ÖZET

FİZİKSEL KATMAN GÜVENLİĞİNE DAYALI BİR GÜVENLİ NOMA YÖNTEMİ

Mevcut buluş, uydu yer bağı PD-NOMA'da bütün kullanıcı bağlantılarını korumak üzere dahili ve harici gizli dinleyicileri içeren bir güvenli şema sunmaktadır. Özellikle sunulan şema, BS'nin karşılık gelen anlık kanal fazına dayalı olarak her bir kullanıcının sembolünde bir faz kaymasına neden olduğunu göstermektedir. Her bir kullanıcının faz kayması, orijinal sembolün, yıldız kümesi diyagramındaki diğer bir sembolün konumuna hareket ettirileceği şekilde sınırlandırılmaktadır. Bu nedenle, her bir kullanıcının sadece anlık kanal fazının farkında olması nedeniyle karşılık gelen sembolünün gerçek fazını kurtarabilecektir. Böylece sunulan şema, verileri sadece gizli dinleyicilere karşı korumamaktadır, aynı zamanda diğer tüm kullanıcılara karşı gizlilik ve mahremiyeti garanti etmektedir.

ABSTRACT

A SECURE NOMA METHOD BASED ON PHYSICAL LAYER SECURITY

The present invention proposes a secure scheme that incorporates both internal and external eavesdroppers to secure all users' links in the downlink PD-NOMA. In particular, the proposed scheme implies that the BS induces a phase shift in each user's symbol based on its corresponding instantaneous channel phase. The phase shift of each user is restricted such that the original symbol is moved to the location of another symbol in the constellation diagram. Therefore, as each user is aware of its instantaneous channel phase only, it will be able to recover the actual phase of its corresponding symbol. Thus, the proposed scheme does not only protect the data against eavesdroppers, but it also guarantees confidentiality and privacy against all other users.

İSTEMLER

1. Bilinmeyen bir dahili gizli dinleyiciye karşı güvenli bir uydu yer bağı NOMA yöntemi olup, özelliği aşağıdaki adımları içermesidir:

- Kullanıcıların kanal koşullarına dayalı olarak bir baz istasyonu tarafından her bir kullanıcıya yönelik farklı güç seviyelerinin tahsis edilmesi,
- Modüle edilen her bir sembol üzerinde bir faz kaymasının başlatılması,
- Ust üste binen sinyalin birleştirilmesi ve baz istasyonundan kullanıcılara gönderilmesi,
- Her bir kullanıcının, her bir tekrarlamada alınan sinyalden tespit edilen sembolü çıkararak ve ortaya çıkan sinyali sonraki tekrarlamaya taşıyarak kendi sembolüne ulaşana kadar birinci kullanıcıdan başlayarak diğer kullanıcıların sembollerinin tespit edilmesi yoluyla ardışık girişim giderimini gerçekleştirmesi,
- Gizli sinyali tespit etmek üzere bir faz kaymasının gerçekleştirilmesi.

2. İstem 1'e göre yöntem olup, özelliği; baz istasyonunun karşılık gelen sembolünü döndürmek için kullanılacak olan, her bir belirli kullanıcıya yönelik spesifik bir faz kaymasını çıkarmasıdır.

3. İstem 1 ve 2'ye göre yöntem olup, özelliği $\phi_n$ile gösterilen, kullanıcının (n) sembol üzerindeki faz kaymasının $\phi_n = \left(\left[\frac{\theta_n}{2\pi/M}\right] + 1\right) \times \frac{2\pi}{M}$ olarak verilmesi, $\theta_n{}'nin$'nin h_n 'nin fazı olması ve $M'\text{nin}$ modülasyon seviyesi olmasıdır.

4. Bir harici gizli dinleyiciye karşı bir güvenli yer uydu bağı masif makine tipi iletişim NOMA yöntemi olup, özelliği aşağıdaki adımları içermesidir:

- Her bir kullanıcının, kendi sembolünü bir baz istasyonuna gönderilecek şekilde modüle etmesi,
- Her bir sembolün bir faz değeri ile kaydırılması,
- Kullanıcı sinyallerinin baz istasyonuna tahsis edilen güce göre iletilmesi,
- Baz istasyonunda eş zamanlı olarak bütün kullanıcılardan sinyallerin alınması,
- En güçlü kullanıcının sinyalinin tespit edilmesi ve en güçlü kullanıcı sinyalini çözmek üzere bir faz kaydırıcısının uygulanması,

- Kalan kullanıcı sinyallerini tespit etmek üzere tekrarlı ardışık girişim gideriminin uygulanması,
- Bütün kullanıcı sinyalleri tespit edilene kadar bir faz kaymasının uygulanması.

5. İstem 4'e göre yöntem olup, özelliği $\phi_n$ile gösterilen, kullanıcının (n) sembol üzerindeki faz kaymasının $\phi_n = \left(\left[\frac{\theta_n}{2\pi/M}\right] + 1\right) \mathrm{x} \frac{2\pi}{M}$ olarak verilmesi, $\theta_n' nin\ h_n$ 'nin fazı olması ve M 'nin modülasyon seviyesi olmasıdır.

CLAIMS

1. A secure downlink NOMA method against an unknown internal eavesdropper, comprising:

- Assigning different power levels for each user by a base station based on users' channel conditions,
- Inducing a phase shift on each modulated symbol,
- merging and sending the superposed signal to the users from the base station,
- Each user performs successive interference cancellation by detecting the other users' symbols starting with the first user until reaching its symbol by subtracting the detected symbol from the received signal at each iteration and carrying the resulting signal to the next iteration,
- Performing a phase shift to detect the confidential signal.

2. The method according to claim 1, wherein the base station extracts a specific phase shift for each particular user that will be used to rotate its corresponding symbol.

3. The method according to claim 1 and 2, wherein the phase shift on the symbol of user n, denoted by ϕ_n, is given as $\phi_n = \left(\left[\frac{\theta_n}{2\pi/M}\right] + 1\right) \times \frac{2\pi}{M}$ wherein θ_n the phase of h_n, and M is the modulation level.

4. A secure uplink massive machine type communication NOMA method against an external eavesdropper, comprising:

- Each user modulates their symbol to be delivered to a base station,
- Shifting each symbol by a phase value,
- Transmitting user signals according to allocated power to the base station,
- Receiving signals from all the users simultaneously at the base station,
- Detecting the signal of the strongest user and applying a phase shifter to demodulate the strongest user signal,
- Applying iterative successive interference cancellation to detect the rest user signals,
- Applying a phase shift until detecting all user signals.

5. The method according to claim 4, wherein the phase shift value on the symbol of user n, denoted by ϕ_n, is given as $\phi_n = \left(\left[\frac{\theta_n}{2\pi/M}\right] + 1\right)$ x $\frac{2\pi}{M}$ wherein θ_n is the phase of h_n, and M is the modulation level.

TARİFNAME

FİZİKSEL KATMAN GÜVENLİĞİNE DAYALI BİR GÜVENLİ NOMA YÖNTEMİ

Teknik Alan

Mevcut buluş, fiziksel katman güvenliği konseptlerine dayalı bir güvenli Ortogonal Olmayan Çoklu Erişim (NOMA) yöntemidir.

Daha özellikle sunulan yöntem, her bir kullanıcının sembolünde farklı bir faz kaymasına neden olmak üzere rastgele ve bağımsız kanal özelliklerini kullanmaktadır. Bir kullanıcı ve baz istasyonu arasındaki anlık kanal fazının sadece her iki uçta mevcut olduğu varsayımına dayalı olarak diğer kullanıcılar, doğru sembolü çözemeyecektir. Sunulan şema, kullanıcı uçlarındaki performansı etkilememektedir ve aynı zamanda, hem dahili hem de harici gizli dinlemeye karşı her bir kullanıcının veri gizliliğini garanti edebilmektedir.

Önceki Teknik

NOMA, istenen özellikleri bakımından 5G konusunda ve kablosuz sistemlerin ötesinde önemli derecede dikkat çekmiştir. Farklı NOMA şemaları arasından Güç Etki Alanı NOMA (PD-NOMA), son zamanlarda gelişmiş bağlanırlığı ve basit uygulaması nedeniyle fazla ilgi görmüştür. Bu şema kritik güvenlik risklerinden muzdariptir. Özellikle bütün sinyallerin aynı kaynaklar üzerinde birlikte yayınlanması nedeniyle bir gizli dinleyicinin iletime engel olması ve kullanıcı sinyallerine erişim elde etmesi riski mevcuttur. Bu nedenle Fiziksel Katman Güvenliği (PLS) teknikleri, klasik kriptografi eksikliklerine yönelik uygulanabilir çözümler olarak ortaya çıkmıştır [7, 8, 9]. PLS, yasal kullanıcı verilerini çözebilirken, gizli dinleyici (Eve) ele geçirilen herhangi bir veriyi çözemeyecek şekilde kablosuz sönümlü kanalın çeşitli özelliklerini (rastgele kanal sönümleme, girişim, gürültü, vb.) kullanmaktadır. Sonuç olarak PLS, NOMA'da bulunan güvenlik endişelerinin ele alınması konusunda büyük potansiyele sahiptir ve bu nedenle son yıllarda önemli bir araştırma aktivitesi elde etmiştir.

NOMA'da birden fazla kullanıcı, iletişim kanalını aynı anda farklı güç seviyeleri ile kullanmaktadır, bu da bir iletişim sisteminde kritik güvenlik sorunlarından biri olarak

kabul edildiği üzere iletişim varlıkları arasındaki bilgi değişimini gizli dinlemeye karşı korunmasız hale getirmektedir. Bir NOMA sistemindeki gizli dinleyici, harici (baz istasyonu (BS) tarafından hizmet verilen yasal kullanıcılarından biri olmayan) veya dahili (hizmet verilen kullanıcılardan biri olan) olmak üzere iki kategoriden birinde yer alabilmektedir [1]. PD-NOMA'da potansiyel dahili gizli dinleyicilere karşı güvenlik seviyesinin artırılmasının ciddi bir zorluk olduğu belirtilmiştir. Bunun nedeni PD-NOMA'da kullanılan ardışık girişim giderimi (SIC) tespit tekniğinin, bir kullanıcının daha yüksek güç seviyelerine sahip olan kullanıcı sinyallerini çözmesini gerektirmesidir, bu durum iletilen sinyalleri gizli dinlemeye karşı korunmasız hale getirmektedir [10].

Harici Eve, farklı kurulumlara ve senaryolara dayalı olarak normal NOMA kullanıcılarını gizli dinlemeye karşı korumak üzere farklı güvenlik mekanizmalarının sunulduğu literatürde kabul edilmiştir. Örneğin yapay gürültü, Eve'de performansı azaltmak üzere [2, 3]'te kabul edilirken korumalı bölge konsepti, herhangi bir Eve'nin bu bölgede bulunamadığı [4, 5]'te kullanılmaktadır. Korumalı bölgenin şekli ve konumu, [6, 7]'de uydu yer bağı mmDalga-tabanlı NOMA sistemleri ve [8]'de yer uydu bağı çoklu anten NOMA sistemleri için optimize edilmektedir. [9]'da iletim anteni seçimi, bir harici Eve'ye karşı iki NOMA kullanıcısına yönelik veriyi korumak üzere kullanılmaktadır. Diğer bir yaklaşımda hüzmeleme ve yapay gürültü, [10, 11]'de harici Eve'de alımı azaltmak üzere birleştirilirken, optimize edici hüzmeleme ve güç tahsisi ise [12, 13, 14]'te değerlendirilmektedir.

Ancak yukarıda bahsedilen çalışmaların tümü, bunları dahili gizli dinleyiciler ile mücadele etme bakımından geçersiz hale getiren şekilde Eve'de alınan sinyalin azaltılmasını amaçlamaktadır. Ayrıca bu yöntemler, gecikme, spektral verimlilik, bağlantı yoğunluğu, veri hızı, enerji verimliliği, hesaplama ve donanım karmaşıklığı bakımından zorlu gerekliliklere dayanamamaktadır. Bu zorluklara dayanan sistemlerin örnekleri, Nesnelerin İnterneti (IoT) sistemi, ultra-güvenilir düşük-gecikmeli iletişim (URLLC) ve masif makine-tipi iletişimdir (mMTC). Daha önceden bahsedildiği üzere dahili Eve, hizmet edilen kullanıcılardan biridir ve bu nedenle kullanılan güvenlik mekanizması, bunun veri alımını etkilememelidir, ayrıca Eve'nin diğerlerinin verilerini ortaya çıkarmasını engellemelidir.

Bu çalışmanın ana odak noktası olan dahili Eve, sadece birkaç çalışmada değerlendirilmiştir [15, 16, 17, 18, 19]. [17]'de kullanıcılar, kümeler arasında

dağıtılmaktadır ve sıfır-zorlamalı hüzmeleme şeması, karşılıklı girişim ve bilgi sızıntısını minimuma indirmek üzere sunulmaktadır. Ancak gizli dinleyicinin uzak kullanıcı olduğu durum, gizli dinleyicinin yakın kullanıcı olduğu durum ila karşılaştırıldığında kolay kabul edilmektedir. Ayrıca gizli dinleyicinin, buna karşı işlemi kolaylaştırması gereken şekilde BS'de tanımlanacağı varsayılmaktadır. [15, 16, 17]'nin aksine [18]'in yazarları, bir dahili yakın gizli dinleyici ve bir harici gizli dinleyicinin varlığının etkisini azaltmak üzere yapay gürültü destekli hüzmeleme ve güç tahsisini birleştirmektedir. Bunun her iki gizli dinleyici türüne (dahili ve harici) karşı etkili bir şekilde çalışmasına rağmen bu, her ikisinin BS'de tanımlanmasını ve bunların anlık kanal kazanımlarının bilinmesini gerektirmektedir. Bu nedenle bir kullanıcının yanlış bir şekilde bir gizli dinleyici olarak tanımlanması halinde bunun performansı azaltılacaktır. Son zamanlarda [19]'da yönsel modülasyon, uzak bir güvenilen kullanıcının verisini bir dahili yakın gizli dinleyici tarafından engellenmekten korumak üzere kullanılmaktadır. Spesifik olarak yönsel modülasyon, gizli dinleyicinin farklı alt-sıra sembollerini alacağı şekilde bunları temsil ederek güvenilen (uzak) kullanıcıya iletilen sembollerin gizlenmesini belirtmektedir. Uzak kullanıcının verilerini etkili bir şekilde koruyabilmesine rağmen birkaç kısıtlamadan muzdariptir. Birinci olarak birden fazla kullanıcının veya birden fazla gizli dinleyicinin bir sistemine yönelik uygulanamamaktadır. İkinci olarak gizli dinleyicinin BS'de tanımlanması ve bilinmesi gerekmektedir. Üçüncü olarak yönsel modülasyonun en uygun vektörüne ulaşılacağına dair herhangi bir garanti yoktur.

US10651961 numaralı başvuru, kablosuz iletişime yönelik teknikleri açıklamaktadır. Birinci yöntem, en azından kısmi olarak birinci UE ve en az bir ikinci UE'yi içeren bir NOMA grubu ile ilişkilendirilen bir grup tanımlayıcıya dayalı birinci kullanıcı ekipmanına (UE) yönelik uydu yer bağı kontrol bilgisinin alınmasını; ve en azından kısmi olarak birinci UE'ye yönelik uydu yer bağı kontrol bilgisine dayalı olan birinci UE'de bir grup NOMA uydu yer bağı iletiminin alınmasını içermektedir. İkinci yöntem, en az bir ikinci UE'nin bir göstergesini içeren birinci UE'ye yönelik uydu yer bağı kontrol bilgisi, bir birinci UE'ye yönelik uydu yer bağı kontrol bilgisinin alınması; en az ikinci UE'nin göstergesine en azından kısmi olarak dayalı olan ikinci UE'ye yönelik uydu yer bağı kontrol bilgisinin alınması; en azından kısmi olarak birinci UE'ye yönelik uydu yer bağı kontrol bilgisi ve ikinci UE'ye yönelik uydu yer bağı kontrol bilgisine dayalı olan birinci UE'de bir grup NOMA uydu yer bağı iletiminin alınmasını içermektedir. Ancak başvuru, dahili ve harici gizli dinlemeye karşı her bir kullanıcının veri gizliliğini garanti edememektedir.

Kısa Açıklama

Uydu yer bağı PD-NOMA'da bütün kullanıcıların bağlantılarını korumak üzere bu buluş, dahili ve harici gizli dinleyicileri içeren yeni bir koruma şeması sunmaktadır. Özellikle sunulan şema, BS'nin karşılık gelen anlık kanal fazına dayalı olarak her bir kullanıcının sembolünde bir faz kaymasına neden olduğunu göstermektedir. Her bir kullanıcının faz kayması, orijinal sembolün, yıldız kümesi diyagramındaki diğer bir sembolün konumuna hareket ettirileceği şekilde sınırlandırılmaktadır. Bu nedenle, her bir kullanıcının sadece anlık kanal fazının farkında olması nedeniyle karşılık gelen sembolünün gerçek fazını kurtarabilecektir. Böylece sunulan şema, verileri sadece gizli dinleyicilere karşı korumakla kalmaz, aynı zamanda diğer tüm kullanıcılara karşı gizlilik ve mahremiyeti de garanti etmektedir. Sunulan şemadaki tek temel varsayım, BS'de tam CSI'nın bulunmasıdır. CSI'nın halihazırda BS'de diğer birçok görev için gerekli olması nedeniyle bu tür bir varsayımın ilave bir gereklilik olmadığının altını çizmek gerekmektedir.

Sunulan algoritma, klasik güvenli PD-NOMA şemaları ile karşılaştırıldığında ek zaman veya güç kaynağı tüketimi olmaksızın dahili ve harici gizli dinlemeye karşı güvenlik sağlayabilmektedir. Bu nedenle sunulan yöntem, Nesnelerin İnterneti (IoT) cihazları, masif makine tipi iletişim (mMTC), ultra-güvenilir düşük gecikmeli iletişim (ULLRC), uzaktan ameliyat ve sağlık uygulaması gibi gecikme, spektral verimlilik, bağlantı yoğunluğu, veri hızı ve enerji verimliliği bakımından zorlu gereklilikleri karşılaşan ağlara yönelik daha uygundur.

Sunulan güvenli planın avantajları aşağıdaki gibi kısaca açıklanabilmektedir:

- Sunulan şema, konumları, kanal sıraları ve SNR'lerden bağımsız olarak dahili ve harici gizli dinleyicilere karşı etkili bir şekilde çalışabilmektedir.
- Sunulan şema, sistemde bulunan herhangi bir sayıda gizli dinleyiciye yönelik etkili bir şekilde çalışabilmektedir.
- Sunulan şema, klasik PD-NOMA sistemi ile ilgili olarak herhangi bir ek zaman veya kaynak tüketimine neden olmamaktadır.
- Sunulan şema, diğer yasal kullanıcıların hata performansını etkilememektedir.

- Gizli dinleyici bir dahili kullanıcı olduğunda sunulan şema, gizli dinleyicinin sadece verilerini almasına izin vermektedir ve diğerlerinin verilerinin gizlice dinlenmesini önlemektedir.
- Sunulan şemanın BS'de gizli dinleyicinin bilinmediğini varsaydığı durumlarda BS'nin gizli dinleyiciyi tanımlaması gerekmektedir.
- Sinyalleri önceden kodlamak üzere kanal fazına güvenmek, sunulan şemanın esnekliğini geliştirmektedir. Bunun nedeni, kanal fazının uzaklıktan bağımsız olması nedeniyle üçüncü bir taraf tarafından tahmin edilmesinin veya öngörülmesinin oldukça olmasıdır.

Şekillerin Kısa Açıklaması

Şekil 1, bilinmeyen bir dahili gizli dinleyiciye karşı güvenli uydu yer bağı NOMA yönteminin akış şemasını göstermektedir.

Şekil 2, harici gizli dinleyiciye karşı güvenli yer uydu bağı mMTC-NOMA yönteminin akış şemasını göstermektedir.

Detaylı Açıklama

Bu buluşta fiziksel katman güvenliği konseptlerine dayalı, yeni bir güvenli Ortogonal-Olmayan Çoklu Erişim (NOMA) şeması sunulmaktadır. Sunulan şema, her bir kullanıcının sembolünde farklı bir faz kaymasına neden olmak üzere rastgele ve bağımsız kanal özelliklerini kullanmaktadır. Bir kullanıcı ile baz istasyonu arasındaki anlık kanal fazının sadece her iki uçta mevcut olduğu varsayımına dayalı olarak diğer kullanıcılar, doğru sembolü çözemeyecektir. Sunulan şema, kullanıcıların uçlarındaki performansı etkilememektedir ve aynı zamanda dahili ve harici gizli dinlemeye karşı her bir kullanıcının veri gizliliğini garanti edebilmektedir.

Birinci senaryoda, bilinmeyen bir dahili gizli dinleyiciye karşı bir güvenli uydu yer bağı NOMA sistemi sunulmaktadır. BS'de her bir kullanıcı sinyali, teslim edilmek üzere modüle edilmektedir. Daha sonra, her bir kullanıcıya yönelik farklı güç seviyeleri, en iyi kullanıcıya (genellikle en yakın olanın) en düşük güç seviyesinin tahsis edildiği ve en yüksek güç seviyesinin en kötü kullanıcıya (genellikle en uzak olan) tahsis edildiği kanal koşullarına dayalı olarak atanmaktadır. Kullanıcının güç katsayısı (n) ρ_n ile

gösterilmektedir, tahsis edilen güç katsayılarının aşağıdaki denklemi karşılaması gerekmektedir:

$$\sum_{n=1}^{N} \rho_n = 1 \text{ ve } \rho_1 < \rho_2 < \ ... \ < \rho_n. \quad (1)$$

Sunulan şemaya dayalı olarak BS, iletilen sembollerin birleştirilmesinden önce her bir sembol üzerinde bir faz kaymasına neden olmaktadır. Spesifik olarak BS, karşılık gelen sembolünü döndürmek için kullanılacak olan her bir belirli kullanıcıya yönelik spesifik bir faz kaymasını çıkarmak amacıyla tüm kullanıcıların CSI bilgisinden faydalanacaktır. Ancak NOMA sistemlerindeki zorluk, bir kullanıcıdaki BER'nin esas olarak diğer kullanıcıların sembollerini doğru bir şekilde tespit etme yeteneğine dayanmasıdır. Böylece bir kullanıcıda başlatılan faz kayması, diğer kullanıcıların performansını etkilemeyecek şekilde dikkatli bir şekilde seçilmelidir.

Bir karmaşık değer olarak blok sönümleme kanalı (h_n), $h_n = j_n e^{i\theta_n}$ olarak ifade edilebilmektedir, burada j_n ve θ_n, sırasıyla h_n büyüklüğünü ve fazını temsil etmektedir ve i, sanal birimdir. Buna göre ϕ_n ile gösterilen kullanıcı (n) sembolündeki faz kayması, aşağıdaki gibi verilmektedir:

$$\phi_n = \left(\left[\frac{\theta_n}{2\pi/M}\right] + 1\right) \times \frac{2\pi}{M} \quad . \quad (2)$$

Faz kaymasının, $\frac{2\pi}{M}$'in bir katı ile karşılık gelen sembolü döndüreceği ve böylece bunun, yıldız kümesi diyagramında diğer bir sembol olarak görüneceği belirtilmelidir. Böylece, kullanıcılar (hedeflenen kullanıcı dışında), bunu aday sembollerden (yıldız kümesi noktaları) biri olarak tespit edecektir ve sadece hedeflenen kullanıcı (ϕ_n'nin farkında olan) sembolün orijinal fazını kurtarabilmektedir. Şekil 1, PD-NOMA sistemlerine yönelik sunulan güvenli şemayı göstermektedir.

Sunulan şemadan sonra kullanıcıda (n) alınan sinyal bu noktada aşağıdaki gibi verilmektedir

$$y_n = \sqrt{P} h_n \left(\sum_{k=1}^{N} \sqrt{\rho_k} e^{-i\phi_k} s_k\right) + w_n. \quad (3)$$

buradaw_n, n'inci kullanıcılarda sıfır ortalamalı ve σ^2 değişkenli ($w_n, \sim \mathcal{N}(0, \sigma^2)$) toplanır beyaz Gauss gürültüsünü (AWGN) gösterir. Ayrıca bütün bağlantılar, büyük ölçekli (yol kaybı) ve küçük ölçekli sönümleme ($h_n = d_n^{-\frac{\eta}{2}} f_n$) ile modellenmektedir, burada f_n,

Rayleigh sönümleme kanalı kazancı $f_n \sim \mathcal{N}(0, \sigma^2)$ ile modellenmektedir. Ve d_n, verici ile alıcı (n) arasındaki ayrıklık uzaklığıdır ve η, yol kaybı üssüdür.

Buna göre aşağıdaki gibi başlatılan fazı bulundurmak üzere SIC tespiti gerçekleştirilmektedir:

$$\hat{s}_n = \arg \min_{l=1:M} \left| y_n - \sqrt{P} h_n \left(\sum_{k=n+1}^{N} \sqrt{\rho_k}\, \hat{s}_k \right) - \sqrt{P \rho_n} h_n e^{-i\phi_n} s_l \right| \quad (4)$$

Her bir kullanıcı SIC'yi gerçekleştirmektedir. SIC, her bir kullanıcının tekrarlı maksimum olabilirlik tespitini gerçekleştirdiğini göstermektedir. Spesifik olarak, güç seviyeleri sırasına göre kullanıcı (n), ilk kullanıcıdan (diğer bir ifadeyle kullanıcıdan (N)) başlayarak kendi sembolüne ulaşana kadar diğer kullanıcıların sembollerini tespit etmektedir. Her bir tekrarlamada, tespit edilen sembol alınan sinyalden çıkarılmaktadır ve sonuç, bir sonraki tekrarlamaya aktarılmaktadır. Bu proses, bir kullanıcının sadece katsayısından daha yüksek güç katsayılarına sahip olan kullanıcıların sembollerini tespit etmesine izin vermektedir. Diğer bir ifadeyle kullanıcı (N) sinyali tespit edilmektedir ve kullanıcı (N-1) sinyalini bulmak üzere alınan sinyalden (y_n) çıkarılmaktadır ve bu prosedürler, hedeflenen kullanıcı sinyalini tespit edene kadar tekrar edilmektedir.

İkinci senaryoda, bir harici gizli dinleyiciye karşı bir güvenli yer uydu bağı mMTC-NOMA şeması tanımlanmaktadır. mMTC, IoT uygulamaları, sağlık sensörleri, akıllı evler vb. gibi az miktarda veri trafiği ileten çok sayıda cihaz arasında masif bir bağlantının sağlanmasını belirtmektedir. Yer uydu bağı NOMA-tabanlı mMTC ağlarında, çoklu MTC cihazları (MTCD'ler), aynı zamanda ancak farklı güç tahsisi ile iletime yönelik alt kanalı kullanmıştır. Ve her bir kullanıcıya, kanal koşuluna dayalı olarak güç tahsis edilmiştir. Böylece, en kötü kanala sahip MTCD'ye, daha iyi kanal koşullarına sahip MTCD ile karşılaştırıldığında daha fazla güç tahsis edilmektedir. Kanal kazancı koşulu $|h_1|^2 < |h_n|^2 < \cdots < |h_N|^2$) nedeniyle tahsis edilen güç katsayılarının $\rho_1 > \rho_2 > \ldots > \rho_n$ olduğu varsayılmaktadır.

Şekil 2'de gösterildiği gibi her bir MTCD, sembolün kendi orijinal fazını Denklem (2)'de belirlenen faz miktarı kadar kaydıracaktır, akabinde sinyali BS'ye iletecektir. Yasal BS ve Eve-BS'de alınan sinyaller aşağıdaki gibi olacaktır:

$$y_d = \sum_{k=1}^{N} h_n \sqrt{\rho_n P_n} s_n e^{-i\phi_k} + w_{d,n} \quad (5)$$

$$y_e = \sum_{k=1}^{N} g_n \sqrt{\rho P_n} s_n e^{-i\phi_k} + w_{e,n} \quad (6)$$

buradaw$_{d,n}$ ve $w_{e,n}$, sırasıyla kullanıcı (n), yasal BS ve Eve-BS arasında sıfır ortalamalı ve σ^2 değişkenli ($w_{d,n},\ w_{e,n} \sim \mathcal{N}\ (0, \sigma^2)$) toplanır beyaz Gauss gürültüsünü (AWGN) göstermektedir. Ayrıca bütün bağlantılar,h_n ve $g_n = d_n^{-\frac{\eta}{2}} f_n$ olacak şekilde büyük ölçekli (yol kaybı) ve küçük ölçekli sönümleme ile modellenmektedir, burada f_n, Rayleigh sönümleme kanalı kazancı $f_n \sim \mathcal{N}\ (0, \sigma^2)$ ile modellenmektedir. Ve d_n, MTCD ile BS arasındaki ayrıklık uzaklığıdır ve η, yol kaybı üssüdür.

Yasal BS ve harici gizli dinleyici, üst üste binen alınan sinyallerin kodunu çözmek üzere SIC teknolojisini kullanmaktadır. SIC, bir BS'nin birinci olarak en güçlü MTCD'nin sinyalini tespit ettiği tekrarlı bir prosedürü ifade etmektedir. Akabinde tüm MTCD alıcı sinyallerinin kodunu çözene kadar bu sinyali alınan sinyalden çıkarmaktadır. Her bir tekrarlamada BS, zayıf MTCD sinyalleri gürültü olarak alırken, diğer tüm güçlü MTCD'nin sinyalleri girişim olarak aldığını kabul etmektedir. Bu nedenle faz kaymasını (ϕ_n) belirlemek ve bilgiyi korumak üzere kullanılan CSI, sadece MTCD'ler ve yasal BS için mevcuttur. Harici gizli dinleyici, faz değerini ($\psi_n = \left(\left[\frac{\Omega_n}{2\pi/M}\right] + 1\right) \times \frac{2\pi}{M}$) farklı bir şekilde değerlendirecektir, burada Ω_n, g_n fazıdır. Böylece yasal BS, her bir kullanıcıya yönelik bilgiyi doğru bir şekilde tespit edebilecekken harici gizli dinleyici, bunu yapmayacaktır.

Referanslar

[1] N. Zhao, D. Li, M. Liu, Y. Cao, Y. Chen, Z. Ding, and X. Wang, “Securetransmissionviajointprecodingoptimizationfordownlink MISO NOMA," IEEE Trans. Veh. Tech.,vol. 68, no. 8, pp. 7603-7615, 2019.

[2] H. Bao, C. Zhang, L. Wu, and M. Li, “Design of physicallayersecuretransmissionschemebased on SWIPT NOMA systems," in IEEE ICCT, 2017, pp. 6-9.

[3] B. Chen, Y. Chen, Y. Chen, Y. Cao, Z. Ding, N. Zhao, and X. Wang, “Secureprimarytransmissionassistedby a secondaryfull-duplex NOMA relay," IEEE Transactions on VehicularTechnology, vol. 68, no. 7, pp. 7214-7219, 2019.

[4] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, “Physicallayersecurityfor 5G non-orthogonalmultipleaccess in large-scalenetworks," in IEEE ICC, 2016, pp. 1-6.

[5] N. Rupasinghe, Y. Yapici, I. Guvenc, H. Dai, and A. Bhuyan, “Enhancingphysicallayersecurityfor NOMA transmission in mmWavedronenetworks," in 2018 52nd Asilomar Conference on Signals, Systems, andComputers. IEEE, 2018, pp. 729-733.

[6] Y. Yapici, I. Guvenc, H. Dai, A. Bhuyan, and N. Rupasinghe, “Physicallayersecurityformmwavedronelinkswithnoma."

[7] Y. Yapici, N. Rupasinghe, I. Guvenc, H. Dai, and A. Bhuyan, \Physicallayersecurityfornomatransmission in mmwavedronenetworks," arXivpreprint arXiv:2001.04863, 2020.

[8] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, “Physicallayersecurity in uplinknomamulti-antennasystemswithrandomlydistributedeavesdroppers," IEEE Access, vol. 7, pp. 70422-70435, 2019.

[9] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, “On secure NOMA systemswithtransmitantennaselectionschemes," IEEE Access, vol. 5, pp. 17450-17464, 2017.

[10] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancingthephysicallayersecurity of nonorthogonalmultipleaccess in large-scalenetworks," IEEE Trans. Wireless Comm.,vol. 16, no. 3, pp. 1656-1672, 2017.

[11] L. Lv, Z. Ding, Q. Ni, and J. Chen, “Secure MISO-NOMA transmissionwitharticialnoise," IEEE Trans. Veh. Tech.,vol. 67, no. 7, pp. 6700-6705, 2018.

[12] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, “Securebeamforming in downlink MISO nonorthogonalmultipleaccesssystems," IEEE Trans. Veh. Tech.,vol. 66, no. 8, pp. 7563-7567, 2017.

[13] B. M. ElHalawanyand K. Wu, “Physical-layersecurity of NOMA systemsunderuntrustedusers," in 2018 IEEE GLOBECOM, 2018, pp. 1-6.

[14] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li, and F. R. Yu, “Securetransmissionviabeamformingoptimizationfor NOMA networks," IEEE Wireless Comm., 2019.

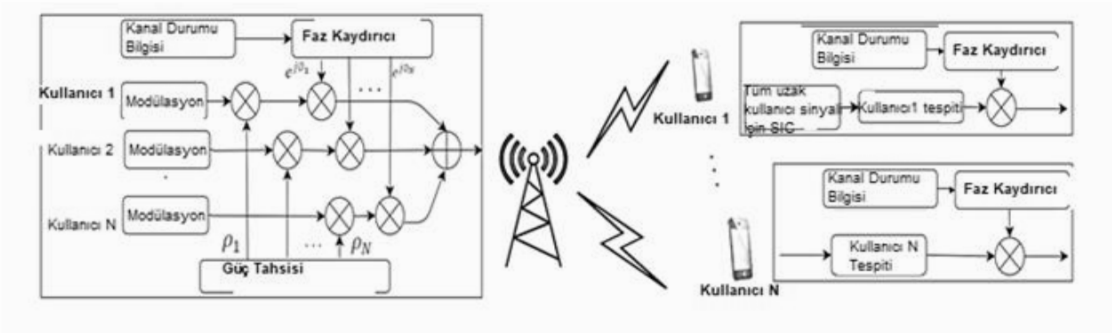
[15] B. M. ElHalawanyand K. Wu, “Physical-layersecurity of nomasystemsunderuntrustedusers," in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6.

[16] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, “Optimal relayselectionforsecurenomasystemsunderuntrustedusers," IEEE Transactions on VehicularTechnology, vol. 69, no. 2, pp. 1942-1955, 2020.

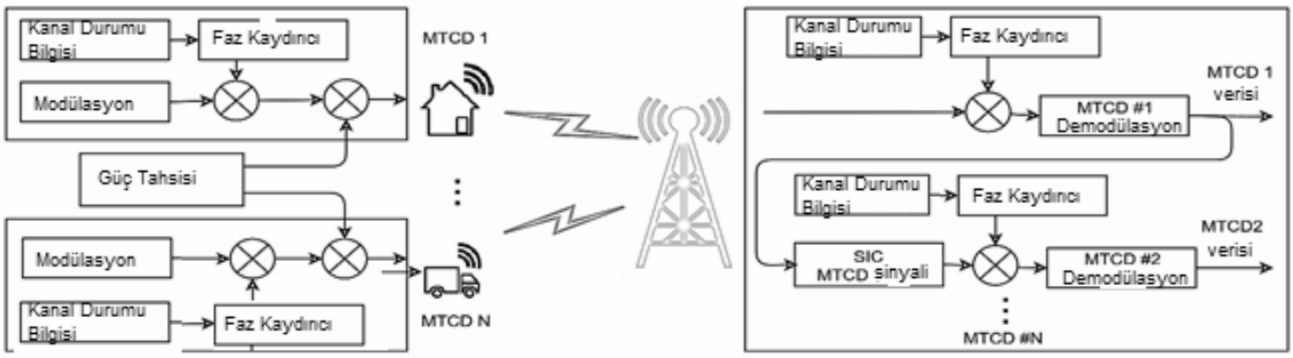
[17] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, “Securebeamforming in downlinkmisononorthogonalmultipleaccesssystems," IEEE Transactions on VehicularTechnology, vol. 66, no. 8, pp. 7563-7567, 2017.

[18] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, “Securetransmissiondesignsfornomasystemsagainstinternalandexternaleavesdropping,” IEEE Transactions on Information Forensicsand Security, vol. 15, pp. 2930–2943, 2020.

[19] R. M. Christopherand D. K. Borah, “Physicallayersecurityforweakuser in misonomausingdirectionalmodulation (nomad),” IEEE Communications Letters, vol. 24, no. 5, pp. 956–960, 2020.



Şekil 1



Şekil 2

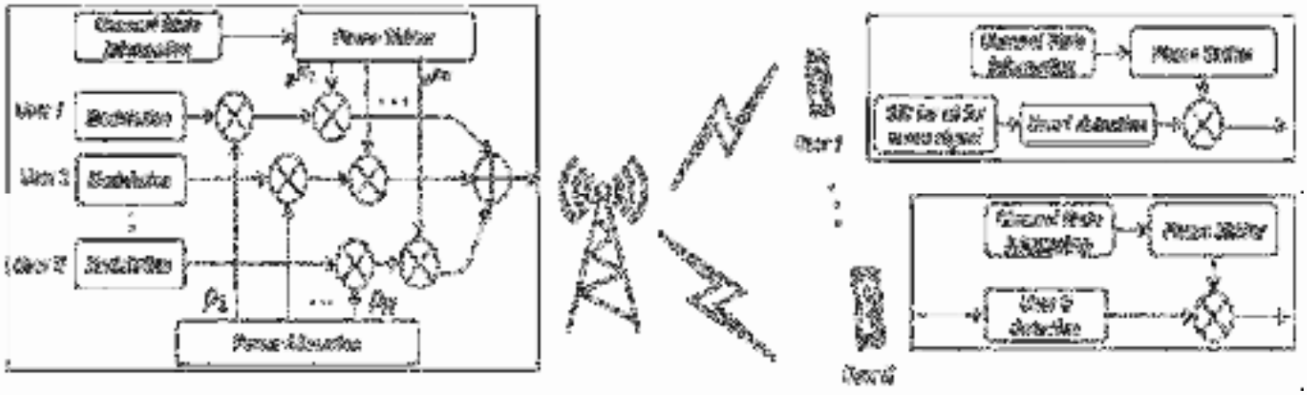


Figure 1

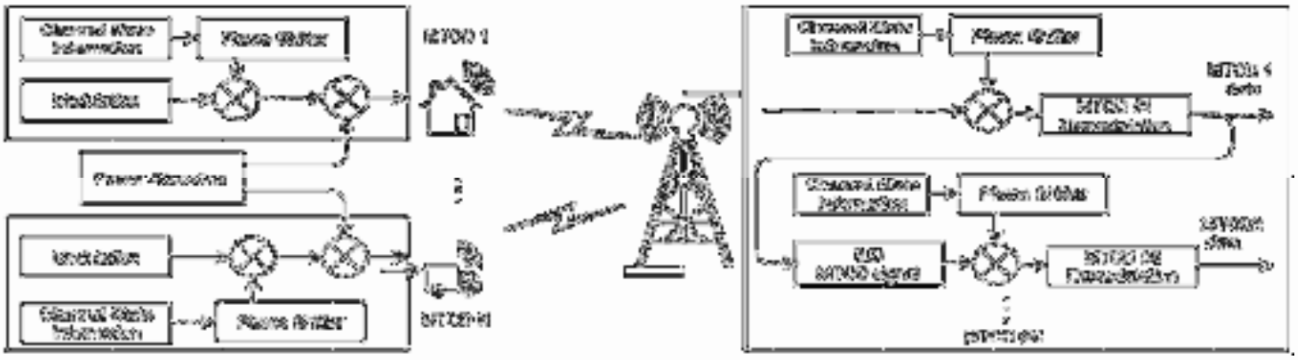


Figure 2