ÖZET

GİZLİ DİNLEME SALDIRILARINA KARŞI KABLOSUZ İLETİŞİMİ KORUMAYA YÖNELİK BİR YÖNTEM

Mevcut buluş, kablosuz iletişim sinyallerinin kötü niyetli gizli dinleyiciler tarafından duyulmasını/engellenmesini önlemeye yönelik bir yöntem sağlamaktadır. Yöntem üç ana adıma sahiptir: iletişiminin korunacağı bir kullanıcıya yönelik koordinasyon TP'lerinin seçilmesi (110), daha önce bahsedilen kullanıcıya iletilecek verilerin N parçaya ayrılması, burada N, kullanılan TP sayısıdır ve gecikme yayılmasının koruma süresinden daha az olmasını sağlama almak için iletilen sinyalin kanala dayalı manipülasyonudur.

İSTEMLER

1. Kablosuz iletişim sinyallerinin kötü niyetli gizli dinleyiciler tarafından duyulmasını/engellenmesini korumaya yönelik bir yöntem olup, özelliği; aşağıdakileri içermesidir:

- iletişimin korunacağı bir cihaza (420) yönelik koordinasyon TP'lerinin seçilmesi (110),
- cihaza (420) iletilecek verilerin koordinasyon TP'leri arasında N parçaya ayrılması, burada N, kullanılan koordineli TP'lerin sayısıdır,
- gecikme yayılımının koruma süresinden az olmasını sağlama almak için iletilen sinyalin kanala dayalı manipülasyonunun uygulanması (130).

2. İstem 1'e göre yöntem olup, özelliği; koordinasyon TP'lerinin seçiminin (110), alınan sinyal gücü belirtecine, sinyal-parazit artı gürültü oranına ve/veya mesafeye dayanmasıdır.

3. İstem 1'e göre yöntem olup, özelliği; kanalı bir manipülasyon tekniğinden geçirerek kanalın gecikme yayılımını kısaltmak için kanala dayalı manipülasyon olarak kanal kısaltmanın kullanılmasıdır.

4. İstem 1'e göre yöntem olup, özelliği; iletişimi sağlama alınacak cihazın (420) gecikme yayılımının koruma süresinden daha az olmasını sağlama almak için kanala dayalı manipülasyon olarak uyarlanabilir korumanın kullanılmasıdır.

TARİFNAME

GİZLİ DİNLEME SALDIRILARINA KARŞI KABLOSUZ İLETİŞİMİ KORUMAYA YÖNELİK BİR YÖNTEM

Teknik Alan

Mevcut buluş, kablosuz iletişim sinyallerinin kötü niyetli gizli dinleyiciler tarafından duyulmasını/engellenmesini önlemeye yönelik bir yöntemdir.

Önceki Teknik

Kablosuz iletişimin yayın niteliği, bunu çeşitli güvenlik tehditlerine açık hale getirmektedir. Bu tehditlerden biri, aynı zamanda gizli dinleme olarak da anılan, iletişim gizliliğinin ihlalidir. Bu durumda, bir kötü niyetli düğüm/cihaz, iki meşru düğüm arasında gerçekleşen iletişimi bölmeyi ve yorumlamayı denemektedir. Geleneksel olarak, kriptografiye dayalı teknikler gibi güvenlik teknikleri, güvenli iletim için kullanılmaktadır. Fakat, bu tür güvenlik teknikleri gelecekteki (5G ve ötesi) merkezi olmayan ve heterojen ağlar için, anahtar yönetimi ve paylaşma mekanizmalarının [1] karmaşıklığından dolayı yeterli olmayabilir.

Fiziksel katman güvenliği (PLS) mekanizmaları son yıllarda gittikçe daha popüler hale gelmiştir. Aşağıdaki yaklaşımlar OFDM gibi çoklu taşıyıcı sistemlerindeki PLS için kullanılmaktadır:

Kablosuz Kanallardan Gizli Sekansların Çıkarılması: Bu tür PLS tekniklerindeki temel fikir, kablosuz kanaldan [2] rastgele sekans çıkarılmasıdır. CN105847629A numaralı başvuru, şifrelenmiş görüntünün bir tersinir bilgi saklama yöntemini açıklamaktadır. Yöntem bir şifreleme anahtarına göre orijinal bir düz metin görüntüsünün şifrelenmesi, bir bilgi gizleme anahtarına göre şifrelenmiş görüntüye gizli bilgilerin gömülmesi, şifreleme anahtarına göre gizli bilgiler dahil olmak üzere şifrelenmiş görüntünün şifresinin çözülmesi ve düz metin görüntüsünün geri kazanılması ve gizli bilgilerin bir gizli sırra göre çıkarılması adımlarını içermektedir. Fakat, anahtar oluşturma yaklaşımı, hatalı kanal tahmini ve kanal karşılıklılık uyumsuzluğuna karşı çok hassastır.

İletilen Sinyaller ile birlikte Parazit (Parazit/Sıkışma) Yapan Sinyallerin Eklenmesi: Bu yaklaşımda, meşru düğüm, meşru alıcıdaki performansı etkilemeksizin, meşru olmayan alıcıda performansı düşürecek şekilde meşru kullanıcının kanalının boş alanını kullanarak kasıtlı bir müdahale sinyali eklemektedir. Ancak, bir miktar güç ve verimi [3] feda edebilmektedir.

Kanala Dayalı Adaptasyon İletimi: Adaptasyona dayalı güvenlik teknikleri aynı zamanda, örneğin, Otomatik Tekrar İsteği (ARQ) ile adaptif modülasyon ve kodlama [4], solma kaynaklı alt taşıyıcı aktivasyon tekniği [5], optimum güç tahsisine dayalı teknikler [6], kanal kısaltma [7] ve PLS'yi geliştirmek için OFDM-alt taşıyıcı indeksi seçimi [8] gibi yalnızca yasal alıcının Hizmet Kalitesi (QoS) gereksinimlerini karşılamak için verici parametrelerinin kanal koşullarına göre ayarlandığı çok popüler PLS teknikleridir. Gizlice dinleyen kişi TP'ye daha yakınsa ve meşru düğümden daha iyi kanal deneyimliyorsa, gizlice dinlemeye karşı korumaya yönelik kanal kısaltma yaklaşımı [7], başarısız olmaktadır. Diğer bir yandan, koordineli çoklu noktalı konsept [9], herhangi bir kanala dayalı manipülasyon kullanmadan sadece meşru düğüm için alınan gücü iyileştirmeye odaklanmaktadır.

Bununla birlikte, kanal adaptasyonuna dayalı mevcut PLS mekanizmaları, gizli dinleyicinin kanalı meşru düğüme kıyasla daha iyi olduğunda gizli dinleme saldırılarına karşı koruma sağlayamamaktadır. Koordineli çok noktalı konsept kullanılarak veriler birden çok parçaya ayrılabilmektedir ve farklı bağlantılar üzerinden gönderilebilmektedir. Bu şekilde, gizli dinleyici koordineli iletim noktalarından (TP'ler) birine daha yakın olsa bile, verilerin diğer bölümlerini temiz bir şekilde almakta zorlanacaktır. Gizli dinleyiciye yönelik bu sorun, kanala dayalı adaptasyon tekniklerinin (örneğin kanal kısaltma veya uyarlamalı koruma bandı kullanımı) kullanılmasıyla daha da şiddetlenmektedir, öyle ki, gizli dinleyicinin deneyimlediği kanal dürtü yanıtı veya gecikme yayılımı (τ_{maks}), veri ayrıklarından en az biri için koruma süresinden (T_g) daha büyüktür ve bu da semboller arası girişime yol açmaktadır.

Kısa Açıklama

Bu buluş, ortogonal frekans bölmeli çoğullamaya (OFDM) dayalı iletişimi gizli dinleme saldırılarına karşı korumak için bir koordineli çok noktalı iletim mekanizması sağlamaktadır. Önerilen mekanizma üç ayrı bölüme sahiptir:

- İletişiminin korunacağı bir kullanıcıya yönelik koordinasyon aktarım noktalarının seçilmesi,
- Daha önce bahsedilen kullanıcıya iletilecek verilerin N parçaya ayrılması, burada N kullanılan koordineli TP'lerin sayısıdır.
- Meşru düğümde alınan sinyalin gecikme yayılımına sahip olmasını sağlama almak için iletilen sinyalin kanala dayalı manipülasyonu, τ_{maks} koruma süresinden daha azdır, yani $\tau_{maks} \leq T_g$ aynı şey, meşru olmayan düğüm, yani gizli dinleyici için geçerli değildir. Sonuç olarak, gizlice dinleyicide alınan sinyal, performansını düşüren semboller arası parazite (ISI) sahiptir.

Koordineli çok noktalı sistemler, geleneksel olarak, farklı TP'lerin koordinasyonundan yararlanılması vasıtasıyla iletişimin güvenilirliğini, özellikle de hücresel kullanıcı deneyimini geliştirmek için kullanılmaktadır. Öte yandan önerilen buluş, güvenli ve gizli iletişim sağlamak için coğrafi olarak dağıtılmış birden fazla TP'nin mevcudiyetini kullanmaktadır. Bu, bu verilerin farklı parçalara bölünmesi ve ayrı TP'lerden gönderilmesiyle elde edilmektedir. Ayrıca, deneyimlediği gecikme yayılımının kullanılan korumadan daha az olmasını sağlama almak için meşru alıcının deneyimlediği kanala dayalı olarak bazı manipülasyonlar gerçekleştirilmektedir. Ancak bu, gizli dinleyiciler için geçerli değildir ve ISI'yi deneyimlemektedir.

Önerilen yöntem, kriptografik yaklaşımdan ziyade gelecekteki kablosuz ağlarda kullanılabilecek düşük karmaşıklıklı (alıcı için) bir yöntem sağlamaktadır. Ayrıca, ağların yoğunlaştırılması koordineli ağların kullanımına izin vermektedir. Önerilen yöntem aynı zamanda, fiziksel katman güvenliğinin mevcut kanala dayalı adaptasyon yöntemlerinin ana sınırlamasını, yani, gizli dinleyicinin kanalı yasal kullanıcıdan daha iyi ise başarısızlıklarını da ele almaktadır.

Şekillerin Kısa Açıklaması

Şekil 1 mevcut açıklamanın belirli yönlerine göre temel işlemlerin bir akış şemasıdır.
Şekil 2 veri bölme işlemini göstermektedir; burada ayrık (1), ayrık (2) ve ayrık (N), birinci, ikinci ve N'inci veri ayrılmasını göstermektedir.
Şekil 3 kanala dayalı manipülasyon işlemini göstermektedir.
Şekil4 mevcut açıklamanın belirli yönlerine göre ayırma ve kanala dayalı manipülasyona sahip koordineli bir ağ örneğidir.

Parça Referansları

110. Koordinasyon TP'lerinin seçilmesi
120. İletilen verilerin koordinasyon TP'leri arasında bölünmesi
130. Kanala dayalı manipülasyonun uygulanması
210. Orijinal veri
221. Ayrık 1
222. Ayrık 2
223. Ayrık N
310. Orijinal kanalın (1) yayılmasının gecikmesi
311. Orijinal kanalın (2) yayılmasının gecikmesi
320. Kanala dayalı manipülasyon aşaması (kanal kısaltma tekniği)
321. Kanala dayalı manipülasyon aşaması (T_g'ın ayarlanması)
330. Deneyimli kanalın (1) yayılmasında gecikme
331. Deneyimli kanalın (2) yayılmasında gecikme
411. TP 1
412. TP N
420. Cihaz
430. Saldırgan
440. Birleştirilmiş ayrıklar
450. Semboller arası müdahaleden muzdarip birleşik ayrıklar

N: N kullanılan koordineli TP'lerin sayısı
T_g: Koruma süresi

Ayrıntılı Açıklama

Önerilen buluş, bir kablosuz iletişim sisteminde, gizlice dinleyen saldırganlara karşı güvenlik sağlamak için, koordine edilmiş çok noktalı ağlar tarafından sunulan, coğrafi olarak dağıtılmış TP'leri (ve bunun sonucu olan farklı gecikme yayılımlarını) kullanmaktadır.

Şekil 1, mevcut açıklamanın belirli yönlerine uygun olarak kablosuz iletişim için temel işlemlerin bir akış diyagramıdır. Şekil 2 ve Şekil 3, iletilen verilerin koordinasyon TP'leri

arasında bölünmesi (120) adımı ve kanala dayalı manipülasyonun uygulanması (130) adımının resimleridir.

Koordinasyon TP'lerinin seçilmesi (110) adımı, iletişimi güvence altına alınacak cihaz (420) için koordinasyon TP'lerinin seçimini sunmaktadır. Seçim prosesi, alınan sinyal gücü belirtecine (RSSI), sinyal-parazit artı gürültü oranına (SINR) ve/veya mesafeye dayalı olabilmektedir.

İletilen verilerin koordinasyon TP'leri arasında bölünmesi (120) adımı veri ayırma prosesini belgelemektedir. Cihaza (420) gönderilecek olan orijinal veriler (210), N parçaya ayrılmıştır, burada, N kullanılan koordinasyon TP sayısıdır. Şekil 2'de gösterildiği gibi, tüm yarık parçalarının kombinasyonu orijinal veriyi (210) sağlamalıdır.

Kanala dayalı manipülasyonun uygulanması (130) adımı, iletilen ayrığın kanala dayalı bir manipülasyon prosesini sunmaktadır. Kanala dayalı manipülasyon prosesi, gecikme yayılımının $(\tau_{maks)}$ koruma süresinden daha az, yani $\tau_{maks} \leq T_g$, olduğunu sağlama almaktadır. Şekil 3'te gösterildiği gibi, orijinal kanalın (1) yayılmasının gecikmesi (310) $\tau_{maks} > T_g$ denklemine sahip olması durumunda, saptama prosesi etkilenmektedir ve bu performans bozulmasına yol açmaktadır. Bununla başa çıkmak için kanal, " kanala dayalı manipülasyon aşaması (kanal kısaltma tekniği) (320) aşamasından geçirilmektedir, kanal $\tau_{maks} \leq T_g$ olacak şekilde manipüle edilmektedir. Deneyimli kanalın (1) yayılmasında gecikme (330) daha iyi bir saptama süreci sağlamaktadır. Ayrıca, orijinal kanalın (2) yayılmasının gecikmesi (311) $T_g > \tau_{maks}$'a sahiptir ve bu da spektral verimin düşmesine yol açmaktadır. Bununla başa çıkmak için kanal, kanala dayalı manipülasyon aşaması (T_g'ın ayarlanması) (321) aşamasından geçirilmektedir, burada T_g, $\tau_{maks} \leq T_g$ olacak şekilde minimum değere ayarlanmaktadır. Deneyimli kanal, amaçlanan alıcının spektral verimliliği için optimize edilmiştir.

Kanala dayalı manipülasyonun uygulanması (130) prosesi, kanalı bir manipülasyon tekniğinden geçirerek kanalın gecikme yayılmasını kısaltmak için kullanılabilmektedir. Kanala dayalı manipülasyonun uygulanması (130) prosesi, cihaz (420) konumuna göre izin verilen minimum koruma süresini (T_g) seçmektedir.

Şekil 4, mevcut açıklamanın belirli yönlerine göre iletilen verilerin koordinasyon TP'leri arasında bölünmesi (120) ve kanala dayalı manipülasyonun uygulanması (130)

prosesine sahip koordineli bir ağ örneğidir. TP 1'den (411) TP N'ye (412) kadar olan TP'ler (birinci ve N'inci koordineli TP'ler), cihazla (420) iletişimi saldırgana (430) karşı güvence altına almak için koordine edilmektedir. İletişim düğümleri tek/çoklu antenlerle donatılabilmektedir.

N-koordinasyon TP'leri, orijinal verileri (210), TP 1 (411) ayrık 1 (221) iletmektedir ve TP N (412), ayrığı N (223) iletmektedir ve benzeri gibi N-ayrıklara bölmektedir.

N-koordinasyon TP'leri, cihazda (420) alınan tüm koordinasyon TP'lerinden alınan ayrıkların koruma süresinden daha az gecikme yayılımı deneyimlemesini sağlama almak için kanala dayalı manipülasyonun uygulanması (130) prosesi uygulamaktadır. Sonuç olarak, bir cihazdaki (420) birleştirilmiş ayrıklar (440) doğru bir şekilde deşifre edilebilmektedir. Ancak, birleştirilmiş ayrıkların (440) performansını düşüren se semboller arası müdahaleden muzdarip birleşik ayrıklar (450) için durum böyle değildir.

Herhangi bir kablosuz iletişim teknolojisi, bu buluşu gizli dinleyicilere karşı koruma sağlamak için kullanabilmektedir. Bununla birlikte, 3GPP'ye dayalı hücresel ve IEEE 802.11'e dayalı Wi-Fi ağları gibi standartlar, her iki standartta [10, 11] sağlanan çok noktalı koordinasyon desteği nedeniyle özellikle buluşla ilgilidir. Ayrıca, açıklanan yöntem, yukarıda belirtilen standartlar kod bölümlü çoklu erişim (CMDA), frekans bölümlü çoklu erişim (FDMA), Mobil iletişim için Küresel Sistem (GSM), GSM/Genel Paket Radyo Hizmeti (GPRS), Gelişmiş Veri GSM Ortamı (EDGE), Geniş Bant-CDMA (W-CDMA), İyileştirilmiş Evrim Verileri (EV-DO), Yüksek Hızlı Paket Erişimi (HSPA), Yüksek Hızlı Aşağı Bağlantı Paket Erişimi (HSDPA), Yüksek Hızlı Yukarı Bağlantı Paket Erişimi (HSUPA), Gelişmiş Yüksek Hızlı Paket Erişimi (HSPA +), Uzun Süreli Evrim (LTE), Kablosuz, hücresel veya nesnelerin interneti (IoT) ağı içinde iletişim kurmak için kullanılan AMPS, 5G Yeni Radyo (NR) veya diğer bilinen sinyallerinden herhangi birini destekleyebilen herhangi bir cihaz, sistem veya ağ üzerinde uygulanabilmektedir.

Referanslar

[1] Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2018). Classificationsandapplications of physicallayersecuritytechniquesforconfidentiality: A comprehensivesurvey. IEEE Communications Surveys&Tutorials, 21(2), 1773-1828.

[2] Wang, Q., Su, H., Ren, K., & Kim, K. (2011, April). Fastandscalablesecretkeygenerationexploitingchannelphaserandomness in wirelessnetworks. In2011 Proceedings IEEE INFOCOM (pp. 1422-1430). IEEE.

[3] Qin, H., Sun, Y., Chang, T. H., Chen, X., Chi, C. Y., Zhao, M., &Wang, J. (2013). Powerallocationand time-domain artificialnoisedesignforwiretap OFDM withdiscreteinputs. IEEE Transactions on Wireless Communications, 12(6), 2717-2729.

[4] Hamamreh, J. M., Yusuf, M., Baykas, T., & Arslan, H. (2016, April). Cross MAC/PHY layersecuritydesignusing ARQ with MRC andadaptivemodulation. In2016 IEEE Wireless Communications and Networking Conference (pp. 1-7). IEEE.

[5] Güvenkaya, E., & Arslan, H. (2014, June). Securecommunication in frequencyselectivechannelswithfade-avoidingsubchannelusage. In2014 IEEE International Conference on Communications Workshops (ICC) (pp. 813-818). IEEE.

[6] Ng, D. W. K., Lo, E. S., &Schober, R. (2012). Energy-efficientresourceallocationforsecure OFDMA systems. IEEE Transactions on VehicularTechnology, 61(6), 2572-2585.

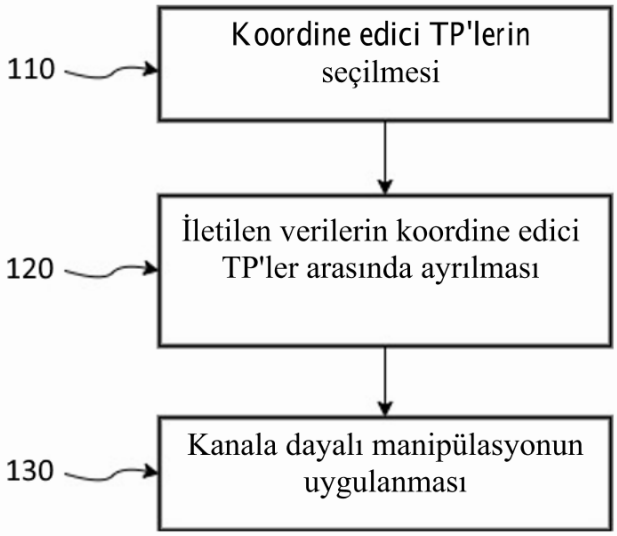
[7] Furqan, H. M., Hamamreh, J. M., & Arslan, H. (2017, October). Enhancingphysicallayersecurity of OFDM systemsusingchannelshortening. In2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE.

[8] Hamamreh, J. M., Basar, E., & Arslan, H. (2017). OFDM-subcarrierindexselectionforenhancingsecurityandreliability of 5G URLLC services. IEEE Access, 5, 25863-25875.

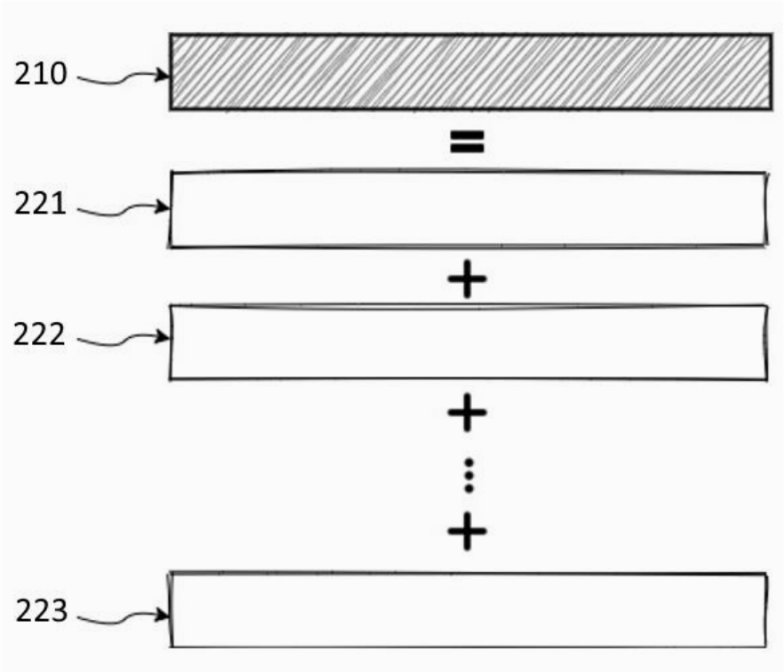
[9] Ozmat, U., Demirkol, M. F., &Yazici, M. A. (2020, September). Service-BasedCoverageforPhysicalLayer Security with Multi-Point CoordinatedBeamforming. In2020 IEEE 25th International Workshop on ComputerAidedModelingand Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

[10] 3rd GenerationPartnership Project (3GPP), “Coordinated Multi-pointOperationfor LTE PhysicalLayerAspects (Rel-11),” Technical Report 36.819, ver 11.2.0, Sept. 2013.

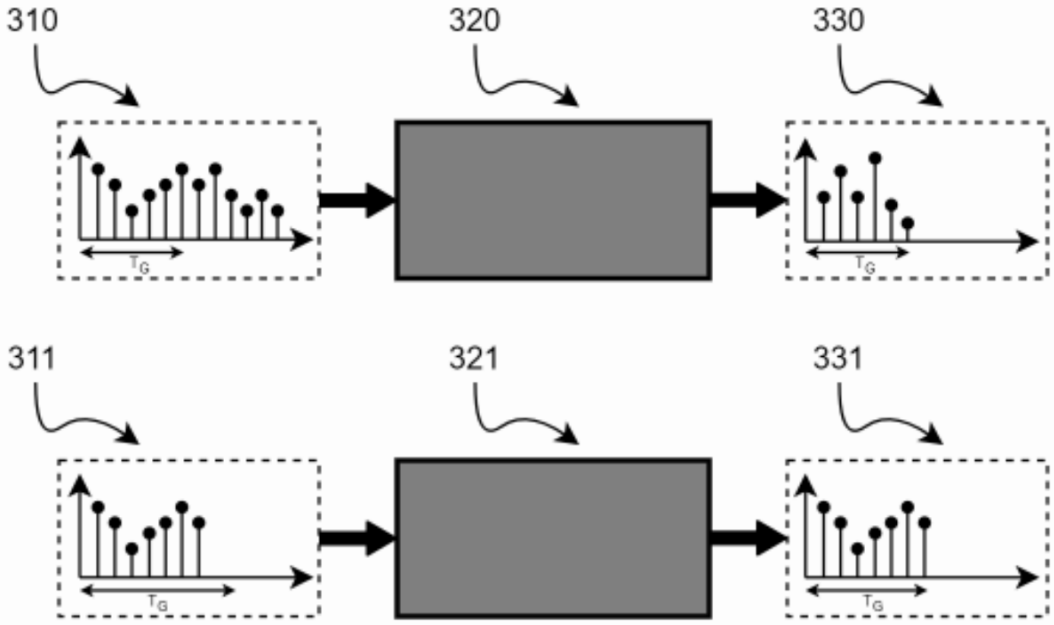
[11] LaurentCariou (Intel). EHT Proposed PAR, IEEE 802.11-18/1231r6, March 2019.



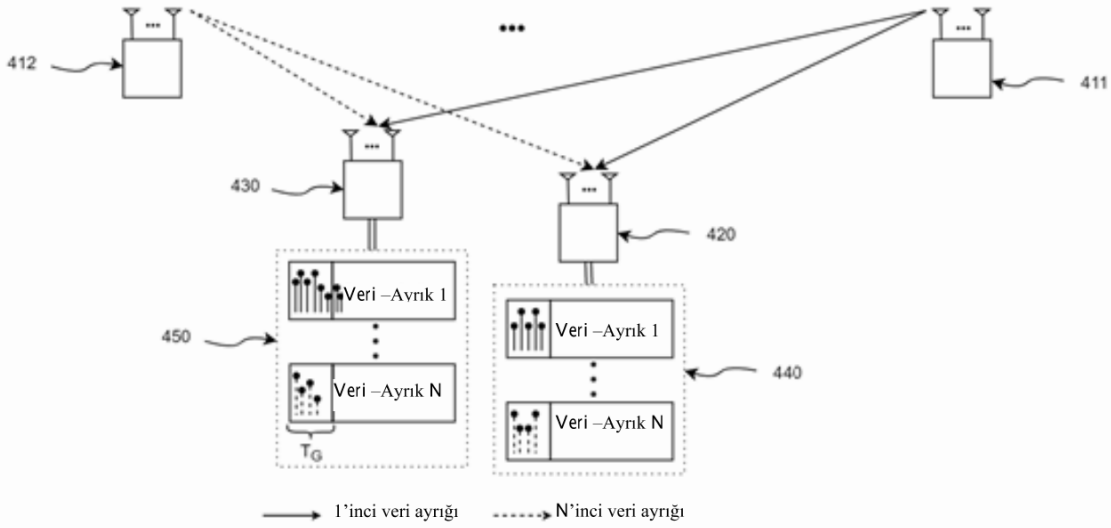
Şekil 1



Şekil 2



Şekil 3


412
411
430
420
450
440
Veri –Ayrık 1
Veri –Ayrık N
Veri –Ayrık 1
Veri –Ayrık N
T_G
1'inci veri ayrığı
N'inci veri ayrığı

Şekil 4