TARİFNAME

YASAL DÜĞÜMLERİN KANAL DURUM BİLGİSİ ÜZERİNDEKİ GİZLİCE GÖZETLEME SALDIRILARINA KARŞI KORUMAYA YÖNELİK KOORDİNELİ ÇOK NOKTALI ŞEMA

Teknik Alan

Fiziksel katman (PHY)-güvenliği, klasik şifreleme tekniklerini tamamlayabilen ve kablosuz iletişim ağlarının genel güvenliğini geliştirebilen ümit verici ve güçlü bir kavram olarak ortaya çıkmıştır. PHY-güvenliği teknikleri, yarı-dalga boyu mesafeleri boyunca ilintisizleştirildiği ve saldıran kişi tarafından tahmin edilememesi durumuna dayalı olarak kanal durum bilgisini (CSI) gözlemlemekte ve kullanmaktadır. Dolayısıyla CSI, şifreler oluşturmak, paket kaynağını doğrulamak, uyum tabanlı güvenlik teknikleri sağlamak ve dinleyen kişileri engellemek için yapay gürültü eklemek üzere kullanılmıştır. Ancak, saldıran bir kişi bir çok kullanıcılı çok antenli sistemde CSI sonucuna ulaşabilmektedir. Böylece CSI'nın fiziksel katman güvenliğini artırmaya yönelik bir araç olarak kullanımının yeniden düşünülmesine yol açılmaktadır. Bu buluşta, yasal düğümlerde performansı bozmadan Eve'de CSI sızmasını en aza indirmeye yönelik yeni bir ön kodlama yöntemi sağlanmaktadır. Özellikle bu buluş, yasal düğümlerin CSI'sını, saldıran kişi tarafından ön kodlayıcı matriksler kullanılarak elde edilmeye karşı korumak üzere bir koordineli çok noktalı iletim mekanizması sağlamaktadır.

Önceki Teknik

Kablosuz iletişimin yayımlama yapısı bunu çeşitli güvenlik tehditlerine eğilimli hale getirmektedir. Bu amaçla, kanal durum bilgisi (CSI), yarı-dalga boyu mesafeleri boyunca ilintisizleştirildiği ve zengin saçılma ortamlarında verici ve alıcının konumlarına dayalı olarak tahmin edilememesi nedeniyle bir verici ile bir alıcı arasında paylaşılan bir giz olarak işlev göstererek fiziksel katman güvenliğini artırmak üzere öne sürülmüştür. Dolayısıyla CSI, şifreler oluşturmak, paket kaynağını doğrulamak, uyum tabanlı güvenlik teknikleri sağlamak ve dinleyen kişileri engellemek için yapay gürültü eklemek üzere kullanılmıştır. Ancak, 2019'da yayımlanan, Zhang, X. ve Knightly, E.W.'ya ait bir yayın olan *IEEE/ACM Transactions on Networking* içinde yazarlar, bir CSIsnoop kavramını sunmakta ve saldıran bir

kişinin, bir çok kullanıcılı çok girişli çok çıkışlı (MIMO) MIMO kablosuz yerel alan ağında (WLAN) CSI sonucuna ulaşabileceğini göstermektedir. Böylece çok kullanıcılı MIMO WLAN'larda CSI'nın fiziksel katman güvenliğini artırmaya yönelik bir araç olarak kullanımının yeniden düşünülmesine yol açılmaktadır.

Bugüne kadar, mevcut sorunu gidermek için sunulan bir çözüm, bir ön kodlayıcı tasarlamaktır, ancak sunulan tasarım ayrıca yasal düğümlerin performansını etkilemektedir. Örneğin, CSI'nın bir saldıran kişide elde edilen orijinal CSI ile ilişkisinin %80'den az olmasını sağlamak amacıyla, yöntemleri, yasal düğümde bit hata oranını (BER) 0.25'e kadar azaltmaktır.

Buluşun Amacı

Sunulan yöntem, yasal düğümlerin performansını bozmadan bir kablosuz iletişim sisteminde yasal düğümler ile ilgili CSI gizlice gözetlemesine karşı güvenlik sağlamak üzere koordineli çok noktalı ağların sunduğu coğrafi olarak dağıtık iletim noktalarını geliştirmektir.

Mevcut mekanizmalar, yasal düğümlerin performansını bozmadan bu tür saldırılara karşı koruma sağlamada başarısız olmaktadır. Özellikle, bu tür saldırıyı gideren başlıca bir çalışma vardır, ancak sunulan yöntem ayrıca yasal düğüm performansını bozmaktadır.

Dolayısıyla buluşun bir amacı, yasal düğümlerin performansını bozmadan veya yasal düğümlerin performansında minimum bozulma ile kablosuz iletişim sistemlerinde yasal düğümler ile ilgili CSI gizlice gözetlemesine karşı güvenlik sağlamaya yönelik bir yöntem sunmaktır.

Buluşun Kısa Açıklaması

Mevcut buluş, yasal düğümlerin CSI'sını, saldıran kişi tarafından ön kodlayıcı matriksler kullanılarak elde edilmeye karşı korumak üzere bir koordineli çok noktalı iletim mekanizması aracılığıyla yasal düğümlerde performansı bozmadan kanal durum bilgisi (CSI) sızmasını en aza indirmeye yönelik bir yöntem ile ilgilidir.

Diğer bir yönde mevcut buluş, yasal düğümlerde performansı bozmadan kanal durum bilgisi

(CSI) sızmasını en aza indirmeye yönelik bir yöntem ile ilgilidir, burada söz konusu yöntem aşağıdaki adımları içermektedir

i. Kanal tahmini ve
ii. Ön kodlama,

Burada ön kodlama adımında, ilk olarak, alınan sinyal gücü göstergesi (RSSI), sinyalin girişime ve gürültüye oranı ve/veya mesafeye dayalı olarak tüm kullanıcılar için koordine edici erişim noktaları (AP'ler) seçilmektedir ve daha sonra CoMP yapısı birlikte, ortaya çıkan ön kodlayıcının, kullanıcılar arası girişimi gidereceği, kanal etkisini gidereceği ve saldıran kişi tarafından CSI gizlice gözetlemesine karşı koruma sağlayacağı şekilde ön kodlayıcı tasarımında kasıtlı hataya neden olma ile birlikte kanala dayalı olarak özel ön kodlayıcı tasarlamaktadır.

Burada, kanal tahminine yönelik olarak; yukarı bağlantı sondajı kullanılmaktadır, burada her bir kullanıcı, erişim noktalarının (AP'ler) ilgili CSI'yı ölçeceği şekilde sondaj dizileri iletmektedir. Bu konfigürasyonda herhangi bir erişim noktası tarafından yayımlanan herhangi bir sondaj dizisi veya yasal tek antenli düğüm (Bob) tarafından gönderilen CSI ölçüm geri bildirimi yoktur.

Buluşun tercih edilen bir yapılandırmasında, yukarıda açıklanan kanal tahmin yöntemi, birden fazla çok antenli erişim noktası (AP'ler), tek antenli istemciler ve çok antenli bir dinleyen kişiden oluşan çok kullanıcılı koordineli çok noktaya (CoMP) dayalı olarak bir modele uygulanabilmektedir.

Yukarıda açıklandığı üzere, mevcut buluşa göre yöntemin bir açısı, ön kodlama adımıdır. Saldıran kişi tarafından yasal düğümler ile ilgili CSI gizlice gözetlenmesine karşı koruma sağlamak amacıyla, ön kodlama adımında yeni birleşik ön kodlayıcı ile birlikte CoMP yapısı kullanılmaktadır.

Ön kodlama adımı, iki alt adımdan, diğer bir deyişle (a) tüm kullanıcılar için koordine edici AP'lerin seçilmesi ve (b) CoMP yapısı aracılığıyla ön kodlayıcı tasarımında kasıtlı hataya neden olma ile birlikte kanala dayalı olarak özel ön kodlayıcı tasarlanmasını içermektedir.

Bu AP'ler, birleşik işlemeyi kolaylaştırmak üzere iletişim kurabilecekleri bir ana taşıyıcı bağlantı üzerinden bağlanmaktadır. Farklı erişim noktaları, çok kullanıcılı birleşik hüzme

oluşturmayı gerçekleştirmekte ve K farklı tek antenli istemcileri eş zamanlı iletebilmektedir. Dinleyen kişinin, aşağı bağlantı iletimi sırasında gönderilen farklı kontrol sinyallerini kullanarak tahmin edilebilen AP'lerden kanalını bildiği varsayılmaktadır.

Buluşun diğer bir yapılandırmasında, mevcut buluşa göre algoritma veya yöntem ayrıca, birden fazla AP'ye sahip olmak yerine, kullanıcı sayısı ile karşılaştırıldığında çok yüksek bir yoğunlukta dağıtık antenlerden oluşan yalnızca bir dağıtık anten yapısı olması halinde uygulanabilmektedir.

Bu buluşta genellikle "Eve", saldıran kişiye veya diğer bir deyişle dinleyen kişiye refere etmektedir; "Alice", erişim noktasına(noktalarına) refere etmektedir ve Bob, yasal bir tek antenli düğüme refere etmektedir. Bu tarifnamede tüm terimler ve refere ettikleri unsurlar birbirinin yerine geçecek şekilde kullanılabilmektedir.

Şekillerin Açıklaması

Şekil 1: Çok antenli erişim noktaları, tek antenli ve çok antenli Dinleyen Kişiden oluşan temel sistem modeli

AP 1: Çok Antenli Erişim Noktası 1

AP 2: Çok Antenli Erişim Noktası 2

AP T: Çok Antenli Erişim Noktası T

B-1: Tek Anten 1

B-2: Tek Anten 2

B-K: Tek Anten K

E: Çok Antenli Dinleyen Kişi

Buluşun Ayrıntılı Açıklaması

Bir yönde mevcut buluş, yasal düğümlerde performansı bozmadan kanal durum bilgisi (CSI) sızmasını en aza indirmeye yönelik bir yöntem ile ilgilidir, burada söz konusu yöntem aşağıdaki adımları içermektedir

i. Kanal tahmini ve
ii. Ön kodlama,

Ön kodlama adımında, ilk olarak alınan sinyal gücü göstergesi (RSSI), sinyalin girişime ve gürültüye oranı ve/veya mesafeye dayalı olarak tüm kullanıcılar için koordine edici erişim noktalarının (AP'ler) seçilmesi ve daha sonra ikinci olarak CoMP yapısının birlikte, ortaya çıkan ön kodlayıcının, kullanıcılar arası girişimi gidereceği, kanal etkisini gidereceği ve saldıran kişi tarafından CSI gizlice gözetlemesine karşı koruma sağlayacağı şekilde ön kodlayıcı tasarımında kasıtlı hataya neden olma ile birlikte kanala dayalı olarak özel ön kodlayıcıyı tasarlaması ile karakterize edilmektedir.

Bir açıda, CoMP yapısında yasal düğümde alınan sinyal aşağıdaki gibidir;

$$y_i = \sum_{t=1}^{t=T} \sqrt{p_{ti}}\, h_{ti}\, e_{ti} w_{ti}\, s_{ti} + \sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj}\, s_{tj} + \sum_{t=1}^{t=T} z_{ti},$$

burada temel kriter kullanıcılar arası girişimi $(\sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj} = 0)$ en aza indirmektedir ve kanal etkisini $(\sum_{t=1}^{t=T} \sqrt{p_{ti}}\, h_{ti}\, e_{ti} w_{ti} = 1)$ en aza indirmektedir.

Alternatif olarak, CoMP yapısında yasal düğümde alınan sinyal için denklem aşağıdaki gibi yeniden yazılabilmektedir;

$$Y = \sum_{t=1}^{t=T} Y_t = \sum_{t=1}^{t=T} H_t W_t' P_t S + Z_t = \sum_{t=1}^{t=T} H_t E_t W_t P_t S + Z_t$$

Burada, E_t'nin dahil edilmesi, birleşik tasarım nedeniyle yasal düğümün performansını etkilemeyecektir. Ancak, CSI gizlice gözetleme saldırısına karşı güvenlik sağlamaktadır.

Diğer bir yönde, dinleyen kişide alınan sinyal aşağıdaki ile gösterilmektedir;

$$Ye = \sum_{t=1}^{t=T} Y_{te} = H_{te} W_t' P_t S + Z_{te}$$

$(H_{te} W_t' P_t = H_{te} E_t W_t P_t)$ 'ye E_t'nin dahil edilmesi nedeniyle, saldıran kişi, ön kodlayıcının doğru tasarımını elde edemeyecektir ve böylece yasal düğümler ile ilgili CSI'yı gizlice gözetleyemeyecektir. Ayrıca, sunulan algoritma aynı zamanda klasik ön kodlayıcı ile karşılaştırıldığında veri içeriğinin güvenliğini artıracaktır.

Örnekler

Örnek 1:

Sistemimiz, Şekil 1'de gösterildiği üzere Alice 1, Alice 2,……, Alice T düğümleri gibi birden fazla çok antenli erişim noktası (AP'ler), her biri Bob olarak adlandırılan K tek antenli istemci ve bir çok antenli dinleyen kişiden (Eve) oluşan çok kullanıcılı koordineli çok noktaya (CoMP) dayalıdır. Bu AP'ler, birleşik işlemeyi kolaylaştırmak üzere iletişim kurabilecekleri bir ana taşıyıcı bağlantı üzerinden bağlanmaktadır. Farklı erişim noktaları, çok kullanıcılı birleşik hüzme oluşturmayı gerçekleştirmekte ve K farklı Bob'ları eş zamanlı iletebilmektedir. Eve'in, aşağı bağlantı iletimi sırasında gönderilen farklı kontrol sinyallerini kullanarak tahmin edilebilen AP'lerden kanalını bildiği varsayılmaktadır. Sunulan algoritmanın ayrıca, birden fazla AP'ye sahip olmak yerine, kullanıcı sayısı ile karşılaştırıldığında çok yüksek bir yoğunlukta dağıtık antenlerden oluşan yalnızca bir dağıtık anten yapısı olması halinde uygulanabildiği anlaşılmalıdır.

Sunulan algoritmaların temel adımları aşağıdaki gibidir:

Adım 1: Kanal tahmini

Birinci adımda, yukarı bağlantı sondajı kullanılmaktadır, burada her bir kullanıcı (Bob), AP'lerin (Alice 1, Alice 2,……, Alice T) ilgili CSI'yı $(H_1, \ldots \ldots H_t \ldots . H_T)$ ölçeceği

şekilde sondaj dizilerini iletmektedir [3]. Bu konfigürasyonda herhangi bir erişim noktası tarafından yayımlanan herhangi bir sondaj dizisi veya Bob tarafından gönderilen CSI ölçüm geri bildirimi yoktur.

Adım 2: Ön kodlama

Burada, ilk olarak bir AP (Alice) olma durumu ve sonrasında saldıran bir kişinin CSI'yı nasıl gizlice gözetleyebileceğini açıklayacağız. Daha sonra, yasal düğümlerin (Bob) performansını bozmadan CSI güvenliğini artırabilen sunulan yöntemimizi açıklayacağız.

2.a. Klasik

Tek bir AP'den (Alice) oluşan klasik bir sistem durumunda, kanal tahmininden sonra Alice, kullanıcı düğümlerinde herhangi bir kullanıcılar arası girişim veya kanal etkisi olmayacağından emin olmak üzere aşağı bağlantı iletimine yönelik bir ön kodlayıcı tasarlayacaktır. ***i*** yasal düğümde bu tür ön kodlayıcı tasarımında alınan sinyal aşağıdaki gibi verilebilmektedir:

$$y_i = \sqrt{p_i}\, h_i w_i s_i + \sum_{j \neq i} \sqrt{p_j}\, h_i w_j s_j + z_i,$$

burada **p**, güç ölçeklendirme faktörüdür, **h**, aşağı bağlantı CSI'dır, **w**, hüzme oluşturma ağırlığıdır, **s**, iletilen sinyaldir ve **z**, gürültüyü temsil etmektedir ve karşılık gelen matriksler için **P, H, W, S** ve **Z** kullanılacaktır. Yukarıdaki denklemdeki birinci terim, istenen terim olurken ikinci terim, kullanıcılar arası girişimi göstermektedir.

Yukarıdaki denklem aşağıdaki gibi yeniden yazılabilmektedir

$$Y_b = H_t W_t P_t S + Z_t$$

Daha önce açıklandığı üzere ön kodlayıcı (W_t), herhangi bir kullanıcılar arası girişim olmaması ile birlikte yasal düğümde herhangi bir kanal etkisi olmayacağı bir şekilde tasarlanmaktadır. Bu tür ön kodlama ayrıca saldıran bir kişinin verileri dinleyemeyeceği

şekilde veri güvenliği sağlamaktadır. Özellikle kanal tabanlı ön kodlayıcı, girişime neden olarak saldıran kişide verilerin kodunu çözme kabiliyetini bozmaktadır. Ancak, bu ön kodlayıcı tasarımı, verinin güvende olmasına rağmen, ön kodlayıcının kendisinin saldıran kişiye yasal düğümlerin CSI'sını sızdırabilmesi nedeniyle risklidir. Bu sızdırma fiziksel katman güvenliği tekniklerinin başarısız olmasına yol açabilmektedir. Tek Alice kullanılarak klasik ön kodlayıcı ile Eve'de alınan sinyal aşağıdaki gibi verilebilmektedir

$$\boldsymbol{Y_e} = \boldsymbol{H_e W_t P_t S} + \boldsymbol{Z_t}.$$

Yukarıdaki denklemden, saldıran kişi, bilinen sinyal saldırısı aracılığıyla kanal tabanını öğrenebilmektedir. Varsayılan sistemimizde özellikle her bir paket, bir başlık ve veri kısmından oluşmaktadır, burada başlık kısmı, bilinen bilgidir. Bilinen sembolden, saldıran kişi CSI'yı gizlice gözetleyebilmektedir. İlk olarak saldıran kişi, aşağıdaki şekilde $\boldsymbol{W_E} = \boldsymbol{H_e W_t P_t}$'yi öğrenecektir

$$\boldsymbol{E\|e\| = E\{\|Y - W_E S\|\}}.$$

Daha sonra saldıran kişi, aşağıdaki gibi $\boldsymbol{W_E}$'den $\boldsymbol{W_t P}$'yi öğrenmek için $\boldsymbol{H_e}$ bilgisini kullanacaktır.

$$\boldsymbol{H_e W_t P = W_E}$$

Son olarak, $\boldsymbol{W_t P}$'den yasal düğüm kanal tabanını elde edebilmektedir, burada $\boldsymbol{W_t = H_t^{\dagger} = (H_t^H H_t)^{-1} H_t}$. Elde edilen bilgiden saldıran kişi, kablosuz kanallardan gizli dizilerin elde edilmesi ve iletilen sinyaller ile birlikte karıştırıcı (gürültü/bozucu) sinyallerin eklenmesi gibi farklı fiziksel katman güvenliği tekniklerine saldırabilmektedir.

2.b. Sunulan ön kodlama

Saldıran kişi tarafından yasal düğümler ile ilgili CSI'nın gizlice gözetlenmesine karşı koruma sağlamak amacıyla, yeni birleşik ön kodlayıcı ile birlikte CoMP yapısını sunduk.

Sunulan yapımızın iki adımı vardır.

Adım 1: Şekil 1'de gösterildiği üzere tüm kullanıcılar (Bob) için koordine edici AP'lerin seçilmesi. Seçim, alınan sinyal gücü göstergesi (RSSI), sinyalin girişime ve gürültüye oranı ve/veya mesafeye dayalı olabilmektedir.

Adım 2: Koordine edici AP'lerin seçilmesinden sonra, sunulan CoMP yapısı birlikte, ön kodlayıcı tasarımında kasıtlı hataya neden olma ile birlikte kanala dayalı olarak özel bir ön kodlayıcı tasarlamaktadır. Ortaya çıkan ön kodlayıcı, kullanıcılar arası girişimi giderebilmekte, kanal etkisini giderebilmekte, aynı zamanda saldıran kişi tarafından CSI-Gizlice gözetlemesine karşı koruma sağlayabilmektedir.

CoMP senaryosu durumu için yasal düğümde alınan sinyal aşağıdaki gibi verilebilmektedir

$$y_t = \sum_{t=1}^{t=T} \sqrt{p_{tt}}\, h_{tt}\, e_{tt} w_{tt}\, s_{tt} + \sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj}\, s_{tj} + \sum_{t=1}^{t=T} z_{ti},$$

burada temel kriter kullanıcılar arası girişimi $(\sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj} = 0)$ en aza indirmek ve kanal etkisini $(\sum_{t=1}^{t=T} \sqrt{p_{ti}}\, h_{ti}\, e_{ti} w_{ti} = 1)$ en aza indirmektir.

Yukarıdaki denklem aşağıdaki gibi yeniden yazılabilmektedir

$$Y = \sum_{t=1}^{t=T} Y_t = \sum_{t=1}^{t=T} H_t W_t' P_t S + Z_t = \sum_{t=1}^{t=T} H_t E_t W_t P_t S + Z_t$$

E_t'nin dahil edilmesi, birleşik tasarım nedeniyle yasal düğümün performansını etkilemeyecektir. Ancak, CSI gizlice gözetleme saldırısına karşı güvenlik sağlayabilmektedir.

Eve'de alınan sinyal aşağıdaki gibi verilebilmektedir

$$Ye = \sum_{t=1}^{t=T} Y_{te} = H_{te}W_t'P_tS + Z_{te}$$

$(H_{te}W_t'P_t = H_{te}E_tW_tP_t)$ 'ye E_t'nin dahil edilmesi nedeniyle, saldıran kişi, ön kodlayıcının doğru tasarımını elde edemeyecektir ve böylece yasal düğümler ile ilgili CSI'yı gizlice gözetleyemeyecektir. Ayrıca, sunulan algoritma aynı zamanda klasik ön kodlayıcı ile karşılaştırıldığında veri içeriğinin güvenliğini artıracaktır.

Buluşun Endüstriyel Uygulanabilirliği

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

Dinleyen kişilere karşı koruma sağlamak için bu buluşu herhangi bir kablosuz iletişim teknolojisi kullanabilmektedir. Ancak, her iki standartta sağlanan çoklu nokta koordinasyonu desteği nedeniyle 3GPP'ye dayalı hücresel ve IEEE 802.11'e dayalı Wi-Fi ağları gibi standartlar buluş ile özellikle ilgilidir. Ayrıca, bu tarifnamede açıklanan buluş yöntemi, söz konusu standartları destekleyebilen herhangi bir cihaz, sistem veya ağda uygulanabilmektedir.

Ayrıca hücresel iletişimin koordineli çoklu nokta konseptini izleyen IEEE 802.11 Tgbe'de (ayrıca Wi-Fi 7 olarak bilinmektedir) çok AP'li koordinasyonun standartlaştırılması ile birlikte, daha fazla incelenmesi beklenmektedir.

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

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

kriterlerinden ve tekniğin durumunu aşma kriterinden yoksun olduğu anlaşılırdır.

İSTEMLER

1. Kablosuz iletişim sinyallerinin kötü niyetli dinleyen kişiler tarafından gizlice dinlenmesine ve/veya dinlenmesine karşı korunmasına yönelik yasal düğümlerde performansı bozmadan kanal durum bilgisi (CSI) sızmasını en aza indirmeye yönelik bir yöntem olup, burada söz konusu yöntem aşağıdaki adımları içermektedir

- Kanal tahmini ve
- Ön kodlama,

ön kodlama adımında, ilk olarak alınan sinyal gücü göstergesi (RSSI), sinyalin girişime ve gürültüye oranı ve/veya mesafeye dayalı olarak tüm kullanıcılar için koordine edici erişim noktalarının (AP'ler) seçilmesi ve daha sonra ikinci olarak CoMP yapısının birlikte, ortaya çıkan ön kodlayıcının, kullanıcılar arası girişimi gidereceği, kanal etkisini gidereceği ve saldıran kişi tarafından CSI gizlice gözetlemesine karşı koruma sağlayacağı şekilde ön kodlayıcı tasarımında kasıtlı hataya neden olma ile birlikte kanala dayalı olarak özel ön kodlayıcıyı tasarlaması ile karakterize edilmektedir.

2. İstem 1'e göre bir yöntem olup, kanal tahminine yönelik olarak; yukarı bağlantı sondajı kullanılması ile karakterize edilmektedir, burada her bir kullanıcı, erişim noktalarının (AP'ler) ilgili CSI'yı ölçeceği şekilde sondaj dizileri iletmektedir.

3. Birden fazla çok antenli erişim noktası (AP'ler), tek antenli istemciler ve çok antenli bir dinleyen kişiden oluşan çok kullanıcılı koordineli çok noktayı (CoMP) içeren bir modelde kullanıma yönelik önceki istemlerden herhangi birine göre bir yöntem.

4. Önceki istemlerden herhangi birine göre bir yöntem olup, ön kodlama adımında, CoMP yapısında yasal düğümde alınan sinyalin aşağıdaki gibi olması ile karakterize edilmektedir;

$$y_i = \sum_{t=1}^{t=T} \sqrt{p_{ti}}\, h_{ti}\, e_{ti} w_{ti}\, s_{ti} + \sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj}\, s_{tj} + \sum_{t=1}^{t=T} z_{ti},$$

burada temel kriter kullanıcılar arası girişimi $(\sum_{t=1}^{t=T} \sum_{jt \neq ti} \sqrt{p_{tj}}\, h_{ti}\, e_{tj} w_{tj} = 0)$ en

aza indirmek ve kanal etkisini $(\sum_{t=1}^{t=T} \sqrt{p_{ti}}\, h_{ti}\, e_{ti} w_{ti} = 1)$ en aza indirmektedir.

5. İstem 4'e göre bir yöntem olup, CoMP yapısında yasal düğümde alınan sinyal için denklemin aşağıdaki gibi yeniden yazılabilmesi ile karakterize edilmektedir;

$$Y = \sum_{t=1}^{t=T} Y_t = \sum_{t=1}^{t=T} H_t W_t' P_t S + Z_t = \sum_{t=1}^{t=T} H_t E_t W_t P_t S + Z_t$$

Burada E_t'nin dahil edilmesi, birleşik tasarım nedeniyle yasal düğümün performansını etkilememektedir, ancak CSI gizlice gözetleme saldırısına karşı güvenlik sağlamaktadır.

6. Önceki istemlerden herhangi birine göre bir yöntem olup, dinleyen kişide alınan sinyalin aşağıdaki gibi olması ile karakterize edilmektedir

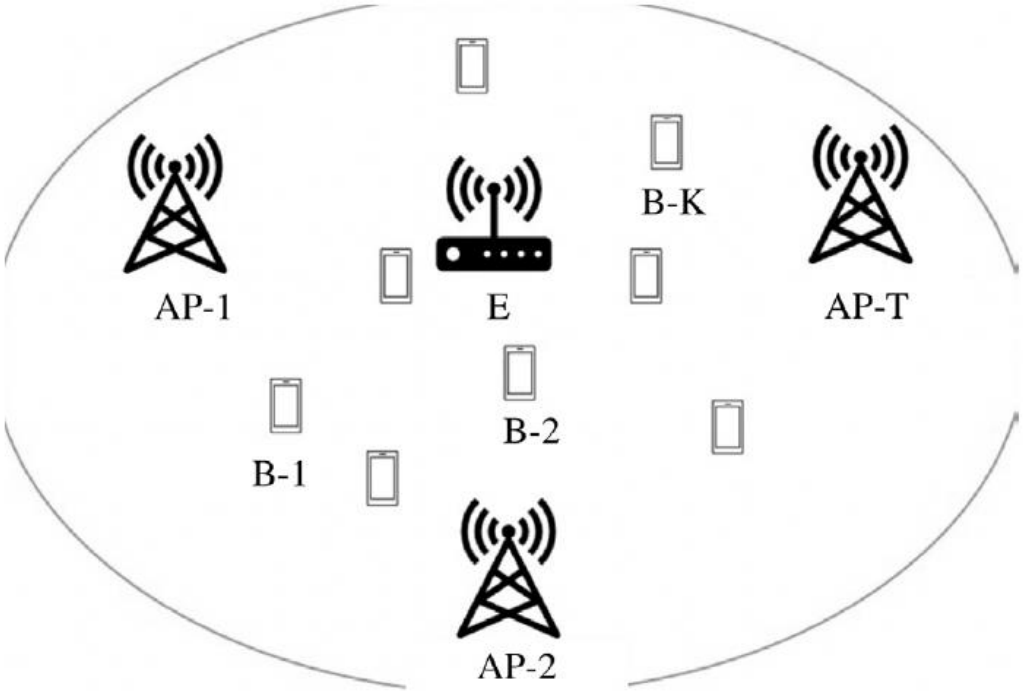
$$Ye = \sum_{t=1}^{t=T} Y_{te} = H_{te} W_t' P_t S + Z_{te}$$

burada $(H_{te} W_t' P_t = H_{te} E_t W_t P_t)$ 'ye E_t'nin dahil edilmesi, saldıran kişinin, ön kodlayıcının doğru tasarımını elde etmesini önlemekte ve yasal düğümler ile ilgili CSI'yı gizlice gözetlemeyi önlemektedir.

ÖZET

YASAL DÜĞÜMLERİN KANAL DURUM BİLGİSİ ÜZERİNDEKİ GİZLİCE GÖZETLEME SALDIRILARINA KARŞI KORUMAYA YÖNELİK KOORDİNELİ ÇOK NOKTALI ŞEMA

Yasal düğümlerde performansı bozmadan dinleyen kişide kanal durum bilgisinin (CSI) sızmasını en aza indirmeye yönelik yeni bir ön kodlama yöntemidir. Özellikle bu buluş, yasal düğümlerin CSI'sını, saldıran kişi tarafından ön kodlayıcı matriksler kullanılarak elde edilmeye karşı korumak üzere bir koordineli çok noktalı iletim mekanizması sağlamaktadır.



ŞEKİL 1