Güvenli çoklu kullanıcılı MISO sistemlerde eşik değerine dayalı kullanıcı seçim performansı
Performance of secure multiuser MISO systems with threshold based user selection

Özgecan Özdoğan*, Berna Özbek* Güneş Karabulut Kurt†
* Elektrik ve Elektronik Mühendisliği Bölümü
İzmir Yüksek Teknoloji Enstitüsü, İzmir, Türkiye
†Telsiz Haberleşme Araştırma Laboratuvarı (THAL)
İstanbul Teknik Üniversitesi,İstanbul, Türkiye
{ozgecanozdogan, bernaozbek}@iyte.edu.tr, gkurt@itu.edu.tr

***Özetçe* —Fiziksel katmanda güvenlik metotları, telsiz ağların yapısından kaynaklanan güvenlik sorunlarının çözülmesi adına umut vaat etmektedir. Bu çalışmada, çoklu kullanıcılı çoklu antenli ve gizli dinleyici bulunduran bir sistem modeli göz önünde bulundurulmuştur. Gizli dinleyicinin pasif olduğu ve kanal bilgisinin (CSI) baz istasyonunda mevcut olmadığı varsayılarak, gizli dinleyicinin algısını bozmak için yetkili kullanıcının boş uzayına yapay gürültü eklenmiştir. Güvenli haberleşme sağlanmasında, kullanıcıların kanal durum bilgisi sistem performansı açısından önemlidir. Fakat her kullanıcının kanal bilgisini baz istasyonuna iletmesi haberleşme sistemindeki yükü (overhead) arttırır. Bu yükü azaltmak amacıyla alıcı tarafında eşik değerine bağlı kullanıcı seçimi algoritması uygulanarak, bu seçimin güvenlik kapasitesi değeri üzerine etkilerini incelenmiştir.**

Anahtar Kelimeler—güvenli haberleşme, çoklu kullanıcılı çoklu antenli sistemler, yapay gürültü

***Abstract*—Physical layer security is a promising approach to enable secure communications by considering the characteristics of wireless channels. In this work, we consider a multiple antenna multiuser system with an eavesdropper which is passive and its channel state information (CSI) is not available at transmitter. We we add artificial noise (AN) in the null space of legitimate user to disturb reception of eavesdropper. For the sake of ensuring secure communication, CSI has great impact on system performance. However, in order to estimate the channel of all users at transmitter, sending pilot signals from all these users increases the system overhead. We perform a threshold based user selection at the receiver side to reduce this overhead. Also, we investigate the effects of the proposed user selection on the secrecy capacity.**

Keywords—secure communications, multiuser multiantenna systems, artificial noise

I. GIRIŞ

Telsiz ağların giderek yaygınlaşması ve uygulama alanlarının çeşitlenmesiyle birlikte güvenlik problemlerinin önemi daha da artmaktadır. Veri iletişiminde taşınabilir ve mobil ağlar, askeri kullanımdan son kullanıcıya kadar ulaşmış, özel bilgi taşınması sebebiyle de güvenlik ihtiyacı kaçınılmaz olmuştur. Fiziksel katmanda güvenlik, bu ihtiyacı karşılamak için kablosuz haberleşme sistemlerinde önem kazanmıştır. Fiziksel katmanda güvenlik konusunda yapılmış olan çalışmaların büyük bir kısmı [1] çalışmasına dayanmaktadır. Bunu takip eden çalışmalarda, öncelikle bilgi kuramı yaklaşımları kullanılmış, güvenli kanal kapasitesi (secret channel capacity) tanımı ortaya atılarak bu kapasitenin sınır değerlerinin bulunması ve arttırılması hedeflenmiştir. Güvenli haberleşme çoklu antenli kablosuz haberleşme sistemlerine de uygulanmıştır [2], [3]. Bilgi kuramı yaklaşımı ile güvenlik uygulamaları kanalın mükemmel bilindiği varsayımına dayanmaktadır ki, bu da pratikte her zaman mümkün değildir.

Anten dizilerinin ve hüzme yönlendirme yöntemlerinin kullanımı ile güvenlik seviyesi arttırılabilmektedir. İlk hüzme yönlendirme çalışmaları, işaret boğma saldırılarını (jamming) önlemek üzere [4]'de ele alınmıştır. Daha sonra [5]'de 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 dinleyicin kanal bilgisi hem tek kullanıcılı hem de çoklu kullanıcılı sistemlerin fiziksel katman güvenliği açısından oldukça önemli bir noktadır. Tekli kullanıcılı sistem çalışmalarının bazılarında [6], [7], [8], verici ile gizli dinleyici arasındaki kanal bilgisinin tam olarak bilindiği varsayılmıştır. Bunun yanı sıra, gizli dinleyici hakkında yön bilgisi gibi bazı kanal özelliklerini bilmek de mümkün olabilir [9], [10]. Gizli dinleyici saldırıları genellikle pasif saldırı türünde olduğundan sistemin gizli dinleyici kanal bilgisine sahip olması her zaman mümkün değildir. Çoklu kullanıcılı çoklu antenli sistemler için, gizli dinleyici kanal bilgisinin vericide mevcut olup olmaması durumuna göre güvenli kanal kapasitesi çeşitli çalışmalarda elde edilmiştir. Gizli dinleyicinin kanal bilgisine yalnızca istatistiksel olarak sahip olunabilen durum [11]'de tartışılmış, kanal koşul parametresinin ve geri besleme miktarının sistem performansına çok büyük etkisi olduğundan bahsedilmişitir.

978-1-5090-1679-2/16/$31.00

Benzer olarak, gizli dinleyicinin sınırlı kanal bilgisinin güvenli kanal kapasitesine etkileri [12] ve [13]'de ele alınmıştır. [13]'de ise, farklı hüzmeleme teknikleri kullanımının güvenli kanal kapasitesine etkileri karşılaştırılmıştır. Bu çalışmada, gizli dinleyicinin kanal durum bilgisinin vericide bilinmediği durumu göz önünde bulundurduk. Literatürdeki çoklu kullanıcılı çoklu antenli sistemlerde tüm kullanıcıların kanal bilgisini baz istasyonuna ilettiği varsayılmaktadır.

Çoklu kullanıcılı sistemlerde tüm kullanıcılara ait kanalları elde etmek, haberleşme sağlanacak kullanıcının seçimini çoklu kullanıcı çeşitlemesini ortaya çıkaracak şekilde yapmak ve bu kullanıcı ile güvenli haberleşme sağlamak önemlidir. Kanal durum bilgisinin (CSI) vericide bilinmesi için, kullanıcılar baz istasyonuna kanal durum bilgilerini iletirler. Bu çalışmada verici tarafında haberleşme için seçilme olasılığı düşük olan kullanıcıların kanal bilgilerini iletmesi, alıcı tarafında yapılan eşik değerine dayalı kullanıcı seçimi ile önlenmiştir. Gizli dinleyici pasif olduğundan, bu seçimin güvenli haberleşme sistem performansı üzerine etkisi vericide gizli dinleyicinin kanal bilgisinin bilinmediği durumda incelenmiştir. Sistem yükü (overhead) önerilen algoritma yardımıyla tüm kullanıcıların kanal bilgisi yollaması engellenerek önemli ölçüde azaltılmıştır.Alıcı tarafında gerçekleştirilen bu seçim kriterinin uygulandığı sistemin güvenlik kapasite değerinin, bütün kullanıcıların baz istasyonuna kanal bilgilerini gönderdiği durumdaki güvenlik kapasite değeriyle aynı değerlere ulaştığı gözlemlenmiştir.

II. Sistem Modeli

Bu çalışmada, bir gizli dinleyici (Eve) ve K kullanıcının bulunduğu çoklu antenli çoklu kullanıcılı bir sistem incelenmiştir. N_t verici antene sahip baz istasyonu eşzamanlı olarak bağımsız gizli mesajları, seçilmiş bir kullanıcıya iletmeyi amaçlamaktadır. Buna paralel olarak, verici gizli dinleyicinin algısını bozmak için dış uzaya yapay gürültü iletmektedir. Hem gizli dinleyici hem de kullanıcılar tek bir antene sahiptirler.

Çoklu girişli tek çıkışlı tek gizli dinleyicili (Eve) sistemlerdeki güvenlik kapasitesi değeri, yetkili kullanıcıların kanal bilgisinin vericide tam ve nicemlenmiş (quantized) olarak bilindiği iki farklı durum için irdelenmiştir. Bizim varsayımlarımıza göre, vericide yetkili kullanıcıların kanal durum bilgisi mevcuttur. Fakat, verici gizli dinleyicinin kanal durum bilgisi hakkında hiç bir veriye sahip değildir. Bu varsayımlar pratik durumda karşılaşılması kuvvetle muhtemel senaryoya uygun olarak oluşturulmuştur.

Çoklu kullanıcılı sistemlerde öncelikle en iyi kanal kazancına sahip kullanıcının (Bob) seçimi yapılır:

$$k = \arg\max_{j} \left\|\mathbf{h}_j\right\|^2. \tag{1}$$

Burada yetkili kullanıcı Bob'un kanalı $\mathbf{h}_k \in \mathcal{C}^{N_t \times 1}$ olarak ortalaması sıfır varyansı 1 olan Gauss dağılımı ile modellenir.

Seçilen k kullanıcısı için yapay gürültü eklenerek iletilen sinyal vektörü $\mathbf{x}_k$:

$$\mathbf{x}_k = \mathbf{f}_k s_k + \mathbf{Q}\mathbf{a}, \tag{2}$$

olarak ifade edilmektedir.

Burada s_k iletilmek istenen mesaj bilgisini içeren $E\{|s_k|^2\} \leq P_s$ gücündeki sinyali belirtmektedir. $\mathbf{f}_k \in \mathcal{C}^{N_t \times 1}$ ise verici tarafındaki hüzmeleme vektörüdür ve $\mathbf{a} = [a_1, a_2, \ldots, a_{Nt-1}]^T$ rastgele Gaussian vektör olan, aynı zamanda $E\{||\mathbf{a}||^2\} \leq P_a$ gücüne sahip yapay gürültüdür (AN). $\mathbf{Q} \in \mathcal{C}^{N_t \times N_t - 1}$, AN altuzayını oluşturan birim dik sütunlu AN hüzmeleyecisidir. $\mathbf{f}_k$ ve $\mathbf{Q}$ hüzmeleri mevcut kanal durum bilgisine göre belirlenmiştir.

Yetkili kullanıcı ve gizli dinleyici tarafından alınmış sinyaller sırasıyla aşağıda ifade edilmiştir:

$$y_k = \mathbf{h}_k^\dagger \mathbf{f}_k s_k + \mathbf{h}_k^\dagger \mathbf{Q}\mathbf{a} + z_k, \tag{3}$$

$$y_e = \mathbf{h}_e^\dagger \mathbf{f} s + \mathbf{h}_e^\dagger \mathbf{Q}\mathbf{a} + z_e, \tag{4}$$

Burada gizli dinleyici Eve'in kanalı $\mathbf{h}_e \in \mathcal{C}^{N_t \times 1}$ olup ortalaması sıfır ve varyansı 1 olan Gauss dağılımı ile modellenir. z_k ise Bob'daki ortalaması 0, varyansı σ^2 olan karmaşık toplamsal beyaz Gauss gürültüsünü (AWGN) ifade etmektedir. Bunun yanı sıra, z_e de ortalaması 0, varyansı σ^2 olan Eve'deki AWGN'ye karşılık gelmektedir.

Bob'un kanal yön bilgisi (CDI), $\mathbf{g}_k = \frac{\mathbf{h}_k}{\|\mathbf{h}_k\|}$ şeklinde ifade edilirken $\|\mathbf{h}_k\|$ kanal kalite bilgisini (CQI) göstermektedir.

Denklem (3) de tanımlanan hüzmeleyiciler $\mathbf{f} = \mathbf{g}_k^H$ ve $\mathbf{Q} = \mathbf{N}_g$ olarak belirlenmiştir ve $\mathbf{N}_g$'nin sütunları $\mathbf{g}_k$'nin boş uzayı için birim dik doğru oluşturmaktadır. Bu ilişki $\mathbf{g}_r^\dagger \mathbf{N}_g = 0_{1 \times N_t - 1}$ olarak tanımlanabilir.

Böylece, iletilmiş sinyal:

$$\mathbf{x}_k = \mathbf{g}_k^\dagger s_k + \mathbf{N}_g \mathbf{a}. \tag{5}$$

Vericideki tam kanal durum bilgisi ile ulaşılabilecek güvenlik kapasitesi değeri

$$R = \max\left\{\mathrm{E}\left\{\log_2\left(1+\gamma_k\right)\right\} - \mathrm{E}\left\{\log_2\left(1+\gamma_e\right)\right\}, 0\right\}^+, \tag{6}$$

iken, γ_k ve γ_e sırasıyla Bob'un ve Eve'in sahip olduğu SNR değerlerine karşılık gelmektedir:

$$\gamma_k = \frac{1}{\sigma^2}\left\|\mathbf{h}_k\right\|^2 \alpha P, \tag{7}$$

ve

$$\gamma_e = \frac{|\mathbf{h}_e^\dagger \mathbf{g}_k|^2 \alpha P}{||\mathbf{h}_e^\dagger \mathbf{N}_g||^2 \frac{1-\alpha}{N_t - 1} P + \sigma^2}. \tag{8}$$

Burada P, toplam gücü ifade etmekte olup bilgi sinyalinin gücü olan P_s ve yapay gürültünün gücü olan P_a'nın toplanması ile elde edilmektedir. Denklem (7) ve Denklem (8)'daki $P_s = \alpha P$ ve $P_a = \frac{1-\alpha}{N_t - 1} P$ olarak tanımlanmaktadır. Ayrıca α parametresi kanal koşul bilgisini ifade etmektedir ve değeri $(0, 1)$ aralığındadır. 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.

III. EŞIK DEĞERINE DAYALI KULLANICI SEÇIMI

Belli bir güç kısıtlaması P altında çalışan baz istasyonu kullanıcı linkinde çoklu kullanıcı çeşitliliğini açığa çıkararak güvenlik kapasitesini enbüyüklemek için en iyi kullanıcıyı seçmek gerekmektedir. Bu sebepten zayıf kanallı (düşük normlu) kullanıcılar , baz istasyonunda yapılan bu seçimde rol almamalıdır. Bu nedenle bu çalışmada, geri besleme yükünü azaltmak amacıyla, alıcı tarafında eşik değerine dayalı kullanıcı seçimi gerçekleştiren $\mathcal{T}_1$ kriterinin kullanılmasını önerilmektedir.

$\mathcal{T}_1$ kriteri için belirlenen eşik değerini aşan kullanıcılardan oluşturulan küme [15]:

$$\mathcal{U}_1 = \left\{ k \in K : \|\mathbf{h}_k\|^2 > \gamma_{th} \right\}. \tag{9}$$

Ortalama $\bar{K}$ kadar kullanıcının kanal bilgisinin baz istasyonuna iletilmesi için gereken eşik değeri γ_{th}, analitik olarak belirlenebilir.

$$\bar{K} = K \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!}. \tag{10}$$

IV. NICEMLENMIŞ GERI BESLEME KANALI

Baz istasyonundaki kanal bilgisinin limitli olması durumunda, CDI ve CQI nicemlenmesi (quantization) yapılmaktadır. Bu çalışmada CQI değerinin eksiksiz olarak bilindiği varsayılmıştır.

Yetkili kullanıcı Bob, kendi kanal yön bilgisi vektörü olan $\mathbf{g}_k$'yı daha önceden belirlenmiş 2^B boyutundaki kod kitapçığından seçilmiş $\hat{\mathbf{h}}_k$'ya nicemlemektedir. B burada nicemleme için bit sayısını ifade etmektedir. Kod kitapçığı $\mathbf{C}_k = \left\{ \hat{\mathbf{h}}_{k_1}, \hat{\mathbf{h}}_{k_2}, \ldots, \hat{\mathbf{h}}_{k_2^B} \right\}$, rastgele vektör nicemlemeye (RVQ) dayalı olarak oluşturulmuştur.

$$k_i = arg \max_{1 \le j \le 2^B} \left| \mathbf{g}_k^{\dagger} \hat{\mathbf{h}}_{k_j} \right|. \tag{11}$$

Kanal yön bilgisi, $\mathbf{g}_k$, ile kod kelimesi, $\hat{\mathbf{h}}_{k_i}$, arasındaki ilişki

$$\mathbf{g}_k = \hat{\mathbf{h}}_{k_i} \cos\theta_k + \mathbf{h}_k^{\perp} \sin\theta_k, \tag{12}$$

olarak ifade edilir. Burada $\mathbf{h}_k^{\perp}$, $\hat{\mathbf{h}}_{k_i}$'ya dik olan bir birim norm vektörünü ifade ederken, nicemleme hatası $\theta_k = \angle(\mathbf{g}_k, \hat{\mathbf{h}}_{k_i})$ ve $E\{\sin\theta_k\} \le 2^{-B/(N_t-1)}$'dir.

Nicemlenmiş CDI durumunda, baz istasyonu tarafından iletilmiş sinyal,

$$\mathbf{x}_k = \hat{\mathbf{h}}_k s_k + \hat{\mathbf{N}}_g \mathbf{a}, \tag{13}$$

olarak yazılabilir. Burada $\hat{\mathbf{N}}_g$ nicemlenmiş CDI kullanılarak elde edilen vektördür.

Böylece yetkili kullanıcıda ve gizli dinleyicide elde edilen sinyaller sırasıyla,

$$y_k = \|\mathbf{h}_k\| (\mathbf{g}_k{}^{\dagger} \hat{\mathbf{h}}_k) s + \|\mathbf{h}_k\| (\mathbf{g}_k{}^{\dagger} \hat{\mathbf{N}}_g) \mathbf{a} + z_k, \tag{14}$$

$$y_e = \mathbf{h}_e^{\dagger} \hat{\mathbf{h}}_k s + \mathbf{h}_e^{\dagger} \hat{\mathbf{N}}_g \mathbf{a} + z_e, \tag{15}$$

olarak ifade edilir.

Nicemlenmiş CDI durumunda, yetkili kullanıcı k'daki (Bob) SNR değeri

$$\hat{\gamma} = \frac{\|\mathbf{h}_k\|^2 |\mathbf{g}_k{}^{\dagger} \hat{\mathbf{h}}_k|^2 \alpha P}{\|\mathbf{h}_k\|^2 |\mathbf{g}_k{}^{\dagger} \hat{\mathbf{N}}_g|^2 \frac{1-\alpha}{N_t-1} P + \sigma^2}, \tag{16}$$

ve gizli dinleyicideki (Eve) SNR değeri

$$\hat{\gamma}_e = \frac{|\mathbf{h}_e{}^{\dagger} \hat{\mathbf{g}}_k|^2 \alpha P}{|\mathbf{h}_e{}^{\dagger} \hat{\mathbf{N}}_g|^2 \frac{1-\alpha}{N_t-1} P + \sigma^2}, \tag{17}$$

olarak ifade edilir.

Nicemlenmiş CDI durumdaki güvenlik kapasitesi değeri aşağıdaki gibi gösterilir [16]:

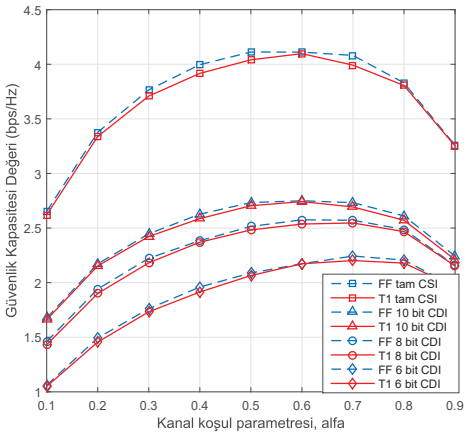
$$R = E\left\{ log_2\left(1 + \frac{\|\mathbf{h}_k\|^2 |\mathbf{g}_k{}^{\dagger} \hat{\mathbf{h}}_k|^2 \alpha P}{\|\mathbf{h}_k\|^2 |\mathbf{g}_k{}^{\dagger} \hat{\mathbf{N}}_g|^2 \frac{1-\alpha}{N_t-1} P + \sigma^2}\right)\right\} - E\left\{ log_2\left(1 + \frac{|\mathbf{h}_e{}^{\dagger} \hat{\mathbf{g}}_k|^2 \alpha P}{|\mathbf{h}_e{}^{\dagger} \hat{\mathbf{N}}_g|^2 \frac{1-\alpha}{N_t-1} P + \sigma^2}\right)\right\}.$$

Yetkili kullanıcının kanal durum bilgisinin vericide tam olarak bilindiği durumun aksine, limitli CDI durumunda bir yapay gürültü sızıntısı (AN leakage) oluşmaktadır. $\|\mathbf{h}_k\|^2 |\mathbf{g}_k{}^{\dagger} \hat{\mathbf{N}}_g|^2$ terimi ile ifade edilen ve yetkili kullanıcının nicemlenmiş kanalının boş uzayından sızan gürültü güvenlik kapasitesi değerini düşürmektedir [17].

V. BENZETIM ÇALIŞMALARI

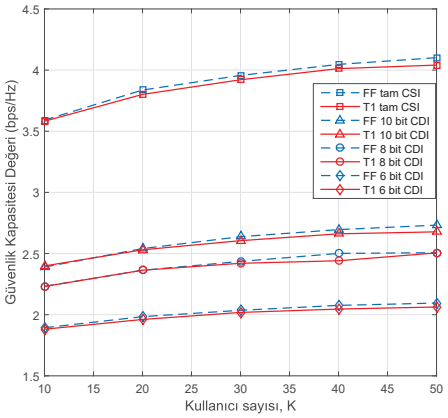
Benzetim çalışmalarında, baz istasyonundaki anten sayısı $N_t = 2$ olarak seçilmiştir. $\mathcal{T}_1$ kriteri için eşik değeri γ_{th}, teorik olarak bir hücre içindeki ortalama kullanıcı sayısı $\bar{K} = 4$, olacak şekilde hesaplanmıştır. Kullanıcı sayıları $K = [10, 20, 30, 40, 50]$ ve onlara uygun olan eşik değerleri $\gamma_{th} = [2, 3, 3.5, 3.9, 4.15]$ olarak hesaplanmıştır. Bu eşik değerlerine göre $\mathcal{U}_1$ kümesi elde edilmiştir. Ayrıca, en kötü senaryo göz önünde bulundurularak, gizli dinleyicinin karşılaştığı gürültü ihmal edilecek kadar küçük kabul edilmiştir.

Şekil 1'de, kanal koşul parametresinin (alfa) güvenlik kapasite değerine etkisini gösterilmektedir. Vericide kanal durum bilgisinin tam olduğu durum için en yüksek güvenlik kapasitesi değeri, bilgi içeren sinyal ile yapay gürültü sinyaline eşit oranda güç ayrıldığı zaman elde edilir. Şekilden de görüleceği üzere, yetkili kullanıcının kanalı hakkındaki bilgimiz azaldıkça, yapay gürültü sinyaline ayrılan güç azalmalıdır. Yetkili kullanıcının kanal bilgisinin vericide limitli olması, bu kullanıcının yapay gürültüden negatif yönde etkilenmesine neden olmaktadır. Bu durum da bir bilgi sızıntısına yol açabilmektedir. Baz istasyonundaki kanal durum bilgisinin niteliğine göre, yapay gürültü sinyali ile bilgi sinyali arasındaki güç, güvenlik kapasitesini maksimuma çıkaracak şekilde verici tarafından ayarlanmalıdır. Güvenlik kapasitesi



Şekil 1: Tam geri besleme (FF) durumu ve T1 kriterinin (T1), SNR=10 dB ve K=50 için kanal koşul parametresine göre karşılaştırılması

sonuçlarını karşılaştırmak için kanal koşul parametresi 0.5 seçilmiştir ve bu durum yapay gürültü ile bilgi içeren sinyale eşit oranda güç ayrılmasına karşılık gelmektedir.



Şekil 2: Tam geri besleme (FF) durumu ve T1 kriterinin (T1), SNR=10 dB ve kanal koşul parametresi 0.5 için karşılaştırılması

Şekil 2'de gösterildiği üzere, T1 kriteri uygulanmış sistemin güvenlik kapasite değeri, bütün kullanıcıların baz istasyonuna kılavuz gönderdiği durumunu oldukça yakından takip etmektedir. T1 kriteri sayesinde güvenlik kapasitesi değerinde herhangi bir kayıp olmadan sistem yükü önemli ölçüde azaltılmıştır. Kullanıcı sayısına göre sistem yükündeki yüzdelik azalma 60 ile 90 arasında değişmektedir.

VI. Sonuçlar

Bu çalışmada çoklu kullanıcılı, çoklu verici antenli ve güvenlik endişesinin bulunduğu sistemler için alıcı tarafında eşik değerine bağlı kullanıcı seçimi algoritması uygulanmıştır. Yapılan bu seçim kriterinin güvenlik performansı üzerine etkileri incelenmiştir. Pratik sistemlerde pasif gizli dinleyicinin yerinin ve kanal durum bilgisinin elde edilmesi genellikle mümkün olamayacağından, gizli dinleyicinin pasif dinleyici olduğu ve kanal bilgisinin bilinmediği durumu göz önünde bulundurulmuştur. Kanal durum bilgisi bilinmediğinden, gizli dinleyicinin algısını bozmak adına yetkili kullanıcının etkilenmeyeceği şekilde dış uzaya yapay gürültü gönderilmektedir. Verici tarafında haberleşme için seçilme olasılığı düşük olan kullanıcıların kanal bilgilerini iletmeleri engellenerek sistem yükü (overhead), güvenlik kapasitesi değerinde kayıp olmadan önemli ölçüde azaltılmıştır.

VII. Bilgilendirme

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

Kaynakça

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

[2] P. GOPALA , L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[3] F. OGGIER, B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug.2011.

[4] 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).

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

[6] Z. LI,W. Trappe,R. Yates, Secret Communication via Multi-Antenna Transmission, Conf. Info. Sci.and Sys., pp. 905-10, (2007).

[7] S. SHAFIEE and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in Proc. IEEE ISIT, Nice, France, June 2007.

[8] 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.

[9] S. GERBRACHT, C. Scheunert, and E.A. Jorswieck. Secrecy outage in MISO systems with partial channel information. Information Forensics and Security, IEEE Transactions on, 7(2):704–716, 2012.

[10] J. ZHU, X.JIANG, Y. ZHOU, Y. ZHANG, O. TAKAHASHI, and N. SHIRATORI "Outage performance for secure communication over correlated fading channels with partial CSI". In Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific, pages 257–262, 2012.

[11] 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

[12] G. GERACI,R. Couillet, J. Yuan, M. Debbah,I. B. Collings, "Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter" ICASSP 2013

[13] N. LI, X. Tao, J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback " IEEE Communications letters, vol.18,No.6,June 2014

[14] N. JINDAL, "MIMO Broadcast Channels with Finite Rate Feedback",IEEE Transactions on Information Theory,Vol.52,Issue 11,Nov.2006

[15] Z. PENG, J. Zhu, H. Zhang, C. Zhao "Impact of Estimated CSI Quantization on Secrecy Rate Loss in Pilot- Aided MIMO systems", Globecom Workshop,2014

[16] D. GESBERT, M. S. Alouini, 'How much feedback is multi-user diversity really worth?', In Proc. IEEE International Conference on Communications, France,2004

[17] S.C. LIN, T.H. Chang, Y.L. Liang, "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem", IEEE Transactions on Wireless Communications, Vol. 10 Issue 3,Mart 2011