OZET

GÜVENLİ KABLOSUZ İLETİŞİME YÖNELİK DAĞITIK TAŞIYICI FREKANS OFSETİ DENGELEMESİ

Bu buluşta, kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine/ele geçirilmesine karşı korunmasına yönelik bir yöntem sunulmaktadır.

İSTEMLER

1. Güvenli kablosuz iletişime yönelik bir dağıtık taşıyıcı frekans ofseti dengelemesi yöntemi olup, aşağıdaki adımları içermektedir;
   - Koordine edici iletim noktalarının seçilmesi,
   - Her bir koordine edici iletim noktası ile istenen kullanıcı arasındaki taşıyıcı frekans ofsetinin tahmin edilmesi,
   - İsteğe bağlı olarak, koordine edici iletim noktası arasında iletilecek verilerin bölünmesi ve/veya her bir koordine edici iletim noktası ile kullanıcı arasındaki kanalın önceden denkleştirilmesi,
   - Tahmini taşıyıcı frekans ofsetinin önceden dengelenmesi,
   - Koordine edici iletim noktalarından iletimin başlatılması.

2. İstem 1'e göre bir yöntem olup, koordine edici iletim noktalarının seçilmesinin, alınan sinyal gücü göstergesi (RSSI), hizmet veren TP'ye göre alınan güç veya bunların bir kombinasyonuna bağlı olabilmesi ile karakterize edilmektedir.

3. İstem 1 veya 2'ye göre bir yöntem olup, koordinasyon takımının seçiminin, kapasite maksimizasyonu, spektral etkinlik veya enerji etkinliğine yönelik gerçekleştirilmesi ile karakterize edilmektedir.

4. İstem 1 veya 2'ye göre bir yöntem olup, koordine edici iletim noktalarının seçilmesinin, TP ile yasal alıcı arasındaki taşıyıcı frekans ofsetine (CFO) bağlı olabilmesi ile karakterize edilmektedir.

5. İstemler 1-4'ten herhangi birine göre bir yöntem olup, her bir koordine edici iletim noktası ile istenen kullanıcı arasındaki taşıyıcı frekans ofsetinin tahmininin, başlama ekleri kullanılarak veya kör bir şekilde gerçekleştirilmesi ile karakterize edilmektedir.

6. İstem 1-5'ten herhangi birine göre bir yöntem olup, derin sönümlemede olan alt taşıyıcıların bu belirli bağlantı için kullanılmadığı dinamik nokta seçiminin (DPS), tüm veya seçilen TP'lerden iletim sırasında derin sönümlemeler halinde gürültü artışları gibi sorunları önlemek için kullanılması ile karakterize edilmektedir.

7. İstemler 1-6'dan herhangi birine göre bir yöntem olup, farklı TP'lerden iletilecek verilerin bölünmesinin, aşağıdaki gibi olması ile karakterize edilmektedir

- bir sembol içi seviyesinde, burada bir TP, sembolün gerçek kısmını iletirken, farklı bir TP aynı sembolün sanal kısmını iletmektedir veya
- bir örnek seviyesinde, burada farklı TP'ler aynı sinyalin farklı örneklerini iletmektedir veya
- bir alt taşıyıcı seviyesinde, burada farklı TP'ler farklı alt taşıyıcıları iletmektedir.

TARİFNAME

GÜVENLİ KABLOSUZ İLETİŞİME YÖNELİK DAĞITIK TAŞIYICI FREKANS OFSETİ DENGELEMESİ

Teknik Alan

Bu buluşta, kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine/ele geçirilmesine karşı korunmasına yönelik bir yöntem sunulmaktadır.

Onceki Teknik

Günümüzde OFDM gibi çok taşıyıcılı sistemlerde fiziksel katman güvenliğine (PLS) yönelik aşağıdaki yaklaşımlar kullanılmaktadır:

Kablosuz Kanallardan Gizli Dizilerin Elde Edilmesi

Bu tür PLS tekniklerinde temel fikir, kablosuz kanaldan rastgele bir dizinin elde edilmesidir. Bu dizi daha sonra alıcı-vericiler arasında değiştirilecek bilginin şifrelenmesine yönelik bir anahtar olarak kullanılmaktadır. Ancak, anahtar oluşturma yaklaşımı, hatalı kanal tahmini ve kanal karşılıklılığı uyuşmazlığına karşı oldukça duyarlıdır.

İletilen Sinyaller ile birlikte Karıştırıcı (Gürültü/Bozucu) Sinyallerin Eklenmesi

Bu yaklaşımda yasal düğüm, yasal alıcıdaki performansı etkilemeden yasal olmayan alıcının performansını bozacak bir şekilde yasal kullanıcı kanalının boş alanından faydalanarak kasıtlı bir karıştırıcı sinyal eklemektedir. Ancak bu, bazı güç ve çıktıyı gözden çıkarabilmektedir.

Kanala Dayalı Uyarlama İletimi

Bu tekniklerde iletim parametreleri spesifik olarak, hizmet kalitesi (QoS) gereksinimlerini karşılamak üzere yasal alıcı-vericiler arasındaki kanala dayalı olarak ayarlanmaktadır. Bazı örnekler, Otomatik Tekrar Talebi (ARQ) ile uyarlama modülasyonu ve kodlaması sönümlemeye dayalı alt taşıyıcı aktivasyon tekniği, optimal güç tahsisine dayalı teknik, kanal kısaltma ve OFDM alt taşıyıcı indeks seçimini içermektedir. Ancak bu yaklaşımların sorunu,

yasal alıcı ile karşılaştırıldığında dinleyen kişi daha iyi bir kanala sahip olursa başarısız olmalarıdır.

Koordineli Çoklu Noktaya (CoMP) Dayalı Güvenlik

PLS'yi kolaylaştırmaya yönelik yukarıda bahsedilen genel yaklaşımların yanı sıra, kablosuz sistemlerin güvenli hale getirilmesine yönelik CoMP konseptinden faydalanmak için bazı çalışmalarda bulunmuştur.

Onceki teknikte, dinleyen kişi, yasal alıcı ile aynı yönde olursa iletişimi güvenli hale getiremediği için yönlü modülasyonun sınırlamasını ele almak için CoMP'den faydalanılmıştır. Koordine edici iletim noktaları (TP'ler), konuma dayalı güvenlik sağlayarak, bunların yalnızca alıcının konumunda doğru bir şekilde alınacağı şekilde yönlü modülasyon kullanarak aynı sinyalin kopyalarını iletmektedir. Ancak, saldıran kişi, yasal alıcı yakınında olursa istenen güvenlik seviyesini sağlamada bu yaklaşım da başarısız olmaktadır.

CoMP ayrıca, diğer konumlarda bozulmuş bir konstelasyon gözlemlenirken verilerin yalnızca bilgi demetlerinin kesişiminde kodunun çözülebileceği şekilde seyrek radyo ortamına yönelik kullanılmaktadır. Bu yaklaşım ayrıca, saldıran kişi yasal alıcıya yakın olursa güvenli iletişimi garanti etmemektedir.

Önceki teknikte, bir su altı senaryosunda dağıtık anten elemanlarından CoMP'ye dayalı iletimler sunulmaktadır, burada iletimlerin gücü ve zamanlaması, mesajların dinleyen kişide örtüşürken (ve karıştırıcı) yasal alıcıda örtüşmeyeceği şekilde manipüle edilmektedir.

Önceki teknikte güvenli kapsamı artırmak için bir dinamik CoMP şeması sunulmaktadır. Sunulan şema, yasal kullanıcıdan uzakta olan TP'lerin güvenlik ve enerji tüketimi endişeleri bakımından engellendiği yasal kullanıcılara yönelik alınan sinyal gücüne dayanmaktadır.

Bir CoMP şeması ayrıca birden çok referans düğümünün, dinleyen kişinin varlığında yasal iletişim performansını artırmak için UAV'den gönderilen yasal bilgiyi birlikte tespit ettiği, gizlilik sağlamak için insansız hava aracı (UAV) sistemlerinde kullanılmaktadır.

Taşıyıcı Frekans Ofseti (CFO) Dengelemesine Dayalı Güvenlik

Onceki teknikte bir CFO ön-dengelemesine dayalı PLS tekniği sunulmaktadır. Teknik, iletişimdeki yasal düğümler arasında yalnızca bir CFO'nun mevcut olduğu bir noktadan noktaya iletimi düşünmektedir. İletişimdeki düğümlerin herhangi bir çiftinden kaynaklanan CFO benzersizliği nedeniyle yazarlar, güvenli iletişimi kolaylaştırmanın bir yolu olarak yasal alıcıya ilişkin olarak vericide CFO'nun önceden dengelenmesini düşünmektedir. Ancak, literatürdeki birçok dayanıklı tek CFO tahmini tekniklerinin varlığı nedeniyle, bu tür yaklaşım tarafından sağlanan güvenlik kolayca bozulabilmektedir. Bu amaçla yazarlar, elde edilen güvenlik kalitesini artırmak amacıyla kanal ön-denkleştirmesi ile yaklaşımlarını tamamlamıştır. Ancak kanal ön-denkleştirmesinin, sinyalin yüksek tepe-ortalama güç oranına (PAPR) ilişkin bariz bir dezavantajı vardır.

Buluşun Amaçları ve Kısa Açıklama

Mevcut buluş, yukarıda bahsedilen dezavantajları gidermek ve ilgili tekniğe yeni avantajlar kazandırmak amacıyla kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine/ele geçirilmesine karşı korunmasına yönelik bir yöntem ile ilgilidir.

Kablosuz iletişimin yayımlama yapısı bunu çeşitli güvenlik tehditlerine eğilimli hale getirmektedir. Bu tehditlerden biri, ayrıca dinleme olarak bahsedilen iletişim gizliliğinin ihlalidir. Bu durumda, kötü niyetli bir düğüm/cihaz, iki yasal düğüm arasında devam eden iletişimi dinlemeye ve yorumlamaya çalışmaktadır. Klasik olarak, iletişimin güvenli hale getirilmesine yönelik kriptografi kullanılmaktadır, ancak gelecekteki kablosuz ağların artan heterojenliği ile bu yaklaşım, anahtar paylaşımı ve yönetimine ilişkin zorluklarla karşılaşmaktadır. Bu da, kablosuz iletimleri güvenli hale getirmek için kablosuz kanal ve donanım özelliklerinden faydalanan fiziksel katman güvenliği (PLS) yaklaşımlarının kullanımına teşvik etmektedir. Bu göz önünde tutularak, bu buluşta bahsedilen gibi PLS mekanizmaları son yıllarda giderek popüler hale gelmiştir.

Bu belgede açıklanan buluş, koordineli çoklu nokta (CoMP) konseptindeki birden çok verici düğümün, Uzun Dönem Evrim (LTE), 5G Yeni Radyo (NR) ve IEEE 802.11 tabanlı Wi-Fi ağları gibi kablosuz iletişim standartlarında yaygın olarak kullanılan ortogonal frekans bölmeli çoklu erişim (OFDM) gibi çok taşıyıcılı sistemlere yönelik güvenli iletişim sağlamak için birlikte çalıştığı bir PLS mekanizması sağlamaktadır.

OFDM gibi çok taşıyıcılı sistemler, kanalı, her birinin uyum bant genişliğinden daha küçük olduğu birçok dar alt kanala (veya alt taşıyıcıya) bölerek, kanalı düz bir sönümleme yapana dönüştürerek frekans seçmeli sönümleme sorununu azaltması nedeniyle popülerdir. Ancak, bu durumda sistem, güvenilir iletişimi sağlamak için frekans alanında alt taşıyıcıların ortogonalliğine dayanmaktadır. Herhangi bir ortogonallik kaybı, ciddi performans bozulmasına yol açan taşıyıcılar arası girişime yol açabilmektedir. Bu da OFDM'yi ve diğer çok taşıyıcılı sistemleri, taşıyıcılar arası girişim (ICI) ile sonuçlanarak, Doppler ve taşıyıcı frekans ofseti (CFO) gibi bozulmalar nedeniyle gerçekleşebilen frekans senkronizasyonunda herhangi bir uyumsuzluğa eğilimli hale getirmektedir.

Bu buluşta, kablosuz iletimleri güvenli hale getirmek için bu OFDM sınırlamasından faydalanılmaktadır. Vericide CFO biliniyorsa bu, iletim gerçekleştirilmeden önce önceden dengelenebilmektedir. Farklı kullanıcı ekipmanı (UE)- iletim noktası (TP) bağlantıları tarafından deneyimlenen CFO'nun farklı olması nedeniyle sunulan buluş, sinyali güvenli hale getirmek için CoMP ağı tarafından sağlanan farklı TP'ler ile istenen kullanıcı arasında farklı CFO'lardan faydalanmaktadır. İstenen kullanıcıya yönelik ön-dengeleme, bunun için herhangi bir bozulma ile sonuçlanmamaktadır, ancak, diğer yandan bu dengelenen ofset, yasal olmayan düğüm için istenmeyen bir girişim olarak görünmektedir. Diğer bir deyişle, birlikte çalışan TP'ler tarafından sağlanan, önceden dengelenen birden çok CFO, yasal olmayan düğüm tarafından alınan sinyalin frekansa yayılmasına neden olmaktadır, böylece dinlemeyi daha zor hale getiren bir ICI sorununa neden olmaktadır.

Özellikle CoMP olmak üzere birlikte çalışan ağlardan faydalanan mevcut PLS yöntemi yalnızca bölgeye dayalı güvenlik sağlayabilmektedir. Diğer bir deyişle, iletişim gizliliği, yalnızca saldıran kişi yasal UE'nin yakınında veya sinyal iletimi yönü boyunca olursa sağlanmaktadır. Bunlara ek olarak, önceki teknikte sunulan CFO ön-dengelemesine dayalı PLS yaklaşımı, saldıran kişinin uygulanan tek frekans kaymasını başarılı bir şekilde tahmin edebilmesi ve dengeleyebilmesi halinde güvenlik kalitesini güçlendirmek üzere kanal ön-denkleştirmesi adımına dayanmaktadır. Ancak, kanal ön-denkleştirmesi potansiyel olarak istenen performansı sürdürmek amacıyla bazı sıkı donanım gereksinimleri uygulayan bir PAPR sorununa neden olabilmektedir.

Sunulan buluş, birlikte çalışan ağ topolojilerinde coğrafi olarak ayrı TP'lerin CFO'larından faydalanarak yukarıdaki sorunların her ikisini çözmektedir. Sunulan güvenlik yönteminin spesifik bir yasal UE'ye ilişkin olarak CFO ön-dengelemesine dayanması nedeniyle, saldıran kişinin sinyalinin kalitesi, saldıran kişi yasal düğüm ile aynı yerde bulunsa dahi bozulacaktır. Bu noktada düşünülen sistemde ayrı olarak önceden dengelenen birden çok CFO'ye sahip olmamız, saldıran kişinin, önceki teknikte sunulan noktadan noktaya iletim durumunda gözlemlenen tek frekans kayması ile karşılaştırıldığında baş etmesi çok daha zor olan birden çok bağımsız frekans kaymasına sahip bir sinyal almasına neden olacaktır.

Ayrıca, saldıran kişinin yasal alıcı yakınında olmaması, ancak koordine edici TP'lerin herhangi birinin kapsama alanında olması halinde, sinyali dinleyebilmesi olasıdır. Bu durumda, sunulan buluş, bahsedilen PAPR sorununu önlemek için bazı modifikasyon ile kanal ön-denkleştirmesi ile bağlantılı olarak kullanılabilmektedir. Yine yasal düğüm ile bağımsız kanallar deneyimleyen coğrafi olarak ayrı birden çok TP varlığından faydalanmaktayız. Bu durumda, bir TP-yasal-UE bağlantısının derin sönümlemelerinde yer alan alt taşıyıcılar, bu belirli TP için kapatılabilmekte ve birlikte çalışan TP'lerin geri kalanından iletilebilmektedir. Bu da, her bir TP için derin sönümlemelerin konumlarında kanal ön-denkleştirmesi gerçekleştirme ihtiyacını ortada kaldırmakta, böylece PAPR sorununu çözmektedir.

Bulunan şema, tüm kapsama alanındaki PLS'yi kolaylaştırmak için kanal ön-denkleştirmesi ve çoklu CFO ön-dengelemesi ile hibrit bir ortak iletim (JT) ve dinamik nokta seçimi (DPS) (H-JT-DPS) mekanizması oluşturmaktadır. Çoklu CFO ön-dengelemesi, saldıran kişi yasal düğüm ile aynı yerde bulunsa dahi iletişim gizliliğini sağlarken, kanal ön-denkleştirmesi, saldıran kişi kapsama alanı içinde herhangi bir diğer konumda olduğunda güvenlik sağlamaktadır. H-JT-DPS, derin sönümleme konumlarında kanal ön-denkleştirmesi nedeniyle ortaya çıkabilen olası PAPR sorununu önlemektedir.

Birlikte çalışan TP'lerin birinin yakınında veya herhangi bir TP'nin iletim yönü boyunca olan saldıran kişiye karşı güvenliği kolaylaştırmak üzere çoklu CFO ön-dengelemesi ile bağlantılı olarak kullanılabilen diğer bir olası yaklaşım, veri bölmedir. Veri bölme ile, birlikte çalışan AP'lerin her biri, uygun bir şekilde bunun şifresini çözebilmek için TP'lerin tamamından

sinyal almanın gerekli olacağı şekilde yasal düğüme yönelik verinin farklı bölümünü iletmektedir.

Aslında, burada bulunan çoklu CFO ön-dengelemesi şeması ayrıca, bölgeye dayalı güvenliklerini kapsama alanı içinde bir tam güvenliğe kadar genişletmek için birlikte çalışan TP'lere dayalı diğer herhangi bir güvenlik şeması tarafından kullanılabilmektedir.

Dinleyen kişilere karşı koruma sağlamak için bu buluşu herhangi bir kablosuz iletişim teknolojisi kullanabilmektedir. Ancak, her iki standartta çoklu nokta koordinasyonu desteği ve OFDM gibi çok taşıyıcılı şemaların kullanımı nedeniyle 3GPP'ye dayalı hücresel ve IEEE 802.11'e dayalı Wi-Fi ağları gibi standartlar buluş ile özellikle ilgilidir.

Buluşun Avantajları:

Teknik Yararlılık

Sunulan buluş, güvenli ve gizli iletişim sağlamak için coğrafi olarak dağıtık birden çok iletim noktasının varlığını kullanan gelecekteki kablosuz ağlara yönelik karmaşıklığı az bir yöntem sağlamaktadır. Bu, her bir bağlantının bağımsız CFO'ya sahip olduğu, birlikte çalışan TP'ler ile yasal alıcı arasındaki farklı bağlantılar aracılığıyla veri gönderilerek gerçekleştirilmektedir. Yasal olmayan alıcı tarafından deneyimlenenlerin yanı sıra bu CFO'ların bağımsızlığı, ön-dengeleme, yasal alıcının herhangi bir ICI deneyimlenmemesini sağlarken, yasal olmayan alıcı için durumun böyle olmamasını sağlamaktadır. Yasal olmayan alıcı, ICI'ye neden olan ve dinleme olasılığını bozan, frekans alanında bir yayılma deneyimlemektedir.

Buluş Şekillerinin Açıklaması

Şekiller, aşağıda açıklandığı gibi mevcut buluş ile geliştirilen güvenli kablosuz iletişime yönelik dağıtık taşıyıcı frekans ofset dengelemesine yönelik bir yöntemi daha fazla açıklamak amacıyla kullanılmıştır:

Şekil 1: Mevcut tarifnamenin belirli yönlerine göre kablosuz iletişime yönelik temel işlemlerin bir akış şeması.

Şekil 2: Mevcut tarifnamenin alternatif bir uygulama seçeneği

Şekil 3: Mevcut tarifnamenin diğer bir alternatif uygulama seçeneği.

Şekil 4: Yasal düğüme ilişkin CFO ön-dengelemesi ve yasal ve saldıran kişinin düğümlerde alınan sinyal üzerindeki etkisinin gösterimi

Şekil 5: Aşağı bağlantı iletiminin gizliliğini kolaylaştırmak için sunulan buluşu uygulayan birlikte çalışan ağ örneği

Şekil 6: Tüm kapsama alanı boyunca güvenlik sağlamak için gelişmiş bir kanal ön-denkleştirmesi tekniği ile çoklu CFO ön-dengelemesi gösterimi.

Şekillerdeki Elemanlar ve Adımların Açıklaması:

TP: İletim Noktası

CFO: Taşıyıcı Frekans Ofseti

UE: Kullanıcı Ekipmanı

Adımlar:

110, koordine edici TP'lerin seçimidir.
120, her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir.
130, Bu adımda, adımda (120) tahmin edilen CFO'ya dayalı olarak gerekli dengeleme hesaplanmaktadır.
140, koordine edici TP'lerden kullanıcı verilerinin iletimidir
210, koordine edici TP'lerin seçimidir.
220, her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir.
230, TP'ler ile kullanıcı arasındaki tüm bağlantılarda deneyimlenen kanal ön-denkleştirmesidir.

240, adımda (220) elde edilen tahmin edilen CFO'nun ön-denkleştirmesidir

250, koordine edici TP'lerden kullanıcı verilerinin iletimidir

310, koordine edici TP'lerin seçimidir.

320, her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir.

330, kullanıcı verileri, koordine edici her bir TP'nin bölünmüş verinin bir kısmını gönderdiği farklı kısımlara bölünmektedir.

340, adımda (220) elde edilen tahmin edilen CFO'nun ön-denkleştirmesidir

350, koordine edici TP'lerden kullanıcı verilerinin iletimidir

410, CFO ön-denkleştirmesi öncesinde taban bant sinyal spektrumudur.

420, CFO ön-denkleştirmesi prosesidir.

430, CFO ön-denkleştirmesi sonrasında taban bant sinyal spektrumudur.

440, yasal TP'dir.

450, yasal alıcı düğümdür.

460, yasal düğüm tarafından alınan doğru şekilde frekans senkronizasyonu uygulanmış taban bant sinyalini göstermektedir.

470, saldıran kişi düğümüdür.

480, hatasız frekans senkronizasyonu ile saldıran kişi tarafından alınan sinyaldir.

510, CFO ön-dengelemesi adımıdır.

520, UE'ye birlikte hizmet veren coğrafi olarak ayrı TP'lerdir.

530, yasal alıcı düğümdür (UE)

540, yasal alıcı düğüm tarafından alınan frekans senkronizasyonu uygulanmış sinyaldir. 550, iletişimi dinlemeyi amaçlayan saldıran kişi düğümüdür.

560, saldıran kişinin düğümünde bozulma (frekans yayılması) ile alınan sinyaldir.

610, birlikte çalışan TP'lerin her birinde bir frekans alanı tek-çıkmalı kanal ön-denkleştirme prosesini temsil etmektedir

620, birlikte çalışan TP'lerin her birinde CFO ön-dengelemesi adımıdır

630, belirli bir yasal UE'ye birlikte hizmet eden coğrafi olarak ayrı TP'leri temsil etmektedir

640, yasal UE'ye ilişkin olarak her bir TP tarafından deneyimlenen bağımsız frekans kanalı yanıtlarını (CFR) temsil etmektedir

650, yasal UE'ye iletilecek olan verileri taşıyan derin sönümlemelere dayalı planlı alt taşıyıcıları temsil etmektedir.

660, bağımsız olarak meydana gelen derin sönümlemeler

Buluşun Ayrıntılı Açıklaması

Buluşun yeniliği, buluş kapsamını sınırlandırmayan ve yalnızca buluş konusunu aydınlatması amaçlanan örnekler ile açıklanmıştır. Mevcut buluş aşağıda ayrıntılı olarak açıklanmıştır.

Buluş, kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine/ele geçirilmesine karşı korunmasına yönelik bir yöntemdir.

Mevcut tarifnamenin belirli açıları:

Buluşun bir yapılandırması, bir kablosuz iletişim aracının kötü niyetli dinleyen kişiler tarafından dinlenmesinin önlenmesine yönelik bir yöntem ile ilgilidir, burada;

- Sunulan buluşun ilk adımı (110), koordine edici iletim noktalarının (TP'ler) seçilmesinden oluşmaktadır. Bu seçim, alınan sinyal gücü göstergesi (RSSI), hizmet veren TP'ye göre alınan güç veya her ikisinin bir kombinasyonu gibi farklı kriterlere bağlı olabilmektedir. Koordinasyon takımı seçimi ayrıca kapasite maksimizasyonu, spektral etkinlik, enerji etkinliği vb. gibi farklı amaçlara/kısıtlamalara yönelik gerçekleştirilebilmektedir. Buna ek olarak, bu buluşa göre, koordine edici TP seçimine yönelik bir kriter olarak TP ile yasal alıcı arasında taşıyıcı frekans ofsetini (CFO) düşünmek mümkündür.
- İkinci adımda (120), her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir. CFO tahmini, başlama ekleri kullanılarak veya kör bir şekilde gerçekleştirilebilmektedir.
- Adımda (120) tahmin edilen CFO'ya dayalı olarak, gerekli dengeleme adımda (130) hesaplanmaktadır.
- Daha sonra adım (140) seçilen TP'lerin tamamından veya bir kısmından iletimi başlatmaktadır. Burada farklı TP'lerden iletim aynı veriyi veya farklı veri kısımlarını taşıyabilmektedir.

Şekil 2, mevcut tarifnamenin alternatif bir uygulamasını açıklayan bir akış şemasıdır, böylece diğer bir buluş yapılandırması, bir kablosuz iletişim aracının kötü niyetli dinleyen kişiler tarafından dinlenmesini önlemeye yönelik bir yöntem ile ilgilidir, burada:

- Sunulan buluşun ilk adımı (210), koordine edici TP'lerin seçilmesinden oluşmaktadır. Bu seçim, alınan sinyal gücü göstergesi (RSSI), hizmet veren TP'ye göre alınan güç veya her ikisinin bir kombinasyonu gibi farklı kriterlere bağlı olabilmektedir. Koordinasyon takımı

seçimi ayrıca kapasite maksimizasyonu, spektral etkinlik, enerji etkinliği vb. gibi farklı amaçlara/kısıtlamalara yönelik gerçekleştirilebilmektedir. Buna ek olarak, bu buluşa göre, koordine edici TP seçimine yönelik bir kriter olarak TP ile yasal alıcı arasında CFO'yu düşünmek mümkündür.

- İkinci adımda (220), her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir. CFO tahmini, başlama ekleri kullanılarak veya kör bir şekilde gerçekleştirilebilmektedir.
- Adımda (220) tahmin edilen CFO'ya dayalı olarak, gerekli dengeleme adımda (230) gerçekleştirilmektedir.
- Adım (240) her bir TP-UE bağlantılarına yönelik kanal ön-denkleştirmesini gerçekleştirilmektedir.
- Daha sonra adım (250) seçilen TP'lerin tamamından veya bir kısmından iletimi başlatmaktadır. Yüksek PAPR gibi sorunları önlemek amacıyla, derin sönümlemede olan alt taşıyıcıların bu belirli bağlantı için kullanılmayacağı şekilde dinamik nokta seçimi (DPS) kullanılabilmektedir.

Şekil 3, mevcut tarifnamenin alternatif bir uygulamasını açıklayan bir akış şemasıdır, böylece diğer bir buluş yapılandırması, bir kablosuz iletişim aracının kötü niyetli dinleyen kişiler tarafından dinlenmesini önlemeye yönelik bir yöntem ile ilgilidir, burada:

- Sunulan buluşun ilk adımı (310), koordine edici TP'lerin seçilmesinden oluşmaktadır. Bu seçim, alınan sinyal gücü göstergesi (RSSI), hizmet veren TP'ye göre alınan güç veya her ikisinin bir kombinasyonu gibi farklı kriterlere bağlı olabilmektedir. Koordinasyon takımı seçimi ayrıca kapasite maksimizasyonu, spektral etkinlik, enerji etkinliği vb. gibi farklı amaçlara/kısıtlamalara yönelik gerçekleştirilebilmektedir. Buna ek olarak, bu buluşa göre, koordine edici TP seçimine yönelik bir kriter olarak TP ile yasal alıcı arasında CFO'yu düşünmek mümkündür.
- İkinci adımda (320), her bir TP kendisi ile istenen kullanıcı arasındaki CFO'yu tahmin etmektedir. CFO tahmini, başlama ekleri kullanılarak veya kör bir şekilde gerçekleştirilebilmektedir
- Adım (330), farklı TP'lerden iletilecek verilerin bölünmesini kapsamaktadır. Bu bölme işlemi, bir sembol içi seviyesinde (örneğin, bir TP, sembolün gerçek kısmını iletebilirken, aynı sembolün sanal kısmı aynı bir sinyal tarafından iletilmektedir) veya bir alt taşıyıcı seviyesinde (burada farklı TP'ler farklı alt taşıyıcıları iletmektedir) olabilmektedir.

- Adımda (320) tahmin edilen CFO'ya dayalı olarak, gerekli dengeleme adımda (340) gerçekleştirilmektedir.
- Daha sonra adım (350) seçilen TP'lerin tamamından veya bir kısmından iletimi başlatmaktadır.

Burada, Şekil 2 ve Şekil 3'ün (ve bunlardaki adımların) karşılıklı olarak dışlayıcı olmadığı, diğer bir deyişle, daha alternatif uygulamalar oluşturmak için farklı uygulamaların farklı yollarda kombine edilebileceği göz önünde tutulmalıdır.

Şekil 4'te açıklanan yöntem, yasal düğüme ilişkin CFO ön-dengelemesi ve yasal düğüm ve saldıran kişinin düğümünde alınan sinyal üzerindeki etkisinin bir gösterimi ile ilgilidir.

Şekil 4'ün Açıklaması:

Adımda (420), frekans ofseti (f_{1-UE}^{CFO}) yasal UE alıcısına (450) yönelik taban bant sinyaline (410) uygulanmaktadır. Frekans ofseti (f_{1-UE}^{CFO}), yasal verici (440) ile yasal alıcı (450) arasındaki beklenen CFO'ya eşittir. Adım (420), daha sonra yasal vericiden (440) iletilen bir frekans kayması uygulanmış sinyal (430) ile sonuçlanmaktadır. Alınması üzerinde frekans kayması uygulanmış sinyal (430) üzerindeki frekans kayması, sorunsuz şekilde alınan bir sinyal (460) ile sonuçlanarak yasal verici (440) ile yasal alıcı (450) arasındaki CFO ile sıfırlanmaktadır.

Saldıran kişinin düğümünde (470), frekans kayması uygulanmış sinyal (430) üzerindeki frekans kayması, yasal verici (440) ile saldıran kişi düğümü (470) arasındaki CFO ile sıfırlanmamaktadır, bunun yerine, hatasız frekans senkronizasyonu (480) ile saldıran kişi tarafından alınan sinyal olan alınan sinyal bir bileşik rastgele frekans kaymasına maruz kalmaktadır.

Şekil 5'in Açıklaması:

Şekil 4'ün birden çok verici TP'lere (520) uzantısı. Frekans kayması adımı, CFO ön-dengeleme adımı olan adımda (510) her bir TP'de gerçekleştirilmektedir. Her bir TP'de (520) taban bant sinyaline uygulanan frekans kayması, ilgili TP ile yasal alıcı düğüm (530) arasındaki CFO ile belirlenmektedir. Şekil 4'te durum bu olduğundan, CFO ön-dengeleme adımında (510) uygulanan frekans kaymalarının her biri, sorunsuz şekilde frekans

senkronizasyonu uygulanmış alınan sinyal (540) ile sonuçlanarak, yasal alıcı düğüme (530) ulaşması üzerine ilgili CFO ile sıfırlanmaktadır. Bu tür sıfırlanmalar, ICI ile doldurulan ve böylece şifresinin çözülmesi zor olan bir frekans yayılmalı sinyale (560) yol açarak saldıran kişinin düğümünde (550) meydana gelmemektedir.

Şekil 5'te açıklanan yöntem, aşağı bağlantı iletiminin gizliliğini kolaylaştırmak için sunulan buluşu uygulayan birlikte çalışan ağın bir örneği ile ilgilidir.

Şekil 6, tüm kapsama alanı boyunca güvenliği kolaylaştırmak için ortak kanal ön-denkleştirmesi ve çoklu CFO ön-dengelemesinin uygulamasını göstermektedir. Gelişmiş ön-denkleştirme yaklaşımı, hibrit bir ortak-iletim ve dinamik-nokta-seçimi (H-JT-DPS) tekniği sunarak derin sönümleme konumlarında ön-denkleştirmeyi önlemektedir.

Şekil 6'da, (660), yasal UE'ye iletilecek olan verileri taşıyan derin sönümlemelere dayalı planlı alt taşıyıcıları temsil etmektedir. Her bir TP'nin CFR'sine dayalı olarak, bu belirli TP için bazı alt taşıyıcılar kapatılmakta ve bu konumda nispeten daha iyi CFR ile diğer TP tarafından iletilmektedir (diğer bir deyişle, alt taşıyıcıya dayalı DPS). Böylece, her bir TP, derin sönümleme konumlarında kanalı önceden denkleştirmek zorunda değildir, böylece yüksek PAPR sorunu önlenmektedir.

Şekil 6'nın Açıklaması:

Bu şekil, PAPR sorununa yol açmadan kanal ön-denkleştirmesini kolaylaştıran H-JT-DPS konseptinin uygulamasını göstermektedir. Birlikte çalışan TP'lerin her biri, derin sönümleme konumlarda (660) iletimi önlemekte ve böylece adımda (610) bu konumlarda kanal yanıtını önceden denkleştirmeyi göz ardı edebilmektedir. İlgili konumlarında derin sönümlemeler nedeniyle bazı TP'ler için bazı alt taşıyıcılar kapatılırken, TP'lerin tamamında nispeten iyi kanal durumu deneyimleyen diğer alt taşıyıcıların bunların tamamından iletildiği anlaşılmalıdır. Bu, bazı alt taşıyıcılara DPS ve diğerlerine JT uygulamaya denktir. Adım (620), yasal UE (şekilde gösterilmemiştir) ile belirli bir TP'nin (630) beklenen CFO'suna dayalı olarak sinyale frekans kayması uygulamaktadır.

Proses adımları;

A. Koordine edici iletim noktalarının seçilmesi (110, 210, 310, 520, 630)

Önceki teknik, koordinasyon TP seçimine yönelik farklı mekanizmalara sahip olurken (önceki bölümde açıklandığı üzere), buluş ayrıca yeni bir alternatif, diğer bir deyişle TP ile yasal alıcı arasındaki CFO'ya dayalı olarak koordine edici TP'lerin seçimini açıklamaktadır.

B. Çoklu/dağıtık CFO tahmini ve dengelemesi (120, 130, 220, 230, 320, 340, 420, 510, 620) Genel olarak CFO tahmini ve dengelemesi iyi çalışılmaktadır. Ancak, güvenli iletişim sağlamak için bir CoMP ortamında birden çok TP ve CFO'dan faydalanılması, yeni bir öneridir.

C. CFO ön dengelemesi, güvenli kapsama bölgesini artırmak üzere kanal ön-denkleştirmesi ile bağlantılı olarak uygulanabilmektedir. İsteğe bağlı kanal ön-denkleştirmesi adımı Şekil 6'da adımda (610) belirtilmektedir.

D. Farklı TP-kullanıcı bağlantılarına yönelik derin sönümlemelerdeki alt taşıyıcıları önlemek üzere hibrit DPS ve JT. Bu da, PAPR sorununu artırmadan her bir TP'de sorunsuz bir kanal ön-denkleştirmesini kolaylaştırmaktadır (610).

E. İletimden önce ayrıca, kanal ön-denkleştirmesi yerine birçok CFO ile bağlantılı olarak veri bölme uygulanabilmektedir. CoMP'ye dayalı yönlü modülasyonlar gibi diğer teknikler de kullanılabilmektedir (330).

Buluş, kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine/ele geçirilmesine karşı korunmasına yönelik bir yöntemdir. Böylece, iletişim güvenliği ile ilgili endüstriye uygulanabilmektedir.

Yukarıdaki tüm bilgilere dayalı olarak, güvenli kablosuz iletişime yönelik bir dağıtık taşıyıcı frekans ofseti dengelemesi yöntemi aşağıdaki adımları içermektedir;

- Koordine edici iletim noktalarının seçilmesi,
- Her bir koordine edici iletim noktası ile istenen kullanıcı arasındaki taşıyıcı frekans ofsetinin tahmin edilmesi,
- Tahmini taşıyıcı frekans ofsetinin dengelenmesi,
- Koordine edici iletim noktalarından iletimin başlatılması.

Güvenli kablosuz iletişime yönelik bir dağıtık taşıyıcı frekans ofseti dengelemesi yöntemi aşağıdaki adımları içermektedir;

- Koordine edici iletim noktalarının seçilmesi,
- Her bir koordine edici iletim noktası ile istenen kullanıcı arasındaki taşıyıcı frekans ofsetinin tahmin edilmesi,
- Her bir koordine edici iletim noktası ile kullanıcı arasındaki kanalın önceden denkleştirilmesi,
- Her bir iletim noktasında tahmini taşıyıcı frekans ofsetinin dengelenmesi,
- Koordine edici iletim noktalarından iletimin başlatılması

Güvenli kablosuz iletişime yönelik bir dağıtık taşıyıcı frekans ofseti dengelemesi yöntemi aşağıdaki adımları içermektedir;

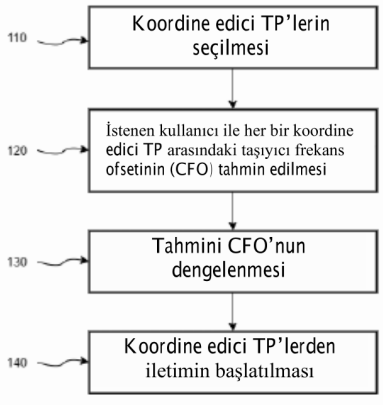
- Koordine edici iletim noktalarının seçilmesi,
- Her bir koordine edici iletim noktası ile istenen kullanıcı arasındaki taşıyıcı frekans ofsetinin tahmin edilmesi,
- Koordine edici iletim noktası arasında iletilecek verilerin bölünmesi,
- Her bir koordine edici iletim noktası ile kullanıcı arasındaki kanalın önceden denkleştirilmesi,
- Her bir iletim noktasında tahmini taşıyıcı frekans ofsetinin dengelenmesi,
- Koordine edici iletim noktalarından iletimin başlatılması.

Bu temel konseptler arasında, buluşun konusuna ilişkin birkaç yapılandırma geliştirmek mümkündür; dolayısıyla buluş, burada açıklanan örnekler ile sınırlandırılamamaktadır ve buluş esas olarak istemlerde tanımlandığı gibidir.

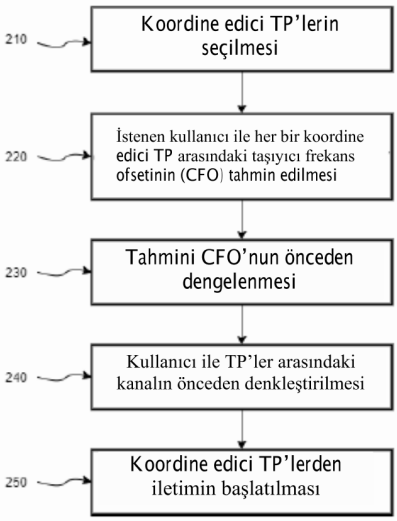
Teknikte uzman bir kişinin, benzer yapılandırmalar kullanarak buluş yeniliğini aktarabileceği ve/veya bu tür yapılandırmaların, ilgili teknikte kullanılanlara benzer diğer alanlara uygulanabileceği anlaşılırdır. Dolayısıyla ayrıca bu tür yapılandırmaların, yenilik kriterlerinden ve tekniğin durumunu aşma kriterinden yoksun olduğu anlaşılırdır.

Buluşun Endüstriyel Uygulanabilirliği

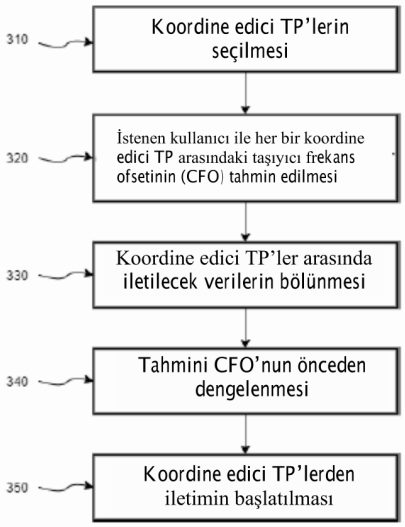
Buluş, dinleme saldırılarına karşı iletişim bağlantılarının gizliliğini artırmaktadır. Kanal ilintisi nedeniyle, dinleyen kişi, yasal kullanıcıya oldukça yakın bulunduğunda iletişim gizliliği sağlayamayan mevcut fiziksel katman güvenliği tekniklerinin çoğunun aksine, bulunan yöntem, bu tür dinleyen kişiye (diğer bir deyişle, yasal kullanıcı ile birlikte bulunan dinleyen kişiler) karşı dahi iletişim gizliliği sağlamaktadır.



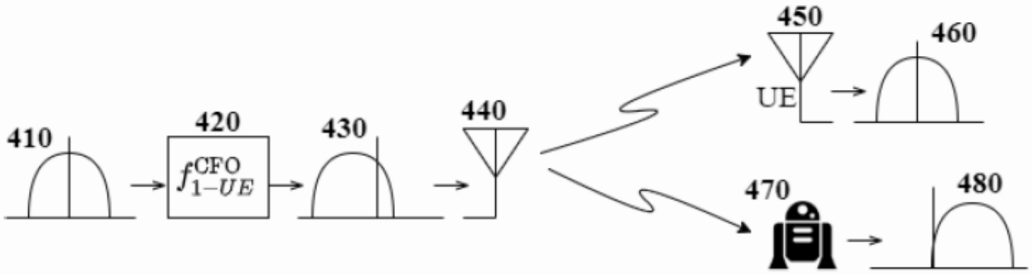
ŞEKİL 1



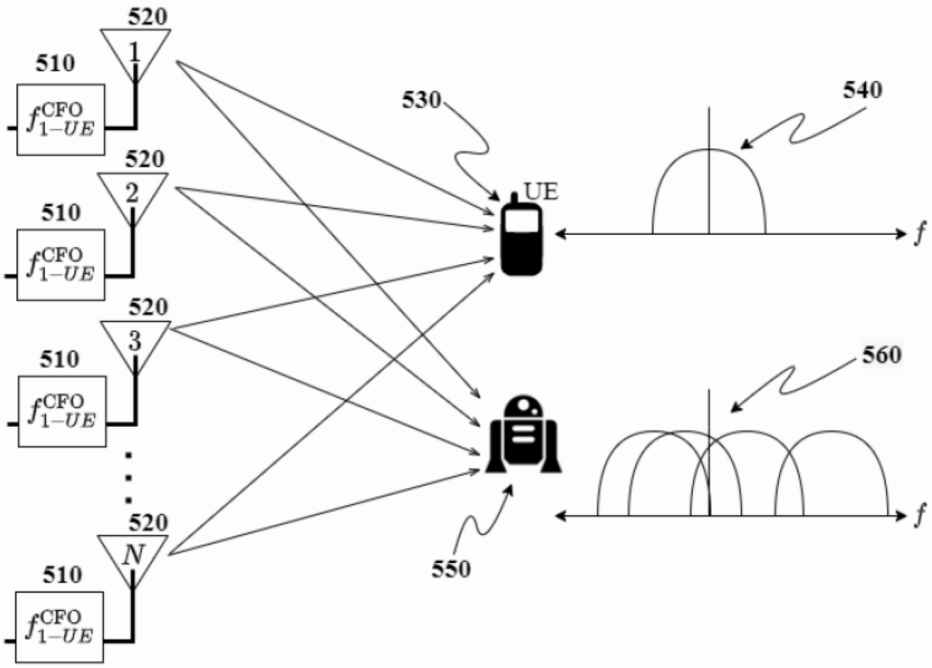
ŞEKİL 2


310
Koordine edici TP'lerin seçilmesi
320
İstenen kullanıcı ile her bir koordine edici TP arasındaki taşıyıcı frekans ofsetinin (CFO) tahmin edilmesi
330
Koordine edici TP'ler arasında iletilecek verilerin bölünmesi
340
Tahmini CFO'nun önceden dengelenmesi
350
Koordine edici TP'lerden iletimin başlatılması

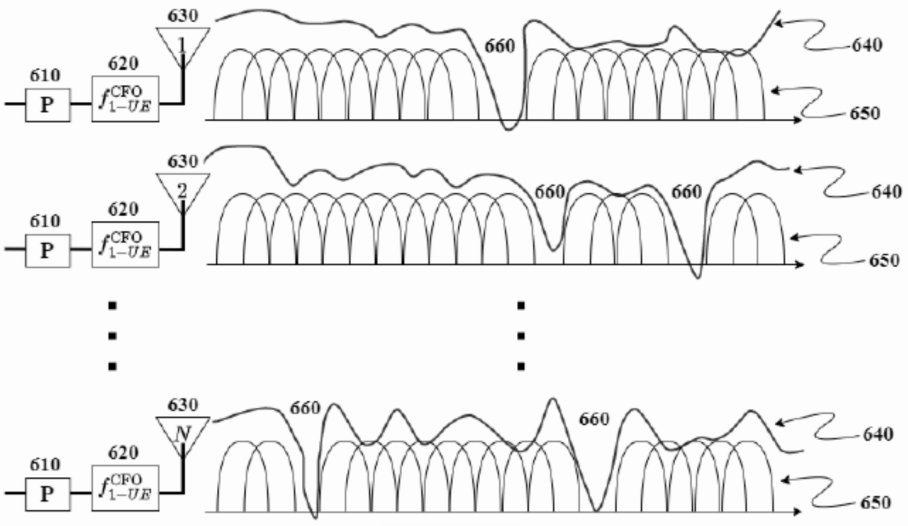
ŞEKİL 3



ŞEKİL 4


520
1
510
f_{1-UE}^{CFO}
530
540
520
2
510
f_{1-UE}^{CFO}
UE
f
520
3
510
f_{1-UE}^{CFO}
560
520
N
510
f_{1-UE}^{CFO}
550
f

ŞEKİL 5


630
1
610
620
P
f^{CFO}_{1-UE}
660
640
650
630
2
610
620
P
f^{CFO}_{1-UE}
660
660
640
650
630
N
610
620
P
f^{CFO}_{1-UE}
660
660
640
650

ŞEKİL 6