ÖZET

OFDM TABANLI ISAC SİSTEMLERİNDE FİZİKSEL KATMAN GÜVENLİĞİNİ ARTTIRMAYA YÖNELİK YÖNTEM

Buluş, en az bir baz istasyonu (100) ve en az bir kullanıcı ekipmanı (201) içeren Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Entegre Algılama ve İletişim (ISAC) sistemi tarafından gerçekleştirilen bir yöntem ile ilgilidir. Buna göre, yeniliği şu adımları içermesi ile karakterize edilmektedir; baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında kanal incelemesinin gerçekleştirilmesi; bir kanal uyuşmazlığı tespit edilirse, baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında mutabakatın gerçekleştirilmesi; baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında bir kanalın belirlenmesi; baz istasyonu (100) tarafından, GAN modelinin girilen bir kanaldan düşman kanallar üretmek üzere yapılandırıldığı önceden eğitilmiş bir üretken düşman ağ (GAN) modeline erişilmesi, burada GAN modeli hem baz istasyonunda (100) hem de kullanıcı ekipmanında (201) depolanmaktadır; baz istasyonu (100) tarafından, belirlenen kanalın GAN modeline ve GAN modelinden gelen düşman kanallara girilmesi; düşman kanallara dayanarak dizilerin üretilmesi; iletilecek bir mesajın OFDM sembollerinin sırasının üretilen dizilere göre düzenlenmesi; baz istasyonu (100) tarafından, düzenlenmiş OFDM sembollerinin kullanıcı ekipmanına (201) iletilmesi; kullanıcı ekipmanı (201) tarafından OFDM sembollerinin alınması; kullanıcı ekipmanı (201) tarafından, belirlenen kanalın GAN modeline girilmesi ve düşman kanalların elde edilmesi; düşman kanallara dayanarak dizilerin üretilmesi; mesajı elde etmek için üretilen dizilere dayanarak OFDM sembollerinin yeniden düzenlenmesi.

İSTEMLER

1. En az bir baz istasyonu (100) ve en az bir kullanıcı ekipmanı (201) içeren Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Entegre Algılama ve İletişim (ISAC) sistemi tarafından gerçekleştirilen bir yöntem olup, aşağıdaki adımları içermesi **ile karakterize edilmektedir;**

- baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında kanal incelemesinin gerçekleştirilmesi;
- bir kanal uyuşmazlığı tespit edilirse, baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında mutabakatın gerçekleştirilmesi;
- baz istasyonu (100) ve kullanıcı ekipmanı (201) arasında bir kanalın belirlenmesi;
- baz istasyonu tarafından, GAN modelinin girilen bir kanaldan düşman kanallar üretmek üzere yapılandırıldığı önceden eğitilmiş bir üretken düşman ağ (GAN) modeline erişilmesi, burada GAN modeli hem baz istasyonunda (100) hem de kullanıcı ekipmanında (201) depolanmaktadır;
- baz istasyonu tarafından, belirlenen kanalın GAN modeline ve GAN modelinden gelen düşman kanallara girilmesi;
- düşman kanallara dayalı dizilerin üretilmesi;
- iletilecek bir mesajın OFDM sembollerinin sırasının üretilen dizilere göre düzenlenmesi;
- baz istasyonu tarafından, düzenlenmiş OFDM sembollerinin kullanıcı ekipmanına (201) iletilmesi;
- kullanıcı ekipmanı (201) tarafından OFDM sembollerinin alınması;
- kullanıcı ekipmanı (201) tarafından, belirlenen kanalın GAN modeline girilmesi ve düşman kanalların elde edilmesi;
- düşman kanallara dayanarak dizilerin üretilmesi;
- mesajı elde etmek için üretilen dizilere dayanarak OFDM sembollerinin yeniden düzenlenmesi.

2. İstem 1’e göre yöntem olup, aşağıdakiler **ile karakterize edilmektedir**

- baz istasyonu tarafından, kanalı GAN modeline girmeden önce belirlenen kanala dayalı olarak GAN modelinin en az bir ağırlığının güncellenmesi;

- kullanıcı ekipmanı (201) tarafından, kanalı GAN modeline girmeden önce belirlenen kanala dayalı olarak GAN modelinin en az bir ağırlığının güncellenmesi.

TARİFNAME

OFDM TABANLI ISAC SİSTEMLERİNDE FİZİKSEL KATMAN GÜVENLİĞİNİ ARTTIRMAYA YÖNELİK YÖNTEM

TEKNİK ALAN

Buluş, en az bir baz istasyonu ve en az bir kullanıcı ekipmanı içeren Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Entegre Algılama ve İletişim (ISAC) sistemi tarafından gerçekleştirilen bir yöntem ile ilgilidir.

ÖNCEKİ TEKNİK

Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Entegre Algılama ve İletişim (ISAC), radar algılama ve iletişimi aynı çerçevede birleştirmek için OFDM dalga biçimlerini kullanan bir sistemdir. LTE ve Wi-Fi gibi kablosuz iletişim sistemlerinde yaygın olarak kullanılan bir modülasyon tekniği olan OFDM, çok yollu sönümlemenin üstesinden gelme yeteneği ve mevcut spektrumu kullanma verimliliği ile bilinmektedir. OFDM tabanlı ISAC, bu özelliklerden yararlanarak tek bir sinyalin aynı anda algılama ve iletişim görevlerini yerine getirmesini sağlamaktadır.

Entegrasyon, OFDM dalga biçimini bu iki işlev arasında paylaştırarak çalışmaktadır ve algılama ve iletişim için ayrı sinyallere olan ihtiyacı ortadan kaldırmaktadır. Bu yaklaşım verimlidir; çünkü spektrum kaynaklarının kullanımını en üst düzeye çıkarırken sistemin karmaşıklığını ve maliyetini azaltmaktadır. OFDM'nin mevcut bant genişliğini birden fazla alt taşıyıcıya bölme kabiliyeti esneklik sağlayarak hem algılama (hassas menzil veya hız çözünürlüğü gibi) hem de iletişimin (yüksek veri hızları veya düşük gecikme süresi gibi) özel ihtiyaçlarını karşılamak için kaynakların tahsis edilmesini mümkün kılmaktadır. Bu da OFDM tabanlı ISAC'ı otonom araçlar, akıllı şehirler ve algılama ile iletişimin sıklıkla bir arada bulunması gereken yeni nesil kablosuz ağlar gibi uygulamalar için uygun hale getirmektedir.

Tek bir sistem içinde birden fazla işlevin entegrasyonu büyük ilgi görmüştür; bu, kaynakları hizmetler veya işlevler arasında daha verimli bir şekilde paylaşmayı veya sinerji yoluyla bir

veya daha fazla hizmetin yeteneklerini geliştirmeyi amaçlamaktadır. Bu bağlamda, entegre algılama ve iletişim (ISAC) için OFDM şemaları üzerinde kapsamlı araştırmalar yürütülmektedir. Bunun nedeni, OFDM'nin yüksek spektrum verimliliği ve çok yollu yayılmaya karşı dayanıklılığı nedeniyle çeşitli kablosuz iletişim sistemlerinde (örneğin 4G, 5G ve Wi-Fi 4'ten itibaren Wi-Fi standartları) yaygın olarak benimsenmiş olması ve donanım yapısında ve sinyalleşme stratejilerinde küçük değişikliklerle hem algılama hem de iletişim işlevlerini tek bir dalga formu üzerinden entegre etme ihtiyacıdır [1].

Geleneksel OFDM tabanlı iletişimde, OFDM pilotları genellikle kanal tahmini için kullanılmaktadır. Şu anda pilot sinyaller uygun maliyetli menzil belirleme, algılama veya kendi kendini konumlandırma için kullanılmaktadır [2]. Geleneksel iletişimde hem algılama hem de kanal kestirimi için pilot sinyallerin kullanılmasıyla, algılama için yeni taşıyıcı sinyaller üretme ihtiyacından kaçınılmış olmaktadır. Kaynak paylaşımının belirgin faydalarına rağmen, algılama ve iletişimin entegre edilmesi, özellikle algılama ve iletişim kullanıcıları iki farklı varlık olduğunda, önemli bilgi sızıntısı ve gizlilik riskleri ortaya çıkarabilmektedir. Örneğin pilot sinyaller hakkında bilgi sahibi olan meşru bir algılama kullanıcısı, iletişim sinyalini eşitleme yeteneğine sahiptir ve bu da onu geleneksel iletişime karşı potansiyel bir gizli dinleyici haline getirmektedir. Bu durum kritik bir güvenlik riski oluşturmakta ve ISAC sistemleri, özellikle de OFDM tabanlı ISAC sistemleri için yeni veya geliştirilmiş güvenlik mekanizmaları gerektirmektedir.

Geleneksel olarak, verileri belirli yöntemlerle şifrelemek ve şifrelerini çözmek için önceden paylaşılan anahtarlar kullanarak iletişimin gizliliğini sağlamak ve korumak için şifreleme şemaları kullanılmaktadır. Bunlar arasında hem şifreleme hem de şifre çözme için tek bir anahtar kullanan simetrik anahtarlı kriptografi (örneğin Gelişmiş Şifreleme Standardı (AES) ve Veri Şifreleme Standardı (DES), Blow Fish, Ronald Rivest (RC)); şifreleme için bir açık anahtar ve şifre çözme için bir özel anahtar olmak üzere bir çift anahtara dayanan açık anahtarlı kriptografi (örneğin Rivest-Shamir-Adleman (RSA) ve Diffie-Hellman) [3]-[5]. Ayrıca herhangi bir uzunluktaki giriş mesajlarını genellikle mesaj özetleri olarak adlandırılan sabit uzunlukta özet değerlerine dönüştüren Güvenli Hashing Algoritması (SHA), RACE Integrity Primitives Evaluation Message Digest (RIPEMD – RACE Bütünlüğü Primitif Değelendirme Mesajı Özümleme) ve Message Digest Algorithm (MD – Mesaj Özümleme Algoritması) gibi Hash fonksiyonları da vardır [3]. Son yıllarda kripto tabanlı algoritmaların yaygın kullanımına rağmen, bu teknikler yüksek anahtar dinamiğinden yoksundur ve aynı

anahtar genellikle uzun süreler boyunca yeniden kullanıldığından uzun vadeli iletişim için uygun değildir. Bu güvenlik açığı, içinde bulunduğumuz çağda hesaplama açısından güçlü saldırganlar karşısında özellikle kritik hale gelmektedir. Birden çok cihazın bulunduğu büyük ölçekli uygulamalarda, her cihaz için birden fazla anahtar üretmek ek zorluklar ortaya çıkarmakta ve mevcut anahtar üretim tekniklerini zorlamaktadır. Ayrıca kablosuz sistemlerin yayın niteliği, herhangi bir varlığın kablosuz sinyalleri anonim olarak yakalamasına ve analiz etmesine olanak tanıyarak anahtarın ele geçirilmesi ve potansiyel bilgi sızıntısı riskini arttırmaktadır. Geleneksel şifreleme teknikleri üzerindeki diğer kısıtlamalar arasında dosya boyutuna, türüne ve platforma bağlı olan matematiksel şifreleme işlevlerinin getirdiği karmaşıklık ve gecikme yer almaktadır [3]. Bu durum, düşük gecikmeli iletişim ve arttırılmış gerçeklik, gerçek zamanlı oyun gibi yoğun veri uygulamaları için performansı kötüleştirmektedir.

Fiziksel Katman Güvenliği: Geleneksel kriptografi teknikleri öncelikle daha yüksek katmanlarda bilgi gizliliği sağlamaya odaklanmış, genellikle fiziksel veya birinci katmanı göz ardı etmiştir [6]. Ancak kablosuz iletişimde, cihazların fiziksel özelliklerinin, dalga biçimlerinin ve verici (TX) ile alıcı (RX) arasındaki kanalın benzersiz ve rastgele doğasının güvenilir, güçlü, düşük maliyetli ve daha az karmaşık güvenlik önlemleri uygulamak için kullanılabileceği keşfedilmiştir [7]. Bu durum, bilgi güvenliğinde Fiziksel Katman Güvenliği (PLS) olarak bilinen ve gizli dinleme, sahtekarlık, kimliğe bürünme ve diğer saldırılara karşı yeni bir koruma katmanı ekleyen yeni bir kavramın önünü açmıştır.

Özellikle kablosuz kanal ve özellikleri, sinyali geçersiz kılmak veya gizli dinleyicideki sinyal-gürültü oranını (SNR) önemli ölçüde düşürmek için bağlantı uyarlaması için PLS'de yaygın olarak kullanılmaktadır [7]. Bu senaryoda, gizli dinleyici sinyali yeniden yapılandırmak için yeterli performans elde edemez. Geleneksel kriptografik tekniklerde genellikle eksik olan anahtar dinamiği sorununu ele almak için, verici (TX) ve alıcı (RX) arasındaki rastgelelik ve karşılıklılık dahil olmak üzere kanalın benzersiz özelliklerinden, gözlemlenen kanallara dayanarak dinamik ve benzersiz olan karşılıklı anahtarlar (özdeş anahtarlar) üretmek için yararlanılmıştır. Kanal tabanlı anahtar üretimi [7] olarak bilinen bu yaklaşım, yasal TX ve RX arasındaki kanal karşılıklılığından yararlanarak yeni bir anahtar değişim sistemine olan ihtiyacı ortadan kaldırmaktadır. Ayrıca diğer çalışmalar, gizli dinleyicinin performansını engellemek için girişim veya gürültülü sinyal enjeksiyonu için yöntemler geliştirmiştir [7] [8].

4G, 5G ve Wi-Fi 4'ten itibaren Wi-Fi standartları gibi OFDM tabanlı iletişim sistemlerinde, gizli dinlemeye karşı güvenlik kapsamlı bir şekilde tartışılmış ve OFDM dalga biçimine uyarlanmış umut verici teknikler önerilmiştir. Gizlice dinleme eşitleme kabiliyetini zorlaştırmak için döngüsel önek (CP) kısaltma, rastgele döngüsel önek, rastgele pilotlar, kasıtlı girişim ekleme ve ortak zaman-frekans alanı yapay gürültü (AN) gibi teknikler önerilmiştir.

OFDM pilotları hem algılama hem de kanal tahmini için kullanıldığında, algılama için yeni taşıyıcı sinyaller üretme ihtiyacı ortadan kalkmaktadır. Ancak bu yaklaşım aynı zamanda iletişim sinyalini meşru algılama kullanıcılarının potansiyel gizli dinlemelerine karşı savunmasız hale getirmektedir, çünkü pilot sinyaller hakkında bilgi sahibi olan meşru algılama kullanıcıları iletişim sinyalini eşitleyebilmektedir. Dolayısıyla iletişim sinyalinin algılayıcı kullanıcılardan da korunması gerekmektedir. Başka bir ifadeyle, OFDM tabanlı iletişim sistemlerine uyarlanmış mevcut PLS teknikleri, iletişim ve algılama arasında güvenli bir birliktelik sağlamakta başarısız olabilmektedir.

Rastgele CP veya kanal kısaltma PLS tekniği: CP, verici (TX) ve geleneksel alıcı (RX) arasındaki bir anlaşmaya veya kanallarının maksimum aşırı gecikmesine göre ayarlanmaktadır. Bu CP potansiyel bir gizli dinleyicinin (Eve) maksimum aşırı gecikmesine göre tasarlanmadığından, gayrimeşru bir kullanıcı (Eve) için çok kısa olabilmektedir ve bu da daha yüksek taşıyıcılar arası girişime (ICI) ve semboller arası girişime (ISI) yol açabilmektedir [9] [10] [11]. Bu, artık iletişim için gayrimeşru olduğu varsayılan meşru bir algılama kullanıcısının OFDM pilot sinyallerinde yüksek ICI ve ISI yaşayacağı ve bunun da başarısız veya düşük algılama performansıyla sonuçlanacağı anlamına gelmektedir.

Pilot Rastgeleleştirme: Bu teknik, farklı OFDM sembolleri arasında pilot tonların konumunu, sırasını veya modelini değiştirerek bir saldırganın (EVE) kanal tahmini için pilotları tanımlamasını ve ayıklamasını daha zor hale getirmeyi içermektedir. Sonuç olarak, meşru algılama kullanıcısı da pilotları tanımlayamaz ve algılama yapmasını engellemektedir [12] [13].

Kasıtlı olarak girişim yaratılması: İçsel girişim, bu girişimi iptal etme kabiliyetine sahip olduğu varsayılan meşru alıcı tarafından bilinen bir modeli takip ederek oluşturulmaktadır. İçsel girişimler zaman-frekans ızgarası boyunca geniş bir şekilde dağılmaktadır ve üst üste

binmektedir, bu da gizli dinleyicinin yükleme modelini bilmeden tamamen ortadan kaldırmasını oldukça zorlaştırmaktadır. İçsel girişim pilot taşıyıcıları da önemli ölçüde etkileyerek ISAC sistemlerinde algılayıcı kullanıcıların performansını düşürebilmektedir [14].

Yapay Gürültü (AN): AN, OFDM sinyalleri ile birlikte iletilmektedir ve alıcının kanal durum bilgisine (CSI) dayanarak üretildiği için meşru alıcıda etkili bir şekilde giderilebilmektedir [6] [15] [16]. Bununla birlikte, algılayıcı bir kullanıcı için, OFDM pilot alt taşıyıcıları boyunca dağıtılabilen AN, algılama sürecini önemli ölçüde saptırabilmektedir ve potansiyel olarak yanlış algılama kararlarına yol açabilmektedir. Frekans alanlı yapay gürültü (AN) belirli veri taşıyıcılarına uygulandığında, TX ve RX'te birden çok antene sahip sistemler için daha uygun olduğundan, tek antenli dinleme kanallarında veya sınırlı sayıda antene sahip cihazlarda gizlilik oranını önemli ölçüde iyileştirmeyebilmektedir. Yukarıdaki tartışma göz önüne alındığında, iletişim kullanıcısının kanal özelliklerine dayalı OFDM sembollerinin güvenliğinin sağlanmasının ISAC sistemlerinde algılama yeteneklerini engelleyebileceği sonucuna varılabilmektedir.

İlginç bir şekilde, [17] ve [18]'deki çalışmalar, konuşma iletim sistemlerinde artık anlaşılabilirliği en aza indirmeyi amaçlayan FFT tabanlı konuşma karıştırma tekniklerini önermiş ve önceki yöntemlerin dinleyiciler tarafından istismar edilebilecek tanımlanabilir desenler bırakan sınırlamalarını ele almıştır. [17]'de, frekans alanındaki Hadamard dönüşümüne dayanan, daha geniş bir anahtar uzayı, düşük artık anlaşılabilirlik ve oldukça iyi geri kazanılmış konuşma kalitesi sunan bir karıştırma algoritması önerilmiştir. [18]'deki çalışma, çeşitli frekans bileşenlerine izin vererek konuşmayı karıştırmak için Karesel Genlik Modülasyonu (QAM) eşlemesini Dikey Frekans Bölmeli Çoğullama (OFDM) ile birleştirmektedir ve artık anlaşılabilirlik olmadan karıştırılmış konuşma ile sonuçlanmaktadır. Ayrıca konuşmadan birden fazla benzersiz karıştırma dizisinin oluşturulmasına izin vermektedir. Bununla birlikte, bu yöntemin bir sınırlaması, alıcının konuşma içeriği hakkında önceden bilgi sahibi olmaması nedeniyle her iki uçta da karıştırma anahtarlarının yeniden üretilmesi için güvenilir bir sürecin olmamasıdır, bu da anahtarlar önceden paylaşılmadıkça çözmeyi zorlaştırmaktadır.

Yukarıda bahsedilen tüm sorunlar, sonuç olarak ilgili teknik alanda bir yenilik yapılmasını gerekli kılmıştır.

1. S. Mura, D. Tagliaferri, M. Mizmizi, U. Spagnolini ve A. Petropulu, “Waveform Design for OFDM-Based ISAC Systems Under Resource Occupancy Constraint,” 2024 IEEE Radar Conference (RadarConf24), Denver, CO, ABD, 2024, s. 1-6, doi: 10.1109/RadarConf2458775.2024.10548861.

2. Y. Wan, Z. Hu, A. Liu, R. Du, T. X. Han ve T. Q. S. Quek, “OFDM-Based Multiband Sensing For ISAC: Resolution Limit, Algorithm Design, and Open Issues,” in IEEE Vehicular Technology Magazine, cilt. 19, no. 2, s. 51-59, Haziran 2024, doi: 10.1109/MVT.2024.3368205.

3. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

4. C. S. KLINE ve G. J. POPEK, “Public key vs. conventional key encryption,” 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, ABD, 1979, s. 831-838, doi: 10.1109/MARK.1979.8817073.

5. Hellman, M. E. (2012). An overview of public key cryptography. IEEE Communications Magazine, 40(5), 42-49.

6. Q. Xu, P. Ren, Q. Du ve L. Sun, “Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission,” in IEEE Transactions on Vehicular Technology, cilt. 67, no. 6, s. 5486-5490, Haziran 2018, doi: 10.1109/TVT.2018.2813318.

7. M. S. J. Solaija, H. Salman ve H. Arslan, “Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks,” in IEEE Open Journal of Vehicular Technology, cilt. 3, s. 321-343, 2022, doi: 10.1109/OJVT.2022.3183218.

8. Q. Xu, P. Ren, Q. Du ve L. Sun, “Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission,” in IEEE Transactions on Vehicular Technology, cilt. 67, no. 6, s. 5486-5490, Haziran 2018, doi: 10.1109/TVT.2018.2813318.

9. Solaija, M. S. J., Salman, H., & Arslan, H. (2021). Enhancing Channel Shortening Based Physical Layer Security Using Coordinated Multipoint. arXiv preprint arXiv:2109.14346.

10. H. M. Furqan, J. M. Hamamreh ve H. Arslan, “Enhancing physical layer security of OFDM systems using channel shortening,” 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292335.

11. M. Bouanen, F. Gagnon, G. Kaddoum, D. Couillard ve C. Thibeault, “An LPI design for secure OFDM systems,” MILCOM 2012 - 2012 IEEE Military Communications Conference, Orlando, FL, ABD, 2012, s. 1-6, doi: 10.1109/MILCOM.2012.6415833.

12. H. Wei, B. Zheng ve X. Hou, “Compressive channel sensing based on random pilot for physical layer communication security,” 2013 22nd Wireless and Optical Communication Conference, Chongqing, China, 2013, s. 693-698, doi: 10.1109/WOCC.2013.6676463.

13. M. Soltani, T. Baykaş ve H. Arslan, “Achieving secure communication through pilot manipulation,” 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hong Kong, Çin, 2015, s. 527-531, doi: 10.1109/PIMRC.2015.7343356.

14. M. Sakai, H. Lin ve K. Yamashita, “Intrinsic Interference Based Physical Layer Encryption for OFDM/OQAM,” in IEEE Communications Letters, cilt. 21, no. 5, s. 1059-1062, Mayıs 2017, doi: 10.1109/LCOMM.2017.2654442.

15. H. Qin vd., “Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs,” in IEEE Transactions on Wireless Communications, cilt. 12, no. 6, s. 2717-2729, Haziran 2013, doi: 10.1109/TCOMM.2013.050713.120730.

16. T. Akitaya, S. Asano ve T. Saba, “Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems,” 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, NSW, Avustralya, 2014, s. 807-812, doi: 10.1109/ICCW.2014.6881299.

17. Yuan Wu ve Boon Poh Ng, “Speech scrambling with Hadamard transform in frequency domain,” 6th International Conference on Signal Processing, 2012., Beijing, Çin, 2012, s. 1560-1563 cilt.2, doi: 10.1109/ICOSP.2012.1180094.

18. D. C. Tseng ve J. H. Chiu, “An OFDM speech scrambler without residual intelligibility,” TENCON 2017 - 2017 IEEE Region 10 Conference, Taipei, Tayvan, 2017, s. 1-4, doi: 10.1109/TENCON.2017.4428903.

BULUŞUN KISA AÇIKLAMASI

Mevcut buluş, yukarıda belirtilen dezavantajları ortadan kaldıracak ve ilgili teknik alana yeni avantajlar getirecek bir yöntemle ilgilidir.

Buluşun amacı, Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Bütünleşik Algılama ve İletişim (ISAC) sistemlerinde hedef kullanıcının alıcı performansını ve algılayıcı kullanıcının

algılama performansını korurken, dahili gizli dinleyicilerin ve harici gizli dinleyicilerin bir baz istasyonundan bir hedef kullanıcıya yapılan iletimin verilerini sızdırmasını önlemektir.

Buluşun bir diğer amacı da düşük değişkenlikteki kanal koşullarında bile gizli dinlemeye karşı koruma sağlamaktır.

Yukarıda belirtilen ve aşağıdaki detaylı açıklamadan ortaya çıkacak olan tüm amaçlara ulaşmak için, mevcut buluş en az bir baz istasyonu ve en az bir kullanıcı ekipmanı içeren Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Entegre Algılama ve İletişim (ISAC) sistemi tarafından gerçekleştirilen bir yöntemle ilgilidir. Buna göre şu adımları içermektedir; baz istasyonu ve kullanıcı ekipmanı arasında kanal incelemesinin gerçekleştirilmesi; bir kanal uyuşmazlığı tespit edilirse, baz istasyonu ve kullanıcı ekipmanı arasında mutabakatın gerçekleştirilmesi; baz istasyonu ve kullanıcı ekipmanı arasında bir kanalın belirlenmesi; baz istasyonu tarafından, GAN modelinin girilen bir kanaldan düşman kanallar üretmek üzere yapılandırıldığı önceden eğitilmiş bir üretken düşman ağ (GAN) modeline erişilmesi, burada GAN modeli hem baz istasyonunda hem de kullanıcı ekipmanında depolanmaktadır; baz istasyonu tarafından, belirlenen kanalın GAN modeline ve GAN modelinden gelen düşman kanallara girilmesi; düşman kanallara dayanarak dizilerin üretilmesi; iletilecek bir mesajın OFDM sembollerinin sırasının üretilen dizilere göre düzenlenmesi; baz istasyonu tarafından, düzenlenmiş OFDM sembollerinin kullanıcı ekipmanına iletilmesi; kullanıcı ekipmanı tarafından OFDM sembollerinin alınması; kullanıcı ekipmanı tarafından, belirlenen kanalın GAN modeline girilmesi ve düşman kanalların elde edilmesi; düşman kanallara dayanarak dizilerin üretilmesi; mesajı elde etmek için üretilen dizilere dayanarak OFDM sembollerinin yeniden düzenlenmesi. Böylece kanal tabanlı fiziksel katman güvenliğine dayanan sistemler için çok önemli olan düşük entropili kanallardan yüksek entropili kanalların üretilmesini sağlamaktadır.

Buluşun olası bir yapılandırması, kanalı GAN modeline girmeden önce baz istasyonu tarafından belirlenen kanala dayanarak GAN modelinin en az bir ağırlığının güncellenmesi; kanalı GAN modeline girmeden önce kullanıcı ekipmanı tarafından belirlenen kanala dayanarak GAN modelinin en az bir ağırlığının güncellenmesi ile karakterize edilmektedir. Bu entropiyi daha da arttırmaktadır.

ŞEKİLLERİN KISA AÇIKLAMASI

Şekil 1, sistemin üst şematik görünümünü gösteren bir çizimdir.

Şekil 2, yöntemin akış şemasını gösteren bir çizimdir.

Şekil 3, bir baz istasyonunun bileşenlerini ve sistemdeki kullanıcı ekipmanını gösteren bir çizimdir.

ŞEKİLDE VERİLEN REFERANS NUMARALARI

100 Baz istasyonu
201 Kullanıcı ekipmanı
202 Algılama kullanıcı ekipmanı
203 Gizli dinleyici kullanıcı ekipmanı

211 Paralelden seriye dönüştürme birimi
212 Seriden paralele dönüştürme birimi
213 FFT birimi
214 IFFT birimi
215 Demodülatör
216 Modülatör
217 Karıştırıcı
218 Çözücü
219 CP toplayıcı
220 CP giderici
221 Yukarı dönüştürme birimi
222 Aşağı dönüştürme birimi

BULUŞUN AYRINTILI AÇIKLAMASI

Bu ayrıntılı açıklamada konu, herhangi bir kısıtlayıcı etki oluşturmadan sadece konunun daha anlaşılır olması amacıyla örneklere atıfta bulunularak açıklanmıştır.

Buluş, Dikey Frekans Bölmeli Çoğullama (OFDM) tabanlı Bütünleşik Algılama ve İletişim (ISAC) sisteminin fiziksel katman güvenliğini arttırmak için bir yöntemdir.

Şekil 1'e atıfta bulunarak, sistem en az bir baz istasyonu (100) ve OFDM kullanarak iletişim kurabilen en az bir kullanıcı ekipmanı (201) içermektedir. Yöntem, algılayıcı kullanıcı ekipmanının (202) veya gizli dinleyici kullanıcı ekipmanının (203) kullanıcı ekipmanına (201) gönderilen verilere gizli dinleme yapmasını önlemeyi amaçlamaktadır. Bu, geleneksel fiziksel katman güvenlik yönteminde olduğu gibi doğrudan incelenmiş kanal kullanmak yerine, baz istasyonu (100) ve kullanıcı ekipmanı (201) arasındaki kanalı kullanarak birden çok yüksek entropili düşman kanal dizileri üreten Generative Adversarial Network (GAN) modeli kullanılarak OFDM sembollerinin yeniden düzenlenmesi ile gerçekleştirilmektedir.

Söz konusu yöntem, ISAC sisteminin baz istasyonu (100) ve kullanıcı ekipmanı (201) tarafından gerçekleştirilmektedir. Şekil 2'ye atıfta bulunarak, yöntem aşağıdaki adımları içermektedir:

Baz istasyonu (100) ve kullanıcı ekipmanı (201) kanal incelemesi gerçekleştirmektedir. Kullanıcı ekipmanı (201) ve baz istasyonu (100) benzer bir kanal gözlemlemektedir. Ancak zamanlama uyumsuzluğu nedeniyle hafif kanal farklılıkları ortaya çıkabilmektedir ve bu da bir dereceye kadar kanal uyumsuzluğuna neden olmaktadır.

Baz istasyonu (100) ve kullanıcı ekipmanı (201) bir kanal uyuşmazlığı tespit edildiğinde mutabakat gerçekleştirmektedir. Mutabakat teknikte iyi bilinmektedir ve bir kablosuz ağdaki iki varlık arasındaki iletişim veya operasyonel parametrelerdeki herhangi bir uyuşmazlığı hizalama veya çözme sürecini ifade etmektedir.

Baz istasyonu (100) ve kullanıcı ekipmanı (201) aralarında bir kanal belirlemektedir.

Baz istasyonu (100), girilen bir kanaldan düşman kanallar üretmek üzere yapılandırılmış, önceden eğitilmiş bir üretken düşman ağ (GAN) modeline erişmektedir. GAN modeli hem baz istasyonunda (100) hem de kullanıcı ekipmanında (201) depolanmaktadır. Böylece her ikisi de iletişimi güvence altına almak için aynı düşman kanalları üretmek için kullanmaktadır.

Baz istasyonu (100) belirlenen kanalı GAN modeline girmektedir ve GAN modelinden düşman kanallara dayalı diziler üretmektedir.

Baz istasyonu (100) gönderilecek bir mesajın OFDM sembollerinin sırasını oluşturulan dizilere göre düzenlemektedir. Daha sonra baz istasyonu (100) düzenlenmiş OFDM sembollerini kullanıcı ekipmanına (201) iletmektedir.

Kullanıcı ekipmanı (201) OFDM sembollerini almaktadır. Belirlenen kanalı GAN modeline girer ve düşman kanalları elde etmektedir. Kullanıcı ekipmanı (201) daha sonra düşman kanallara dayalı diziler üretmektedir. Kullanıcı ekipmanı (201) mesajı elde etmek için üretilen dizilere dayanarak OFDM sembollerini yeniden düzenlemektedir. Böylece gizli dinleyici kullanıcı ekipmanı (203) ve algılayıcı kullanıcı ekipmanı (202) iletimdeki verileri eşitleyemez ve sızdıramaz.

İkinci bir yapılandırmada, baz istasyonu (100) ve kullanıcı ekipmanı (201) belirlenen kanala dayanarak GAN modelinin ağırlıklarını güncellemektedir. Bu, iletişim için dinleyiciler tarafından kolayca kopyalanamayan benzersiz bir GAN modeline sahip olmalarını sağlamaktadır.

GAN modelleri teknikte iyi bilinmektedir. Generative Adversarial Networks (GAN'lar), sentetik veri üretmek veya mevcut veri kümelerini arttırmak için tasarlanmış bir derin sinir ağları sınıfıdır. Birbiriyle yarışan iki sinir ağından oluşurlar: bir Üreteç ve bir Ayrıştırıcı [Z. Pan, W. Yu, X. Yi, A. Khan, F. Yuan ve Y. Zheng, "Recent Progress on Generative Adversarial Networks (GANs): A Survey," IEEE Access, cilt. 7, s. 36322-36333, 2019, doi: 10.1109/ACCESS.2019.2905015.], [A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta ve A. A. Bharath, "Generative Adversarial Networks: An Overview," IEEE Signal Processing Magazine, cilt. 35, no. 1, s. 53-65, Ocak 2018, doi: 10.1109/MSP.2017.2765202.]. Üretecin rolü yeni veri örnekleri oluşturmaktır, Ayrıştırıcı ise bu örnekleri değerlendirerek 'gerçek' (orijinal eğitim verilerinden) veya 'sahte' (Üreteç tarafından oluşturulan) olup olmadıklarını belirlemektedir.

Üreteç, Ayrıştırıcıyı kandırmak için yeterince eğitildikten sonra, bir GAN gerçekçi sentetik veriler üretebilmektedir. GAN'ların temel bir özelliği doğaları gereği deterministik olmalarıdır; eğitildikten sonra sinir ağı katmanlarının ağırlıkları ve önyargıları

sabitlenmektedir. Bu, eğitilmiş bir GAN'a aynı girdinin sağlanmasının sürekli olarak aynı çıktıyı vereceği anlamına gelmektedir. Birden fazla GAN, tek bir girdiden çeşitli sentetik çıktılar üretmek için aynı anda eğitilebilmektedir ve bu da çeşitli veri üretimine olanak tanımaktadır. Böylece bir baz istasyonu (100) ve bir kullanıcı ekipmanı (201) aynı kanalı GAN'a girdiklerinde aynı düşman kanal çıktılarını alırlar.

GAN modelleri önceden eğitilmiştir. Ağ, GAN'ları eğitmek için farklı kullanıcıların faaliyetlerinden işlediği kanal setlerini kullanabilmektedir. Simülasyonlarda kanal veri kümesi, ortamın yayılma özelliklerine ve zenginliğine karşılık gelen belirli kanal modelleri veya dağılımları kullanılarak oluşturulabilmektedir.

GAN'ların eğitim sürecinde, mevcut veri kümesi birden fazla eğitim alt kümesine bölünmektedir. Eğitim alt kümelerinin sayısı, ihtiyaç duyulan düşman kanalların sayısına karşılık gelmektedir. GAN'ların aynı giriş düşük entropili kanaldan farklı yüksek entropili düşman kanallar üretmesini sağlayarak düşman kanal zenginliğini ve çeşitliliğini garanti etmek için, giriş kanalından farklı özellikleri ayıklayan farklı filtrelerin belirlenmesi ve uygulanması gerekmektedir.

GAN'lar deterministik sinir ağları olduğu için, eğitildikten sonra sinir ağı katmanlarının ağırlıkları ve önyargıları sabitlenmektedir. Ağ eğitilmiş ağırlıkları saklayabilmektedir ve bunları kullanıcı ekipmanı (201) ve baz istasyonları (100) ile paylaşabilmektedir. Farklı kullanıcıların farklı kanalları gözlemleyeceği düşünüldüğünde, belirli kullanıcı kanalı gözlem geçmişine dayanarak GAN'ların yeniden eğitilmesine gerek kalmadan tüm kullanıcılar aynı ağırlıklara sahip olabilmektedir. Kritik uygulamalarda, kullanıcıların farklı ağırlıklara sahip olması gerekebilmektedir, böylece kanallar bir zaman anında benzer veya ilişkili olsa bile, farklı ağırlıklara sahip olmak farklı düşman kanallarla sonuçlanacaktır.

Bu amaçla, sınırlı miktardaki kullanıcı kanalı geçmişiyle tüm GAN yapısını yeniden eğitmek yerine, genel eğitimden elde edilen ağırlıklar kullanıcının veri kümesine dayanarak güncellenebilmektedir. Ağırlıkları güncellemek için kullanılan kullanıcı kanalı veri kümesi tamamen aynı olmalıdır, yani ağ ve ilgili kullanıcı arasındaki farklı mutabakat süreçlerinden ayıklanırlar. Ağın ve kullanıcının uzlaştırılmış kanal veri setine sahip olduğu varsayıldığında, ağ ve belirli kullanıcı, ikinci yapılandırmada olduğu gibi GAN'ları aynı ağırlıklara doğru güncellemektedir.

Yalnızca jeneratörün ağırlıkları aktarılıp güncellendiğinden, her bir kullanıcı ekipmanında (201) ve baz istasyonunda (100) ihtiyaç duyulan depolama alanı önemli ölçüde azaltılmaktadır.

Şekil 1'de pilotlar iki amaç için kullanılmaktadır: geleneksel iletişim veya veri iletimi sırasında algılama ve kanal tahmini. Baz istasyonu (100) OFDM kullanarak kablosuz bir kanal üzerinden kullanıcı ekipmanı (201) ile veri alışverişi yapmaktadır. Kanal tahmini için kullanılan pilotlara, meşru bir algılama/yer belirleme kullanıcısı veya cihazı olan algılayıcı kullanıcı ekipmanı (202) tarafından da erişilebilmektedir. Doğru algılama/yer belirleme işlevselliğini sağlamak için baz istasyonu (100) pilotları gizleyemez, böylece baz istasyonunun (100) algılayıcı kullanıcı ekipmanının (202) eşitlemesini ve iletilen verilerin yeniden yapılandırılmasını engellemesini önlemektedir. Baz istasyonu (100) tarafından iletilen sinyali alan herhangi bir kullanıcı, verileri ayıklamak için çözme işlemi gerçekleştirmelidir. Çözme dizisi, karıştırma dizisine karşılık gelmektedir ancak ters işlemde kullanılmaktadır. Bu senaryoda, baz istasyonu (100) ve kullanıcı ekipmanı (201) inceleme ve mutabakat işlemi sırasında aynı kanalı gözlemlediği için, her ikisi de önerilen yöntemleri kullanarak aynı dizileri üretecektir. Baz istasyonu (100) veriyi karıştırırken kullanıcı ekipmanı (201) veriyi çözecektir. Ancak algılayıcı kullanıcı ekipmanı (202) da GAN'ların ağırlıklarına sahip olduğu ve önerilen yöntemleri uygulayabildiği için diziyi üretmeye çalışacaktır. Bununla birlikte, farklı bir kanalı gözlemlediği için, dizileri baz istasyonu (100) ve kullanıcı ekipmanının (201) dizilerinden farklı olacak ve dizileri kırmadığı sürece verileri düzgün bir şekilde çözmesini engelleyecektir. Farklı OFDM sembolleri farklı dizilerle karıştırıldığı için, algılayıcı kullanıcı ekipmanının (202) birden fazla diziyi kırması gerekmektedir ve bu da veri yeniden yapılandırma görevini karmaşıklaştırmaktadır.

Algılayıcı kullanıcı ekipmanı (202) ile karşılaştırıldığında, gizli dinleyici kullanıcı ekipmanı (203) sistem tarafından tanınmaz ve hem iletişim hem de algılama işlevleri için yetkili değildir. Karıştırma mekanizması iletişim verilerini bu gizli dinleyici kullanıcı ekipmanından (203) korumaktadır. Ancak gizli dinleyici kullanıcı ekipmanı (203) pilotların ve konumlarının farkında olduğu için yine de algılama yapabilmektedir.

Bu durumda, biri veri için diğeri pilotlar için olmak üzere iki karıştırma dizisi oluşturma süreci kullanılabilmektedir. İkinci işlem esas olarak pilot sinyallerini ağ içindeki yetkisiz

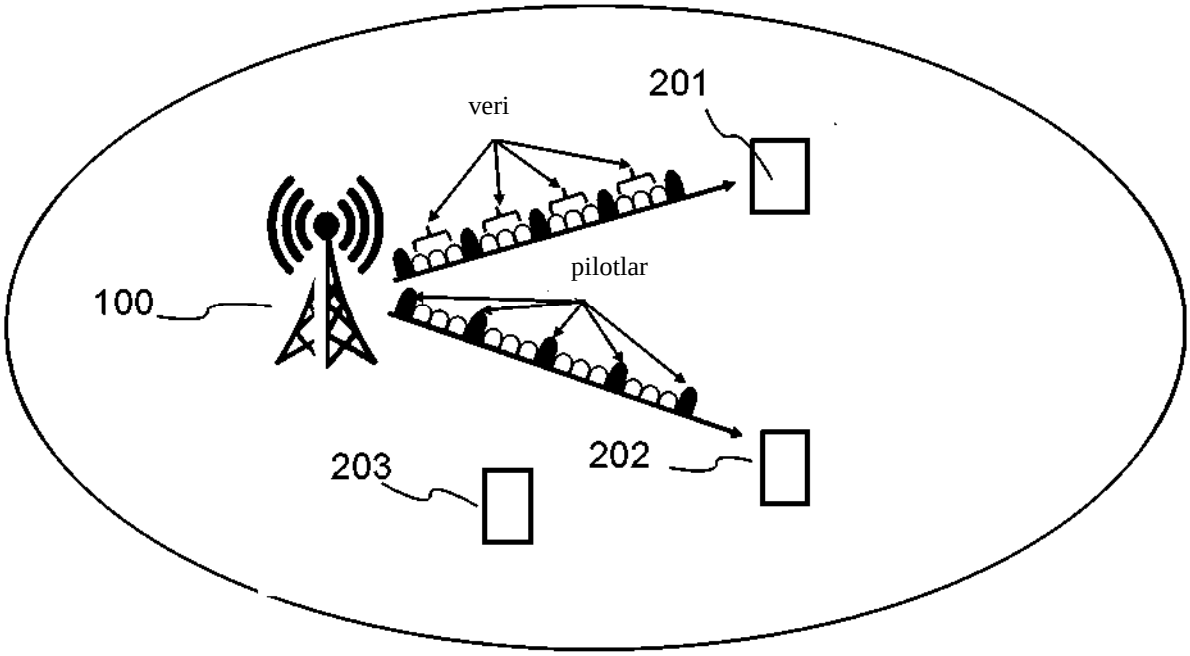
kullanıcılardan gizlemek içindir. Burada ağ (baz istasyonu (100)) kullanıcılar arasında bireysel kanalların bölümlerini paylaşarak tüm yetkili kullanıcıların aynı bilgilere erişmesini sağlamaktadır. Bu, Fiziksel Katman Güvenliğindeki (PLS) grup anahtarı oluşturma konseptiyle uyumludur. Paylaşılan kanal bilgileri daha sonra pilot karıştırma dizileri oluşturmak için kullanılabilmektedir. Sonuç olarak, ortak kanal bilgisine erişimi olan tüm kullanıcılar, aynı pilot konumları üretmek için önerilen Üretken Çekişmeli Ağlar (GAN'lar) destekli yöntemlerden faydalanabilmektedir. 'İletişim Verilerinin Güvenliğinin Sağlanması' ile ilgili önceki bölümde sunulan tüm karıştırma dizisi oluşturma süreçleri ve kullanımı aynı kalmaktadır. Aradaki fark, ortak pilot karıştırma dizileri üretmek için ortak bilgi girmemiz gerektiğidir. Harici dinleyiciler bu ortak bilgiye sahip olmadıklarından, GAN'ları konuşlandırmış olsalar bile pilot konum dizilerini oluşturamayacaklardır.

Şekil 3'e atıfta bulunarak örnek bir baz istasyonu (100), gelen seri veri akışlarını işlenmek üzere paralel veri akışlarına dönüştürmek için bir seriden paralele dönüştürme birimi (212), bilgileri kodlamak için verileri belirli modülasyon şemalarına eşlemek için bir modülatör (216), belirlenen dizilere dayanarak OFDM sembollerini yeniden düzenleyen bir karıştırıcı (217), OFDM dalga formları oluşturmak için frekans alanı verilerini zaman alanı sinyallerine dönüştürmek için bir IFFT (Ters Hızlı Fourier Dönüşümü) birimi (214), paralel işlenmiş verileri iletim için tekrar seri formata dönüştürmek üzere bir paralelden seriye dönüştürme birimi (211), semboller arası girişimi (ISI) azaltmak ve sağlam iletişim sağlamak üzere bir döngüsel önek eklemek için bir CP (Döngüsel Önek) toplayıcı (219) ve temel bant sinyalini kablosuz ortam üzerinden iletime uygun daha yüksek bir frekansa dönüştürmek için bir yukarı dönüştürme birimini (221) içerebilmektedir.

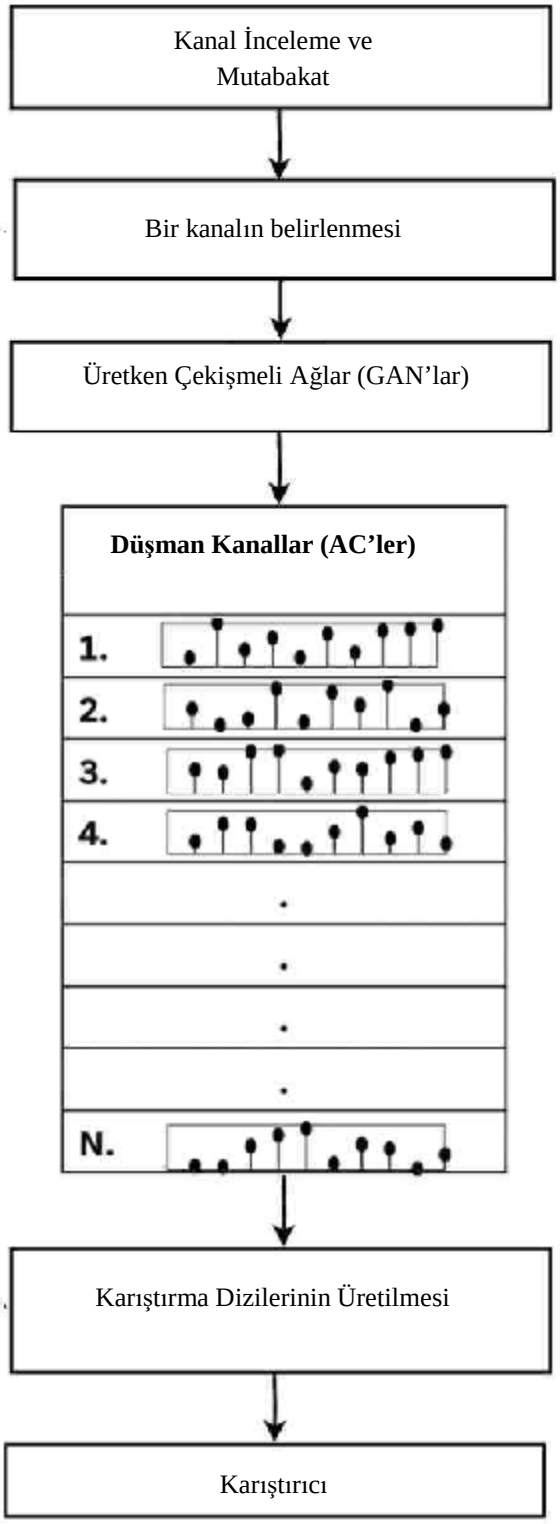
Örnek bir kullanıcı ekipmanı (201), gelen paralel veri akışlarını daha sonraki işlemler için seri formata dönüştürmek üzere bir paralelden seriye dönüştürme birimi (211), modülasyon işlemini tersine çevirerek alınan sinyalden kodlanmış bilgileri çıkarmak için bir demodülatör (215), belirlenen dizileri kullanarak karıştırma işlemini tersine çevirerek orijinal veri modellerini geri yüklemek için bir çözücü (218), OFDM sembol tespitini kolaylaştırmak amacıyla zaman alanı sinyallerini frekans alanı verilerine dönüştürmek için bir FFT (Hızlı Fourier Dönüşümü) birimi (213), işlenmiş seri verileri ek işlem için paralel akışlara dönüştürmek için bir seriden paralele dönüştürme birimi (212), orijinal veri çerçevesini geri yüklemek için alınan sinyalden döngüsel ön eki ortadan kaldırmak için bir CP (Döngüsel Ön

Ek) giderici (220) ve yüksek frekanslı alınan sinyali temel bant işlemeye uygun daha düşük bir frekansa çevirmek için bir aşağı dönüştürme birimini (222) içerebilmektedir.

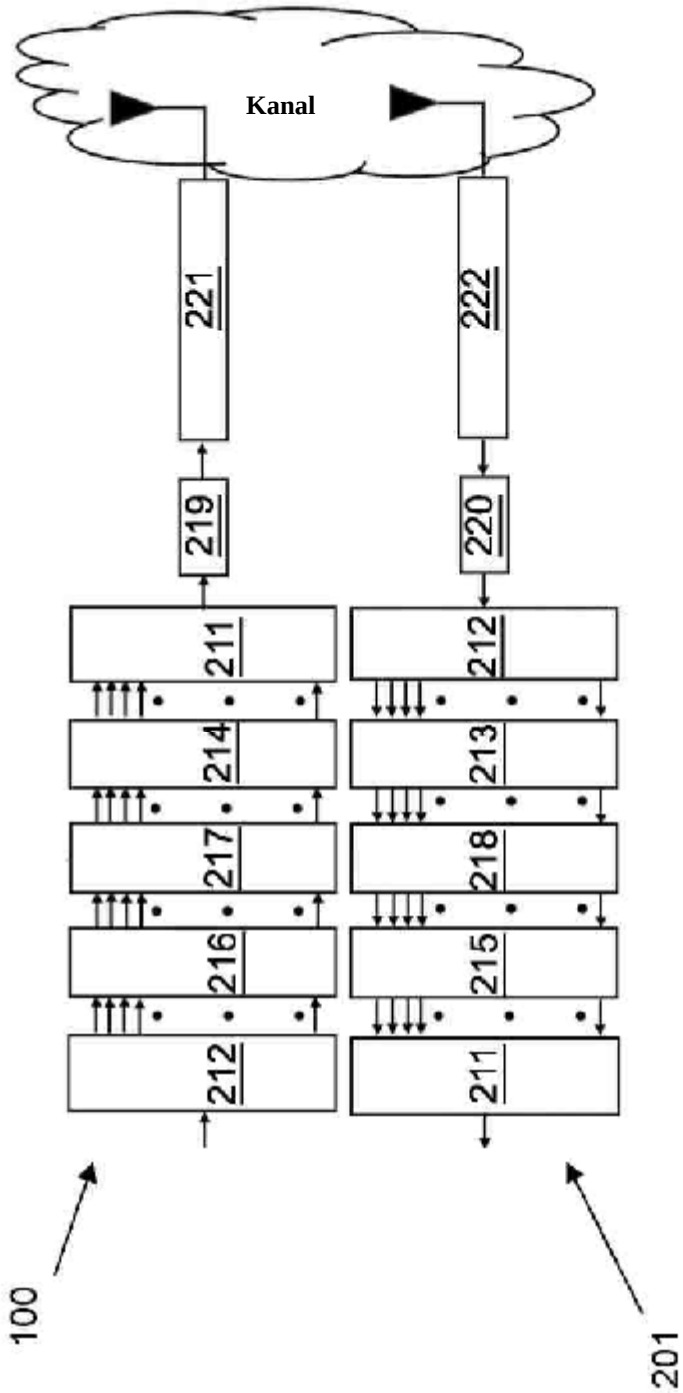
Buluşun koruma kapsamı ekli istemlerde belirtilmiştir ve bu ayrıntılı açıklamada örnekleme amacıyla açıklananlarla sınırlandırılamaz. Teknikte uzman bir kişinin, buluşun ana temasından uzaklaşmaksızın yukarıda belirtilen gerçekler ışığında benzer yapılandırmalar sergileyebileceği açıktır.



ŞEKİL 1


Kanal İnceleme ve
Mutabakat
Bir kanalın belirlenmesi
Üretken Çekişmeli Ağlar (GAN'lar)
Düşman Kanallar (AC'ler)
1.
2.
3.
4.
N.
Karıştırma Dizilerinin Üretilmesi
Karıştırıcı

ŞEKİL 2


Kanal
221
222
219
220
211
212
214
213
217
218
216
215
212
211
100
201

ŞEKİL 3