OZET

KANAL TABANLI FAZ ÖN DENKLEŞTİRMESİ KULLANILARAK GİZLİ DİNLEMENİN ONLENMESİ

Mevcut buluş, kablosuz haberleşmede gizli dinlemeye karşı gizliliği geliştirmek üzere bir yöntem ile ilgilidir. Söz konusu yöntem, meşru alıcı-vericiler arasındaki kanal fazının ön denkleştirilmesini içermektedir.

İSTEMLER

1. Kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntem olup, burada söz konusu yöntem aşağıdaki adımları içermektedir;

- Kablosuz kanalın tahmin edilmesi, burada söz konusu süreç (a) vericinin bir kanal (kazanç ve faz) tahmin sürecini başlatması ve (b) alıcının bir kanal kazanç tahmin sürecini başlatmasından oluşmaktadır,
- Vericide kanal tahmin sürecinden kanal fazı vektörünün elde edilmesi,
- Vericide bir dijital modülasyon şemasına dayalı olarak modüle sembollere iletilen bitlerin eşleştirilmesi,
- Modüle sembollerin, anlık kanal fazının negatifine eşit olan bir açı ile döndürülmesi ile karakterize edilen, vericide sembol fazı ön denkleştirmesinin gerçekleştirilmesi
- Alıcıda alınan sembollerin kodunun çözülmesi.

2. İstem 1'e göre bir yöntem olup, burada kanal tahmin süreci gerçekleştirilmektedir. Haberleşmesinin güvenliği sağlanacak olan iletim noktası (**310, 411, 412**) ve cihaz (**330, 430**) kablosuz kanalı tahmin etmektedir.

3. İstem 2'ye göre bir yöntem olup, burada iletim noktası (**310, 411, 412**) kablosuz kanalın hem kazancı hem de fazını tahmin ederken, cihaz (**330, 430**) yalnızca kablosuz kanalların kazancını tahmin etmektedir.

4. İstem 3'e göre bir yöntem olup, burada modüle semboller, yalnızca kanal kazancı tarafından ölçeklenen cihaza (**330, 430**) varacaktır.

5. İstemler 1 ila 4'ten herhangi birine göre bir yöntem olup, burada kanal fazı ayıklama süreci, iletim noktası (**310, 411, 412**) ve cihaz (**330, 430**) arasında kablosuz kanaldan (**341, 442, 443**) kanal fazı vektörünün ayıklanmasını içermektedir. Kanal karşılıklılık özelliği nedeniyle meşru varlıklar arasında herhangi bir paylaşım yapılmasına gerek yoktur.

6. İstemler 1 ila 5'ten herhangi birine göre bir yöntem olup, burada iletilen bitlerin modüle sembollere eşleştirilmesi bir dijital modülasyon şemasını takiben yapılmaktadır.

7. İstemler 1 ila 6'dan herhangi birine göre bir yöntem olup, burada sembol fazı ön denkleştirmesi, modüle sembollerin, anlık kanal fazının negatifine eşit olan bir açı ile döndürülmesi ile gerçekleştirilmektedir.

8. İstem 6 veya 7'den herhangi birine göre bir yöntem olup, burada modüle semboller ayıklanan kanal fazı vektörüne dayalı olarak birbirinden bağımsız olarak döndürülmektedir.

9. İstemler 6 ila 8'den herhangi birine göre bir yöntem olup, burada sembol fazı ön denkleştirmesi yoklanan kanal fazlarına dayalı olarak gerçekleştirilmektedir.

10. İstemler 7 ila 9'dan herhangi birine göre bir yöntem olup, burada kanal fazları, bir kanal karşılıklılık süreci ile meşru varlıklar arasında gizli olarak tutulmaktadır.

11. İstem 8'e göre bir yöntem olup, burada kanal karşılıklılık süreci, kablosuz kanalın bir geri bildirim bağlantısı olmaksızın haberleşen uçların ikisi tarafından da tahmin edilmesini içermektedir.

12. İstemler 1 ila 10'dan herhangi birine göre bir yöntem olup, burada alınan semboller yalnızca meşru cihazda kazanç denkleştirmesini gerektirmektedir.

13. İstemler 1 ila 12'den herhangi birine göre bir yöntem olup, (a) bir meşru TP (**310**), (b) meşru cihaz/alıcı (**330**) ve (c) bir saldırgandan (**320**) oluşan basit bir ağa yöneliktir; burada söz konusu yöntem aşağıdaki adımları içermektedir;

- meşru TP'nin saldırgana (**320**) karşı cihaz (**330**) ile güvenli bir haberleşme gerçekleştirmesi, burada haberleşme düğümleri tekli ve/veya çoklu antenler ile donatılmaktadır,
- saldırganın (**320**) kablosuz kanalı (**341**) pasif olarak öğrenmeye çalışması**,**

- iletilen verilerin cihaza (**330**) güvenliğini sağlamak üzere kablosuz kanalın karşılıklılık özelliğinin varsayılması, kanal fazı vektörü kablosuz kanala (**341**) dayalı olarak ayıklanmaktadır.
- TP'nin, iletilen sembolü, kablosuz kanalın (**341**) anlık fazının negatifine eşit olan bir açı ile döndürmesi, böylece cihazda (**330**), alınan sembolün doğru faza sahip olması ancak yalnızca kazanç denkleştirmesine ihtiyaç duyması ve saldırganda (320), alınan sembolün doğru olmayan faza ve kazanca sahip olması.

14. İstemler 1 ila 11'den herhangi birine göre bir yöntem olup, sembol fazı ön denkleştirmesine sahip bir koordineli ağa yöneliktir; burada söz konusu yöntem aşağıdaki adımları içermektedir;

- TP-1'den (**411**) TP-N'ye (**412**) kadar olan TP'lerin, saldırgana (**420**) karşı cihaz (**430**) ile haberleşmenin güvenliğini sağlamak üzere koordine edilmesi, burada haberleşme düğümleri tekli/çoklu antenler ile donatılmaktadır,
- TP-1 (**411**) kablosuz kanaldan (**442**) ayıklanan kanal fazı vektörünü kullanırken TP-N (**412**) kablosuz kanaldan (**444**) ayıklanan kanal fazı vektörünü kullandığından, NN-koordineli TP'ler tarafından, bunlar ve cihaz (**430**) arasındaki kablosuz kanallardan ayıklanan fazlı vektöre dayalı olarak bir sembol fazı ön denkleştirme sürecinin (**130**) uygulanması, böylece cihazda (**330**), alınan sembolün doğru faza sahip olması ancak yalnızca kazanç denkleştirmesine ihtiyaç duyması ve saldırganda, alınan sembolün doğru olmayan faza ve kazanca sahip olması.

15. İstem 13 veya 14'e göre bir yöntem olup, burada kazanç denkleştirmesi, kablosuz kanalın (**442**) kazancı ile kablosuz kanalın (**443**) kazancının kombinasyonu olan etkili kazanca dayalıdır.

16. İstemler 1 ila 15'ten herhangi birine göre yöntemin, gizli dinlemeye karşı gizliliği geliştirmek üzere 3GPP-tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağları, kod bölmeli çoklu erişim (CDMA), frekans bölmeli çoklu erişim (FDMA), Küresel Mobil Haberleşme Sistemi (GSM), GSM/Genel Paket Radyo Hizmeti (GPRS), Gelişmiş Veri GSM Ortamı (EDGE), Geniş bant-CDMA (W-CDMA), Optimize Edilmiş Evrim Verileri (EV-DO), Yüksek Hızlı Paket Erişimi (HSPA), Yüksek Hızlı Paket İndirme Erişimi (HSDPA), Yüksek Hızlı Paket Yükleme Erişimi (HSUPA), Evrimleşmiş

Yüksek Hızlı Paket Erişimi (HSPA+), Uzun Vadeli Evrim (LTE), AMPS, 5G Yeni Radyo (NR), veya bir kablosuz, hücresel veya nesnelerin interneti (IoT) ağı içerisinde haberleşmek üzere kullanılan diğer bilinen sinyalleri destekleyebilen sistemler ve/veya cihazlar ve/veya ağlarda kullanımı.

17. İstemler 1 ila 15'ten herhangi birine göre bir yöntemin kullanımı olup, bir meşru TP (**310**), meşru cihaz/alıcı ve bir saldırgandan oluşan basit bir ağda gizli dinlemeyi önlemeye yöneliktir.

18. İstemler 1 ila 15'ten herhangi birine göre bir yöntemin kullanımı olup, bir koordineli ağda gizli dinlemeyi önlemeye yöneliktir.

TARİFNAME

KANAL TABANLI FAZ ÖN DENKLEŞTİRMESİ KULLANILARAK GİZLİ DİNLEMENİN ÖNLENMESİ

Teknik Alan

Mevcut buluş, kablosuz haberleşmede gizli dinlemeye karşı gizliliği geliştirmek üzere bir yöntem ile ilgilidir. Söz konusu yöntem meşru alıcı-vericiler arasındaki kanal fazının ön denkleştirilmesini içermektedir.

Onceki Teknik

Kablosuz sistemler, bir kötü niyetli düğümün meşru varlıklar arasında devam etmekte olan iletimleri kesmeye çalıştığı gizli dinleme dahil çeşitli tehditlere yatkındır. Ön denkleştirme yaklaşımı, bir gizli dinleyici, meşru kablosuz kanal hakkında hiçbir bilgiye sahip olmadığı için alınan sinyallerin doğru şekilde kodunu çözemeyecek şekilde meşru kablosuz kanal tarafından iletilen verileri denkleştirerek azaltılmış karmaşıklıkla iyi bir performans göstermiş olan fiziksel katman güvenliği (PLS) yaklaşımlarından biri olarak düşünülmektedir. Dolayısıyla, yalnızca güvenliği değil, ancak aynı zamanda alıcı karmaşıklığını da sağlayan, bu buluşta bahsedilen gibi basit, hafi ve etkili şemalara artan bir ilgi yönlendirilmektedir.

Konstelasyon dönüşü: modüle semboller iletimden önce bir açı ile döndürülmektedir ve alıcı açı dönüşünü ters çevirdikten sonra alınan sembollerin kodunu çözebilmektedir. Dönüş açısı aşağıdakiler olabilmektedir:

1) Geleneksel konstellasyon dönüşü: tüm modüle semboller için sabit açı dönüşü uygulanmaktadır.
2) Sözde Rastgele konstelasyon dönüşü: sembole özgü dönüş açıları sözde rastgele üreteç kullanılarak üretilmektedir.

Konstelasyon şekli/tipi: konstelasyon şekli veya tipi verici ve alıcı arasındaki bir ön paylaşımlı diziye dayalı olarak değiştirilmektedir.

Konstelasyon eşleştirme karartma: konstelasyon eşleştirme kuralı, bit akışının modüle sembollere eşleştirilmesini karartmak üzere her bir paket iletiminde değiştirilmektedir.

Yapay olarak karıştırıcı sinyallerin eklenmesi: modüle semboller kasıtlı olarak karıştırıcı sinyallere eklenmektedir.

Onceki teknikte sunulan çözümler, esasen, konstelasyonu karartmak üzere yöntemler ve tekniklerdir ve kurallar/teselli ile ilgili bilgilerin bilinmemesi halinde doğru olmayan tespit nedeniyle performans bozulmasına yol açmaktadırlar. Ek olarak, meşru alıcının, veri tespit aşamasından önce birtakım süreçlerin uygulanmasını gerektirmesi nedeniyle alıcı tasarımını karmaşık hale getirmektedirler.

Daha özel olarak, yukarıda bahsedilen çözümlerin dezavantajları güvenlik perspektifinden sunulmaktadır:

Geleneksel konstelasyon dönüşü: bu yaklaşımdaki bir zayıflık, çok sayıda sembole yönelik bir kaba kuvvet arama algoritmasının, sabit olması nedeniyle dönüş açısını doğru şekilde tanımlayabilmesidir.

Sözde Rastgele konstelasyon dönüşü: Bu yaklaşımda, meşru varlıklar arasında dizi üretecinin detayları paylaşılmalıdır, bu da sinyalleşme yükü anahtar yönetimi ve anlaşmasını gerektirmektedir.

Konstelasyon şekli/tipi: Bu yaklaşımda şema halen, geleneksel simetrik anahtar şifrelemede olduğu gibi haberleşmeciler arasında bir ön paylaşımlı veriye bağlıdır. Bu tür bir çekince, bunu, adaptif belgeyle şifre kırma saldırıları ve kaba kuvvet arama saldırıları gibi iyi bilinen saldırılara karşı savunmasız hale getirmektedir. Ek olarak, modülasyon tipinin değiştirilmesi kablosuz bağlantı koşullarında değişiklik gerektirmektedir, aksi takdirde kaynakların boşa harcanmasına yol açmaktadır.

Konstelasyon eşleştirme karartması: Burada da meşru varlıklar arasında eşleştirme kuralının nasıl güvenli bir şekilde paylaşılacağı ile ilgili aynı problem ortaya çıkmaktadır. Ek olarak, eşleştirme kuralındaki herhangi bir yanlışlık, özellikle de yüksek modülasyonlu taleplerde meşru alıcı performansında şiddetli bozulmaya yol açabilecektir.

Yapay olarak karıştırıcı sinyallerin eklenmesi: Bu yaklaşım kanal kapasitesini ve sonuç olarak veri hacmini bozulmaya uğratmaktadır. Ek olarak, yapay sinyalin uygun şekilde tasarlanmaması halinde PAPR artışına neden olabilecektir.

Sonuç olarak, son teknoloji dikkate alındığında, teknikte, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliği geliştirmek üzere hafif, etkili ve dirençli bir yöntem ihtiyacı olduğu görülmektedir.

Buluşun Amaçları ve Kısa Açıklama

Mevcut buluş, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntem ile ilgilidir, burada söz konusu yöntem aşağıdaki adımları içermektedir

- Kablosuz kanalın tahmin edilmesi, burada verici bir kanal (kazanç ve faz) tahmin süreci ve alıcı bir kanal kazanç tahmin süreci başlatmaktadır
- Vericide kanal tahmin sürecinden kanal fazı vektörünün elde edilmesi
- Vericide bir dijital modülasyon şemasına dayalı olarak modüle sembollere iletilen bitlerinin eşleştirilmesi
- Modüle sembollerin anlık kanal fazının negatifine eşit bir açı ile döndürülmesi ile karakterize edilen, vericide sembol fazı ön denkleştirmesinin gerçekleştirilmesi
- Alınan sembollerin alıcıda kodunun çözülmesi

Bu buluş, esasen, herhangi ön paylaşımlı dizi olmaksızın bir faz ön denkleştirme tekniği hakkındadır. Açı dizisi, kanal karşılıklılık özelliğinin yardımı ile meşru varlıklar arasındaki kablosuz bağlantının fazlarından ayıklanmaktadır. Modüle semboller ilgili açı ile döndürülmektedir ve meşru varlıklar arasındaki kablosuz bağlantı yoluyla geçtiğinde, geriye yalnızca kanal kazancı etkisi kalmaktadır. Çok noktalı koordinasyon, farklı fazlara sahip sinyallerin kombinasyonunun aynı zamanda alınan verilerin genliğini rastgeleleştirmesi nedeniyle alınan verileri ayrıca karartmak üzere kullanılmaktadır.

Buluşun yöntemi, gizli dinleyicilere karşı koruma sağlamak üzere herhangi kablosuz haberleşme teknolojisi tarafından kullanılabilmektedir.

Ozel olarak, 3GPP-tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağları gibi standartlar, iki standartta da sağlanan çok noktalı koordinasyon desteği nedeniyle buluşla özellikle ilgilidir.

Bir başka yapılandırmada buluş, 3GPP-tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağlarını destekleyebilen sistemler ve/veya cihazlar ve/veya ağlarda mevcut buluşa göre bir yöntemim kullanılmasına yöneliktir.

İlaveten, bu buluşta açıklanan yöntem, yukarıda bahsedilen standartlar, kod bölmeli çoklu erişim (CDMA), frekans bölmeli çoklu erişim (FDMA), Küresel Mobil Haberleşme Sistemi (GSM), GSM/Genel Paket Radyo Hizmeti (GPRS), Gelişmiş Veri GSM Ortamı (EDGE), Geniş bant-CDMA (W-CDMA), Optimize Edilmiş Evrim Verileri (EV-DO), Yüksek Hızlı Paket Erişimi (HSPA), Yüksek Hızlı Paket İndirme Erişimi (HSDPA), Yüksek Hızlı Paket Yükleme Erişimi (HSUPA), Evrimleşmiş Yüksek Hızlı Paket Erişimi (HSPA+), Uzun Vadeli Evrim (LTE), AMPS, 5G Yeni Radyo (NR), veya bir kablosuz, hücresel veya nesnelerin interneti (IoT) ağı içerisinde haberleşmek üzere kullanılan diğer bilinen sinyallerden herhangi birini destekleyebilen herhangi cihaz, sistem veya ağ üzerinde uygulanabilmektedir.

Buluşun tercih edilen bir yapılandırmasında, buluş, 3GPP-tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağları, kod bölmeli çoklu erişim (CDMA), frekans bölmeli çoklu erişim (FDMA), Küresel Mobil Haberleşme Sistemi (GSM), GSM/Genel Paket Radyo Hizmeti (GPRS), Gelişmiş Veri GSM Ortamı (EDGE), Geniş bant-CDMA (W-CDMA), Optimize Edilmiş Evrim Verileri (EV-DO), Yüksek Hızlı Paket Erişimi (HSPA), Yüksek Hızlı Paket İndirme Erişimi (HSDPA), Yüksek Hızlı Paket Yükleme Erişimi (HSUPA), Evrimleşmiş Yüksek Hızlı Paket Erişimi (HSPA+), Uzun Vadeli Evrim (LTE), AMPS, 5G Yeni Radyo (NR), veya bir kablosuz, hücresel veya nesnelerin interneti (IoT) ağı içerisinde haberleşmek üzere kullanılan diğer bilinen sinyalleri destekleyebilen sistemler ve/veya cihazlar ve/veya ağlarda mevcut buluşa göre bir yöntemin kullanılması ile ilgilidir.

Buluşa göre yöntem, iletilen verilerin güvenliğini sağlamak amacıyla meşru kanal fazına dayalı olarak modüle sembolün fazının ön denkleştirmesi ile gizli dinleyicilere karşı gizliliği geliştirmektedir.

Hiçbir ön paylaşıma, uzlaşmaya veya sabit gizli değerlere/anahtarlara ihtiyaç olmayan salt fiziksel katman yaklaşımlarına yönelik ihtiyaçtan yola çıkan bu buluş, gizli dinleyicilere karşı hafif, etkili ve dirençli bir fiziksel katman güvenlik şeması sunmaktadır.

Önerilen buluş, iletilen verilerin gizliliğini garantilemek amacıyla kanal fazından faydalanmaktadır ve her bir modül sembolünün bağımsız olarak ön denkleştirilmesine dayalıdır.

Sembol fazı ön denkleştirme, yoklanan kanal fazlarına dayalı olarak gerçekleştirilmektedir. Böyle olduğunda, kanal fazları meşru varlıklar arasında gizli tutulmak zorundadır, bu da kanal yanıtının bir geri bildirim bağlantısı olmaksızın haberleşen iki uç tarafından da tahmin edildiği kanal karşılıklılık süreci ile başarılabilmektedir. Diğer bir deyişle, kanal fazı kanal yanıtından ayıklanmaktadır. Kanal fazlarının tahmin edilmesinin ardından, iletilen bitler bir sembole eşleştirilir ve ardından modüle sembolün fazı, anlık kanal fazının negatifine eşit olan bir açı ile denkleştirilir.

Onerilen yöntem, gelecekteki kablosuz cihazlar, örneğin, nesnelerin interneti (IoT) cihazlarında kullanılabilen bir düşük karmaşıklıklı alıcı sağlamaktadır.

Onerilen yöntem yalnızca, kanal tahmin sürecini basitleştiren bir kanal kazanç tahmini gerektirmektedir.

Önerilen buluş, iletilen verilerin güvenliğini sağlamanın yanı sıra, modülasyon tipi bilgileri gizleyebilen koordineli çok noktalı ağlar tarafından sunulan coğrafi olarak dağıtık iletim noktalarına ağırlık vermektedir, bu da meşru olmayan kod çözümünü oldukça zor hale getirmektedir.

Şekillerin Açıklaması

Şekil 1: Mevcut açıklamanın belirli yönlerine uygun olarak temel operasyonların akış şeması.

110: Kablosuz kanalın tahmin edilmesi: verici bir kanal (kazanç ve faz) tahmin sürecini ve alıcı bir kanal kazanç tahmin sürecini başlatır.

120: Vericide kanal tahmin sürecinden kanal fazı vektörünün elde edilmesi

130: Vericide bir dijital modülasyon şemasına dayalı olarak modüle sembollere iletilen bitlerin eşleştirilmesi

140: Modüle sembollerin, anlık kanal fazının negatifine eşit olan bir açı ile döndürülmesi ile karakterize edilen, vericide sembol fazı ön denkleştirmesinin gerçekleştirilmesi

150: Alıcıda alınan sembollerin kodunun çözülmesi

Şekil 2: Mevcut buluşun belirli yönlerine göre sembol fazı ön denkleştirmesi ile cihaz ve saldırganı, tekli iletim noktasını (TP) içeren basit ağın örneği.

310: İletim noktası (TP)

330: Cihaz (D)

320: Saldırgan (A)

341: Modüle sembollerini ön denkleştirmek üzere TP (311) tarafından kullanılan TP ve Cihaz arasındaki Kablosuz kanal

342: TP ve Cihaz arasındaki Kablosuz kanal

Şekil 3: Mevcut buluşun belirli yönlerine göre sembol fazı dönüşüne sahip koordineli ağın örneği.

411: Birinci koordineli iletim noktası (TP-1)

412: N'inci koordineli iletim noktası (TP-N)

441: TP-1 ve Saldırgan arasındaki Kablosuz kanal

442: Modüle sembollerini ön denkleştirmek üzere TP-1 (411) tarafından kullanılan TP-1 ve Cihaz arasındaki Kablosuz kanal

443: Modüle sembollerini ön denkleştirmek üzere TP-N (412) tarafından kullanılan TP-N ve Cihaz arasındaki Kablosuz kanal

444: TP-N ve Saldırgan arasındaki Kablosuz kanal

420: Saldırgan (A)

430: Cihaz (D)

Buluşun Detaylı Açıklaması

Yukarıda bahsedildiği üzere, mevcut buluş kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntem ile ilgilidir, burada söz konusu yöntem aşağıdaki adımları içermektedir

- Kablosuz kanalın tahmin edilmesi, **burada söz konusu süreç (a)** vericinin bir kanal (kazanç ve faz) tahmin sürecini **başlatması** ve **(b)** alıcının bir kanal kazanç tahmin sürecini **başlatmasından oluşmaktadır**
- Vericide kanal tahmin sürecinden kanal fazı vektörünün elde edilmesi
- Vericide bir dijital modülasyon şemasına dayalı olarak modüle sembollere iletilen bitlerin eşleştirilmesi
- Modüle sembollerin, anlık kanal fazının negatifine eşit olan bir açı ile döndürülmesi ile karakterize edilen, vericide sembol fazı ön denkleştirmesinin gerçekleştirilmesi
- Alıcıda alınan sembollerin kodunun çözülmesi

Şekil 1'de, mevcut buluşun belirli yönlerine göre kablosuz haberleşmeye yönelik temel operasyonların bir akış diyagramı verilmektedir.

Adım (**110**) kanal tahmin sürecinin çalışmasını sunar. İletişimi güvenli hale getirilecek olan iletim noktası (**310, 411, 412**) ve cihaz (**330, 430**), iletim noktasının (**310, 411, 412**) cihazın bulunduğu kablosuz kanalın hem kazancını hem de fazını tahmin ettiği kablosuz kanalı tahmin

eder. (330, 430), modüle edilmiş semboller cihaza (330, 430) yalnızca kanal kazancı ile ölçeklenmiş olarak ulaşacağından, yalnızca kablosuz kanalın kazancını tahmin eder.

Adım (120) faz vektörü aşamasının faz ayıklanmasını sunmaktadır. İletim noktası (310, 411, 412), kanal tahmin sürecinden (110) kanal fazı vektörünü elde etmektedir.

Adım (130), eşleştirme sürecini sunmaktadır. İletim noktası (310, 411, 412), bir dijital modülasyon şemasını takiben modüle sembollere cihazın (330, 420) iletilen bitlerini eşleştirmektedir.

Adım (140), bir sembol fazı ön denkleştirme sürecini sunmaktadır. İletim noktası (310, 411, 412), modüle sembolleri anlık kanal fazının negatifine eşit bir açı ile döndürmektedir. Modüle semboller, kablosuz kanalın (341,442, 443) bir düz yanıta sahip olmaması nedeniyle birbirinden bağımsız olarak döndürülmektedir.

Adım (150), bir sembol kod çözme sürecini sunmaktadır. Cihaz (330, 420), kanal kazancı etkisini kaldırdıktan sonra alınan sembollerin kodunu çözmektedir.

Dolayısıyla, buluşun bir yapılandırması, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntem ile ilgilidir, burada meşru varlıklar (iletim noktası (310, 411, 412) ve cihaz (330, 420)) arasındaki kablosuz kanal tahmininde, cihaz (330, 430), modüle semboller yalnızca kanal kazancı ile ölçeklenen cihaza (330, 430) varacağı için yalnızca kablosuz kanalın kazancını tahmin etmektedir.

Buluşun bir başka yapılandırması, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntemdir, burada iletim noktasındaki (310, 411, 412) kanal fazı ayıklama süreci, iletim noktası (310, 411, 412) ve cihaz (330, 430) arasındaki kablosuz kanaldan (341, 442, 443) kanal fazı vektörünün ayıklanmasını içermektedir. Kanal karşılıklılık özelliği nedeniyle meşru varlıklar arasında herhangi bir paylaşım yapılmasına gerek yoktur.

Buluşun bir başka yapılandırması, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntemdir, burada iletilen bitlerin modüle sembollere eşleştirilmesi, bir dijital modülasyonu takiben iletim noktasında (310, 411, 412) yapılmaktadır. Bu belge

içerisinde "dijital modülasyon," tüm sembollerin özel şema ile aynı modülasyon kurallarını takip edeceği anlamına gelmektedir.

Buluşun bir başka yapılandırması, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntemdir, burada sembol fazı ön denkleştirmesinin, modüle sembollerin anlık kanal fazının negatifi ile eşit bir açı ile döndürülmesi ile gerçekleştirildiği anlamına gelmektedir. Modüle semboller, kablosuz kanalın (341,442, 443) düz bir yanıta sahip olmaması nedeniyle birbirinden bağımsız olarak döndürülmektedir.

Buluşun bir başka yapılandırması, kablosuz haberleşmelerde gizli dinlemeye karşı gizliliğin geliştirilmesine yönelik bir yöntemdir, burada alınan sembollerin, kanal kazancı etkisinin kaldırılmasından sonra cihazda (330, 430) kodu çözülmektedir.

Buluşa göre yöntemin farklı adımları ile ilgili olan buluşun yapılandırmaları, herhangi bir şekilde birleştirilebilmektedir, bu da bu açıklamada açıklanan tüm yapılandırmaların birleştirilebildiği veya burada açıklanan bazı yapılandırmaların birleştirilebildiği anlamına gelmektedir.

ŞEKİL 2, üç tip cihazdan oluşan basit bir ağın örneğidir: bir meşru TP (310), meşru cihaz (330) ve bir saldırgan (320).

TP (310), saldırgana (320) karşı cihaz (330) ile güvenli bir haberleşme gerçekleştirmektedir. Haberleşme düğümleri tekli/çoklu antenler ile donatılabilmektedir.

Saldırgan (320), kablosuz kanalı (341) pasif olarak öğrenmeye çalışır. Böylece, saldırganın (320) konumu ve kanal bilgisi (342), hem TP (310) hem de cihaz (330) için erişilemez olur.

Kablosuz kanalın karşılıklılık özelliği varsayılmaktadır. İletilen verileri cihaza (330) güvenli hale getirmek üzere, kanal fazı vektörü kablosuz kanala (341) dayalı olarak ayıklanır.

TP (310), modüle sembolleri, kablosuz kanalın (341) anlık fazının negatifine eşit bir açı ile döndürür.

İletilen semboller kanal (341) kazancı tarafından ölçeklenen cihaza (330) varacaktır. Kanal kazancı etkisinin kaldırılmasından sonra, iletilen sembollerin doğru şekilde kodu çözülür.

Saldırganda (320), alınan semboller doğru olmayan faza ve kazanca sahiptir, böylece saldırgan (320) bunların kodunu doğru şekilde çözemez.

Sonuç olarak, cihazda (330) alınan sembol doğru şekilde çözülebilmektedir. Ancak bu, alınan sembolün yüksek kod çözüm hatalarından muzdarip olduğu, bunun da performansı bozduğu saldırgan (320) tarafındaki durum böyle değildir.

ŞEKİL 3, mevcut açıklamanın belirli yönlerine göre sembol fazı ön denkleştirmesine sahip koordineli ağın bir örneğidir.

TP-1'den (411) TP-N'ye (412) kadar olan TP'ler, saldırgana (420) karşı cihaz (430) ile haberleşmenin güvenliğini sağlamak üzere koordine edilmektedir. Haberleşme düğümleri tekli/çoklu antenler ile donatılabilmektedir.

N-koordineli TP'ler, bunlar ve cihaz (430) arasındaki kablosuz kanallardan ayıklanan fazlı vektöre dayalı olarak bir sembol fazı ön denkleştirme sürecini (130) uygularken, TP-1 (411) kablosuz kanaldan (442) ayıklanan kanal fazı vektörünü kullanır ve TP-N (412) kablosuz kanaldan (444) ayıklanan kanal fazı vektörünü kullanır, ve böyle devam eder.

Cihazda (430), iletilen semboller, kanal (341) kazancı tarafından ölçeklenen cihaza (330) varacaktır. Kanal kazancı etkisinin kaldırılmasından sonra, iletilen sembollerin doğru şekilde kodu çözülmektedir. Kanal kazancı denkleştirmesi, kablosuz kanalın (442) kazancı ve kablosuz kanalın (444) kazancının kombinasyonu olan etkili kazanca dayalıdır.

Saldırganda (420), alınan semboller, doğru olmayan faza ve kazanca sahiptir, böylece saldırgan (320) bunların kodunu doğru şekilde çözememektedir.

Sonuç olarak, cihazdaki (430) birleşik alınan semboller doğru şekilde çözülebilmektedir. Ancak bu, birleşik alınan sembollerin yüksek kod çözüm hatalarından muzdarip olduğu, bunun da performansı bozduğu saldırgan (420) tarafındaki durum böyle değildir.

Koordinasyon ağı, yalnızca iletilen bilgilerin güvenliğini sağlamayan, ancak aynı zamanda modülasyon bilgilerinin gizlenmesine de yardımcı olan, modüle sembollerdeki karartmanın gerçekleştirilmesine yardımcı olmaktadır.

Buluşun bir yapılandırması, bir meşru TP (310), meşru cihaz (330) ve bir saldırgandan (320) oluşan basit bir ağda gizli dinlemeyi önlemek üzere mevcut buluşa göre bir yöntemin kullanımıdır.

Buluşun bir yapılandırması, bir koordineli ağda gizli dinlemeyi önlemek üzere mevcut buluşa göre bir yöntemin kullanımıdır.

Buluşun bir yapılandırması, yukarıda bahsedilen standartlar, kod bölmeli çoklu erişim (CDMA), frekans bölmeli çoklu erişim (FDMA), Küresel Mobil Haberleşme Sistemi (GSM), GSM/Genel Paket Radyo Hizmeti (GPRS), Gelişmiş Veri GSM Ortamı (EDGE), Geniş bant-CDMA (W-CDMA), Optimize Edilmiş Evrim Verileri (EV-DO), Yüksek Hızlı Paket Erişimi (HSPA), Yüksek Hızlı Paket İndirme Erişimi (HSDPA), Yüksek Hızlı Paket Yükleme Erişimi (HSUPA), Evrimleşmiş Yüksek Hızlı Paket Erişimi (HSPA+), Uzun Vadeli Evrim (LTE), AMPS, 5G Yeni Radyo (NR), veya bir kablosuz, hücresel veya nesnelerin interneti (IoT) ağı içerisinde haberleşmek üzere kullanılan diğer bilinen sinyallerden herhangi birini destekleyebilen herhangi cihaz, sistem veya ağ üzerinde mevcut buluşa göre bir yöntemin kullanımıdır.

Bu belgede "**Eşleştirme**" terimi, bir dijital bilgi sinyalinin (bit akışı), iletilen sinyalin (modüle semboller) genlik, faz veya frekansına kodlandığı bir sürece atıfta bulunmaktadır.

Bu belgede **"Sembol fazı ön denkleştirme"** terimi, modüle sembolün fazının, anlık kanal fazının negatifine eşit olan bir açı ile döndürüldüğü bir sürece atıfta bulunmaktadır.

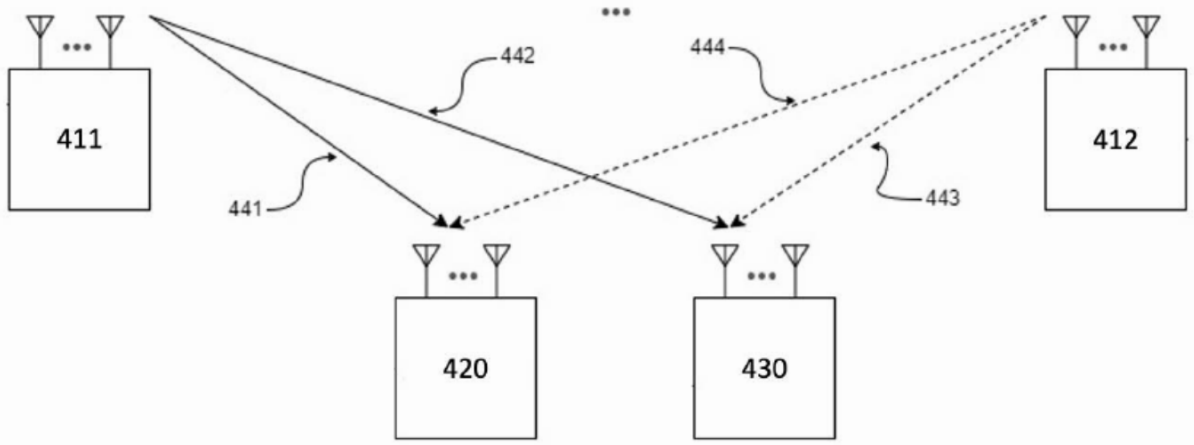
Bu temel kavramlar çevresinde, buluşun konusu ile ilgili birkaç yapılandırmanın geliştirilmesi mümkündür; dolayısıyla buluş, burada açıklanan örnekler ile sınırlandırılamamaktadır ve buluş, esasen, istemlerde tanımlandığı üzeredir.

Teknikte uzman bir kişinin benzer yapılandırmaları kullanarak buluşun yeniliğini aktarabileceği ve/veya bu tür yapılandırmaların ilgili teknikte kullanılanlara benzer diğer

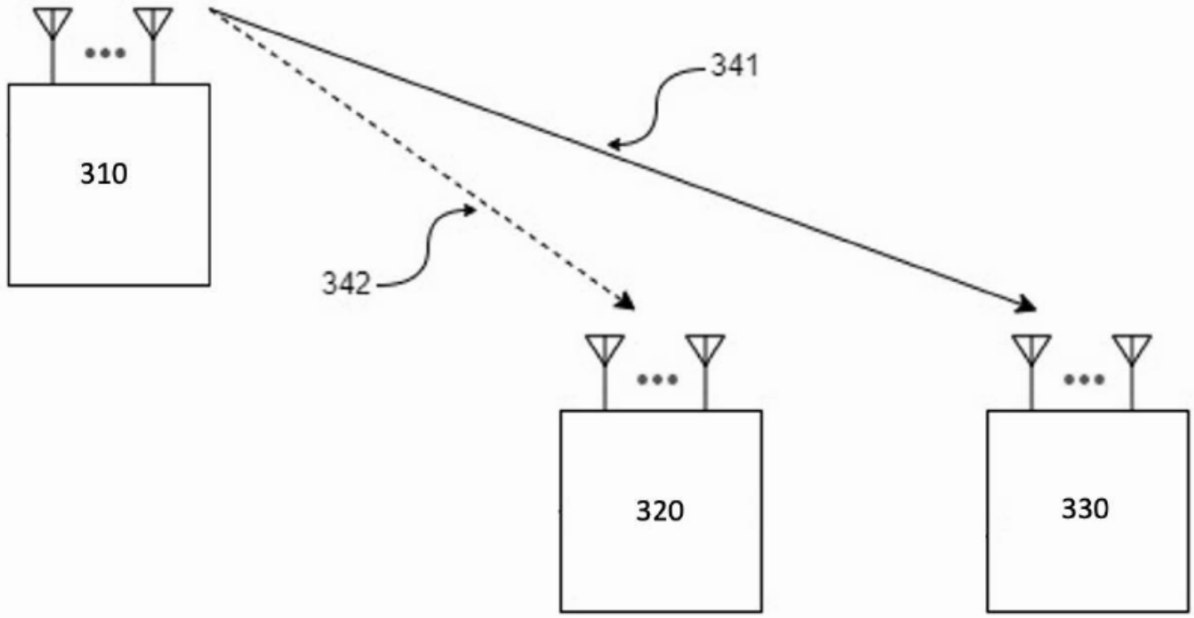
alanlara uygulanabileceği açıktır. Dolayısıyla, aynı zamanda, bu tür yapılandırmaların yenilik kriterlerinden ve tekniğin bilinen durumunu aşma kriterlerinden yoksun olduğu açıktır.

Buluşun Endüstriyel Uygulaması

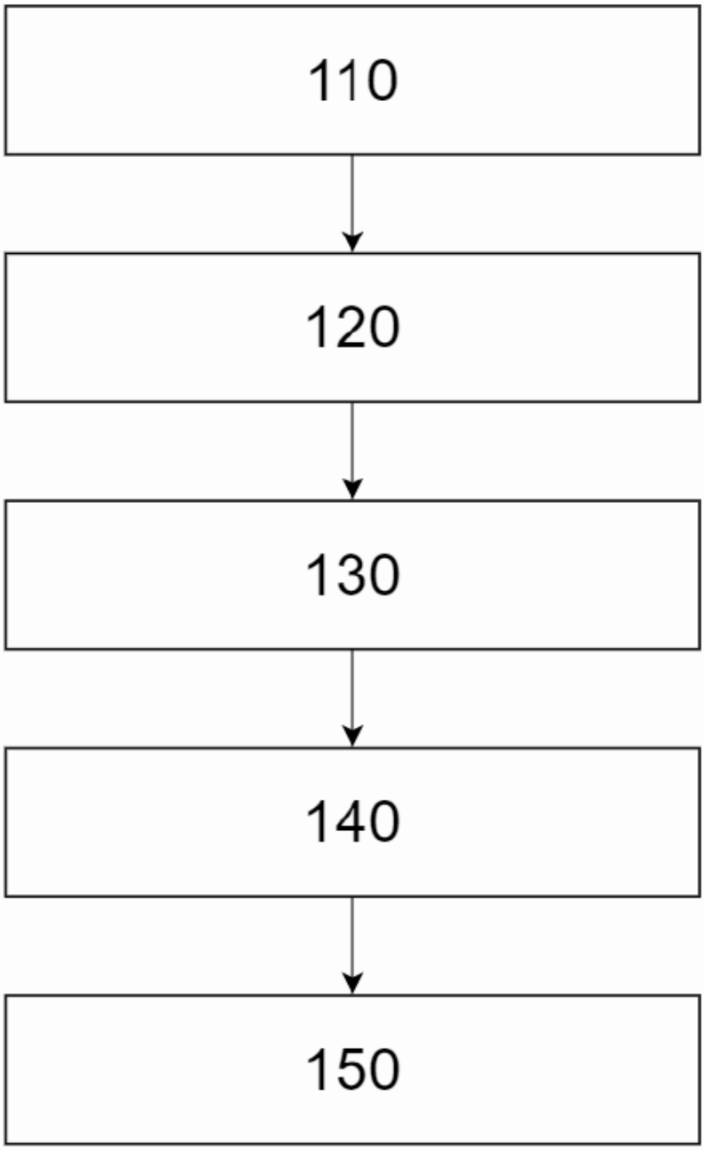
Kablosuz haberleşme, bankacılıktan sağlığa, eğitimden ticarete, endüstriden tarıma çeşitli alanlardaki uygulamaları ile insan hayatının gittikçe önemli bir parçası haline gelmektedir. Bu bakımdan en önemli zorluklardan bir tanesi, veri alışverişinin kötü niyetli bir düğüm tarafından kesilmeye karşı korunmasını sağlamaktır. Bu amaçla, özellikle de hassas tarım, otonom sürüş, akıllı evler vb. gibi kullanım senaryolarında yoğun olarak kullanılan Nesnelerin İnterneti (IoT) düğümleri gibi düşük sınıf cihazlara yönelik olarak basit, hafif ve sağlam mekanizmalar, gerekmektedir. Mevcut buluş, kablosuz haberleşmede gizli dinlemeye karşı gizliliği geliştirmek üzere basit bir yöntem sağlamaktadır. Söz konusu yöntem, meşru alıcı-vericiler arasındaki kanal fazının ön denkleştirilmesini içermektedir. Bu yöntem, herhangi bir ilave yük getirmeksizin haberleşmenin güvenlik gereksinimlerini karşılamaktadır, bu da onu düşük sınıf cihazlara yönelik olarak uygulanabilir hale getirmektedir.



ŞEKİL 3



ŞEKİL 2



ŞEKİL 1