Zamanla İlintili Kanallarda Güvenli MISO Sistemlerinin Başarımı
Performance of Limited Feedback Secure MISO Systems in Temporally Correlated Channels

Özgecan Özdoğan ve Berna Özbek
Elektronik ve Haberleşme Mühendisliği Bölümü
İzmir Yüksek Teknoloji Enstitüsü
İzmir, Türkiye
ozgecanozdogan@iyte.edu.tr, bernaozbek@iyte.edu.tr

Güneş Karabulut Kurt
Telsiz Haberleşme Araştırma Laboratuvarı (THAL)
İstanbul Teknik Üniversitesi
İstanbul, Türkiye
gkurt@itu.edu.tr

***Özetçe* — Bu çalışmada, zamanla ilintili kanallarda çoklu anten iletimi ile güvenli haberleşme problemi göz önüne alınmıştır. Güvenlik kapasitesinde kazanç elde etmek için vericide hedeflenen alıcının kablosuz kanal durum bilgisi gereklidir. Bu çalışmada, güvenli çoklu antenli sistemler için kablosuz kanalın zamanda ilintisini kullanan diferansiyel kod kitapçığı içeren bir geribesleme linki sunulmuştur. Farklı kanal ilinti değerleri için güvenlik kapasite performansı gösterilmiştir.**

***Anahtar Kelimeler*—zamansal ilintili kanallar, güvenlik kapasitesi, fiziksel katman güvenliği, diferensiyal kod kitapçığı.**

***Abstract*— We consider the problem of secure communication with multiple antenna transmission in temporally correlated channels. In order to achieve a secrecy gain, a channel state information of the intended receiver at the transmitter is required. In this work, we present a limited feedback link by employing differential codebook which utilizes the temporal correlation properties of the wireless channels for a secure multi-antenna system. The secrecy performances are shown for different channel correlations.**

***Keywords*—temporally correlated channels, secrecy capacity, physical layer security, differential codebook.**

I. Giriş

Telsiz haberleşme sistemlerinde verici ile alıcı arasındaki güvenli haberleşme, telsiz ortamının açık yapısından dolayı gizli dinleyicilere karşı hassastır. Fiziksel katman güvenliği yöntemleri, bu sorunu çözmek için geleneksel yüksek karmaşıklık içeren şifreleme tabanlı güvenlik yöntemlerine yardımcı olarak ortaya çıkmıştır. Ağ modelinin yüksek katmanlarında uygulanan bu şifreleme yöntemlerinden farklı olarak, kanalın raslantısal özelliklerini kullanmaktadır.

Fiziksel katmanda güvenlik konusunda yapılmış olan ilk çalışmalardan biri olan [1]'de, güvenli haberleşme kapasitesi tanımı ortaya atılmıştır. Telsiz haberleşme ağlarının yaygınlaşmasından sonra, farklı kanal modelleri için fiziksel katman güvenlik yöntemleri üzerine çalışmalar yapılmıştır. Bilgi kuramı yaklaşımı ile Gaussian kanalların [2] ve sönümlü kanalların [3]–[5] incelendiği çalışmalardan sonra güvenli haberleşme çoklu antenli kablosuz haberleşme sistemlerine de uygulanmıştır [6], [7]. Anten dizilerinin ve hüzme yönlendirme yöntemlerinin kullanımı ile güvenlik seviyesi arttırılabilmektedir. İlk hüzme yönlendirme çalışmaları, işaret boğma saldırılarını (jamming) önlemek üzere [8]'de ele alınmıştır. Daha sonra [9]'da sinyale yapay gürültü (artificial noise) eklenmesinin sistem güvenliğine etkileri incelenmiştir. Bu yaklaşımda yapay gürültü, yetkili alıcının dışındaki uzaya gönderilmekte ve yetkili alıcı bu gürültüden etkilenmemektedir. Bu durumda yeterli çıkış gücü kullanılırsa gizli dinleyicinin (eavesdropper) kanalı, yetkili alıcının kanalından daha iyi olsa bile güvenlik sağlanabilmektedir.

Gizli dinleyicinin kanal durum bilgisinin vericide mevcut olup olmaması da güvenli haberleşme kapasitesi açısından önemli bir noktadır. Bu konuda yapılan çalışmaların bazılarında [12], verici ile gizli dinleyici arasındaki kanal bilgisinin tam olarak bilindigi varsayılmıştır. Bunun yanı sıra, gizli dinleyici hakkında yön bilgisi gibi bazı kanal özelliklerini bilmek de mümkün olabilir [13]. Gizli dinleyici saldırıları genelde pasif türde olduğundan, vericide gizli dinleyicinin kanal durum bilgisinin var olduğunu varsayılması her zaman pratik bir çözüm değildir.

Vericideki kanal durum bilgisi (CSIT), anten dizileri ve hüzme yönlendirme yöntemleriyle kullanıcı kapasitesi arttırlamasında önemli bir role sahiptir. Vericide alıcının kanal durum bilgisinin tam olarak bilinmesi durumunda güvenlik kapasitesinde önemli kazançlar sağlanabilmektedir [10]. Fakat pratikte kullanılan sistemlerde geri besleme kanalı sınırlı olduğundan mükemmel kanal durum bilgisine sahip olmak oldukça zordur. Bu durum kanalı nicemleyen kod kitapçıklarının kullanılması zorunluluğunu doğurmuştur. Uygun bir kod kitapçığı çoğunlukla kanal istatistiklerini göz önünde bulundurmaktadır. Biz bu çalışmamızda, diferansiyel kod kitapçığının [11] güvenlik kapasitesine etkilerini inceledik. Diferansiyel kod kitapçığı, sönümlü kanalların zamansal ilintisini (korelasyon) kullanarak sistem performansını arttırmayı hedefleyen bir limitli geri besleme yöntemi başarımlarını gösterdik.

978-1-5090-6494-6/17/$31.00

II. SISTEM MODELI

Ele aldığımız sistem modeli bir verici, bir alıcı ve bir gizli dinleyiciden oluşmaktadır. Bu çalışma, gizli dinleyicinin kanal durum bilgisinin bilinmediği durumu incelenmektedir. Vericide N_t, alıcıda tek ve gizli dinleyicide N_e anten bulunmaktadır. Kullanıcıya yollanmak istenen mesajlar, gizli dinleyici tarafından çözülmesini engellemek adına, yapay gürültü ile maskelenmiştir.

τ anındaki mesaj sinyali,

$$\mathbf{x}_\tau = \mathbf{w}_\tau s + \mathbf{Q}_\tau \mathbf{a}, \tag{1}$$

şeklinde ifade edilebilir. Burada s iletilmek istenen bilgi sinyali iken $\mathbf{a} \in \mathcal{C}^{(N_t-1)\times 1}$ yapay gürültü vektörüdür. Ayrıca, $\mathbf{w}_\tau \in \mathcal{C}^{N_t \times 1}$ diferansiyel kod kitapçığı yardımıyla verici tarafından τ anında oluşturulan hüzmeleme vektördür. $\mathbf{Q}_\tau \in \mathcal{C}^{(N_t-1)\times N_t}$ matrisi ise $\mathbf{w}_\tau$'nun boş uzayında (null space) oluşturulmuş yapay gürültünün hüzmeleme vektörüdür. $\mathbf{Q}_\tau$'nun boş uzayda oluşturulmasının sebebi, kullanıcının sinyalinin bu gürültüden etkilenmesini olabildiğince azaltmaktır.

Kullanıcı ve gizli dinleyici tarafından alınan sinyaller ise,

$$y_\tau = \mathbf{h}_\tau^H \mathbf{w}_\tau s + \mathbf{h}_\tau^H \mathbf{Q}_\tau \mathbf{a} + n_\tau, \tag{2}$$

$$\mathbf{y}_\tau^e = \mathbf{H}^e \mathbf{w}_\tau s + \mathbf{H}^e \mathbf{Q}_\tau \mathbf{a} + \mathbf{n}_\tau^e, \tag{3}$$

olarak ifade edilir. Kullanıcının kanal vektörü $\mathbf{h}_\tau \in \mathcal{C}^{N_t \times 1}$ ile gösterilirken, $\mathbf{H}^e \in \mathcal{C}^{N_e \times N_t}$ gizli dinleyicinin kanal vektörüne karşılık gelmektedir. Burada gizli dinleyicinin kanalı $\mathcal{CN}(0, \mathbf{I}_{N_t})$ olarak modellenmiştir. Bu bölümde durağan olmayan kanal modeline sahip yetkili kullanıcının kanal durum bilgisinin vericiye iletilmesi aşamasında nicemlenmesi için diferansiyel kod kitapçığı kullanılmıştır. Bu kanal modelinde kanalın bir önceki zaman çerçevesi ile ilintili olduğu durum incelenmiştir. Yetkili kullanıcıdaki ve gizli dinleyicideki karmaşık toplanır beyaz Gauss gürültüleri (AWGN) sırasıyla $\mathcal{CN}(0, \sigma^2)$ ve $\mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$ dağılımlarına sahiptir.

Diferansiyel kod kitapçığı, sönümlü kanalların zamansal ilintisini (korelasyon) kullanarak sistem performansını arttırmayı hedefleyen bir limitli geri besleme yöntemidir. Bu yöntemde, vericinin hüzmeleme vektörünün bir zaman birimi önceki durumunu bildiği ve kanalın zamanda ilintili olduğu varsayılır. Vericideki bir önceki kanal yön bilgisinin ve mevcut andaki normalize edilmiş kanal vektörünün yönsel değişimleri kullanılarak yeni hüzmeleme vektörü oluşturulur. Ardışık zaman aralıklarında gerçekleşen bu yönsel değişimler Grassmann manifold'unun kesellerine (geodesics) karşılık gelmektedir.

Gizli dinleyicinin kanalı ile hiçbir bilgi bilinmediği durumda Diferansiyel kod kitapçığı kullanılarak oluşturulan kod kitapçığı ile elde edilen hüzmeleme vektörlerine göre yetkili kullanıcıda ve gizli dinleyicide τ anında elde edilen sinyal gürültü oranları (SNR) sırasıyla aşağıda verilmiştir:

$$SNR_\tau = \frac{\alpha |\mathbf{h}_\tau^H \mathbf{w}_\tau|^2}{\frac{1-\alpha}{N_t-1} |\mathbf{h}_\tau^H \mathbf{Q}_\tau|^2 + \frac{1}{\gamma}}, \tag{4}$$

$$SNR_\tau^e = \alpha \left(\mathbf{H}^e \mathbf{w}_\tau\right)^H \left(\frac{1-\alpha}{N_t - 1} (\mathbf{H}^e \mathbf{Q}_\tau)(\mathbf{H}^e \mathbf{Q}_\tau)^H \right)^{-1} (\mathbf{H}^e \mathbf{w}_\tau), \tag{5}$$

şeklinde yazılabilir. Burada, $\gamma = \frac{P}{\sigma^2}$'dir ve P toplam güce karşılık gelmektedir. α güç paylaşım parametresidir ve değeri $(0, 1)$ aralığında değişmektedir. α'nın artması ile bilgi sinyaline ayrılan güç artarken, yapay gürültüye ayrılan güç azalmaktadır. Bu durum güvenlik kapasitesini etkilemektedir. Vericideki farklı kanal durum bilgisinin (tam ya da nicemsel) mevcudiyetine göre α parametresinin değeri optimal kanal güvenlik kapasitesini sağlayacak şekilde seçilmelidir.

Güvenlik kapasitesi, vericiden yetkili alıcıya güvenli bir şekilde iletilebilen maksimum bilgi miktarı olarak tanımlanır. Bu değer, alıcı ile gizli dinleyicinin kanal kapasitelerinin farkları olarak ifade edilmektedir [1]. Böylece elde edebileceğimiz ortalama güvenlik kapasitesi,

$$C_\tau = \max\{(\mathrm{E}\left\{\log_2(1 + SNR_\tau)\right\} - \mathrm{E}\left\{\log_2(1 + SNR_\tau^e)\right\}), 0\}^+, \tag{6}$$

olarak bulunur.

III. DIFERANSIYEL KOD KITAPÇIĞI

Durağan olmayan kanallarda, kanalın zamanda ilintisinin modellenmesi için kullanıcı kanalının zamanda değişimi Gauss-Markov süreci olarak tanımlanır:

$$\mathbf{h}_\tau = z \mathbf{h}_{\tau-1} + \sqrt{1 - z^2} v_\tau. \tag{7}$$

Burada v_τ karmaşık normal Gauss dağılımına sahip inovasyon sürecini belirtmektedir. z ise kanalın zamansal ilinti katsayısı olup $(0 \leq z \leq 1)$ kanalın ardışık zaman aralıklarında birbiriyle ilişkisinin ölçütüdür. Eğer z büyük bir değere sahipse, bu durum $\mathbf{h}_{\tau-1}$ vektörü ile $\mathbf{h}_\tau$ vektörünün ilintisinin yüksek olduğu anlamına gelir. Beklendiği üzere, yüksek z değerleri için diferansiyel kod kitapçığının performansı daha iyi olmaktadır.

Diferansiyel kod kitapçığının algoritması aşağıdaki gibi gerçekleştirilmiştir [11]:

- $\tau = 0$ anında:
  İlk zaman dilimindeki kanal bilgisi rasgele vektör nicemleyici kullanılarak oluşturulan başlangıç kod kitapçığı kullanılarak, minimum uzaklığa göre nicemlenir. Rasgele vektör nicemleyicisi, $\zeta = \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^B}\} \in \mathcal{C}^{N_t \times 2^B}$ formundadır ve B kullanılan nicemeleme biti sayısını ifade etmektedir.

$$j^* = \arg \min_{1 \leq j \leq 2^B} |1 - \mathbf{g}_0{}^H \mathbf{c}_j|. \tag{8}$$

Burada, $\mathbf{g}_0 = \frac{\mathbf{h}_0}{||\mathbf{h}_0||}$ yetkili kullanıcının kanal yön vektörünün $(\mathbf{h}_\tau)$ başlangıç anında normalize edilmiş halidir. Böylece hüzmeleme vektörü, minimum uzaklık kriteri kullanılarak aşağıdaki gibi elde edilir:

$$\mathbf{w}_0 = \mathbf{c}_{j^*}. \tag{9}$$

- $\tau = 1, 2, ...\tau_{max}$ anları için:
  Önceden belirlenmiş temel kutupsal kap (polar-cap) diferansiyel kod kitapçığı kullanılır. Temel kutupsal kap diferansiyel kod kitapçığı $\tilde{\mathcal{W}}^\tau$'nin oluşturulması için aşağıdaki yapı kullanılmıştır:

$$\tilde{\mathcal{W}}^\tau = \left\{ \tilde{\mathbf{w}}_{1,\tau}, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \mathbf{f_2} \end{bmatrix}, \ldots, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \mathbf{f_{2^B}} \end{bmatrix} \right\}, \tag{10}$$

$\tilde{\mathbf{w}}_{1,\tau}$ herhangi bir birim vektör olabilir. Bu çalışmada $\tilde{\mathbf{w}}_{1,\tau} = [1, 0, \ldots, 0]^T$ olarak seçilmiştir. Kutupsal kap boyutunu belirten δ_τ, sistem performansını önemli ölçüde etkilemektedir. Bu parametre uyarlamalı ya da sabit olarak ayarlanabilir. $\tilde{\mathbf{w}}_{1,\tau}$ ve δ_τ'nun seçilmesiyle kutupsal kabın çevresine yerleştirilmiş kod sözcükleri oluşturulabilir. Diğer kod sözcükleri karmaşık Grasmannian çizgi paketlemesi vektörleri (complex Grassmannian Line Packing), $\{\mathbf{f_2}, \mathbf{f_3}, \ldots, \mathbf{f}_{2^B}\}$ ile oluşturulmuştur. Burada $\mathbf{f}_i \in \mathcal{C}^{(N_t-1)\times 1}$'dır. Burada kullanılmasının sebebi Grasmannian çizgi paketlemesi kod kitapçığının bağımsız ve aynı dağımlı Rayleigh sönümlemeli kanallar için bilinen en iyi yöntem olmasıdır.
Kutupsal kap kod kitapçığı bir kere oluşturulduktan sonra farklı τ anları için tekrar tekrar kullanılabilir. Kod kitapçığının belirlenmesinden sonra, kullanıcı ve verici $\tilde{\mathbf{w}}_{1,\tau}$ vektörünü bir önceki anın nicemlenmiş kanal yön vektörü olan $\hat{\mathbf{h}}_{\tau-1}$ yönüne çeviren rotasyon matrisi, $\mathbf{R}_{\hat{h}_{\tau-1}}$'i oluşturur.
Rotasyon fonksiyonu aşağıdaki gibi tanımlanır:

$$\mathbf{r} : \mathcal{B}_{\delta_\tau}(\tilde{\mathbf{w}}_{1,\tau}) \mapsto \mathcal{B}_{\delta_\tau}(\hat{\mathbf{h}}_{\tau-1}), \tag{11}$$

$$\hat{\mathbf{h}}_{\tau-1} = \mathbf{r}(\hat{\mathbf{h}}_{\tau-1})\tilde{\mathbf{w}}_{1,\tau}, \tag{12}$$

$$= \mathbf{R}_{\hat{h}_{\tau-1}}\tilde{\mathbf{w}}_{1,\tau}. \tag{13}$$

Rotasyon matrisinin oluşturulabilmesi için Householder transformasyonu kullanılmıştır:

$$\mathbf{v} = \tilde{\mathbf{w}}_{1,\tau} - \hat{\mathbf{h}}_{\tau-1}, \tag{14}$$

$$\mathbf{R}_{\hat{h}_{\tau-1}} = \mathbf{I} - \frac{\mathbf{v}\mathbf{v}^\dagger}{\mathbf{v}^\dagger\tilde{\mathbf{w}}_{1,\tau}}. \tag{15}$$

Rotasyon matrisinin Householder transformasyonuyla yukarıdaki gibi elde edilmesinden sonra, rotasyon matrisi ile bütün temel kutupsal kap kitapçığı döndürülür.

$$\mathcal{W}^\tau = \left\{\mathbf{R}_{\hat{h}_{\tau-1}}\tilde{\mathbf{w}}_{j,\tau}; \quad j = 1, 2, ..., 2^B\right\}. \tag{16}$$

Temel kutupsal kod kitapçığının her bir kolonu rotasyon matrisi ile çarpılarak döndürülmüş olan yeni kod kitapçığı $\mathcal{W}^\tau = \left\{\mathbf{w}_{1,\tau}, \mathbf{w}_{2,\tau}, \ldots, \mathbf{w}_{2^B,\tau}\right\}$ oluşturulmuştur. Kullanıcı τ anındaki kanal bilgisini bu kod kitapçığına göre nicemler ve vericiye yollar. Verici ise bu bilgiyi hüzmeleyici vektörü $\mathbf{w}_\tau$ olarak kullanır.

$$j^* = \arg\min_{1<k<2^B} |1 - \mathbf{g}_\tau{}^H\mathbf{w}_{j,\tau}|, \tag{17}$$

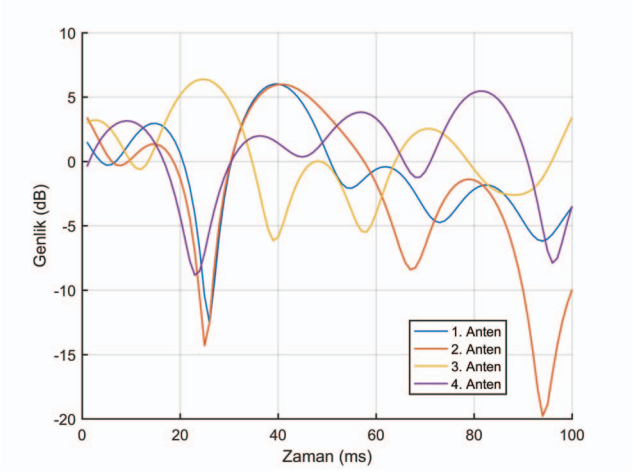
$$\mathbf{w}_\tau = \mathbf{w}_{j^*,\tau}. \tag{18}$$

- $\tau = \tau_{max} + 1$
  Belirlenen τ_{max} süresinden sonraki zamanlarda işlemler sıfırlanır. τ_{max} süresi kanalın tutarlı olduğu süre (coherence time) olarak seçilebilir.

IV. Benzetim Sonuçları

Diferansiyel kod kitapçığı kullanılan sistemin güvenlik kapasitesi performansı Monte Carlo benzetimleri ile elde edilmiştir. Benzetimler için vericideki anten sayısı $N_t = 4$ seçilirken, kullanıcıdaki ve gizli dinleyicideki anten sayıları sırasıyla $N_r = 1$ ve $N_e = 2$'dir. Rayleigh sönümlü kanal Jakes modeline dayanılarak tasarlanmıştır. Kanal ilinti parametresi $z = J_0(2\pi f_D T)$ ile hesaplanır. J_0 birinci tipten sıfırıncı derece Bessel fonksiyonuna karşılık gelir. Maksimum Doppler frekansı $f_D = \frac{vf_c}{c}$, $f_c = 2.4$ GHz, $T = 5$ms olarak verilmiştir. Benzetim çalışmalarında $v = 0.45$km/sa, $v = 2.25$km/sa ve $v = 4.5$km/sa olarak seçilmiştir. Bu değerlere karşılık gelen $f_D = 1, 5, 10$ Hz olup ilinti değerleri $z = 0.9998, 0.9938, 0.9755$'dır.

Benzetim çalışmalarında karşılaştırma için kullanılan Tam CSI ifadesi, vericide kanal durum bilgisinin mükemmel bir şekilde elde edilebilmesidir. Başlangıçta tam CSI durumu ise, başlangıç anındaki kanal yön bilgisinin mükemmel bir şekilde vericide bilinmesi ve daha sonra bu bilginin zaman içerisinde güncellenmemesine karşılık gelmektedir. Rasgele vektör nicemleyicileri (RVQ) literatürde sıklıkla karşılaştırmalar için kullanılmakta olup matematiksel analizinin kolaylığından dolayı tercih edilmektedir.

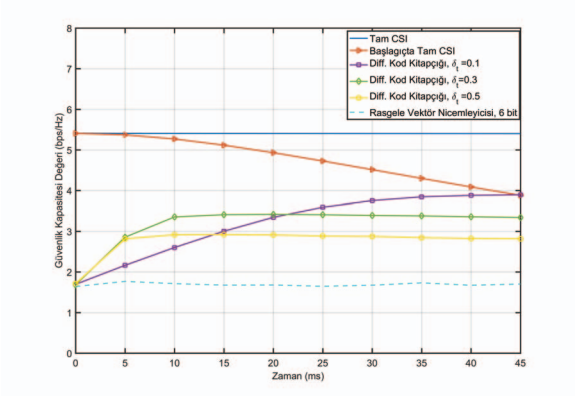


Şekil 1: Kanal genlik değerinin zamanla değişimi.

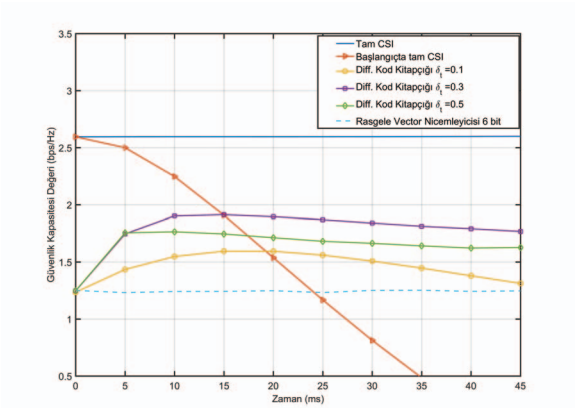
Şekil 1'de kanal genlik değerinin zamanla değişimi $f_D = 5$ için gösterilmiştir. Şekil 2, Şekil 3 ve Şekil 4'de farklı hız değerlerinde $\gamma = 10$dB için güvenlik kapasitesi sonuçları gösterilmiş ve diferansiyel kod kitapçığının RVQ'ya göre çok daha iyi sonuçlar verdiği gözlemlenmiştir. Şekil 2'de görüldüğü üzere, düşük hızlarda (v=0.45 km/sa) diferansiyel kod kitapçığı kanal değişimlerini başarılı bir şekilde takip edebilmektedir. Farklı kutupsal kap boyutu δ_τ için kanalı takip edebilme hızı ve performansı değişmektedir.

Şekil 4'de görüldüğü üzere, daha yüksek hızlarda sadece başlangıçta tam kanal durum bilgisine sahip olmak yeterli değildir. Bu durumda güvenli haberleşme sağlanamamaktadır. Ayrıca, δ_τ 'nun küçük seçilmesi diferansiyel kod kitapçığının kanal değişimlerini takip edebilmesini engellemektedir. δ_τ'nun boyutu hıza göre en iyi güvenlik kapasitesini sağlayacak şekilde seçilmelidir.

Şekil 5 ise $\gamma = 20$dB için güvenlik kapasitesi sonuçları gösterilmiş ve diferansiyel kod kitapçığının kanalın zamanla değişimi takip ettiği ve güvenlik kapasitesinin hemen hemen aynı kaldığı gösterilmiştir.



Şekil 2: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 10$dB, $f_D = 1$Hz.



Şekil 3: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 10$dB, $f_D = 5$ Hz.

V. Sonuç

Bu çalışmada, güvenli haberleşme problemi çoklu antenli sistemlerde zamanda ilintili kanallar için incelenmiştir. Pratik sistemler göz önünde bulundurularak, alıcının kanal yön bilgisinin vericide nicemlenmiş olduğu durum göz önüne alınmıştır. Nicemlemede kullanılan diferansiyel kod kitapçığı, sönümlü kanalların zamansal ilintisini kullanılarak güvenli haberleşme sistem performansı farklı kanal ilintisi değerleri için elde edilmiştir. Diferansiyel kod kitapçığı düşük hızlarda önemli ölçüde güvenlik kapasitesi kazancı sağlamaktadır.

Bilgilendirme

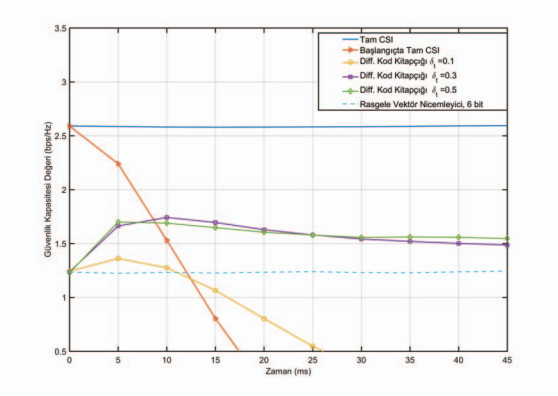
Bu çalışma 114E626 nolu Tübitak-Ardeb-1005 projesi kapsamında desteklenmektedir.

Kaynaklar

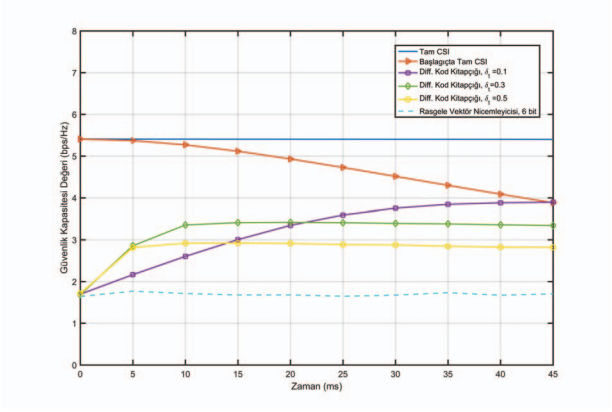
[1] A. D. Wyner, "The Wire-tap Channel", The Bell System Technical Journal, vol. 54, pp. 1355-1387, (1975).

[2] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," IEEE Trans. Inf. Theory, vol. 37, pp. 634–638, May 1991.

[3] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in 2006 IEEE Inter. Sym. Inf. Theory, pp. 356–360, July 2006.



Şekil 4: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 10$dB, $f_D = 10$Hz.



Şekil 5: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 20$dB, $f_D = 1$Hz.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, pp. 4687–4698, Oct 2008

[5] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, pp. 2470–2492, June 2008.

[6] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," IEEE Trans. Commun., vol. 58, pp. 1877–1886, June 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, pp. 4961–4972, Aug 2011.

[8] G. Noubir,"On Connectivity in Ad Hoc Network Under Jamming Using Directional Antennas and Mobility," Int. Conf. Wired and Wireless Internet Commun., pp. 54-62, (2004).

[9] S. Goel, R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, June 2008

[10] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033-4039, Sep. 2009.

[11] J. Choi, B. Clerckx, N. Lee and G. Kim, "A New Design of Polar-Cap Differential Codebook for Temporally/Spatially Correlated MISO Channels," in IEEE Transactions on Wireless Communications, vol. 11, no. 2, pp. 703-711, February 2012.

[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, pp. 3088–3104, July 2010.

[13] X. Chen,R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback" IEEE Wireless Communications letters, Vol. 2,No. 5,October 2013