ÖZET

GELECEKTEKİ KABLOSUZ AĞLARA YÖNELİK KANAL AYRIŞTIRMA TABANLI UYARLAMALI FİZİKSEL KATMAN GÜVENLİĞİ

Bu buluşta, Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizma önerilmektedir.

İSTEMLER

1. Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizmanın bir operasyon yöntemi olup,

- kanalın minimum faz ve tam geçirgen bileşenlere ayrıştırılması ve
- kanalın bileşenlerinin, veri ve pilot güvenliğine yönelik algoritmayı tasarlamak üzere kullanılması adımlarını ve

veri güvenliği sürecine yönelik olarak

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\ H_{MIN}$);
- Verilerin (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpılması ve meşru alıcıya doğru iletilmesi,
- Sinyalin meşru alıcıda R olarak alınması,

Meşru alıcı tarafından verilerin kodunu çözmek üzere H_{MIN}'in denkleştirilmesi adımlarını içermesidir.

2. İstem 1'e göre yöntem olup, pilot güvenlik sürecine yönelik olarak aşağıdaki adımları içermektedir;

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\ H_{MIN}$);
- Pilot sinyalinin (P) kanalın tam geçirgen bileşeni ile $T_1 = H_{AP}\ P$ olarak çarpılması ve meşru verici tarafından meşru alıcıya doğru iletilmesi,
- Sinyalin meşru alıcıda $R_1 = H.H_{AP}\ P$ olarak alınması,
- Tahmin edilen kanalın tam geçirgen $(H_{APb})^2$ ve minimum faz (H_{MPb}) olarak ayrıştırılması,
- Kanalın meşru alıcıda $\widehat{H}_b = \sqrt{(H_{AP})^2} H_{MIN}$ olarak tahmin edilmesi.

3. İstem 1'e göre yöntem olup, **birlikte pilot ve veri güvenliği sürecine** yönelik olarak aşağıdaki adımları içermektedir;

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\, H_{MIN}$);
- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\, H_{MIN}$);
- Sinyalin meşru alıcıda $R_1 = H.H_{AP}\, P$ olarak alınması,
- Tahmin edilen kanalın tam geçirgen $(H_{APb})^2$ ve minimum faz (H_{MPb}) olarak ayrıştırılması,
- Kanalın meşru alıcıda $\widehat{H}_b = \sqrt{(H_{AP})^2} H_{MIN}$ olarak tahmin edilmesi,
- Verilerin (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpılması ve meşru alıcıya doğru iletilmesi,
- Sinyalin meşru alıcıda R olarak alınması,
- Meşru alıcı tarafından verilerin kodunu çözmek üzere H_{MIN}'in denkleştirilmesi.

4. İstemler 1 ila 3'ten herhangi birine göre bir yöntemin kullanımı olup, herhangi kablosuz haberleşme teknolojisinde verilere, pilotlara veya birlikte verilere ve pilotlara gizli dinleyicilere karşı koruma sağlamaya yöneliktir.

5. İstem 4'e göre bir yöntemin kullanımı olup, burada kablosuz haberleşme teknolojisi 3GPP tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağlarını destekleyebilen herhangi cihaz, sistem veya ağ, veya hem 3GPP tabanlı hücresel hem de IEEE 802.11 tabanlı Wi-Fi ağlarında sağlanan çok noktalı koordinasyonu destekleyen herhangi kablosuz ağdır.

6. İstem 5'e göre bir yöntemin kullanımı olup, burada3GPP tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağlarını destekleyebilen herhangi cihaz, sistem veya ağ, veya hem 3GPP tabanlı hücresel hem de IEEE 802.11 tabanlı Wi-Fi ağlarında sağlanan çok noktalı koordinasyonu destekleyen herhangi kablosuz ağ, kod bölmeli çoklu erişim (CMDA); 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 sinyallerdir.

TARİFNAME

GELECEKTEKİ KABLOSUZ AĞLARA YÖNELİK KANAL AYRIŞTIRMA TABANLI UYARLAMALI FİZİKSEL KATMAN GÜVENLİĞİ

Teknik Alan

Bu buluşta, Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizma önerilmektedir.

Önceki Teknik

Fiziksel katman güvenliğinde (PLS) başı çeken alanlar arasında, zengin saçılım kanallarında haberleşmenin güvenliğinin sağlanması son zamanlarda büyük ilgi çekmiştir. Literatürde farklı güvenlik teknikleri önerilmiştir. Bu teknikler anahtar üretimi tabanlı yaklaşımları, adaptif haberleşme tabanlı yaklaşımları, yapay gürültü tabanlı teknikleri ve dalga boyu özellikleri gizleme tekniklerini içermektedir. Anahtar üretimi tabanlı teknikler, rastgeleliğin bir ortak kaynağı olarak meşru düğümler arasında kanal karşılıklılığı özelliğinden faydalanılmasına dayanmaktadır. Örneğin, alınan sinyal gücü (RSS), kanal dürtü yanıtı (CIR), kanal frekans yanıtı (CFR) ile ilgili genlik ve faz, ve diğer geri bildirimler, anahtar üretmek için kullanılabilmektedir. Bu teknikler, anahtar yönetimi ve gelecekteki çoktürlü kablosuz ağlarda dağıtım ile ilgili geleneksel kriptografi tabanlı algoritmaların karşılaştığı problemleri çözebilmeleri bakımından ilginçtir. Ne var ki, karşılıklılık uyuşmazlığına ve özellikle de düşük sinyal-gürültü oranında (SNR) kanal tahmin hatasına çok hassastırlar. Adaptif iletim tabanlı tekniklerde, parametreler, yalnızca meşru alıcının konum, kanal koşulları ve hizmet kalitesi (QoS) gereksinimlerine dayalı olarak ayarlanmakta/uyarlanmaktadır. Örneğin, güvenlik sağlayan ancak yüksek tepe-ortalama güç oranı (PAPR) ile sonuçlanan ön denkleştirme tabanlı teknikler, alt taşıyıcı seçilimi tabanlı teknikler spektral verimliliğin kaybı pahasına güvenlik sağlamaktadır. Yapay gürültü tabanlı teknikte, girişim sinyali, meşru alıcının performansını etkilemeksizin bir meşru düğümün performansını düşürmek üzere güvenilir düğüm tarafından eklenmektedir. Ne var ki girişim

sinyali, PAPR'de bir artışa ve gürültü üretimine yönelik güç kaynaklarının feda edilmesi nedeniyle az miktarda güç düşmesine neden olabilmektedir.

Pilot tonu manipülasyonu, yapay gürültü yerleştirme ve gizli dinleme karşıtı pilot tasarımı dahil referans sinyallerinin güvenliğini sağlamak üzere literatürde çeşitli teknikler önerilmiştir. Önceki teknikte, pilotların gazları vericideki alt taşıyıcıların önceki anlık kanal bilgilerine dayalı olarak döndürülmektedir. Bu, yalnızca amaçlanan alıcının kanalı doğru şekilde tahmin edebildiği kanal tahmin fazı esnasında gizli dinleme kapasitesini bozmaktadır. Önceki teknikte, ana sistemden uç birime iletim esnasında saldırgan tarafında kanal tahmin performansını düşürmek üzere alt sistemden ana sisteme CSI'ya dayalı olarak pilot sinyaline yapay gürültü yerleştirilmektedir. Özellikle de, meşru düğümlerden gelen pilotlar, kompozit pilot matrisi, meşru düğümlere yönelik dolu bir kerteye sahipken, saldırgana göre kerte yetersizliğine sahip olacak şekilde tasarlanmaktadır. Bu, saldırganın, meşru pilotları kullanan CSI'larının alt uzayını gözlemleyememesini sağlamaktadır.

Buluşun Amaçları ve Kısa Açıklaması

Mevcut buluş, yukarıda bahsedilen dezavantajları ortadan kaldırmak ve ilgili teknik alana yeni avantajlar getirmek amacıyla Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizmaya yönelik bir yöntem ile ilgilidir.

Bu buluş, Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere yeni bir kanal tabanlı mekanizma sağlamaktadır.

Kablosuz haberleşmenin yayın yapan doğası, onu çeşitli güvenlik tehditlerine yatkın hale getirmektedir. Bu tehditlerden biri, gizli dinleme olarak da atıfta bulunulan, haberleşmenin gizliliğinin ihlalidir. Bu durumda, kötü niyetli bir düğüm/cihaz, iki meşru düğüm arasında devam etmekte olan haberleşmeyi kesmeye ve anlamaya çalışır. Geleneksel olarak, üst katmanlardaki, kriptografi tabanlı teknikler gibi güvenlik teknikleri, güvenli iletim için kullanılagelmiştir. Ne var ki, bu tür güvenlik teknikleri, artan anahtar yönetimi ve paylaşım mekanizmaları karmaşıklığı

nedeniyle gelecekteki (5G ve ötesi) merkeziyetsizleştirilmiş ve çoktürlü ağlara yönelik olarak uygun olmayabilir. Bu akılda tutularak, bu buluşta bahsedilen gibi fiziksel katman güvenliği (PLS) mekanizmaları son yıllarda git gide popüler hale gelmiştir.

Önerilen algoritmalar, geleneksel kriptografi tabanlı güvenlik çözümlerine bağlı olmaksızın güvenli ve verimli haberleşme sağlayabilmektedir. Daha özel olarak, fiziksel katman (PHY) güvenliği konseptine dayalı önerilen algoritma, geleneksel güvenlik ile ilgili aşağıdaki problemleri çözebilmektedir:

1. Gelecekteki ağların, 5G Dokunsal İnternet, Nesnelerin İnterneti (IoT), Ultra Güvenilir Düşük Gecikmeli Haberleşme (ULLRC), uzak cerrahi gibi yeni kablosuz teknolojileri desteklemesi gerekmektedir. Ne var ki, bu uygulamalarda kullanılan cihazlar doğal olarak güç sınırlamalı, işleme kısıtlamalı ve gecikmeye karşı hassastırlar, bu da kriptografi tabanlı teknikleri bu türden teknolojilere yönelik olarak gerçekleştirilemez hale getirmektedir.

2. Gelecekteki ağların, farklı güvenlik gereksinimlerine sahip çeşitli hizmetleri ve senaryoları desteklemesi beklenmektedir. Şifreleme tabanlı yöntem, senaryoya özgü güvenlik sağlayamamaktadır.

3. Saldırgan, pilotların güvenliğinin sağlanmaması halinde ortamı öğrenebilmektedir. Dahası, pilotların gönderilmesi de saldırganın meşru vericide tasarlanan ön kodlayıcıyı öğrenmesine olanak verebilmekte, bu da önceki teknikte bahsedildiği gibi meşru düğümlerin kanal durumu bilgilerinin saldırgana sızdırılmasına yol açmaktadır.

4. PHY güvenlik algoritmalarının çoğunluğu, kanalın iletimin iki düğümünde de (veya en azından bir tarafta) bilindiğini varsaymaktadır. Kanalın tahmin edilmesi ve geri bildirilmesi aşamasında, güvenlik gizli dinleyiciye karşı çok savunmasızdır ve saldırganın kanalı öğrenmesi halinde, PHY güvenlik algoritması çözülebilir.

Herhangi bir kablosuz haberleşme teknolojisi, verilere, pilotlara veya birlikte verilere ve pilotlara gizli dinleyicilere karşı koruma sağlamak üzere bu buluşu kullanabilmektedir. Ne var ki, 3GPP

tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağları gibi standartlar veya herhangi bir kablosuz ağ, iki standartta da sağlanan çok noktalı koordinasyon desteği nedeniyle özellikle buluş ile ilgilidir. İlaveten, bu buluşta açıklanan yöntem, yukarıda bahsedilen standartlardan herhangi birini destekleyebilen herhangi cihaz, sistem veya ağda, örneğin: kod bölmeli çoklu erişim (CMDA), 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 sinyallerde uygulanabilmektedir.

Buluşun Avantajları;

1- Önerilen algoritma geleneksel kriptografi tabanlı yöntemler olmaksızın güvenlik sağlayabilmekte, dolayısıyla gelecekteki ağlar için anahtar paylaşımı, dağıtımı ve yönetimi sorunlarından kaçınabilmektedir.

2- Önerilen algoritma yalnızca verilerin, yalnızca pilotların, veya verilerin ve pilotların birlikte güvenliğini sağlayarak esnek ve senaryoya özgü güvenlik sağlamak üzere uygulanabilmektedir.

3- Geleneksel PLS yöntemi ile karşılaştırıldığında, önerilen algoritma meşru düğümün BER performansını düşürmeksizin güvenlik sağlayabilmekte, vericideki PAPR'de bir artışa neden olmakta, spektral verimlilikte bir kayba neden olmakta, ve gürültü için güçten ödün vermektedir. Tasarım, kanalın tam geçirgen ve minimum faz kanallarına ayrıştırılmasına ve güvenlik sağlamak üzere ayrıştırılan kanalların özelliklerinden faydalanılmasına dayalıdır.

4- Önerilen algoritma, saldırgan doğru pilotları öğrenemeyecek, dolayısıyla ortamı öğrenemeyecek şekilde pilota yönelik güvenlik sağlayabilmektedir.

5- Gizli dinleyici, pilot güvenliği nedeniyle alınan sinyalden gelen meşru düğümlere karşılık gelen ön kodlayıcının bilgilerini çekemeyecektir.

6- Önerilen algoritma, RF tabanlı PHY doğrulamasında donanım bozulmalarını gizlemeye yönelik olarak uygulanabilmektedir.

7- Açıklanan yöntem, kablosuz ağlarda geri bildirim güvenliğine yönelik olarak oldukça uygundur.

8- Açıklanan yöntem, PHY doğrulamasına yönelik olarak kullanılabilmektedir.

9- Açıklanan yöntem, eş konumlu gizli dinleyici durumunda dahi güvenlik sağlamaktadır.

10- Açıklanan yöntem, tekli kullanıcı, çoklu kullanıcı, tekli anten, çoklu anten, merkezileştirilmiş ve dağıtık sistemlere uygulanabilirdir.

Buluşun Şekillerinin Açıklaması

Şekiller mevcut buluş tarafından geliştirilenleri ayrıca açıklama amacıyla kullanılmaktadır, bu Şekiller aşağıda açıklanmaktadır:

Şekil 1: Sistem modeli.

Şekil 1'deki unsurların açıklaması:

EVE: Gizli dinleyici

ALICE: Meşru verici

BOB: Meşru alıcı

$H = H_{AP} H_{MIN}$: Alice, kanalı (H) tam geçirgen (H_{AP}) ve minimum faz H_{MIN} bileşenlere ayrıştıracaktır.

H_{ae} = Alice'den Eve'de gözlemlenen kanal

H_{be} = Eve from Bob'dan Eve'de gözlemlenen kanal

Şekil 1'de gösterildiği üzere, bir meşru verici (Alice, {a}), meşru alıcı (Bob, {b}) ve Alice ve Bob arasındaki iletimi kesmeye çalışan pasif gizli dinleyiciden (Eve, {e}) oluşan bir OFDM sistemi düşünülmektedir. Bob'dan Alice'de (H{ba}), Alice'den Bob'da (H{ab}), Bob'dan Eve'de (H{be}), ve Alice'den Eve'de (H{ae}) gözlemlenen kanalların Rayleigh sönümlemeli dağılımına sahip olan üstel olarak bozulan bağlantı uçlarına sahip çok yollu yavaş değişken kanallar olarak düşünülmektedir. Dahası, kanal karşılıklılığı varsayımı nedeniyle, Alice-Bob arasındaki (H{ab}) kanal, {ab}=H_{ba}^T olduğu Bob-Alice arasındaki (H{ba}) kanaldan tahmin edilebilmektedir.

Buluşun Detaylı Açıklaması

Buluşun yeniliği buluşun kapsamını sınırlandırmayan ve yalnızca buluşun konusunu netleştirmesi amaçlanan örnekler ile açıklanmıştır. Mevcut buluş, aşağıda detaylı olarak açıklanmaktadır.

Önerilen algoritma, pilot ve veri güvenliğine yönelik minimum faz (MP) ve tam geçirgen (AP) kanal ayrışmasının yeni kullanımına dayanmaktadır. Kanalın MP ve AP bileşenleri güvenli PHY algoritmaları tasarlamaya yönelik olarak kullanılmaktadır.

Kanal ayrışması:

Kablosuz kanal, bir Sonlu Dürtü Yanıtına (FIR) sahiptir; dolayısıyla stabildir. Ek olarak, kablosuz kanal bir gerçek hayat sistemidir, nedensel olması zorunludur. Bu iki koşul, kanalın aşağıdaki gibi MP ve AP kanallarına ayrıştırılabilmesini sağlamaktadır:

$$H(z) = \underbrace{\left(H_1(z)\prod_{k=1}^{q}(1-p_k^* z^{-1})\right)}_{H_{MIN}(z)} \overbrace{\left(\prod_{k=1}^{q}\left(\frac{z^{-1}-p_k}{1-p_k^* z^{-1}}\right)\right)}^{H_{AP}(z)}$$

burada $H(z)$ kanalın aktarım fonksiyonudur; $H_{MIN}(z)$ ve $H_{AP}(z)$, $H(z)$'nin minimum faz ve tam geçirgen bileşenleridir; q birim çemberinin dışındaki sıfır sayısını belirtmektedir; ve p, $1/p_k$ sistemin sıfırlarının konumu olacak şekilde tanımlanan bir karmaşık sayıdır. Birim çemberinin içindeki sıfırlar $H_1(z)$ teriminin içinde verilmektedir.

Örneğin, iki meşru taraf Alice ve Bob'un olduğu varsayılmaktadır, burada Alice (verici) Bob (alıcı) ile Şekil 1'de gösterildiği gibi bir gizli dinleyicinin mevcudiyetinde güvenli bir şekilde haberleşmek istemektedir. PHY güvenlik algoritması Alice'deki kanal durum bilgilerine (CSI) dayalıdır. Geleneksel olarak CSI, Bob'un Alice'e kanal tahmini ve dolayısıyla CSI edinimine yönelik bilinen pilot sinyalini gönderdiği alt sistemden ana sisteme alıştırma aracılığıyla erişilebilir olmaktadır. Bu durumda Eve, Bob ve kendisi arasındaki kanalı ve ortamı öğrenebilmektedir.

PHY güvenlik yöntemi, Alice'deki kanal durumu bilgisine (CSI) dayalıdır, bu da verilerin veya pilotların, veya verilerin ve pilotların birlikte güvenliğini sağlamak üzere kullanılmaktadır.

Algoritma I: Pilot güvenliği:

Adım1: Birinci adımda, Alice kanalı tam geçirgen ve minimum faz bileşenlerine ayrıştıracaktır ($H \Rightarrow H_{AP}\, H_{MIN}$).

Adım2: Ardından, pilot sinyalini (P) kanalın tam geçirgen bileşeni ile $T_1 = H_{AP}\, P$ olarak çarpar ve Bob'a doğru iletir.

Adım3: Bob'da alınan sinyal $R_1 = H.H_{AP}\, P$ olarak verilebilir. Kanal ayrıştırma konsepti kullanılarak, alınan sinyal $R_1 = H_{AP}\, H_{MIN}\, H_{AP}\, P = H_{MIN}\, (H_{AP})^2 P$ olarak yeniden yazılabilir.

Adım4: Tahmin edilen kanal tam geçirgen $(H_{APb})^2$ ve minimum faz H_{MPb} olarak ayrıştırılabilir. Son olarak, Bob'da tahmin edilen kanal aşağıdaki gibi verilebilir:

$$\hat{H}_b = \sqrt{(H_{AP})^2} H_{MIN}.$$

Adım5: $\sqrt{(H_{AP})^2} = \pm H_{AP}$ olduğu, ancak tahmin edilen kanalın simgesini tanımlamak üzere kanal yanıtının devamlılığından yararlanıldığı not edilmelidir.

Önerilen algoritma nedeniyle yalnızca meşru düğümün kanalı tahmin edebileceği, saldırganın ise onun kanalını tahmin edemeyeceği not edilmelidir. Özellikle de, kanal ilişkisizliği varsayımı nedeniyle, meşru ve meşru olmayan düğümler tarafından gözlemlenen kanallar bağımsızdır ve dolayısıyla saldırganın önerilen kanala bağımlı tasarımda kanalı tahmin etmesini oldukça zor hale getirmektedir.

<u>Algoritma II: Veri güvenliği:</u>

Veri güvenliği algoritmasına yönelik temel adımlar aşağıdaki gibidir:

Adım1: Birinci adımda, Alice kanalı tam geçirgen ve minimum faz bileşenlerine ayrıştıracaktır ($H \Rightarrow H_{AP}\, H_{MIN}$).

Adım2: Ardından, verileri (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpar ve Bob'a doğru iletir.

Adım3: Bob'da alınan sinyal R olarak verilebilir. Kanal ayrıştırma konsepti kullanılarak, alınan sinyal $R = H_{AP}\, H_{MIN}\, \frac{D}{H_{AP}} = H_{MIN}\, D$ olarak yeniden yazılabilir.

Adım4: Son olarak, verilerin kodunu çözmek üzere Bob H_{MIN}'i denkleştirir.

Önerilen algoritma nedeniyle yalnızca meşru düğümün kanalı tahmin edebileceği, saldırganın ise onun kanalını tahmin edemeyeceği not edilmelidir. Özellikle de, kanal ilişkisizliği varsayımı nedeniyle, meşru ve meşru olmayan düğümler tarafından gözlemlenen kanallar bağımsızdır ve dolayısıyla saldırganın önerilen kanala bağımlı tasarımda kanalı tahmin etmesini oldukça zor hale getirmektedir.

Algoritma III: Birlikte Pilot & Veri güvenliği:

Buluş, aynı zamanda, veri ve pilot güvenliğini birlikte sağlayabilmektedir. Pilotlar (P) ve verilerden (D) oluşan bir çerçeve düşünülsün.

Adım1: Birinci adımda, Alice kanalı tam geçirgen ve minimum faz bileşenlerine ayrıştıracaktır ($H \Rightarrow H_{AP}\, H_{MIN}$).

Adım2: Ardından, pilot sinyalini (P) kanalın tam geçirgen bileşenleri ile $T_1 = H_{AP}P$ olarak çarpar ve Bob'a doğru iletir.

Adım3: Bob'da alınan sinyal $R_1 = H.H_{AP}\, P$ olarak verilebilir. Kanal ayrıştırma konsepti kullanılarak, alınan sinyal $R_1 = H_{AP}\, H_{MIN}\, H_{AP}\, P = H_{MIN}\, (H_{AP})^2 P$ olarak yeniden yazılabilir.

Adım4: Tahmin edilen kanal tam geçirgen $(H_{AP})^2$ ve minimum faz H_{MPb} olarak ayrıştırılabilir. Son olarak, Bob'da tahmin edilen kanal aşağıdaki gibi verilebilir:

$$\widehat{H}_b = \sqrt{(H_{AP})^2}\, H_{MIN}.$$

Adım5: $\sqrt{(H_{AP})^2} = \pm H_{AP}$ olduğu, ancak tahmin edilen kanalın simgesini tanımlamak üzere kanal yanıtının devamlılığından yararlanıldığı not edilmelidir.

Adım6: Ardından, verileri (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpar ve Bob'a doğru iletir.

Adım7: Bob'da alınan sinyal R olarak verilebilir. Kanal ayrıştırma konsepti kullanılarak, alınan sinyal $R=H_{AP}\,H_{MIN}\,\frac{D}{H_{AP}}=H_{MIN}\,D$ olarak yeniden yazılabilir.

Adım8: Son olarak, verilerin kodunu çözmek üzere Bob H_{MIN}'i denkleştirir.

Yukarıdaki tüm bilgilere bağlı olarak, Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizmanın operasyon yöntemi şu adımları içermektedir; ilk olarak kanalın minimum faz ve tam geçirgen faz bileşenlerine ayrılması. Ardından, kanalın bileşenlerinin akıllı bir şekilde veri ve pilot güvenliğine yönelik algoritmaları tasarlamak üzere kullanılması. Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında pilotların yanı sıra verileri korumak üzere kanal tabanlı mekanizmanın operasyon yöntemi olup, aşağıdaki adımları içermektedir;

Pilot güvenlik sürecine yönelik olarak;

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\,H_{MIN}$);
- Pilot sinyalinin (P) kanalın tam geçirgen bileşeni ile $T_1 = H_{AP}\,P$ olarak çarpılması ve meşru verici tarafından meşru alıcıya doğru iletilmesi,
- Sinyalin meşru alıcıda $R_1 = H.H_{AP}\,P$ olarak alınması,
- Tahmin edilen kanalın tam geçirgen $(H_{APb})^2$ ve minimum faz (H_{MPb}) olarak ayrıştırılması,
- Kanalın meşru alıcıda $\hat{H}_b = \sqrt{(H_{AP})^2}H_{MIN}$· olarak tahmin edilmesi.

Veri güvenliği sürecine yönelik olarak;

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\,H_{MIN}$);
- Verilerin (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpılması ve meşru alıcıya doğru iletilmesi,

- Sinyalin meşru alıcıda R olarak alınması,
- Meşru alıcı tarafından verilerin kodunu çözmek üzere H_{MIN}'in denkleştirilmesi.

Birlikte Pilot & Veri güvenliği sürecine yönelik olarak:

- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\, H_{MIN}$);
- Kanalın meşru verici tarafından tam geçirgen ve minimum faz bileşenlerine ayrıştırılması ($H \Rightarrow H_{AP}\, H_{MIN}$);
- Sinyalin meşru alıcıda $R_1 = H.H_{AP}\, P$ olarak alınması,
- Tahmin edilen kanalın tam geçirgen $(H_{APb})^2$ ve minimum faz (H_{MPb}) olarak ayrıştırılması,
- Kanalın meşru alıcıda $\hat{H}_b = \sqrt{(H_{AP})^2} H_{MIN}$. olarak tahmin edilmesi,
- Verilerin (D) kanalın tam geçirgen bileşenlerinin karşılığı ile $1/H_{AP}$ olarak çarpılması ve meşru alıcıya doğru iletilmesi,
- Sinyalin meşru alıcıda R olarak alınması,
- Meşru alıcı tarafından verilerin kodunu çözmek üzere H_{MIN}'in denkleştirilmesi.

Bu temel kavramlar çevresinde, buluşun konusu ile ilgili birkaç yapılandırma 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.

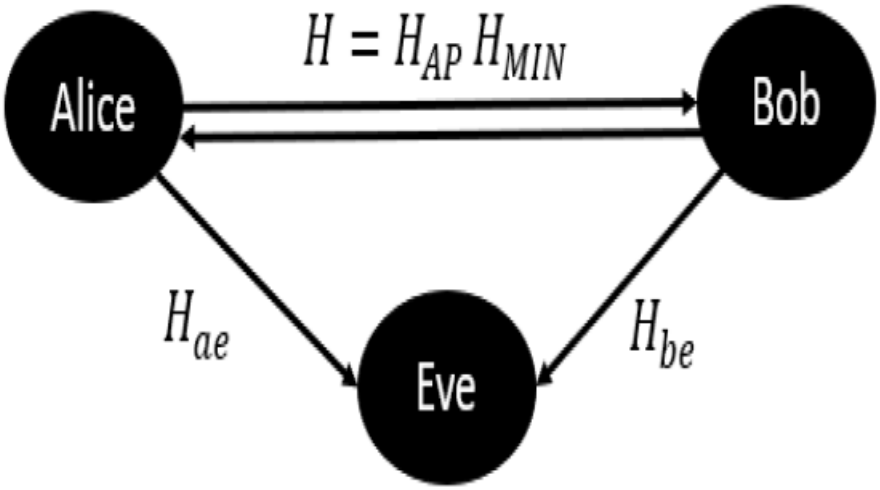
Buluşun Endüstriyel Uygulaması

Mevcut buluş, Gizli Dinleme saldırılarına karşı zengin saçılım kanallarında verilerin ve/veya pilotların korunmasına yönelik bir yöntem sağlamaktadır. Buluşun yöntemi, verilere, pilotlara veya verilere ve pilotlara birlikte gizli dinleyicilere karşı koruma sağlamak üzere herhangi kablosuz teknolojiye uygulanabilmektedir.

Özellikle de, 3GPP tabanlı hücresel ve IEEE 802.11 tabanlı Wi-Fi ağları gibi standartlar veya herhangi bir kablosuz ağ, iki standartta da sağlanan çok noktalı koordinasyon desteği nedeniyle özellikle buluş ile ilgilidir. İlaveten, buluşun yöntemi, yukarıda bahsedilen standartlardan herhangi birini destekleyebilen herhangi cihaz, sistem veya ağda, örneğin: kod bölmeli çoklu erişim (CMDA), 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 sinyallerde uygulanabilmektedir.

Aynı zamanda, gelecekteki ağların 5G Dokunsal İnternet, Nesnelerin İnterneti (IoT), Ultra Güvenilir Düşük Gecikmeli Haberleşme (ULLRC), uzak cerrahi vb. yeni kablosuz teknolojileri desteklemesi gerekmektedir, ne var ki, bu uygulamalarda kullanılan cihazlar doğal olarak güç sınırlamalı, işleme kısıtlamalı ve gecikmeye karşı hassastırlar, bu da önceki tekniği bu türden teknolojilere yönelik olarak gerçekleştirilemez hale getirmektedir.

Buluşun yöntemi, farklı güvenlik gereksinimlerine sahip çeşitli hizmetleri ve senaryoları desteklemesi beklenen gelecekteki ağlara yönelik olarak senaryoya özgü güvenlik sağlama potansiyeline sahiptir.



ŞEKİL 1