Kablolu Telefon Şebekeleri İçin Fiziksel Katmanda Çalışan Bir Güvenli Haberleşme Modülü Prototip Gerçeklemesi
A Secure Communications Prototype Implementation for PSTNs operating on Physical Layer

Sezer Can Tokgöz[1], Ali Boyacı[1], Serhan Yarkan[1]

[1]İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi,
Elektrik–Elektronik Mühendisliği Bölümü, Küçükyalı, 34840, İstanbul
scan.tokgoz@istanbulticaret.edu.tr, aboyaci@ticaret.edu.tr, syarkan@ticaret.edu.tr

Özet

Her geçen gün daha da yaygınlaşan veri iletişim uygulamaları ile başarımı gittikçe artan yeni haberleşme teknikleri, bu teknolojileri kullanan kişileri, kurumları ve hatta devletleri iletişim hizmetlerinin verildiği altyapıya bağımlı kılmaktadır. Açıktır ki, altyapı bağımlılığı, altyapı üzerinden aktarılan bilgilerin güvenliği, güvenilirliği, yetkinliği ve bütünlüğü anlamında önemli kaygıları beraberinde getirmektedir. Dolayısıyla bu çalışmada, kablolu telefon şebekeleri üzerinde bölgesel standartlara (ITU-R, Avrupa) göre işleyebilen, steganografik veri alışverişini destekleyen, hem analog hem de dijital veri aktarımını çeşitli güvenlik seviyeleri üzerinden sağlayabilen sayısal işaret işleyici tabanlı bir prototip ortaya konmuştur. Ayrıca, prototipin kullanacağı fiziksel haberleşme kanalının istatistiki yapısı ölçümler aracılığı ile belirlenmiş ve iki haberleşme uçbirimi arasında bulunan santralin de davranışı hesaba katılarak, sayısal işaret işleyiciler yardımı ile haberleşme sağlanmıştır. Geleceğe yönelik çalışmalar, bu çalışmada elde edilen sonuçlar ve tartışmalar ışığında verilmiştir.

Abstract

Widespread use of data communications applications along with recently emerging high–performance telecommunication techniques enforce people, organizations, and even countries to rely on the infrastructures with which these communication services are provided. It is clear that dependence on infrastructure leads to critical concerns about security, reliability, authenticity, and integrity of the data carried over the same infrastructure. Therefore, a prototype based on digital signal processor (DSP) is implemented, which operates on public switched telephone network (PSTN) lines in accordance with the regional (ITU-R, European) standards, supports steganographic information exchange, and allows both analog and digital data transfer in several security levels. In addition, statistical characteristics of the physical layer channel are identified via measurements and communication between two end nodes is established with the use of DSPs by taking into account the behaviors of the switching center. Future directions are provided in light of the results and relevant discussions as well.

Bu çalışma, İstanbul Ticaret Üniversitesi Yayın, Araştırma ve Proje Koordinasyon Kurulu tarafından desteklenmektedir (Proje No: YAP–2015-02-001).

1. Giriş

Kablosuz haberleşme, gündelik yaşamın vazgeçilmezleri arasında sayılmaktadır. Her geçen gün daha fazla sayıda kullanıcı, herhangi bir yere bağlı kalmadan yüksek hızda hareketlilik desteğine sahip kablosuz hizmetlerle buluşmaktadır. Kullanıcı sayısındaki artışın eğilimi göz önünde bulundurulduğunda, 2020 yılında yedi milyar kişiye yedi trilyon kablosuz cihazın hizmet vereceği öngörülmektedir [1].

Yukarıda sözü edilen artış, yalnızca kullanıcı sayısıyla sınırlı kalmayıp, kablosuz haberleşme kullanılarak taşınan veri hacmini de kapsamaktadır. Açıktır ki, kablosuz haberleşme aracılığı ile aktarılan verilerin oldukça önemli bir kısmı da özellikle Internet üzerine/üzerinden bir biçimde kablo altyapısı kullanılarak taşınmaktadır. Kestirimlere göre, şu anda 1ZB eşiğine ulaşan Internet trafiği 2020 yılında 2.3ZB'e ulaşacaktır ve bu trafiğin %34'ünün de kablolu altyapı üzerinden taşınacağı düşünülmektedir [2]. Ötesinde, yakın gelecekte "Nesnelerin Internet'i" kavramı çerçevesinde çok çeşitli cihazların, algılayıcıların ve bileşenlerin birbirleri ile ve altyapı ile bağlantılı olduğu kablolu ve kablosuz şebekeler düşlenmektedir [3]. Hem mevcut hem de yakın gelecek için düşlenen veri hacmi, kablosuz haberleşmenin oldukça fazla öne çıktığı bir zaman aralığında kablolu haberleşmenin göz ardı edilmemesi gerektiğini ortaya koymaktadır. Halihazırda oldukça yaygın olarak ve çeşitli ölçeklerde (evlerden, kurum içi kablolu haberleşme sistemlerine ve kıtalar arası hatlara) kullanılan kablolu iletişimin, hem daha verimli hem de daha güvenli hale getirilmesi oldukça büyük bir önem taşımaktadır.

Yerel döngüler, kablolu iletişim ağlarının berlirli bir işaretleşme protokolüne göre işleyen en yalın sürümleridir. Bu nedenle, birçok platformda halihazırda kullanılmaktadır. Ötesinde, hizmet sağlayıcılar piyasadaki hazır cihazlar ya da kendilerine ait ürünler aracılığı ile son kullanıcılara yerel döngü ve kablolu hatlar üzerinden "üçü bir arada" olarak bilinen telefon, televizyon ve Internet uygulamalarını aynı anda verebilmektedir. Bu hizmetler arasında konser, gösteri, sinema; spor karşılaşmaları gibi telif haklarına tabi çokluortam aktarımı [4]; evdeki tıbbi cihazlardan toplanan verilerin ilgili sağlık kuruluşlarına iletimi [5]; kullanıcının şebekeye erişiminde gerekli ayarların ve gömülü yazılımların güncellenmesine ilişkin verilerin gönderimi bulunmaktadır. Açıktır ki, yukarıda sözü edilen hizmetler üzerinden taşınan veriler oldukça önemli olup, güvenliğinin sağlanması gereklidir; çünkü bu başlıklar altında yapılan her türlü saldırı, ciddi sorunları beraberinde getirecektir [6]. Örneğin gömülü yazılımın güncellenmesi ile ilgili saldırı

konusu [7] içerisinde ele alınırken, Internet erişiminde kullanılan adresleme mekanizması üzerinden yapılacak saldırılar da incelenmektedir [8]. Araştırma sonuçlarına bakıldığında kablolu hat üzerinden geçen verilerin koklanması, izlenmesi, hatta içeriklerinin değiştirilmesi söz konusudur. Bu da kablolu hatlar üzerinden taşınan verilerin fiziksel katmandan başlanarak güvenli hale getirilmesini zorunlu kılar [9, 10].

Bilimsel dizinde yerel döngü üzerinde işleyen güvenli veri aktarımına ilişkin birçok çalışma bulunmaktadır. Örneğin [11–13]'de, yerel döngü üzerinden konuşma ve/veya veri saklama, işaretin frekans düzlemindeki yapısı üzerinde değişiklikler yapılmasına ilişkin yöntemlerle ortaya konmuştur. İşaretin akış oranı üzerinde ses tanıma yardımıyla değişiklikler yapılarak da yerel döngü üzerinden güvenlikli ses aktaran çalışmalara rastlanmaktadır [14, 15]. Ancak bu ve benzeri çalışmalar, kuramsal düzlemde kalıp, uygulama, prototip geliştirme ve saha sonuçları elde etme konusunda eksik kalmaktadır. Prototip geliştirme açısından bakıldığında, bilimsel dizinde yerel döngü üzerinde koşan güvenlikli platform gerçeklemeleri arasında [16] öne çıkmaktadır. Ancak [16]'da her ne kadar sayısal işaret işleyici (Sİİ) teknolojisinden yararlanılsa da, temel bileşenlerin (kodlayıcılar, modem, sıkıştırıcılar, vb.) hazır olarak bulunması ve fiziksel hattı tamamen kendisine ayırması, esnek bir tasarımın ortaya konmasını engellemektedir. Bu çalışmada ise, kablolu telefon şebekeleri üzerinde bölgesel standartlara (ITU-R, Avrupa) göre fiziksel katman üzerinde çalışan, steganografik veri alışverişini destekleyen, hem analog hem de dijital veri aktarımını telefon kullanımda iken çeşitli güvenlik seviyeleri ile sağlayabilen Sİİ tabanlı esnek bir prototip ortaya konmuştur. Özetle, bu çalışmanın bilimsel dizine üç temel katkısı bulunmaktadır: (K.1) Yerel döngü üzerinde işleyen Sİİ tabanlı ve hazır modüller kullanılmadan ortaya konan fiziksel katman alıcı–verici tasarımı, (K.2) telefon hattı üzerinden sesli görüşme ile eş zamanlı olarak istenen kipte (steganografik ya da diğer) hem analog hem de dijital veri aktarımını destekleyen yazılım tabanlı modül gerçeklemesi ve (K.3) yerel döngü mimarisinde kullanılan fiziksel katman kanal modelinin istatistiki olarak ortaya konmasına yönelik ölçümlerin ortaya konması. Ayrıca, prototipin kullanacağı fiziksel haberleşme kanalının istatistiki yapısına ek olarak iki haberleşme uçbirimi arasında bulunan merkezi anahtarlama biriminin (santralin) de davranışı hesaba katılarak, Sİİ'ler yardımı ile haberleşmenin sağlanabileceği uygulamalı olarak gösterilmiştir. Geleceğe yönelik çalışmalar, bu çalışmada elde edilen sonuçlar ve tartışmalar ışığında verilmiştir.

2. Sistem ve İşaret Modeli

Kablolu telefon şebekeleri, Dünya'nın çeşitli bölgelerinde birbirinden belirli ölçüde farklılaşmış standartlar uyarınca veri taşımaktadır. Bölgesel standartlar, hemen hemen her katmanda farklılıklar barındırmaktadır. Buna karşın, kablolu telefon şebekelerinin fiziksel katmandaki genel yapısı aynıdır. Kablolu telefon şebekelerinde alıcı–verici uçbirimleri birbirlerine kablo ve anahtarlamadan sorumlu santral olarak bilinen merkezi bir öge üzerinden bağlanmaktadır. Dolayısıyla, alıcı–verici çifti için fiziksel kanal, verici ile merkezi anahtarlama ögesi arasındaki hattan, merkezi anahtarlama ögesinden ve merkezi öge ile alıcı arasındaki hattan oluşur. Kablolu telefon şebekeleri için fiziksel kanalın en önemli özelliği, merkezi anahtarlama ögesinin 300–3400Hz arasındaki işaretlerin en yüksek kazançla anahtarlanması üzerine kurulu oluşudur. Merkezi anahtarlama ögesi tarafındaki süzgecin frekans düzlemindeki kazanç karakteristiği kusursuz olmadığından, koruyucu frekans bölgelerindeki davranışları (0–300Hz ve 3400–4000Hz bantları) kazanç yönünden değişkenlik gösterir. Açıktır ki, yerel döngüde kullanılacak fiziksel kanal modeli için bant geçiren bir yapıdan daha çok alçak geçiren bir yapı, sistemin ve işaretin modelini matematiksel olarak ortaya koymada oldukça büyük kolaylıklar sağlayacaktır. Yerel döngü fiziksel kanalı için temel bantta kanal birim darbe tepkisi, bağlantı yapısı, kullanılan kablo türü ve diğer bileşenler bir arada düşünülerek [17, 18]:

Çizelge 1. Ölçüm İstatistikleri

İstatistik	Ahize Kapalı (V)	Ahize Açık (V)
Asgari	-48.6	-6.55
Azami	-49.2	-9.1
Beklenen Değer	-49.06	-7.14
Varyans	0.01	0.78
Standart Sapma	0.12	0.88

$$h(t) = \sum_{l=0}^{L-1} h_l(t - \tau_l) \tag{1}$$

şeklinde verilirken L, dikkate değer azami yankı sayısını; τ_l ise l'inci yankıya ait gecikmeyi; $h_l(\cdot)$ ise yine l'inci yankının genliğini belirtir. Kablolu telefon hatları için:

$$h_l(t) = \int_{-\infty}^{\infty} g_l(f) e^{\alpha(f) v_l \tau_l} e^{\jmath 2\pi f t} df \tag{2}$$

olarak modellenir. Yukarıda, $_l$ dizini l'inci yankıya ait bileşeni ve $\jmath = \sqrt{-1}$ göstermek üzere $g_l(f)$, ilgili f frekansına ait genliği; v_l, iletim hızını; $\alpha(f)$, kullanılan kablolamaya ilişkin dielektrik ve yüzey katmanı etkisini içeren kaybı temsil eder. Dolayısıyla, alıcı tarafa ulaşan işaret için:

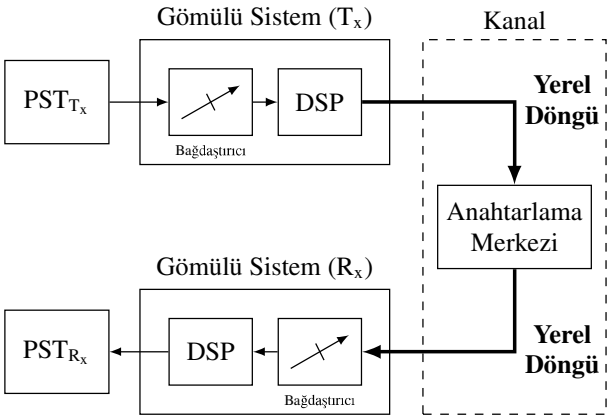
$$r(t) = \int_{0}^{T} h(\tau) x(t - \tau) d\tau + n(t) \tag{3}$$

yazılabilir. Yukarıda $r(t)$ alınan işareti; $x(t)$ kanala verilen işareti ve $n(t)$ ise toplamsal gürültüyü temsil eder. Fiziksel kanal ölçümlerinde, toplamsal gürültü $n(t)$, yanses, elektromanyetik indüksiyon sonucu ortaya çıkan gerilim sıçramaları gibi diğer etkileri de içermektedir. Ancak bu çalışma özelinde toplamsal gürültü, yalnızca beyaz Gauss gürültüsü şeklinde ele alınarak, modelin yalınlığı göz önünde bulundurulmuştur.

Her ne kadar (1), (2) ve (3) kanal modelini ve alınan işareti modellese de, kablolu telefon şebekelerinde ahize kapalı iken (anahtar açıkken), çalma anında ve ahize açıkken (anahtar kapalı iken) olmak üzere üç ana kip bulunmaktadır. Bu kipler, telefon şebekesine dahil edilecek gömülü sistemin de çalışma kiplerini belirleyeceğinden oldukça büyük önem taşır. Bu çalışma dahilinde yapılan ölçümlerin sonuçları ahize kapalı iken (anahtar açıkken) ve ahize açıkken (anahtar kapalı iken) olmak üzere sınıflandırılmış biçimde Çizelge 1'de verilmiştir. Ölçüm istatistiklerine ek olarak çalma anında azami mutlak potansiyel farkı 168V olarak ölçülmüştür.

3. Fiziksel Kanal Frekans Tepkisi, Prototip Gerçeklemesi ve Sonuçlar

Prototip, Bölüm 2'de sözü edilen yerel döngü kanalı ile telefon uçbirimleri arasında yer almaktadır. Prototipin blok diyagramı

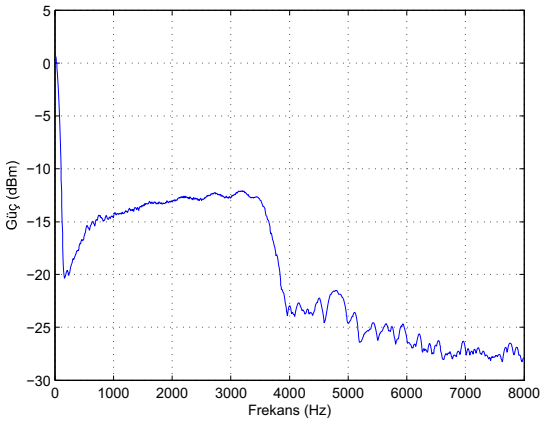


Şekil 1. Prototipin blok diyagramı.

Şekil 1'de verilmiştir. Bu bölümde, prototipin yerel döngü üzerinde çalışacağı fiziksel kanal frekans tepkisi, gerçekleme ve bu gerçeklemenin gerçek–zamanlı olarak çalıştırılması ile elde edilen sonuçlar tartışılmıştır.

3.1. Fiziksel Kanal Frekans Tepkisi

Daha önce Bölüm 2'de değinilen yerel döngü kanalının değişkenlik gösteren özellikleri nedeniyle, öncelikle prototipin üzerinde çalışacağı kanalın frekans ve birim darbe tepkisi ölçülmüştür. Uçbirimlerde bulunan süzgecin yapısı da düşünülerek, kanalın frekans tepkisi frekans tarama yöntemiyle belirlenmiştir. ITU-R standartları çerçevesinde verici tarafta uygun bağlantılarla 0–8kHz arası, 10s'lik süreyle taranıp, ortalama alınarak alıcı tarafta frekans tepkisi elde edilmiştir. Elde edilen frekans tepkisi Şekil 2'de verilmiştir. Şekil 2'de doğru akım bileşeni, 0Hz ile ölçüm esnasında referans olabilmesi için korunmuş olup, kanaldaki kaybın frekans düzlemindeki etkisini belirgin olarak göstermektedir.



Şekil 2. Frekans tarama yöntemi ile belirlenen kanalın frekans tepkisi.

3.2. Prototip Gerçeklemesi

Prototip Sİİ'ye dayanan bir gömülü sistem olarak düşünüldüğünden, fiziksel katmanda gerçeklenecek alıcı–verici tasarımı tamamen yazılım tabanlı olarak inşa edilebilmektedir. Bu çalışmada alıcı–verici algoritmalarının gerçeklendiği platform olarak, ARM tabanlı 32–bit Cortex–M4 çekirdekli yüksek performanslı Sİİ STM32F429ZI Discovery seçilmiştir. Yüksek performanslı Sİİ, 2MB flaş belleğe, 256+4KB SRAM'e, 64Mbit harici SDRAM'e, 16MHz dahili osilatöre, 4–26MHz kristal osilatöre ve 180MHz'e kadar çalışma frekansına sahiptir.

Verici tarafta açık–kapalı anahtarlama, spektrum yayma, frekans atlama gibi birçok teknikten istenileni, gereksinimler çerçevesinde kolayca gerçeklenebilir. Bu çalışmada ise hem gerçek–zamanlı veri aktarımını gösterebilmek hem de fiziksel katmanda belirli düzeyde bir güvenlik sağlayabilmek adına frekans atlamalı ve darbe genlikli kiplenim tekniklerini bir arada kullanan bir gerçekleme yapılmıştır. Prototip, sahip olduğu yerel osilatör ile Şekil 2'deki frekans tepkisine göre belirlenmiş bantta:

$$x(t) = \sqrt{2A}m(t)\cos\left(2\pi f_H^k t\right) \tag{4}$$

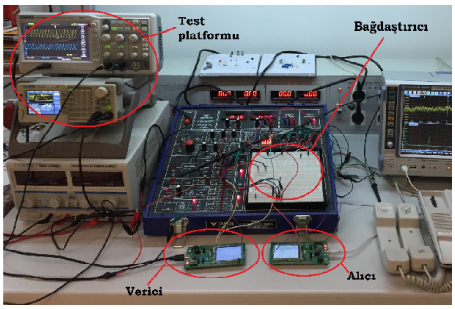
biçiminde frekans atlamalı olarak işaret üretir. Burada A, işaretin gücünü; $m(t)$, darbe genlikli kiplenim üzerinden ikili veriyi; f_H^k ise k'inci atlama esnasında iletimin yapılacağı frekansı eşdağılımlı olarak $f_H^k \sim U(300\text{Hz}, 3400\text{Hz})$ olacak biçimde belirtir. Alıcı tarafta ise (4) içerisindeki k dizini ile belirtilen atlama sırası/dizini önceden bilindiğinden, ilgili frekans aralıklarına doğru zamanda bakılarak verilerin alınması sağlanmış olur. Çalışmada, frekans atlamalı değerler için $U(1750\text{Hz}, 3400\text{Hz})$ seçilmiştir. Seçilen değerler, yerel döngü üzerindeki gerilim salınımlarından ve Sİİ'den kaynaklanan nedenlerle üretilen işaretlerin kırpılma olasılığı göz önünde bulundurularak belirlenmiştir çünkü kırpılma, hat üzerinde istenmeyen harmonik bileşenler oluşturacaktır. Kırpılmanın sorun oluşturmayacağı aralık, doğal olarak, seçilen frekansların ikinci (ve daha sonraki diğer tüm) harmoniklerinin hattın frekans tepkisinin sönümlendiği kesme bölgesine denk düşürülmesiyle elde edilir. Dolayısıyla, kuramsal olarak $f_H^k \sim U(300\text{Hz}, 3400\text{Hz})$ olacak şekilde seçilebilecek frekans atlamalı dizi, uygulamada $f_H^k \sim U(1750\text{Hz}, 3400\text{Hz})$ arasında değerlendirilmelidir.

Gömülü sistemin sorunsuzca işleyebilmesi için, yerel döngünün olağan çalışma koşullarının göz önüne alınması gerekir. Bu da yerel döngü üzerindeki işaretlerin gömülü sistemin çalışma aralıklarına uygun hale dönüştürülmesini zorunlu kılar. Yapılan ölçümler sonucunda ahize kapalı durumda iken hattaki potansiyel farkın -49V olduğu; gelen arama sırasında ulaşılan azami potansiyel farkının -168V'a ulaştığı belirlenmiştir. Bu nedenle projede kullanılan Sİİ'lerin çalışma aralıkları göz önünde bulundurularak bir devre tasarlanmıştır. Bu devre üç kısımdan oluşmaktadır: İlk kısım, gelen arama sırasında -49V ile -168V arasında değişen potansiyel farkı -5V ile 0V arasına indirgeyen gerilim bölücü devre ile ters kutuplama metodundan oluşmaktadır. İkinci kısım, -5V ile 0V aralığına düşürülen potansiyel farkı 0V ile 5V aralığına çeviren evirici işlemsel yükseltgeçten oluşmaktadır. Üçüncü kısım ise yerel döngü hattı üzerinde bulunan sabit gerilimi engellemek için kullanılan kondansatörden oluşmaktadır. Tasarlanan devre Sİİ'lere genel amaçlı giriş–çıkış (GAGÇ) noktaları üzerinden bağlanmıştır. Bu devre Şekil 1'de "bağdaştırıcı" etiketi ile gösterilmektedir.

3.3. Sonuçlar

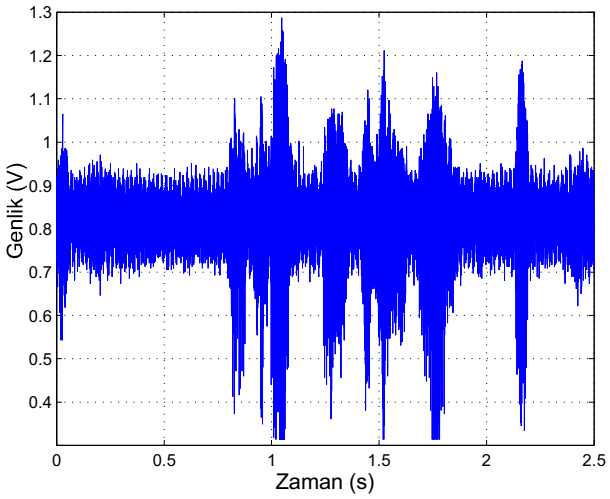
Prototip kurulumu, İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, TLab. laboratuvarlarında gerçekleştirilmiştir.

Yerel döngü, yine İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi bünyesindeki Karel DS200L telefon santraline bağlı iki dahili hat üzerinden uygun bağdaştırıcı ve bağlantılarla sağlanmıştır. Prototipler, alıcı ve verici çifti olmak üzere dahili hatların uygun noktalarına tümleştirilmiştir. Test işaretleri, gönderilen ve alınan işaretlerin denetlenebilmesi için Rohde&Schwarz RTO1044 sayısal osiloskopu da prototiplere bağlanmıştır. Prototipin, test donanım ve teçhizatının çalışır haldeki görüntüsü Şekil 3'de verilmiştir.

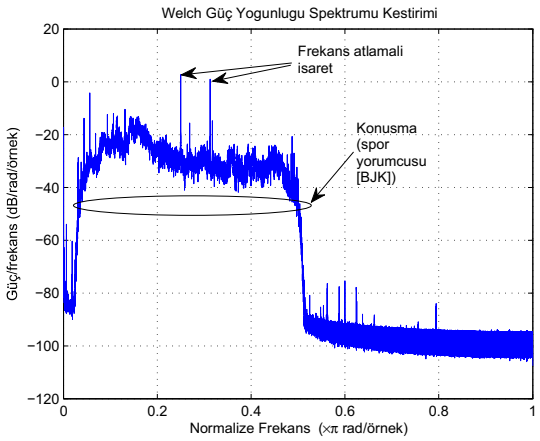


Şekil 3. Prototipin test platformları ile birlikte çalışır haldeki görüntüsü.

Prototip, verici taraftaki gömülü sistem üzerinden, önceden belirlenmiş ve alıcı tarafta da bilinen sırasıyla frekans atlamalı iletişimi her iki telefon açıkken ve telefonlardan birinde (vericide) bir spor yorumcusunun konuşması eşliğinde gerçekleştirmiştir. Frekans atlama dizisi 2kHz, 2.5kHz ve 3kHz değerlerinden herhangi bir anda rastgele seçilen birisi olacak şekilde belirlenmiş ve her bir frekansta 1s kalınarak iletişim sağlanmıştır. Verici taraf, bu parametreleri kullanarak Morse kodu ile imdat çağrısı olarak bilinen "S.O.S" işaretini arka arkaya göndermiş ve alıcı tarafın da bu işareti başarı ile aldığı belirlenmiştir. Yerel döngü üzerinden verici tarafta spor yorumcusunun konuşması esnasında frekans atlamalı olarak gönderilen işaretin bir kısmının anlık görüntüsü Şekil 4'de verilmiştir. İlgili ölçüme denk düşen işaretin frekans düzlemindeki karşılığı ise Şekil 5'de gösterilmektedir.



Şekil 4. Prototipin alıcı taraftaki Sİİ'sine ulaşan işaretin zamandaki 2.5s'lik görüntüsü. Verici taraftan iletilen spor yorumcusunun konuşması açıkça görülebilmektedir.



Şekil 5. Prototipin alıcı taraftaki Sİİ'sine ulaşan işaretin 2.5s'lik dilimine ait frekans düzlemindeki görüntüsü.

Bu noktada, prototipin başarıyla çalışabilmesi için yerel döngü kapalı devre sistemlerde kullanılan ve oldukça sınırlayıcı bir takım koşullara ve sınırlamalara değinmek yerinde olacaktır. Örneğin, yerel döngünün ucunda bulunan anahtarlama merkezi, hatta 2.2V'un altında gerilim algıladığı anda bağlantıyı kesmektedir ancak hemen sonlandırmamaktadır. Yapılan ölçümlere göre hat eğer 2.2V'un altında 500ms'den az geçici bir süre kalıp, 2.5V'un üzerine hemen çıkarsa, anahtarlama merkezi bağlantıyı sürdürmektedir. Benzer şekilde, ölçümler sonucunda, yerel döngünün ucunda bulunan telefon cihazlarının (ahize ve baz) markadan markaya değişkenlik gösteren hat besleme gerilimleri bulunmaktadır. Bu durum, iletişimin sağlıklı olabilmesi için prototipin bağlantılandırılacağı telefon cihazlarının hattı beslediği göz önünde bulundurularak sürekli ölçümlere dayanan uyarlamalı bir çözüm üretilmesini gerektirmektedir.

4. Sonuç ve Geleceğe Yönelik Tartışmalar

Bilimsel dizindeki çalışmalar, halihazırda oldukça yoğun olarak kullanılan ve yakın gelecekte de yoğun kullanılmaya devam edeceği düşünülen yerel döngü tabanlı şebekelerin oldukça önemli güvenlik açıkları barındırdığını göstermektedir. Bu çalışmada, yerel döngü üzerinde çalışan; bölgesel standartlara uygun; steganografik veri alışverişini destekleyen; hem analog hem de dijital haberleşmeyi yerel döngü üzerinden ses aktarımı devam ederken çeşitli güvenlik seviyeleri ile sağlayabilen; Sİİ tabanlı bir prototip ortaya konmuş ve çalıştırılmıştır. Prototip, Sİİ sayesinde fiziksel katman seviyesinde istenilen her alıcı–verici yapısının yazılım tabanlı olarak gerçeklenebileceği esnekliktedir. Prototip, bilimsel dizindeki diğer çalışmaların aksine yerel döngünün en yalın sürümü olan ve yalnızca ses iletişimi için kullanılıp, oldukça önemli sınırlamalarla (bant genişliği, anahtarlama merkezinin gerilim sınırlamaları, vb.) birlikte gelen kapalı devre telefon sisteminde sınanmış ve başarıyla çalıştırılmıştır.

Prototip, özellikle sesli konuşma esnasında hattan veri aktarımını yaparken frekans atlamalı bir haberleşmeyi tercih etmektedir. Ancak frekans atlama sırası bu çalışma kapsamında tamamen rastgele üretilmiş bir diziden ibarettir. Doğal olarak, sesli iletişimde, konuşmacıların ses karakteristikleri dahilinde en yüksek gücün olduğu frekans bantlarında kayıplar büyük ol-

maktadır. Bunun engellenmesi için prototipin iletişime geçmeden hemen önce konuşmacıların ses karakteristiklerini öğrenip, bu çerçevede bir frekans atlama sırası belirlenmesi gerekmektedir. Yine bu çalışmada, hat üzerinden ses aktarımı esnasında iletilen veriler için en uygun sıkıştırma ve kodlama yöntemlerinin belirlenmesi gerekmektedir. Prototipin bu noktada anahtar değişimi ve benzeri süreçler için de geliştirilmesi gereken protokollere ihtiyacı vardır. Prototip Sİİ tabanlı olduğu için, alıcı–verici tasarımından sıkıştırma ve kodlama yöntemlerine kadar bütünleşik tasarımlar, test aşamasından sonra doğrudan sistem içerisine gömülüp, çalıştırılabilecektir.

Son olarak da prototip, çeşitli sayısal kullanıcı hatları ile birbirine bağlanan ve Internet tabanlı iletişime izin veren anahtarlama merkezleri ile de bağdaşımlı çalışabilecek duruma getirilmelidir. Ötesinde, halihazırda kullanılmakta olan Global System for Mobile (GSM) teknolojisi üzerinden ses iletişimi yapılan kanaldan veri aktarmak da mümkün olacaktır.

5. Kaynaklar

[1] W. W. R. Forum, "Visions and Research Directions for The Wireless World," Wireless World Research Forum, Zurich, Switzerland, White Paper November 2013, v2.0, November 2013.

[2] Cisco, "White Paper: The Zettabyte Era-Trends and Analysis," Cisco, Tech. Rep., June 2016.

[3] J. Voas, "Demystifying The Internet of Things," *Computer*, vol. 49, no. 6, pp. 80–83, June 2016.

[4] D. Diaz-Sanchez, F. Sanvido, D. Proserpio, and A. Marin, "DLNA, DVB-CA and DVB-CPCM Integration for Commercial Content Management," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 79–87, February 2010.

[5] Y.-J. Lin, M.-J. Su, H.-S. Chen, and C.-I. Lin, "A Study of Integrating Digital Health Network with UPnP in An Elderly Nursing Home," in *Computer Systems Architecture Conference, 2008. ACSAC 2008. 13th Asia-Pacific*, Hsinchu, Taiwan, August 4–6 2008, pp. 1–7.

[6] G. Loukas, *Cyber-physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann, 2015.

[7] A. Cui, M. Costello, and S. J. Stolfo, "When Firmware Modifications Attack: A Case Study of Embedded Exploitation." in *NDSS*, San Diego, CA United States, April 23 2013.

[8] F. Raynal and G. Campana, "An Attack Path to Jailbreaking Your Home Router," *Proc. of Hack In The Box (HITB), Kuala Lumpur, Malaysia*, 2012.

[9] P. Geissler and S. Ketelaar, "How I Met Your Modem: Advanced Exploitation & Trojan Development for Consumer DSL Devices," *Proc. of Hack In The Box (HITB), Amsterdam, The Netherlands*, 2013.

[10] Y. Bachy, V. Nicomette, E. Alata, M. Kaâniche, and J.-C. Courrège, "Security of ISP Access Networks: Practical Experiments," in *Dependable Computing Conference (EDCC), 2015 Eleventh European*. Paris, France: IEEE, September 7–11 2015, pp. 205–212.

[11] S. Chen and H. Leung, "Artificial Bandwidth Extension of Telephony Speech by Data Hiding," in *2005 IEEE International Symposium on Circuits and Systems*, Kobe, Japan, May 23–26 2005, pp. 3151–3154 Vol. 4.

[12] S. Chen, H. Leung, and H. Ding, "Telephony Speech Enhancement by Data Hiding," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 1, pp. 63–74, February 2007.

[13] P. Nizampatnam and T. K. Kumar, "Evaluation of Bandwidth Extension of Telephony Speech by Data Hiding in Three Languages," in *2015 International Conference on Microwave, Optical and Communication Engineering (ICMOCE)*, Bhubaneswar, India, December 18–20 2015, pp. 1–4.

[14] Z. Deng, Z. Yang, and L. Deng, "A Real-time Secure Voice Communication System Based on Speech Recognition," in *Systems and Networks Communications, 2006. ICSNC '06. International Conference on*, Tahiti, French Polynesia, October 29 November 03 2006, pp. 22–22.

[15] T. Xu, Z. Yang, and X. Shao, "Novel Speech Secure Communication System Based on Information Hiding and Compressed Sensing," in *2009 Fourth International Conference on Systems and Networks Communications*, Porto, Portugal, September 20–25 2009, pp. 201–206.

[16] L. Diez-Del-Rio, S. Moreno-Perez, R. Sarmiento, J. Parera, M. Veiga-Perez, and R. Garcia-Gomez, "Secure Speech and Data Communication Over The Public Switching Telephone Network," in *Acoustics, Speech, and Signal Processing, 1994. ICASSP-94., 1994 IEEE International Conference on*, vol. ii, Adelaide, South Australia, April 19–22 1994, pp. II/425–II/428 vol.2.

[17] M. Zimmermann and K. Dostert, "A Multipath Model for The Powerline Channel," *IEEE Transactions on Communications*, vol. 50, no. 4, pp. 553–559, April 2002.

[18] S. Galli, "A Novel Approach to The Statistical Modeling of Wireline Channels," *CoRR*, vol. abs/1101.1915, 2011. [Online]. Available: http://arxiv.org/abs/1101.1915