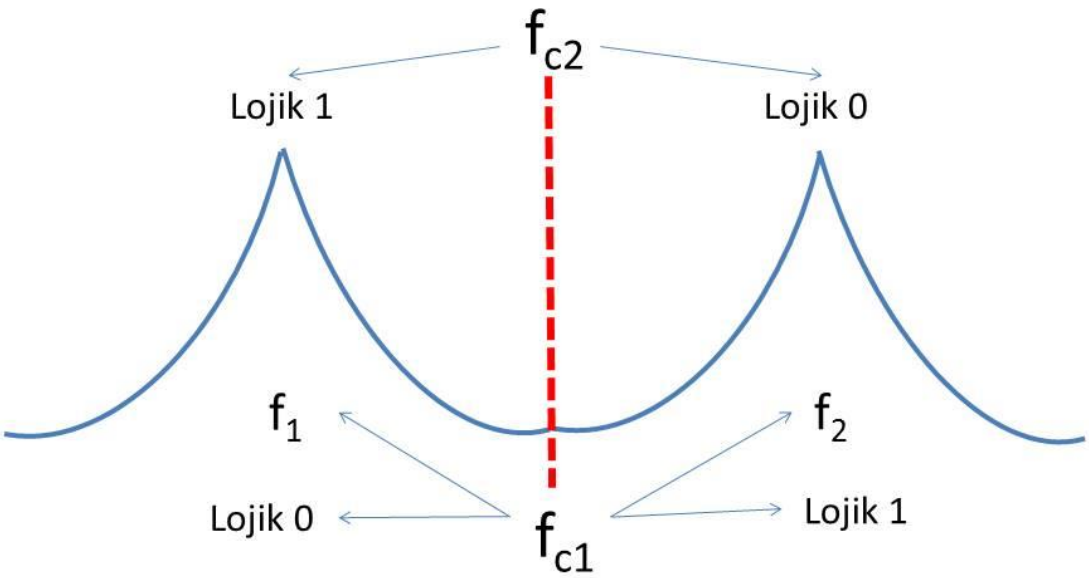
2. ÖNERİLEN KOMUT KORUMA MODELİ (PROPOSED COMMAND PROTECTION MODEL)

Şekil 1'de FSK modüle edilmiş ve toplanır beyaz Gauss gürültülü (TBGG, AWGN) kanaldan geçirilmiş temel banddaki bir sinyalin güç spektrumu yoğunluğu verilmiştir.



Şekil 1. *FSK modüle edilmiş ve TBGG kanaldan geçirilmiş bir işaretin temel banddaki güç spektrumu yoğunluğu.*

Şekil 1'de de görüldüğü üzere normal şartlarda 300 kHz'lik bir band genişliğine sahip bir sinyal için zirve spektral değerlere ulaşılan iki değer bit değerlerini ifade eder [7]. Örneğin şekilde düşük frekans değeri (100 kHz) lojik sıfır'a '0' (space) ve yüksek frekans değeri (200 kHz) lojik bir'e '1' (mark) karşılık gelmektedir. Bu çalışmada ise uygun bir kodlama ile düşük frekans değeri kimi zaman lojik sıfır'a '0' (space), kimi zaman da lojik bir'e '1' (mark) karşılık gelir. Aynı şekilde yüksek frekans değeri kimi zaman lojik sıfır'a '0' (space), kimi zaman da lojik bir'e '1' (mark) karşılık gelir. Ne zaman hangi değere karşılık geleceği sadece alıcı ve verici tarafından tesbit edilebilir. Çünkü bu bilgiler alıcı ve verici'de dolaylı olarak ve çok küçük boyutta yer işgal edecek şekilde saklı tutulur. Bu da, taşıyıcı veya merkez frekans ataması, kodlaması ve saklanması ile mümkündür ki, bu frekans şekilde 150 kHz olarak gözükmektedir.

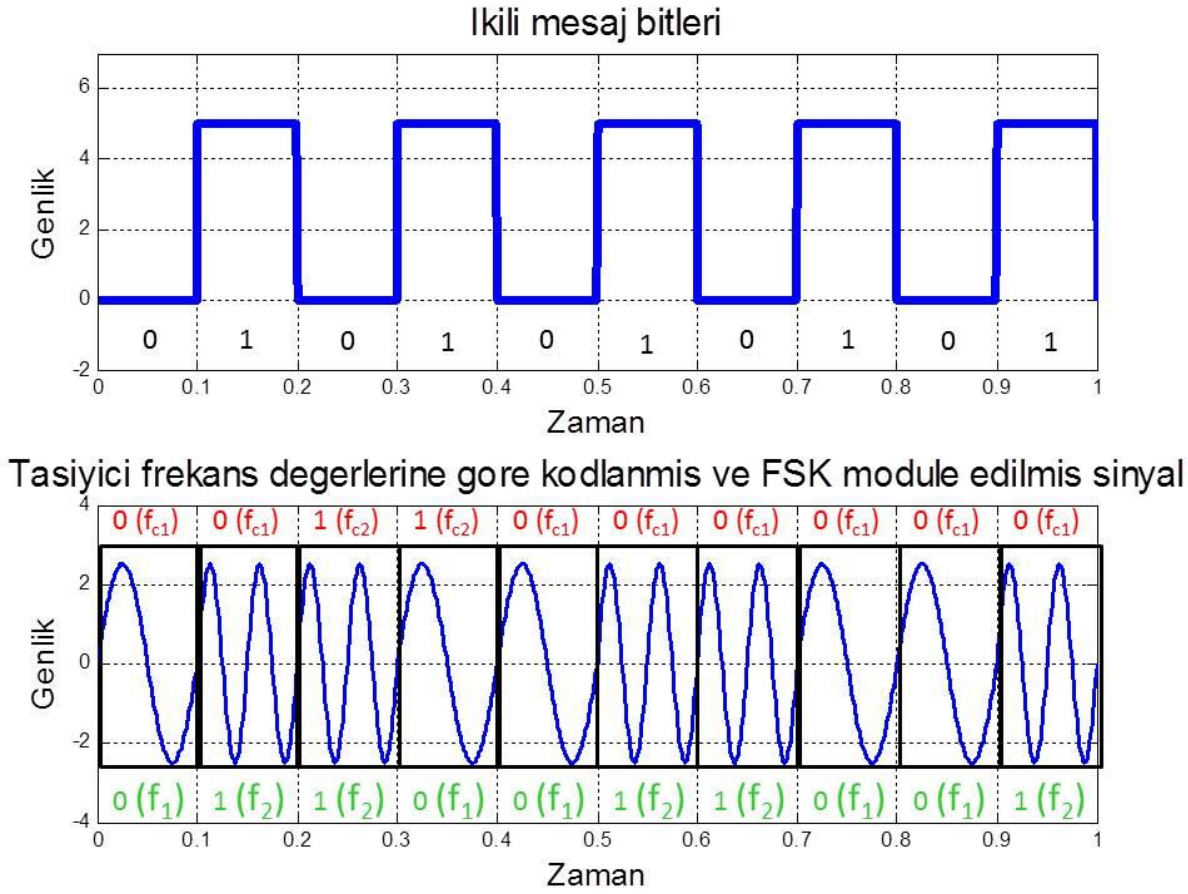


Şekil 2. *Frekans bölgesinde dalga şekli kodlama.*

Şekil 2'de önerilen merkez frekans kodlaması mevcuttur. Bu kodlamada aynı frekans değerine sahip merkez frekansı iki farklı şekilde ifade edilir, kodlanır ve bir nevi dikgenlik sağlanır. Merkez frekansı f_{c1} durumunda düşük frekans değeri f_1 lojik 0 ile ve yüksek frekans değeri f_2 ise lojik 1 ile ifade edilir. Merkez frekansı f_{c2} durumunda düşük frekans değeri f_1 lojik 1 ile ve yüksek frekans değeri f_2 ise lojik 0 ile ifade edilir.

Önerilen yöntemde sadece vericide ve alıcıda hızlı ulaşılabilen bir bellek (memory) birimi gereklidir. Bu bellek birimi sadece okunabilir bellek (SOB, ROM) veya aramalı tablo (AT, LUT) tipinde olabilir. Her bir IMC'ye özgü rasgele sıralı dizilmiş merkez frekansı durumları, bu bellek hücrelerine yerleştirilir. Burada önerilen yöntem [14] 'le kıyaslandığında, çoklu taşıyıcı kullanılmadığı için MetAids ve diğer MİHS kullanıcılar için aynı anda yoğun kullanıcının olduğu ortamda avantaj sağlamaktadır. Ayrıca bu çalışmada, bellekteki her bir adresteki data 1 bit'le ifade edilerek çok daha küçük bellek boyutu imkanı sunulmaktadır.

Tablo 1'de ve Şekil 3'te her bir zaman aralığı için vericideki olası tüm durumlar verilmiştir. Vericide iletilen bitlerin lojik değerleri aynı sıradaki merkez frekansı ifade kodu lojik karşılığı ile EX-OR işlemine tabi tutularak gözlenen anlık spektral (frekans) değerlerinin lojik karşılıkları elde edilir ve her bir bit süresince 0 --> f_1 ve 1 --> f_2 dönüşümü ile düşük ve yüksek anlık frekans değerleri ile iletim yapılır. İletilen işaret tipik FSK modüleli dalga şekli görünümündedir.



Şekil 3. *Merkez frekans değerlerine göre kodlanmış ve FSK modüle edilmiş sinyal.*

Tablo 1. *Her bir zaman aralığı için vericideki olası tüm durumlar.*

D **İletilen bitlerin lojik değerleri**	**F_c** **Merkez frekans ifade kodu (lojik karşılığı)**	**F_s= XOR(D,F_c)** **Gözlenen anlık spektral değerler (lojik karşılığı)**
0	f_{c1} (0)	f_1 (0)
1	f_{c1} (0)	f_2 (1)
0	f_{c2} (1)	f_2 (1)
1	f_{c2} (1)	f_1 (0)

Tablo 2'de her bir zaman aralığı için alıcıdaki olası tüm durumlar verilmiştir. Alıcıda ise tipik FSK modüleli dalga şekli alınır. Her bir zaman aralığı için f_1 --> 0 ve f_2 --> 1 dönüşümü ile düşük ve yüksek anlık spektral lojik karşılıkları elde edilerek, alıcıdaki bellekteki rasgele sıralı saklı aynı sıradaki merkez frekansı ifade kodu lojik karşılığı ile EX-OR işlemine tabi tutularak alınan bit dizisine ulaşılır.

Tablo 2. *Her bir zaman aralığı için alıcıdaki olası tüm durumlar.*

F_s **Gözlenen anlık spektral değerler (lojik karşılığı)**	**F_c** **Merkez frekans ifade kodu (lojik karşılığı)**	**D= XOR(F_s,F_c)** **Alınan bitlerin lojik değerleri**
f_1 (0)	f_{c1} (0)	0
f_2 (1)	f_{c1} (0)	1
f_2 (1)	f_{c2} (1)	0
f_1 (0)	f_{c2} (1)	1

3. BAŞARIM DEĞERLENDİRMESİ (PERFORMANCE EVALUATION)

Önerilen yöntem ile karmaşıklığın düşük hale getirilmesi, IMC'nin basit bir tasarım olarak gerçeklenmesi anlamına gelmektedir. IMC tasarımının basit olması ise içindeki parça sayısının az olması ve iç parçalarının işlem/fonksiyon veya kayıt kapasitelerinin düşük olması olarak kabul edilebilir. Bu sayede cihazın arıza yapma ihtimali azalacak ve arızasız ömrü de uzun olacaktır. Çünkü her bir IMC arızası, IMC'ye müdahale veya değişim demektir ki, bu durumda hastaya cerrahi müdahale yapılarak ameliyat gerektirir. Bu da istenmeyen bir durumdur.

Önerilen yöntem ile karmaşıklığın düşürülmesi, kriptografik yöntemler içermemesi, FSK modülatörünün diğer sayısal modulator türlerine göre daha basit olması nedeni ile tercih edilmesi, iki taşıyıcılı yapı kurulmasına rağmen frekans atlamalı alım yapılmadığından ek bir frekans sentezleyici devresine ve daha geniş bantta çalışacak RF donanıma gerek kalmaması, düşük kapasiteli bellek kullanımı ile sağlanabilmektedir.

Önerilen yöntemin başarım açısından değerlendirilmesi ise, öncelikli olarak pasif dinleyicinin güvenli iletilen komutu ne kadar zamanda çözebileceği ile yapılacaktır. Geliştirilen herhangi bir kriptografik method için pasif dinleyicinin kanalda iletilen bilgiden yararlanarak geliştirilen kriptografik methodu

çözme veya deşifre etme süresi bu çalışmada başarım metriği olarak kullanılmıştır.

Pasif dinleyicinin dünyanın en güçlü bilgisayara sahip olduğu varsayılırsa bir oturumda gönderilen bit sayısına göre tüm seçeneklerin denenmesi için geçen süre (T_z) aşağıdaki denklemle ifade edilir.

$$T_z = \frac{2^N}{S_Y H_s} \tag{3.1}$$

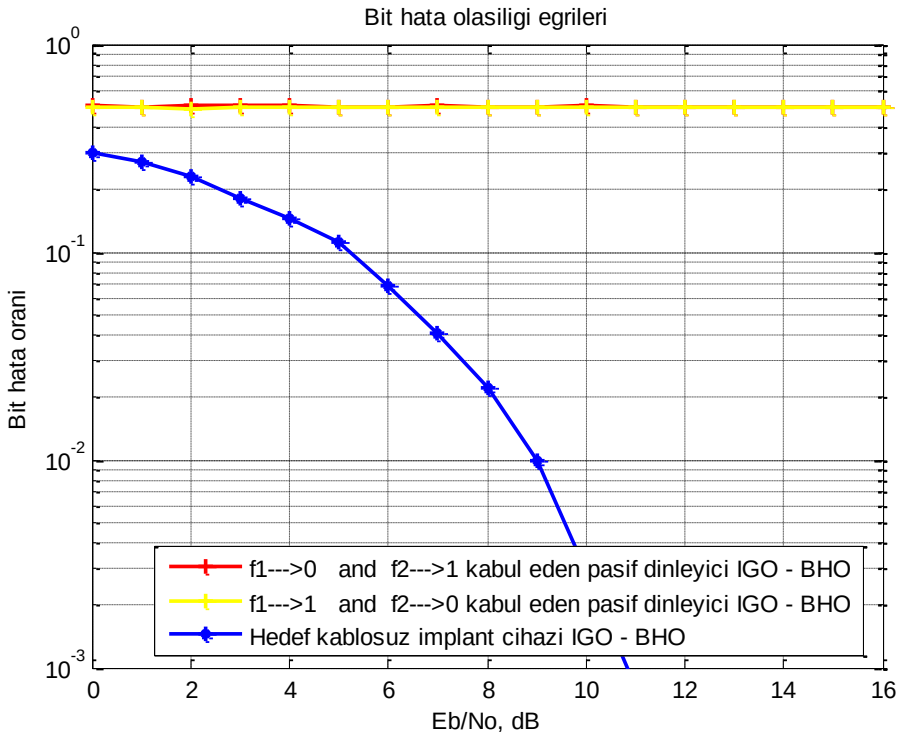
Burada N her bir oturum için toplam bit sayısını, S_Y bir yıl içinde geçen toplam saniye adedini ve H_s ise saniyedeki hesaplama miktarını karşılık gelir [15]. Buna göre bir oturumda gönderilen bit sayısına göre komut yapısını çözme süreleri Tablo 3'te verilmiştir.

Tablo 3. *Bir oturumda gönderilen bit sayısına göre komut yapısını çözme süreleri.*

Bir oturumda gönderilen bit sayısı	**Süre (Yıl)**
100 bit	4.3216e+05
205 bit	1.7530e+37
300 bit	6.9445e+65
400 bit	8.8033e+95

Şekil 4'te de pasif dinleyici için ve hedef alıcı için işaret gürültü oranına (IGO) göre bit hata olasılığı (BHO) başarımları verilmiştir. Literatürde, kablosuz iletişim'de fiziksel katman güvenliğinde hedef alıcı ile pasif dinleyici IGO-BHO eğrileri arasındaki açıklık ne kadar güvenlik sağladığı ile ilgili bilgi vermekte ve metrik aracı olarak kullanılmakta olduğundan, burada da önerilen yöntemin benzetimi gerçekleştirilerek, benzetim çıktısı olarak sunulmuştur [16,17].

Şekil 4'ten de anlaşıldığı üzere IGO arttıkça hedef implant cihazına komut gönderiminde BHO azalmaktadır. Fakat pasif dinleyici için BHO değişmemekte ve çok yüksek değerlerde kalmaktadır. Burada, pasif dinleyici komut iletiminde, iletilen mesaj bit değerlerini, doğrudan iki frekans spektral değerlerine göre, düşük frekans için f_1 --> 0 olacak şekilde ve yüksek frekans için f_2 --> 1 olacak şekilde atayarak yapmıştır. Pasif dinleyici tersi durumu da (f_1 --> 1 ve f_2 --> 0) uygulasa aynı başarım sonucuna ulaşıldığı şekilde gözükmektedir.



Şekil 4. *Pasif dinleyici için ve hedef alıcı için işaret gürültü oranına (IGO) göre bit hata olasılığı (BHO) başarımları*

4. SONUÇ (CONCLUSION)

Günümüzde implante edilebilen medikal sistemler kablosuz iletişim yeteneğine sahiptirler. Fakat bu kablosuz iletişimin güvenli olması hem hasta hakları hem de hasta sağlığı açısından çok önemlidir. Bu nedenle kablosuz IMC sistemlerinin iletimlerinin güvenli olması ve aktif ve pasif saldırganlara karşı korunması gerekir. Bu çalışmada, bir özel örtüşmeli ve kodlamalı FSK tekniği önerilmiş ve bu teknikle komut iletiminde band genişliği verimli karmaşıklığı düşük güvenlik sağlanmıştır.

KAYNAKLAR (REFERENCES)

[1] Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff (2016); http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[2] M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," 2014 IEEE Symposium on Security and Privacy**,** San Jose, CA, 2014, pp. 524-539.doi: 10.1109/SP.2014.40

[3] J. Choi, J. Ha and H. Jeon, "Physical layer security for wireless sensor networks," *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London*, 2013, pp. 1-6.doi: 10.1109/PIMRC.2013.6666094.

[4] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder:New directions for implantable medical device security," in Proceedings of the 3rd Conference on Hot Topics in Security, ser. HOTSEC'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 5:1–5:7. [Online].Available:http://dl.acm.org/citation.cfm?id=1496671.1496676

[5] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, Imdguard: Securing implantable medical devices with the external wearable guardian," in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 1862–1870.

[6] M. Zhang, A. Raghunathan, and N. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," IEEE Transactions on Biomedical Circuits and Systems, vol. 7, no. 6, pp.871–881, Dec 2013.

[7] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," SIGCOMM Comput. Commun. Rev., vol. 41, no. 4, pp. 2–13, Aug. 2011.

[8] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in IEEE Symposium on Security and Privacy (SP), May 2008,pp. 129–142.

[9] M. Zhang, A. Raghunathan, and N. Jha, "Trustworthiness of medical devices and body area networks," Proceedings of the IEEE, vol. 102,no. 8, pp. 1174–1188, Aug 2014.

[10] MICS Medical Implant Communication Services, FCC 47CFR95.601– 95.673 Subpart E/I Rules for MedRadio Services, Federal Communications Commission Std.

[11] ITU-R Recommendation RS.1346: Sharing between the meteorological aids service and medical implant communication systems (MICS) operating in the mobile service in the frequency band 401–406 MHz, 1998.,International Telecommunications Union. Std.

[12] Y.-H. Liu, C.-J. Tung, and T.-H. Lin, "A low-power asymmetrical mics wireless interface and transceiver design for medical imaging," in IEEE Biomedical Circuits and Systems Conference (BioCAS), Nov 2006, pp.162–165.

[13] K. Zhu, M. Haider, S. Yuan, and S. Islam, "A sub-1 ua low-power fsk modulator for biomedical sensor circuits," in IEEE Computer Society Annual Symposium on VLSI (ISVLSI), July 2010, pp. 265–268.

[14] S. Kulac¸ and H. Arslan, "Reliable listen-before-talk mechanism for medical implant communication systems," 2016 *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom),* Munich, 2016,pp.1-4.doi:10.1109/HealthCom.2016.7749531

[15][Online].Available: http://www.top500.org/lists/2016/11/

[16] H. Chen, W. Zhu, L. Zeng and X. Cai, "Secrecy capacity based on suboptimal multi-antennas selection and power allocation," 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, 2016, pp. 83-86.

[17] Q. Zou, B. Zhang, Y. Ma and D. Guo, "Increasing physical layer security through reliability-based HARQ," 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, 2016, pp. 1-5.