ÖZET

GÜVENLİ KABLOSUZ İLETİŞİM İÇİN GECİKME-DOPPLER TABANLI ŞİFRE ÜRETİM YÖNTEMİ

En az iki cihaz arasında güvenli kablosuz iletişime yönelik bilgisayar uygulamalı bir Gecikme-Doppler etki alanı tabanlı şifre oluşturma yöntemi.

İSTEMLER

1. En az iki cihaz arasında güvenli kablosuz iletişime yönelik bilgisayar tarafından uygulanan bir şifre oluşturma yöntemi olup, aşağıdaki adımlar ile karakterize edilmektedir;

Bir Gecikme-Doppler ızgarasının tasarlanması ve bir pilot sembolün yerinin belirlenmesi,

Gecikme-Doppler pilot sinyallerinin her iki cihazda da zaman alanına dönüştürülmesi,

Zaman alanlı pilot sinyallerin cihazlar tarafından birbirine iletilmesi ve pilot sinyallerin cihazlar tarafından tekrar Gecikme-Doppler alanına dönüştürülmesi,

Her iki cihazda Gecikme-Doppler değerlerinin elde edilmesi,

Her iki cihazda Gecikme-Doppler değerlerinin endekslerinin elde edilmesi,

Her iki cihazda fraksiyonel Gecikme-Doppler değerlerinin elde edilmesi ve nicelenmesi,

Endeksler ve nicelenmiş fraksiyonel Gecikme ve Doppler değerleri, güvenlik şifresi olarak kullanılmak üzere ikili gösterime dönüştürülmektedir.

2. Ayrıca, sistemin frekans bölmeli çift yönlü veya zaman bölmeli çift yönlü sistemden hangisi olduğunun belirlenmesi adımını içermesi ile karakterize edilen, İstem 1'e göre yöntem.

3. Dönüştürülen pilot sinyallerin birbirlerine eş zamanlı olarak iletilmesi ile karakterize edilen, İstem 1 veya 2'ye göre yöntem.

4. Öncelikle dönüştürülen pilot sinyalin cihazlardan birine diğer cihazlardan biri tarafından iletilmesi ve alıcı cihazda Gecikme-Doppler değerlerinin elde edilmesi ve ardından pilot sinyalinin verici cihaza iletilmesi ve verici cihazda Gecikme-Doppler değerlerinin elde edilmesi ile karakterize edilen, İstem 1 veya 2'ye göre yöntem.

5. Gecikme-Doppler değerlerinin endekslerini bir kanal tahmin çerçeve yöntemi veya çerçevesi ile elde edilmesi ile karakterize edilen, İstem 1'e göre yöntem.

6. Izgaranın her iki yöndeki boyutunun, mevcut bant genişliği, mevcut alt taşıyıcı sayısı, alt taşıyıcı aralığı ve iletim süresinden en az birine göre hesaplanması ile karakterize edilen, İstem 1'e göre yöntem.

7. Gecikme-Doppler alanının zaman alanına dönüştürülmesinin, ters basit Fourier dönüşümü ve ardından Heisenberg dönüşümü ile gerçekleştirilmesi ile karakterize edilen, İstem 1'e göre yöntem.

8. Zaman alanının Gecikme-Doppler alanına dönüştürülmesinin, Wigner dönüşümü ve ardından basit Fourier dönüşümü ile gerçekleştirilmesi ile karakterize edilen, İstem 1'e göre yöntem.

9. Ayrıca, şifre uyuşmazlığını ortadan kaldırmak üzere bilgi mutabakatını uygulama adımını içermesi ile karakterize edilen, İstem 1'e göre yöntem.

10. Ayrıca, oluşturulan şifrenin rastgeleliğini artırmak üzere gizlilik yükseltmesi uygulama adımını içermesi ile karakterize edilen, İstem 1'e göre yöntem.

11. Önceki istemlerden herhangi birine göre yöntemin adımlarını gerçekleştirmeye yönelik araçları içeren bir sistem.

12. Program bir bilgisayar tarafından yürütüldüğünde, bilgisayarın İstem 1 ila 11'den herhangi birinin yönteminin adımlarını gerçekleştirmesine neden olan talimatları içeren bir bilgisayar programı.

13. İstem 12'ye göre bilgisayar programını üzerinde depolayan bilgisayar tarafından okunabilen bir ortam.

TARİFNAME

GÜVENLİ KABLOSUZ İLETİŞİM İÇİN GECİKME-DOPPLER TABANLI ŞİFRE ÜRETİM YÖNTEMİ

Teknik Alan

Buluş, en az iki cihaz arasında güvenli kablosuz iletişime yönelik bilgisayar uygulamalı bir şifre oluşturma yöntemi ile ilgilidir.

Önceki Teknik

Heterojen ağların kullanımıyla birlikte kablosuz bağlantıların güvenliği giderek daha zor hale gelmektedir. Ağ varlıklarının yeteneklerindeki farklılıklar nedeniyle, geleneksel kriptografik yöntemlerin tüm düğümlerde uygulanması mümkün değildir.

Kablosuz sistemlerde kullanılan geleneksel kriptografik mekanizmalar, iletişim kuran düğümler için bazı hesaplama yeterlilikleri gerektirmektedir. Ayrıca, şifreleme/şifre çözme işlemleri ilave gecikmeye neden olmaktadır. Fiziksel katman güvenliği (PLS), bunları kablosuz kanalın özelliklerini kullanarak gerçekleştirmenin bir alternatifini sunmaktadır. Bu, gizli dizilerin paylaşılan yayılma ortamından çıkarıldığı şifre üretme tabanlı teknikleri içermektedir. Şifre oluşturma teknikleri, genellikle uygulanabilirliklerini yalnızca zaman bölmeli çift yönlü (TDD) sistemlere sınırlayan kanal dürtü yanıtı (CIR), kanal frekans yanıtı (CFR) ve alınan sinyal gücü (RSS) gibi kanal özelliklerinin karşılıklılığına dayanmaktadır. Öte yandan, frekans bölmeli çift yönlü (FDD) sistemler karşılıklı kanalı deneyimlememekte, bu da bu tür sistemlerde paylaşılan şifrelerin üretilmesini zorlaştırmaktadır.

Frekans bölmeli çift yönlü (FDD) sistemler, gecikme açısından zaman bölmeli çift yönlü (TDD) sistemlere kıyasla açık bir avantaja sahiptir, ancak kanal tahmini açısından daha fazla karmaşıklığı beraberinde getirirler. Özellikle de, TDD sistemleri, kanalın yukarı yönlü bağlantı (UL) ve aşağı yönlü bağlantı (DL) içindeki karşılıklılığından yararlanmakta, böylece kanal tahmini ek yükü azaltılmaktadır. Ne var ki, bu sadece uzun (böylece hem UL hem de

DL iletimleri bu süre içinde gerçekleştirilmektedir) tutarlılık süresine sahip kanallarda geçerlidir.

Bununla birlikte, FDD sistemleri karşılıklı kanal yanıtı deneyimlememektedir. Bu nedenle, paylaşılan şifreler oluşturmak üzere, ya birleştirilmiş UL ve DL kanallarına (bu, TDD sistemleriyle aynı tutarlılık süresini gerektirmektedir) ya da her iki iletişim düğümünde benzer şekilde gözlenen parametrelere güvenmektedirler. İkincisinin örnekleri arasında, aynı şifreleri oluşturmak üzere düğümler arasındaki gecikme ve açının kullanılması yer almaktadır. Gecikme karşılıklı olsa da, yeterli çözünürlüğü sağlamak üzere geniş bir bant genişliği gerektirirken, açının kullanılması iletişim kuran düğümlerde birden fazla antenin bulunmasını gerektirmektedir.

Kablosuz kanal özelliklerini kullanan FDD sistemlerinin PLS'si için önerilen birkaç çalışma bulunmaktadır. Bu çalışmaların çoğu, pilot döngü [1], birleşik CFR [2] ve ön kodlamalı matris göstergesi (PMI) geri bildirimi [3] gibi iletişim düğümleri arasındaki bazı geri bildirimleri kullanarak birleşik (yukarı yönlü ve aşağı yönlü) kanalın tahminini içermektedir.

Bir alternatif, gecikme [4] veya açı [5] gibi frekansla değişmeyen kanal parametrelerini kullanmaktır. Birincisi, şifre üretimi için zamanla değişen mesafenin (veya yayılma Gecikmesinin) kullanıldığı bir cihazdan cihaza (D2D) senaryosunu dikkate almaktadır.

Şifre [6] oluşturmak için hem yükseklik hem de azimut boyutlarında varış açısı (AoA) yöntemi kullanılmaktadır. Açı tabanlı yaklaşım [6], meşru düğümler arasındaki üç boyutlu uzamsal açının şifreyi oluşturmak üzere kullanıldığı bir insansız hava aracı (UAV) çoklu giriş çoklu çıkış (MIMO) sistemine genişletilmektedir. Kanalın kovaryans matrisinin [7] özdeğer karşılıklılığı da kullanılırken, daha sonra şifre oluşturmak üzere kullanılacak olan bir karşılıklı kanal [8] oluşturulmaktadır.

Yukarıda bahsedilen çalışmalar arasında, birleşik kanal tabanlı yaklaşımlar, geri bildirim sürecinden kaynaklanan fazla gecikmeden muzdariptir. Öte yandan, açı tabanlı yöntemler, iletişim düğümlerinde çok sayıda anten gerektirmektedir. Dahası, kovaryans matrisine dayalı teknik, düşük şifre oluşturma oranı (KGR) sunmaktadır [9].

Mevcut buluş, hızlı kaybolan bir kablosuz kanalı (zaman-frekans alanında) yavaş değişen bir kanala (gecikme-Doppler alanında) dönüştürmek üzere ortogonal zaman frekans uzayının (OTFS) ve altta yatan basit Fourier dönüşümünün yeterliliğinden faydalanmaktadır. Son zamanlarda, OTFS tabanlı iletimlerin gizlilik performansı, yukarı yönlü uydu [10] ve tek noktaya yayın hizmetleri [11] için incelenmiştir. Birincisi, gizli dinleyen bir uyduyu ve işbirlikçi bir İHA bozucuyu dikkate alırken, ikincisi, gizli dinleyicinin hareketliliğinin gizlilik üzerindeki etkisini analiz etmektedir. Gizli dinleyicide takımuydu bozulmasına yol açan kanal tabanlı bir ön dönüş [12] önerilmiştir. [13]'te kullanılan kanala bağımlı kaynak, daha sonra OTFS modülasyonunu bozmak ve iletimi güvence altına almak için kullanılan bir Gosudarstvennyi standardına dayalı dizi oluşturmak üzere kullanılmaktadır.

Sonuç olarak, yukarıda belirtilen sorunların tümü, ilgili alanda bir yenilik yapılmasını gerekli kılmıştır.

Buluşun Amaçları

Mevcut buluşun temel amacı, FDD ve TDD sistemlerindeki en az iki cihaz arasında, özellikle yüksek hareketlilik senaryolarında, gizli dinleme, sinyal bozma ve yanıltma gibi farklı güvenlik tehditlerini azaltmak üzere güvenli kablosuz iletişime yönelik güvenli bir şifre oluşturma yöntemi oluşturmaktır.

Buluşun diğer bir amacı, FDD ve TDD sistemlerinde, cihazlarda/iletişim düğümlerinde yüksek sayıda anten gerektirmeyen güvenlik şifresi oluşturma yöntemi sağlamaktır.

Şekillerin Kısa Açıklaması

Mevcut buluşta, bir güvenli şifre oluşturma yöntemi açıklanmaktadır. Bu yöntemde, güvenlik şifreleri Gecikme-Doppler alanına göre oluşturulmaktadır. Daha spesifik olarak, şifreler, Gecikme ve Doppler kutularının endekslerine ve nicelenmiş fraksiyonel Gecikme ve Doppler değerlerine dayalı olarak üretilmektedir.

Buluşun Şekillerinin Açıklaması

Buluş konusunun daha iyi anlaşılabilmesi için gerekli şekiller ve ilgili açıklamalar aşağıda verilmiştir.

Şekil 1. Birbiriyle haberleşen cihazların şematik görünümü.
Şekil 2. Buluşun başlangıç adımlarını gösteren akış şeması.
Şekil 2a. Buluşun TDD sistemlerindeki adımlarını gösteren akış şeması.
Şekil 2b. Buluşun FDD sistemlerindeki adımlarını gösteren akış şeması.
Şekil 2c. Buluşun final adımlarını gösteren akış şeması.
Şekil 3. Buluşun yöntemini gerçekleştirmek üzere konfigüre edilmiş bir sistemin şematik görünümü.

Referans Numaraları

Buluş konusunun daha iyi anlaşılabilmesi için şekillerde verilen parça ve bileşenlere atıfta bulunulmuştur.

10a. A Cihazı
10b. B Cihazı
A. Anten
PU. İşlem Birimi
WC. Kablosuz kanal
I. Yasa dışı kullanıcı

Buluşun Detaylı Açıklaması

Buluş, en az iki cihaz arasında güvenli kablosuz iletişime yönelik bir şifre oluşturma yöntemi uygulanan bir bilgisayar ile ilgilidir, ve bir iletişim yöntemi, bahsedilen güvenlik şifresini kullanmakta, bir sistem, bahsedilen şifre oluşturma yöntemini veya iletişim yöntemini gerçekleştirmekte ve bir bilgisayarın örneğin söz konusu yöntemleri yürütmesine neden olan talimatları içeren bir program içermektedir.

Bahsedilen cihazlar birbirleriyle haberleşecek şekilde konfigüre edilmektedir. Buluşun cihazları, kablosuz iletişim kurabilen herhangi cihaz olabilmektedir. Cihazlar, iletişim

düğümleri, baz istasyonları, mobil cihazlar (örneğin akıllı telefon, dizüstü bilgisayar vb.) veya sabit cihazlar olabilmektedir.

İki cihaz, Şekil 1'de bir A cihazı (10a) ve bir B cihazı (10b) olarak örnekle açıklanmaktadır. A cihazı (10a) bir baz istasyonu olarak, B cihazı (10b) ise ok yönünde hareket eden hareket halindeki bir araca yerleştirilmiş bir cihaz olarak gösterilmektedir. Noktalı çizgi ile gösterilen araç, aracın önceki konumunu temsil etmektedir. Ayrıca, yasa dışı kullanıcı (I) Şekil 1'de gösterilmektedir ve yasa dışı kullanıcı (I), gizli dinleme, sinyal bozma ve yanılma gibi güvenlik tehditlerine neden olan bir kişi veya sistemdir.

Şekil 2'ye atfen; ilk olarak Gecikme-Doppler ızgarası tasarlanmakta ve pilot sembolün söz konusu ızgara içindeki yeri belirlenmektedir. Pilot sinyalin ızgara üzerindeki konumu hem A cihazı (10a) hem de B cihazı (10b) tarafından bilinmektedir.

Tercih edilen bir yapılandırmada, Gecikme-Doppler ızgarasının her iki yöndeki boyutları, mevcut bant genişliklerinden, mevcut alt taşıyıcıların sayısından, alt taşıyıcı aralığından ve iletim süresinden en az birine göre, tercihen hepsine göre hesaplanmaktadır.

Pilot sinyaller, yöntemin ilk aşamasında Gecikme-Doppler alanındadır. Söz konusu sinyal, A cihazı (10a) ve B cihazı (10b) arasında iletilmek üzere zaman-alana dönüştürülmektedir. Bir yapılandırmada, dönüştürme, ters basit Fourier dönüşümü (ISFT) ve ardından Heisenberg dönüşümü kullanılarak gerçekleştirilmektedir.

A cihazında (10a) ve B cihazında (10b) zaman-alan pilot sinyalleri tekrar Gecikme-Doppler alanına dönüştürülmekte ve hem A cihazında (10a) hem de B cihazında (10b) söz konusu sinyallerden Gecikme ve Doppler değerleri elde edilmektedir. Gecikme ve Doppler değerlerinin elde edilmesi için tercihen kanal tahmin çerçeve yöntemi veya çerçevesi kullanılmaktadır. Tercihen, dönüşüm, bir Wigner dönüşümü ve ardından basit Fourier dönüşümü (SFT) kullanılarak gerçekleştirilmektedir.

Şekil 2c'ye atfen; bunun ardından, paylaşılan kablosuz kanallar (WC) için Gecikme ve Doppler kutularının endeksleri elde edilmekte ve hesaplanarak veya sistem kontrol edilerek fraksiyonel Gecikme ve Doppler değerleri elde edilmektedir, burada endeksler paylaşılan

sırrın ilk parçasıdır. Ardından, bu fraksiyonel Gecikme ve Doppler değerleri nicelenmektedir, burada nicelenen değerler paylaşılan sırrın ikinci parçasıdır. Bu değerler, paylaşılan güvenlik şifresini oluşturmak için kullanılmaktadır.

Paylaşılan güvenlik şifresini oluşturmak üzere, Gecikme ve Doppler kutularının endeksleri ve nicelenmiş fraksiyonel Gecikme ve Doppler değerleri ikili bir gösterime dönüştürülmektedir. Tamsayı gecikmesi ve Doppler endekslerine yönelik ondalık gösterim (10 tabanı) doğrudan ikili ölçeğe (2 tabanı) dönüştürülmektedir. Gecikmenin fraksiyonel kısımları ve Doppler kaymaları için, değer önce bir niceleme aralığına bölünmekte ve sonuç, tamsayı kısımlarına benzer bir ikili sayıya dönüştürülmektedir. Tam (tamsayı ve fraksiyonel) gecikme ve Doppler değerlerini doğrudan niceleme aralıklarına bölmek ve ikili gösterime dönüştürmek de mümkündür.

En az iki cihaz arasında güvenli kablosuz iletişime yönelik bir güvenlik şifresi oluşturma yöntemi şu adımları içermektedir; bir Gecikme-Doppler ızgarası tasarlanması ve bir pilot sembolün yerinin belirlenmesi, Gecikme-Doppler pilot sinyallerinin her iki cihazda da zaman alanına dönüştürülmesi, zaman alanlı pilot sinyallerin cihazlar tarafından birbirine iletilmesi ve pilot sinyallerin cihazlar tarafından tekrar Gecikme-Doppler alanına dönüştürülmesi, her iki cihazda Gecikme-Doppler değerlerinin alınması, her iki cihazda Gecikme-Doppler değerlerinin endekslerinin alınması, her iki cihazda fraksiyonel Gecikme-Doppler değerlerinin elde edilmesi ve nicelenmesi.

Şekil 2'de görüldüğü gibi, bu noktada sistemin frekans bölmeli çift yönlü (FDD) veya zaman bölmeli çift yönlü sistem (TDD) olup olmadığını belirleyen bir belirleme aşaması bulunmaktadır. Ne var ki, bu belirleme adımı isteğe bağlıdır. Yöntem, yalnızca frekans bölmeli çift yönlü veya zaman bölmeli çift yönlü sistemlerle çalışacak şekilde konfigüre edilebilmektedir. Hem frekans bölmeli çift yönlü (FDD) hem de zaman bölmeli çift yönlü sistem (TDD) için yöntem aynı adımlarla gerçekleştirilmekte ancak adımların sırası farklı olabilmektedir.

Şekil 2a'ya atfen; frekans bölmeli çift yönlü sistem (FDD) olarak belirlenen sistem ise, her iki cihazın da (A cihazı (10a) ve cihaz B cihazı (10b)) dönüştürülen pilot sinyalleri birbirine iletmesi eş zamanlı olarak gerçekleştirilmektedir. Ardından, A cihazı (10a) ve B cihazının

(10b) her biri sinyalleri Gecikme-Doppler alanına çevirerek söz konusu sinyallerden Gecikme ve Doppler değerlerini elde etmektedir.

Şekil 2b'ye atfen; sistemin, zaman bölmeli çift yönlü sistem (TDD) olarak belirlenmesi halinde, A cihazı (10a), B cihazına (10b) dönüştürülen pilot sinyali iletmektedir. B cihazı (10b), alınan sinyali Gecikme-Doppler alanına dönüştürmekte ve bahsedilen sinyallerden Gecikme ve Doppler değerlerini elde etmektedir. Ardından, B cihazı (10b), zaman alanına dönüştürülen pilot sinyali A cihazına (10a) iletmektedir. A Cihazı (10a), söz konusu sinyallerden Gecikme ve Doppler değerleri elde etmek üzere geri sinyali Gecikme-Doppler alanına dönüştürmektedir.

Şekil 2a ve 2b'ye atfen; hem zaman bölmeli çift yönlü sistem (TDD) hem de frekans bölmeli çift yönlü sistem (FDD) için pilot sinyaller cihazlar arasında iletilmekte ve alınan sinyaller Gecikme-Doppler alanına dönüştürülerek söz konusu sinyallerden Gecikme ve Doppler değerleri elde edilmektedir. Buradaki tek fark, iletimin sırasıdır. Zaman bölmeli çift yönlü sistemlerde eşzamanlı olarak cihazlar arasında iletim yapılırken, frekans bölmeli çift yönlü sistemlerde aynı iletim sıralı olarak yapılmaktadır.

Hem zaman bölmeli çift yönlü sistem (TDD) hem de frekans bölmeli çift yönlü sistem (FDD) için, kalan adımlar yukarıda bahsedilen şifre oluşturma adımları ile aynıdır.

Tercih edilen yapılandırmada, yukarıdaki adımlardan sonra bir bilgi mutabakatı gerçekleştirilmektedir. Bu adım, şifre uyuşmazlığını gidermek üzere kullanılmaktadır. Mevcut buluşta, özellikle Doppler'in karşılıklı olmadığı, ancak yukarı yönlü/aşağı yönlü iletimlerinin belirli taşıyıcı frekansı ile ilişkili olduğu FDD senaryosuna yönelik her iki düğüm için Doppler kaymalarına çözüm bulmak üzere kullanılmaktadır.

Tercih edilen yapılandırmada, yukarıdaki adımlardan sonra bir gizlilik yükseltmesi gerçekleştirilmektedir. Bu adım, oluşturulan şifrenin rastgeleliğini artırmak için kullanılmaktadır.

Söz konusu yöntem bir bilgisayar veya aşağıda bahsedilen sistem tarafından gerçekleştirilmektedir. Program, söz konusu bilgisayarda veya aşağıda bahsedilen sistemde

yöntemin yürütülmesi için talimatlar içermektedir. Program, bilgisayar tarafından okunabilen bir ortamda saklanabilmektedir.

Şekil 3'e atfen; bir sistem, yukarıda bahsedilen aynı yöntemi yürütmek üzere yapılandırılmaktadır. Sistem, en az iki cihaz (A cihazı (10a) ve B cihazı (10b)) içermektedir ve her iki cihaz da bir kablosuz kanal (WC) üzerinden birbirleriyle iletişim kurmak için en az bir anten (A) içermektedir.

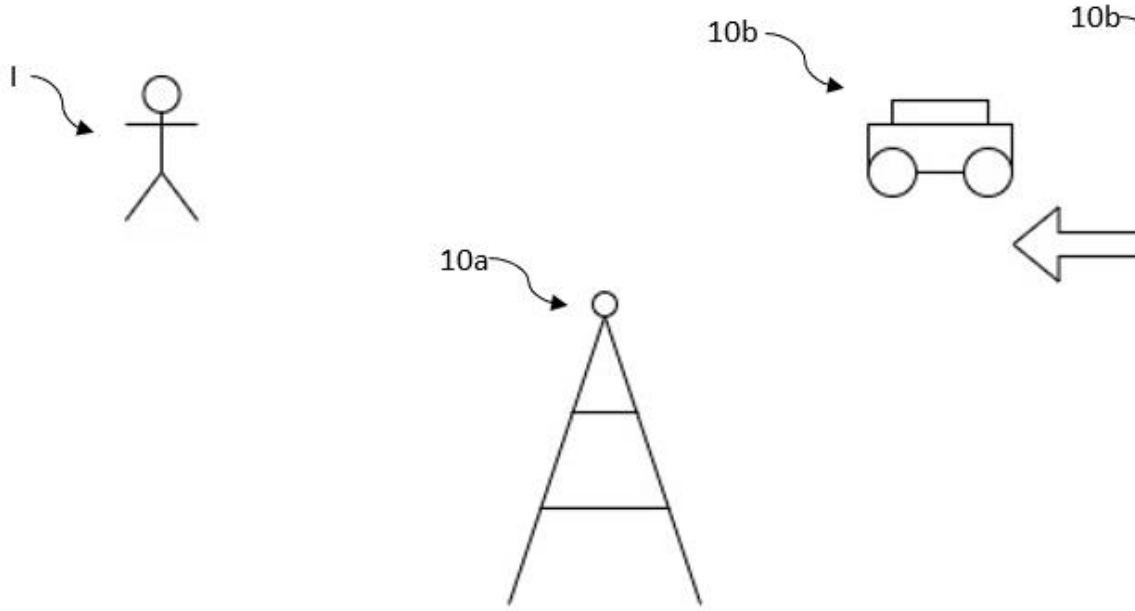
Her iki cihaz da yukarıda belirtilen aynı yöntemin adımlarını gerçekleştirmeye yönelik en az bir işlem birimi (PU) içermektedir.

Tercih edilen yapılandırmada işlem birimleri (PU), mevcut buluşun yönteminin belirli adımlarını gerçekleştirmek üzere konfigüre edilmektedir. Örneğin, A cihazı (10a), gecikme-Doppler ızgarasını ve pilot atamayı tasarlamak ve bir gecikme-Doppleri zaman alanı sinyaline dönüştürmek üzere konfigüre edilmiş işlem birimini (PU) içermektedir. B cihazı (10b), zaman alanını gecikme-Doppler alanına dönüştürmek ve gecikmeyi ve Doppler değerini tahmin etmek ve tahmini gecikme/Doppler değerlerini endekslemek ve nicelemek üzere konfigüre edilmiş işlem birimini (PU) içermektedir. Alternatif olarak, her işlev için ayrı ayrı belirli bir işlem birimi (PU) kullanılabilmektedir.

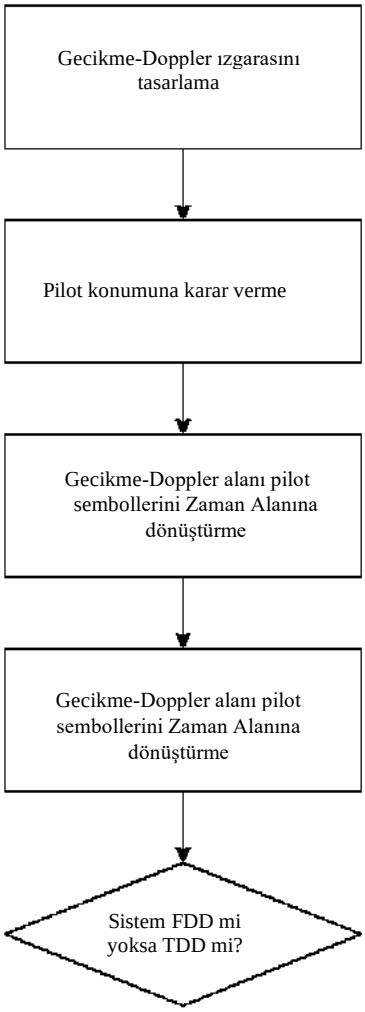
Alternatif bir yapılandırmada, her iki cihaz da tüm adımları ve fonksiyonları taşımak üzere konfigüre edilmiş işlem birimlerini (PU) içermektedir. Tercihen, her iki cihazın işlem birimleri (PU) aynıdır.

Referanslar

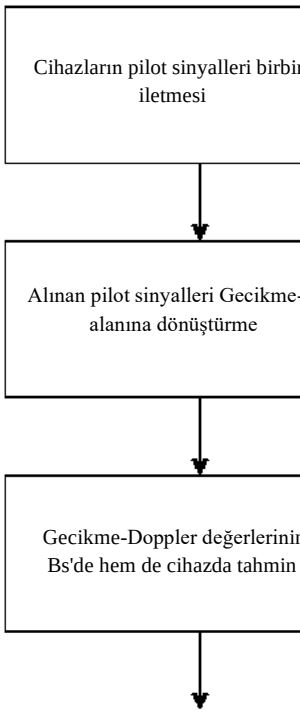
1. S. J. Goldberg, Y. C. Shah, ve A. Reznik, “Method and apparatus for performing JRNSO in FDD, TDD and MIMO communications,” 19 Mart 2013, 8,401,196 Sayılı ABD Patenti.
2. X. Wu vd., “A secret key generation method based on CSI in OFDMFDD system,” in Globecom Workshops (GC Wkshps). IEEE, 2013, s. 1297–1302.
3. H. Taha ve E. Alsusa, “Secret key exchange using private random precoding in MIMO FDD and TDD systems,” IEEE Trans. Veh. Technol., vol. 66, no. 6, s. 4823–4833, 2016.
4. O. Gungor, F. Chen, ve C. E. Koksal, “Secret key generation from mobility,” in Globecom Workshops (GC Wkshps). IEEE, 2011, s. 874–878.
5. Badawy vd., “Secret key generation based on AoA estimation for low SNR conditions,” in 81st Veh. Technol. Conf. (VTC Spring). IEEE, 2015, s. 1–7.
6. K. Lin vd., “Secret key generation based on 3D spatial angles for UAV communications,” in Wireless Commun. Netw. Conf. (WCNC). IEEE, 2021, s. 1–6.
7. B. Liu, A. Hu, ve G. Li, “Secret key generation scheme based on the channel covariance matrix eigenvalues in FDD systems,” IEEE Commun. Lett., vol. 23, no. 9, s. 1493–1496, 2019.
8. G. Li vd., “Constructing reciprocal channel coefficients for secret key generation in FDD systems,” IEEE Commun. Lett., vol. 22, no. 12, s. 2487–2490, 2018.
9. J. Zhang vd., “A new frontier for IoT security emerging from three decades of key generation relying on wireless channels,” IEEE Access, vol. 8, s. 138 406–138 446, 2020.
10. J. Hu vd., “Secrecy analysis for orthogonal time frequency space scheme based uplink LEO satellite communication,” IEEE Wireless Commun. Lett., vol. 10, no. 8, s. 1623–1627, 2021.
11. Z. Tie vd., “Security performance analysis for an OTFS-based joint unicast-multicast streaming system,” IEEE Trans. Commun., vol. 70, no. 10, s. 6764–6777, 2022.
12. J. Sun, Z. Wang, ve Q. Huang, “Secure precoded orthogonal time frequency space modulation,” in 13th Int. Conf. Wireless Commun. Signal Process. (WCSP). IEEE, 2021, s. 1–5.
13. W. Liang vd., “Underlying security transmission design for orthogonal time frequency space (OTFS) modulation,” Sensors, vol. 22, no. 20, s. 7919, 2022.



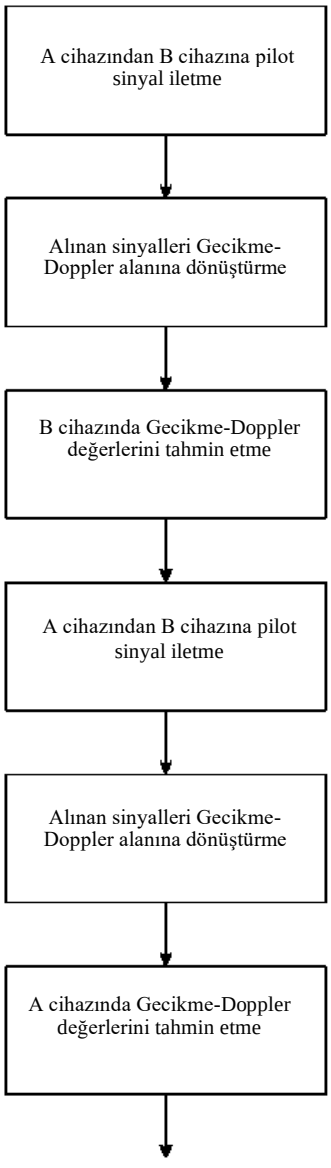
ŞEKİL 1



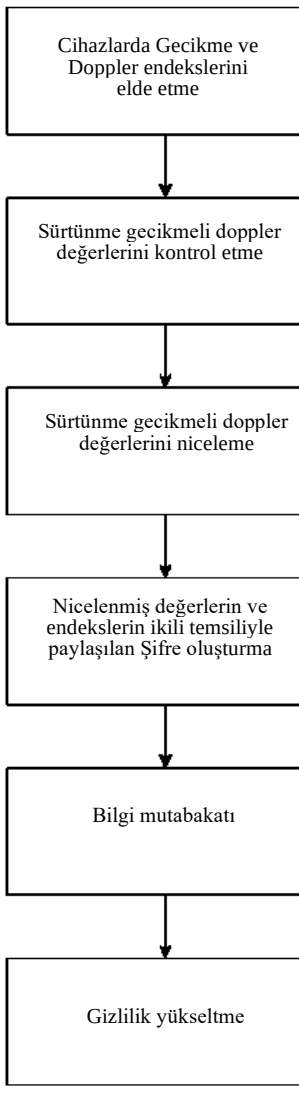
ŞEKİL 2



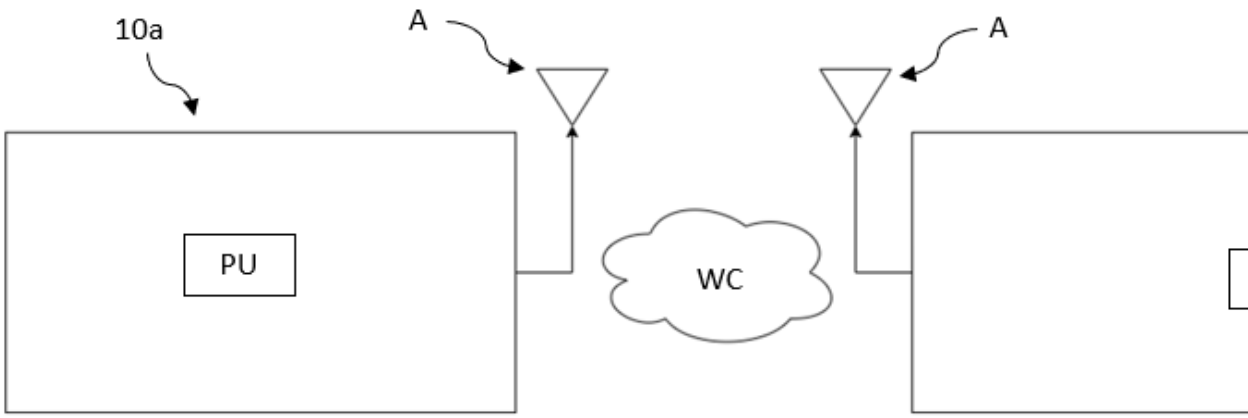
ŞEKİL 2a



ŞEKİL 2b



ŞEKİL 2c



ŞEKİL 3