ÖZET

YENİ FİZİKSEL KATMAN ANAHTAR ÜRETİM BOYUTLARI: ALT TAŞIYICI SAYISI VE DİZİN TABANLI ANAHTAR ÜRETİMİ

Çok taşıyıcılı sistemlerde kablosuz kanaldan gizli anahtar üretimine yönelik yeni boyutlar, kablosuz iletişim sistemlerinde gizliliğin ve kimlik doğrulamasının sağlanması için önerilmektedir. Önerilen algoritmaların yeniliği, yalnızca çok taşıyıcılı sistemin (OFDM)) alt kanallarının büyüklüklerinden değil, aynı zamanda en iyi kanal kazançlarına karşılık gelen çok taşıyıcı bloğun her bir alt bloğundaki alt kanalların sayısından ve dizinlerinden ve kanal kazançları, karşılık gelen alt bloğun ortalamasının üzerinde olan her bir alt bloktaki alt kanalların sayısından rastgele gizli bitlerin üretimine dayanmaktadır. İlaveten, ayrıca bir statik ortamda kanal tabanlı anahtar yaklaşımının rastgeleliğinin arttırılmasına yönelik RIS destekli yaklaşım da sunulmaktadır.

ABSTRACT

NOVEL PHYSICAL LAYER KEY GENERATION DIMENSIONS: SUBCARRIER NUMBER AND INDICES-BASED KEY GENERATION

Novel dimensions for key generation from the wireless channel in multi-carrier systems are proposed for ensuring confidentiality and authentication in wireless communication systems. The novelty of the proposed algorithms lies in the generation of random secret bits not just from the magnitudes of multi-carrier system's (orthogonal frequency division multiplexing (OFDM)) subchannels but also from the indices and numbers of subchannels in each subblock of the multi-carrier block corresponding to best channel gains and from the number of subchannels in each subblock whose channel gains are above the mean of the corresponding subblock. Furthermore, RIS assisted approach for enhancing the randomness of the channel-based key approach in a static environment is also presented.

İSTEMLER

1. Yeni fiziksel katman anahtar üretimi boyutlarına yönelik bir sistem olup özelliği; alt taşıyıcı sayısı ve dizin tabanlı anahtar üretimi olup; dizin tabanlı anahtar üretimi (IKG) veya birleşik dizin tabanlı anahtar üretimi (JIKG) veya sayı tabanlı anahtar üretimi (NKG) veya birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG) ve kanal tabanlı anahtarın rastgeleliğini arttırmak amacıyla kanal manipülasyonu için yeniden yapılandırılabilir akıllı yüzey (RIS) içermesidir.

2. İstem 1'e göre sistemde bir dizin tabanlı anahtar üretim (IKG) yöntemi olup özeliği;

   i. Meşru verici ve meşru alıcı tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,

   ii. Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ve $\boldsymbol{h_f}$ = diyagonal (**HR**) olarak elde edilen vektörün çarpılması,

   iii. Bütün $\boldsymbol{h_f}$ vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $\boldsymbol{h_f} = [\boldsymbol{h_1}, \ldots\ldots, \boldsymbol{h_G}]$, $\boldsymbol{h_\beta} = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$, olması,

   iv. $h_{\beta,j}$'nin $\boldsymbol{h_\beta}$ alt bloğunun j'inci ögesi olduğu, her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,1}|$ şeklinde hesaplanması,

   v. $|h_{\beta,j}|$ değerlerine dayanarak veya özellikle meşru düğümlerdeki alt taşıyıcıların sinyal-gürültü oranına göre her bir $\boldsymbol{h_\beta}$ alt bloğundaki en güçlü alt taşıyıcıların sayısının m_β seçilmesi,

   vi. Dizinlerin anahtar bitlerine olan pozisyonuna yönelik bir eşleme tablosu olan arama Tablosu I'e dayanarak anahtar bitlerinin üretilmesine yönelik seçilen alt taşıyıcıların pozisyonlarının/dizinlerinin kullanılması

   işlem adımlarını içermesidir.

3. İstem 2'ye göre sistemdeki bir dizin tabanlı anahtar üretim (IKG) yöntemi olup özelliği; yeniden yapılandırılabilir akıllı yüzeyin (RIS) yönteminin birinci adımı için kullanılmasıdır.

4. İstem 1'e göre olan sistemde bir birleşik dizin tabanlı anahtar üretim (JIKG) yöntemi olup, özelliği;

i. Meşru verici ve meşru alıcı tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,

ii. Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ve $\boldsymbol{h_f}$ = diyagonal (**HR**) olarak elde edilen vektörün çarpılması,

iii. Bütün $\boldsymbol{h_f}$ vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $\boldsymbol{h_f} = [\boldsymbol{h_1}, \ldots\ldots, \boldsymbol{h_G}]$, $\boldsymbol{h_\beta} = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$, olması,

iv. $h_{\beta,j}$'nin $\boldsymbol{h_\beta}$ alt bloğunun j'inci ögesi olduğu, her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,1}|$ şeklinde hesaplanması,

v. Arama Tablosu I kullanılarak $\mathbf{h}_\beta$ alt bloğunun dizinlerinden anahtar bitlerinin üretilmesi,

vi. Alt blok ögesinin mutlak değerlerinin ortalamasının, aşağıdaki gibi hesaplanması

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n} \text{ burada } \beta \epsilon \{1, \ldots\ldots, G\},$$

vii. $\boldsymbol{h_\beta}$ alt bloğunun her bir ögesinin, gizli anahtar bitleri üretmek için ortalama, av_β ile karşılaştırılması,

viii. $|h_{\beta,j}| > av_\beta$, olması halinde, anahtar biti olarak 1'in üretilmesi, aksi takdirde 0'ın üretilmesi.

işlem adımlarını içermesidir.

5. İstem 4'e göre sistemdeki bir birleşik dizin tabanlı anahtar üretim (JIKG) yöntemi olup özelliği; yeniden yapılandırılabilir akıllı yüzeyin (RIS) yöntemin birinci adımı için kullanılmasıdır.

6. İstem 1'e göre sistemde sayı tabanlı anahtar üretim (NKG) yöntemi olup, özelliği;

i. Meşru verici ve meşru alıcı tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,

ii. Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ve $\boldsymbol{h_f}$ = diyagonal (HR) olarak elde edilen vektörün çarpılması,

iii. Bütün $\boldsymbol{h_f}$ vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $\boldsymbol{h_f} = [\boldsymbol{h_1}, \ldots\ldots, \boldsymbol{h_G}]$, $\boldsymbol{h_\beta} = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$, olması,

iv. $h_{\beta,j}$'nin $\boldsymbol{h_\beta}$ alt bloğunun j'inci ögesi olduğu, her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,1}|$ şeklinde hesaplanması,

v. Alt blok ögesinin mutlak değerlerinin ortalamasının hesaplanması, aşağıdaki gibidir:

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n},$$

vi. $\boldsymbol{h_\beta}$ alt bloğunun her bir ögesinin, her bir alt blokta av_β ve alt taşıyıcıların sayısı için sayılan ortalama ile karşılaştırılması,

vii. Kanal kazançları, av_β üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına dayalı olan Tablo II kullanılarak meşru düğümlerde bir gizli anahtarın üretilmesi işlem adımlarını içermesidir.

7. İstem 6'ya göre sistemdeki sayı tabanlı anahtar üretim (NKG) yöntemi olup özelliği; yeniden yapılandırılabilir akıllı yüzeyin (RIS) yöntemin birinci adımı için kullanılmasıdır.

8. İstem 1'e göre sistemde sayı ve dizin tabanlı anahtar üretim (JNIKG) yöntemi olup özelliği;

i. Meşru verici ve meşru alıcı tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,

ii. Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ve $\boldsymbol{h_f}$ = diyagonal (**HR**) olarak elde edilen vektörün çarpımı,

iii. Bütün $\boldsymbol{h_f}$ vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $\boldsymbol{h_f} = [\boldsymbol{h_1}, \ldots\ldots, \boldsymbol{h_G}]$, $\boldsymbol{h_\beta} = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$, olması,

iv. $h_{\beta,j}$'nin $\boldsymbol{h_\beta}$ alt bloğunun j'inci ögesi olduğu, her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,1}|$ şeklinde hesaplanması,

v. Alt blok ögesinin mutlak değerlerinin ortalamasının hesaplanması, aşağıdaki gibidir:

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n},$$

vi. $\boldsymbol{h_\beta}$ alt bloğunun her bir ögesinin, ortalama, av_β ile karşılaştırılması ve ortalamanın üzerinde alt taşıyıcıların sayısı, her bir alt taşıyıcı için sayılması,

vii. Kanal kazançları, av_β üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına ve pozisyonlarına dayalı Tablo III kullanılarak meşru düğümlerde gizli anahtar bitlerinin üretilmesi,

viii. $\boldsymbol{h_\beta}$ alt bloğunun her bir ögesinin ortalama, av_β ile karşılaştırması, farklı alt taşıyıcıların genliklerinden gizli anahtar üretmek için gerçekleştirilmesi,

ix. $|h_{\beta,j}| > av_\beta$, olması halinde, anahtar biti olarak 1'in üretilmesi, aksi takdirde 0'ın üretilmesi

işlem adımlarını içermesidir.

9. İstem 8'e göre sistemdeki birleşik sayı ve dizin tabanlı anahtar üretim (JNIKG) yöntemi olup özelliği; Yeniden yapılandırılabilir akıllı yüzeyin (RIS) yöntemin birinci adımı için kullanılmasıdır.

CLAIMS

1. A system of novel physical layer key generation dimensions: subcarrier number and indices-based key generation, comprising**;** indices based key generation (IKG) or joint indices based key generation (JIKG) or number-based key generation (NKG) or joint number and indices-based key generation (JNIKG), and reconfigurable intelligent surface (RIS) for channel manipulation in order to enhance the randomness of the channel-based key.
2. An indices based key generation (IKG) method in the system according to claim 1, the method comprising the steps of;

    i. Sending pilot signals to each other within the coherence time of the channel to estimate the channel at any node in the frequency domain as **H** by legitimate transmitter and legitimate receiver,

    ii. Multiplication of the resultant diagonal channel matrix (**H**) at any with a random interleaver (**R**), and the resultant vector as $\boldsymbol{h_f}$ = diagonal (**HR**),

    iii. Dividing the whole $\boldsymbol{h_f}$ vector into **G** subblocks with "n" elements in each subblock (h_f), where $\boldsymbol{h_f} = [\boldsymbol{h}_1, \ldots\ldots, \boldsymbol{h}_G]$, $\boldsymbol{h}_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, and $\beta \epsilon \{1, \ldots\ldots, G\}$,

    iv. Calculation of the absolute values of each of the subblock's elements as $|h_{\beta,1}|$, where $h_{\beta,j}$ is the jth element of $\boldsymbol{h}_\beta$ subblock,

    v. Selection of the number of strongest subcarriers m_β in each of $\boldsymbol{h}_\beta$ subblock-based on the values of $|h_{\beta,j}|$ or particularly with respect to signal to noise ratio of subcarriers at legitimate nodes,

    vi. Using the positions/indices of selected subcarriers for the generation of key bits by based on look-up Table I which is a mapping table for the position of indices to key bits.

3. An indices based key generation (IKG) method in the system according to claim 2, wherein reconfigurable intelligent surface (RIS) used for first step of method.

4. A joint indices based key generation (JIKG) method in the system according to claim 1, the method comprising the steps of;

   i. Sending pilot signals to each other within the coherence time of the channel to estimate the channel at any node in the frequency domain as **H** by legitimate transmitter and legitimate receiver,

   ii. Multiplication of the resultant diagonal channel matrix (**H**) at any with a random interleaver (**R**), and the resultant vector as $\boldsymbol{h_f}$ = diagonal (**HR**),

   iii. Dividing the whole $\boldsymbol{h_f}$ vector into **G** subblocks with "n" elements in each subblock (h_f), where $\boldsymbol{h_f} = [\boldsymbol{h}_1, \ldots\ldots, \boldsymbol{h}_G]$, $\boldsymbol{h}_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, and $\beta \epsilon \{1, \ldots, G\}$,

   iv. Calculation of the absolute values of each of the subblock's elements as $|h_{\beta,1}|$, where $h_{\beta,j}$ is the jth element of $\boldsymbol{h}_\beta$ subblock,

   v. Generation of the key bits from the indices of $\boldsymbol{h}_\beta$ subblock using look up Table I.,

   vi. Calculation of the average of absolute values of the subblock's element as follows

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n} \text{ where } \beta \epsilon \{1, \ldots, G\},$$

   vii. Comparison of each element of $\boldsymbol{h}_\beta$ subblock with its mean, av_β, to generate secret key bits,

   viii. If $|h_{\beta,j}| > av_\beta$, generation of 1 as key bit otherwise generation of 0.

5. A joint indices based key generation (JIKG) method in the system according to claim 4, wherein reconfigurable intelligent surface (RIS) used for first step of method.

6. A number-based key generation (NKG) method in the system according to claim 1, the method comprising the steps of;

   i. Sending pilot signals to each other within the coherence time of the channel to estimate the channel at any node in the frequency domain as **H** by legitimate transmitter and legitimate receiver,

ii. Multiplication of the resultant diagonal channel matrix (**H**) at any with a random interleaver (**R**), and the resultant vector as $\boldsymbol{h_f}$ = diagonal (HR),

iii. Dividing the whole $\boldsymbol{h_f}$ vector into G subblocks with "n" elements in each subblock (h_f), where $\boldsymbol{h_f} = [\boldsymbol{h}_1, \ldots\ldots, \boldsymbol{h}_G]$, $\boldsymbol{h}_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, and $\beta\epsilon\{1, \ldots\ldots, G\}$,

iv. Calculation of the absolute values of each of the subblock's elements as $|h_{\beta,1}|$, where $h_{\beta,j}$ is the jth element of $\boldsymbol{h}_\beta$ subblock,

v. Calculation of the average of absolute values of the subblock's element is as follows: $av_\beta = \frac{\sum_{j=1}^{n}|h_{\beta,j}|}{n}$,

vi. Comparing of each element of $\boldsymbol{h}_\beta$ subblock with mean which are counted for each subblock, av_β, and the number of subcarriers,

vii. Generation of a secret key at the legitimate nodes by using Table II based on the number of subcarriers in each subblock whose channel gains are above av_β.

7. A number-based key generation (NKG) method in the system according to claim 6, wherein reconfigurable intelligent surface (RIS) used for first step of method.

8. A joint number and indices-based key generation (JNIKG) method in the system according to claim 1, the method comprising the steps of;

i. Sending pilot signals to each other within the coherence time of the channel to estimate the channel at any node in the frequency domain as **H** by legitimate transmitter and legitimate receiver,

ii. Multiplication of the resultant diagonal channel matrix (**H**) at any with a random interleaver (**R**) and the resultant vector as $\boldsymbol{h_f}$ = diagonal (**HR**),

iii. Dividing of the whole $\boldsymbol{h_f}$ vector into **G** subblocks with "n" elements in each subblock (h_f), where $\boldsymbol{h_f} = [\boldsymbol{h}_1, \ldots\ldots, \boldsymbol{h}_G]$, $\boldsymbol{h}_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, and $\beta\epsilon\{1, \ldots\ldots, G\}$,

iv. Calculation of the absolute values of each of the subblock's elements as $|h_{\beta,1}|$, where $h_{\beta,j}$ is the jth element of $\boldsymbol{h}_\beta$ subblock,

v. Calculation of the absolute values of the subblock's element is calculated as follows: $av_\beta = \frac{\sum_{j=1}^{n}|h_{\beta,j}|}{n}$,

vi. Comparison of the each element of $\boldsymbol{h}_{\beta}$ subblock with mean, av_{β}, and number of subcarriers that are above mean are counted for each subblock,

vii. Generation of the secret key bits at the legitimate nodes by using Table III based on the number and positions of subcarriers in each subblock whose channel gains is above av_{β}.,

viii. A comparison of each element of $\boldsymbol{h}_{\beta}$ subblock with mean, av_{β}, is done to generate secret key from amplitudes of different subcarriers,

ix. If $\left|h_{\beta,j}\right| > av_{\beta}$, generation of 1 is as key bit otherwise generation of 0.

9. A joint number and indices-based key generation (JNIKG) method in the system according to claim 8, wherein reconfigurable intelligent surface (RIS) used for first step of method.

TARİFNAME

YENİ FİZİKSEL KATMAN ANAHTAR ÜRETİM BOYUTLARI: ALT TAŞIYICI SAYISI VE DİZİN TABANLI ANAHTAR ÜRETİMİ

Teknik Alan

Mevcut buluşta, çok taşıyıcılı sistemlerde kanal tabanlı anahtar üretimine yönelik yeni yöntemler önerilmektedir. Ayrıca statik kanal koşullarında anahtar üretimini geliştirecek yöntemler de sunulmaktadır.

Önceki Teknik

Fiziksel katman anahtar üretimi alanındaki birçok önemli araştırma alanı arasında, Ortogonal frekans bölmeli çoklama (OFDM) dalga biçiminin güvenliğinin sağlanması, çok ilgi görmüştür [1, 2, 3]. Literatürde OFDM tabanlı sistemlerde gizli anahtar üretimine yönelik farklı teknikler öneren çeşitli çalışmalar bulunmaktadır. Bu teknikler, kanal dürtü yanıtı (CIR), alınan sinyal gücü (RSS) ve anahtar üretimine yönelik diğer geri bildirimlerin genliklerinin ve fazlarının açıklarından yararlanmaya dayanmaktadır [3]. Referans [4]'teki yazarlar, iç mekan ve dış mekan ortamlarındaki OFDM sistemine yönelik kanal durumu bilgisi (CSI) tabanlı anahtar üretimini önermektedir. Referans [5]'de, birden çok bağımsız faz, çok tonlu iletişim sisteminde gizli anahtarlar üretmek için nicelendirilmektedir. Diğer yandan, referans [6]'nın yazarları, zamanla değişen kanal frekansı yanıtının faz değişikliğine dayalı bir OFDM sisteminin gizli anahtar üretimini incelemiştir. Referans [7]'de, OFDM alt taşıyıcıları ile birlikte ön kodlama matris dizinlerinin, gizli anahtarlar üretmek için açıklarından yararlanılmaktadır. Kanal tabanlı anahtar üretimindeki ana zorluklardan biri, anahtarın tekdüzeliğini ve rastgeleliğini korurken gizli anahtar uzunluğunun arttırılmasıdır. Bahsi geçen teknikler, esasen rastgele ve tekdüze gizli anahtar üretimi için RSS veya kanal kazançlarının fazlarının ve genliklerinin açıklarından yararlanmaktadır. Ancak, bu yöntemlerin tamamı, gizli anahtar üretim hızı açısından belirli sınırlamalara sahiptir [8] [9].

Buluşun Amaçları ve Kısa Açıklaması

Mevcut buluş, bahsi geçen sınırlamaları ortadan kaldırmak ve ilgili teknik alana yeni avantajlar getirmek amacıyla çok taşıyıcılı sistemlere yönelik yeni anahtar üretimine ilişkin yöntemler ile ilgilidir.

Buluş, geleneksel anahtar üretim yöntemlerinin anahtar hızının geliştirilmesi oranını sunmaktadır.

Mevcut buluşta, çok taşıyıcılı sistemlerde kablosuz kanaldan gizli anahtar üretimine yönelik yeni algoritmalar, kablosuz iletişim sistemlerinde gizliliğin ve kimlik doğrulamasının sağlanması için önerilmektedir. Önerilen algoritmaların yeniliği, yalnızca literatürde geleneksel olarak yapıldığı gibi çok taşıyıcılı sistemin ortogonal (OFDM) alt kanallarının büyüklüklerinden değil, aynı zamanda en iyi kanal kazançlarına karşılık gelen çok taşıyıcı bloğun her bir alt bloğundaki alt kanalların sayısından ve dizinlerinden ve kanal kazançlarına karşılık gelen alt bloğun ortalamasının üzerinde olan her bir alt bloktaki alt kanalların sayısından rastgele gizli bitlerin üretimine dayanmaktadır. Önerilen algoritmalar, gizli anahtar üretimine yönelik ekstra boyutlar sağlanarak fiziksel katman anahtarı tabanlı algoritmaların genel performansını arttırabilmektedir. Gizli anahtar üretiminin önerilen algoritmalarının ayrıca zaman, alan, kod gibi diğer etki alanlarına ve bunların hibrit etki alanlarına uzatılmasını da içerdiği unutulmamalıdır. Bununla birlikte, konsepti açıklamak için frekans etki alanı ile ilgili ayrıntılar üzerinde durulacaktır.

Kablosuz iletişimin yayın yapısı, çekişmeli izinsiz dinlemelere ve müdahalelere karşı savunmasız hale getirmektedir. Mevcut kablosuz ağlarda, kablosuz iletişimin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamak amacıyla klasik şifreleme tabanlı teknikler, üst katmanlarda kullanılmaktadır [9].

Ancak bu teknikler, bu tür ağlarda gizli anahtarların kurulması, yönetimi ve dağıtımının karmaşıklığından dolayı beşinci nesil (5G) ve ötesi heterojen kablosuz ağlar için uygun olmayabilmektedir. Ayrıca, güçlü programlama cihazlarının geliştirilmesi ile bu şifreleme tabanlı teknikler, sofistike düşmanlara daha duyarlı hale gelmiştir. Geleneksel güvenlik tekniklerinin

karşılaştığı sorunları çözmek amacıyla, fiziksel katman anahtar üretimi, hem asimetrik hem simetrik şifreleme algoritmaları için bir verimli tamamlayıcı çözüm sağlamaktadır. Temel fikir, gizli anahtar üretimine yönelik temel rastgelelik kaynağı olarak iletişim kuran düğümler arasındaki kanal karşılıklılığı özelliğinden yararlanmaktır. Ayrıca bir zengin çok yollu saçılım ortamında izinsiz bir dinleyici, meşru düğümlerden yarım dalga boyu ayrı olması durumunda korelasyonsuz kanal ölçümlerini deneyimleyecektir. Böylelikle, Eve meşru düğümler tarafından ayıklananlara benzer anahtar bitlerini ayıklayamamaktadır. Ayrıca, kanaldan anahtar üretimi, dağıtımına ve yönetimine yönelik herhangi bir altyapıya ihtiyaç duymamaktadır [1].

Önerilen algoritmalar, geleneksel kriptografi tabanlı güvenlik çözümlerine bağlı kalmadan kablosuz iletişim sistemlerinin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamak için kullanılabilmektedir.

Önerilen algoritmanın amacı, geleneksel kriptografi tabanlı algoritmalar tarafından karşılaşılan sorunun çözülmesidir. Geleneksel kriptografi tabanlı çözümler, bu tür ağlarda gizli anahtarların kurulması, yönetimi ve dağıtımının karmaşıklığından dolayı beşinci nesil (5G) ve ötesi heterojen kablosuz ağlar için uygun olmayabilmektedir [3]. Buna ek olarak, güçlü programlama cihazlarının geliştirilmesi ile bu şifreleme tabanlı teknikler, sofistike düşmanlara daha duyarlı hale gelmektedir. Ayrıca, gelecek ağların; 5G-dokunsal internet, nesnelerin interneti (IoT), ULLRC, uzaktan ameliyat gibi yeni kablosuz teknolojileri desteklemesi gerekmektedir. Ancak, bu uygulamalarda kullanılan cihazların doğal olarak gücü sınırlı, işlemi kısıtlı ve gecikmeye duyarlıdır ve bu kriptografi tabanlı teknikler, bu tür teknolojiler için olanaksız kılmaktadır.

Geleneksel güvenlik tekniklerinin karşılaştığı sorunları çözmek amacıyla, fiziksel katman anahtar üretimi, hem asimetrik hem simetrik şifreleme algoritmaları için bir verimli tamamlayıcı çözüm sağlamaktadır. Temel fikir, gizli anahtar üretimine yönelik temel rastgelelik kaynağı olarak iletişim kuran düğümler arasındaki kanal karşılıklılığı özelliğinden yararlanmaktır.

Buluşun Avantajları;

- Önerilen algoritma, geleneksel kriptografi tabanlı yöntemler olmadan güvenlik sağlayabilmektedir ve böylelikle gelecek ağlara yönelik anahtar paylaşımı, dağıtımı ve yönetimi sorunlarını önlemektedir.

- Önerilen algoritma, gecikmeye duyarlı, gücü sınırlı ve işlemi kısıtlı hizmetler için uygun kılan daha basit sinyal işleme işlemlerini gerektirmektedir.
- Önerilen algoritma, geleneksel kriptografi tabanlı algoritmayı geliştirmek için kullanılabilmektedir.
- Ayrıca önerilen algoritmalar, kanal çok fazla değişmese bile anahtar üretimini sağlayacaktır.

Buluş, sanayileşme için uygulanabilir özelliktedir. Önerilen algoritmalar, geleneksel kriptografi tabanlı güvenlik çözümlerine bağlı kalmadan kablosuz iletişimin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamak için kullanılabilmektedir.

Referanslar

1 Alice

2 Bob

3 Eve

4 Alice-Bob (h_b)

5 Alice-Eve (h_e)

6 RIS

Buluşun Şekillerinin Tanımı

Şekiller, mevcut buluş tarafından geliştirileni daha fazla açıklamak için kullanılmıştır.

Şekil 1: Düşünülen güvenlik algoritmasına yönelik basitleştirilmiş bir sistem modeli

Şekil 2: Bob ve Eve (şeklin üst kısmında gösterilen) kanalının frekans yanıtlarına yönelik frekans dizinine (FI) karşılık gelen kanal büyüklüğü (CM)

Şekil 1'de:
Alice: bir meşru verici

Bob: bir meşru alıcı

Eve: bir izinsiz dinleyici (saldırgan)

Şekil 3: RIS ile düşünülen güvenlik algoritmasına yönelik basitleştirilmiş bir sistem modeli

Buluşun Ayrıntılı Açıklaması

Buluşun yeniliği, buluşun kapsamını sınırlamayan ve yalnızca buluşun konusunu açıklığa kavuşturmayı amaçlayan, frekans etki alanındaki spesifik örneklerle açıklanmıştır. Mevcut buluş, aşağıda ayrıntılı olarak açıklanmıştır.

Yeni fiziksel katman anahtar üretimi boyutlarına yönelik bir sistem: alt taşıyıcı sayısı ve dizin tabanlı anahtar üretimi olup, aşağıdakileri içermektedir; dizin tabanlı anahtar üretimi (IKG) veya birleşik dizin tabanlı anahtar üretimi (JIKG) veya sayı tabanlı anahtar üretimi (NKG) veya birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG) ve kanal tabanlı anahtarın rastgeleliğini arttırmak amacıyla kanal manipülasyonuna yönelik yeniden yapılandırılabilir akıllı yüzey (RIS).

Sistem modeli, zaman bölmeli çift yönlü kullanma (TDD) ile tek girdili tek çıktılı (SISO)-ortogonal frekans bölmeli çoklama (OFDM) kablosuz sistem olduğu varsayılmaktadır, burada meşru verici (Alice), Şekil 1'de gösterildiği gibi bir pasif izinsiz dinleyicinin (Eve) varlığında bir meşru alıcı (Bob) ile güvenli bir şekilde iletişim kurmaya çalışmaktadır. Alice-Bob (h_b) Bob-Alice (h_a) ve Alice-Eve (h_e) arasındaki kanalların dörtü yanıtlarının L üssel olarak bozulan dokunmalara sahip yavaş değişen Rayleigh sönümlü kanal olduğu varsayılmaktadır. Ayrıca karşılıklılık özelliği de benimsenmektedir, burada Alice'den Bob'a olan kanal, Bob'dan Alice'ye olan kanaldan tahmin edilebilmektedir. Buna ek olarak, konum ve ortam farklılıklarından dolayı hem Bob hem de Eve'nin farklı kanallar deneyimlediği varsayılmaktadır.

Çok taşıyıcılı sistemlerde kablosuz kanaldan gizli anahtar üretimine yönelik yeni boyutlar, kablosuz iletişim sistemlerinde gizliliğin ve kimlik doğrulamasının sağlanması için önerilmektedir. Önerilen algoritmaların yeniliği, yalnızca çok taşıyıcılı sistemin ortogonal (OFDM) alt kanallarının büyüklüklerinden değil, aynı zamanda en iyi kanal kazançlarına karşılık gelen çok taşıyıcı bloğun her bir alt bloğundaki alt kanalların sayısından ve dizinlerinden ve

kanal kazançlar, karşılık gelen alt bloğun ortalamasının üzerinde olan her bir alt bloktaki alt kanalların sayısından rastgele gizli bitlerin üretimine dayanmaktadır.

Özellikle, dizin tabanlı anahtar üretimi (IKG) veya birleşik dizin tabanlı anahtar üretimi (JIKG) veya sayı tabanlı anahtar üretimi (NKG) veya birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG) dahil dört anahtar üretimi yöntemi mevcut buluşta önerilmektedir. Ayrıca, statik ve ilişkili ortamda anahtar üretimi mekanizmasının RIS destekli geliştirilmesine yönelik bir yöntem de önerilmektedir.

Gizli anahtar üretiminde önerilen algoritmalar, ayrıca zaman, alan, şın, açılar, kod gibi diğer etki alanlarına ve bunların hibrit etki alanlarına uzatılmasını da içermektedir.

Önerilen Algoritmalar:

Örneğin dizin tabanlı anahtar üretimi (IKG) veya birleşik dizin tabanlı anahtar üretimi (JIKG) veya sayı tabanlı anahtar üretimi (NKG) veya birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG) gibi dört anahtar üretimi yöntemi mevcut buluşta önerilmektedir. Sonrasında, ayrıca statik ortamda anahtar üretiminin geliştirilmesine yönelik yeniden yapılandırılabilir akıllı yüzey (RIS) destekli yaklaşım da sunulmaktadır.

Ayrıntılar aşağıdaki gibidir:

Önerilen Algoritma 1: Dizin tabanlı anahtar üretimi (IKG)

IKG (dizin tabanlı anahtar üretimi) algoritmasına yönelik temel adımlar, aşağıdaki gibi olmaktadır:

1) Birinci adımda, Alice ve Bob, kanalı tahmin etmek için kanalın uyumluluk süresi içinde birbirine pilot sinyalleri göndermektedir. Frekans etki alanındaki herhangi düğümdeki (Alice/Bob) tahmin edilen kanal, **"H"** şeklinde verilebilmektedir.
2) Herhangi bir düğümde elde edilen diyagonal kanal matrisi (**H**), rastgele serpiştirici (**R**) ile çarpılmaktadır ve ortaya çıkan vektör, $\boldsymbol{h_f}$ = diyagonal (**HR**) şeklinde verilebilmektedir. Serpiştirme işleminin, OFDM bloğunun tamamı üzerinde alt kanal tekdüzeliğinin derin

sönümlemeleri dağıtmak ve bunlar Şekil 2'de sunulduğu gibi rastgele ve korelasyonsuz görünmelerini sağlamak için kullanıldığı unutulmamalıdır.

3) Daha sonra, bütün h_f vektörleri her bir alt bloktaki "n" ögesine sahip(h_f), **G** alt bloklarına bölünmektedir, burada $h_f = [h_1, \ldots\ldots, h_G]$, $h_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$. olmaktadır.

4) Bir sonraki adımda, her bir alt bloğun ögelerinin mutlak değerleri, $|h_{\beta,1}|$ şeklinde hesaplanmaktadır ve burada $h_{\beta,j}$, h_β alt bloğunun j'inci ögesidir.

5) Daha sonra, en güçlü alt taşıyıcıların sayısı m_β , $|h_{\beta,j}|$ değerlerine dayanarak her bir h_β alt bloğunda seçilmektedir (veya özellikle meşru düğümlerde alt taşıyıcıların sinyal - gürültü oranına (SNR) göre).

6) Son olarak, seçilen alt taşıyıcıların pozisyonları/dizinleri, bir arama tablosu kullanılarak anahtar bitleri üretmek için kullanılmaktadır. Arama tablosu, dizinlerin pozisyonlarını anahtar bitlerine eşlemektedir. Tablo I'de, bir arama tablosu örneği, n = 4, m_β=2'ye yönelik Tablo I'de sunulmaktadır. Tablo I'deki ilk sütun, h_β alt bloğundaki m_β en güçlü alt taşıyıcıları göstermektedir, ikinci sütun, en güçlü alt taşıyıcıların pozisyonunu/dizinlerini göstermektedir ve üçüncü sütun ise bu dizinlere karşılık gelen üretilen anahtar bitlerini göstermektedir. Herhangi bir OFDM bloğunda üretilen anahtar bitlerinin toplam sayısı, m_β, n, N, ve G'nin bir fonksiyonu olmaktadır, burada G, h_f'deki alt blokların sayısıdır ve her bir alt blokta "n" ögesi bulunmaktadır ve N ise toplam alt taşıyıcı sayısıdır.

IKG'yi daha fazla açıklığa kavuşturmak için, aşağıdaki örnek göz önünde bulundurulmaktadır. N = 128, m_β = 2, ve n = 4 olduğunu varsayalım. Daha sonra, h_f, $G = \frac{N}{n}$ = 128/4 = 32 alt bloğuna bölünmektedir. Her alt blokta, m_β = 2 en güçlü alt taşıyıcıları seçilmektedir. Sonrasında, her bir alt bloğa yönelik bu alt taşıyıcıların pozisyonları, Tablo I kullanılarak anahtar bitleri üretmek için eşlenmektedir. OFDM bloğu tarafından üretilen anahtar bitlerinin toplam sayısı, IKG algoritması için 64'tür.

Alt bloklar	Dizinler	Anahtar bitleri
$[\lvert h_{g,1}\rvert\ 0\ 0\ \lvert h_{g,4}\rvert]$	{1, 4}	[0 0]
$[0\ \lvert h_{g,2}\rvert\ 0\ \lvert h_{g,4}\rvert]$	{2, 4}	[0 1]
$[\lvert h_{g,1}\rvert\ 0\ \lvert h_{g,3}\rvert\ 0]$	{1, 3}	[1 0]
$[0\ \lvert h_{g,2}\rvert\ \lvert h_{g,3}\rvert\ 0]$	{2, 3}	[1 1]

Tablo I: m_g = 2 VE n=4'e YÖNELİK IKG ALGORİTMASINA İLİŞKİN ARAMA TABLOSU

Önerilen Algoritma 2: Birleşik dizin tabanlı anahtar (JIKG) üretimi

IKG'nin anahtar hızını daha fazla arttırmak için, bir JIKG yaklaşımı önerilmektedir. JIKG yaklaşımında, alt taşıyıcıların hem dizinleri hem de genlikleri/fazları kullanılarak bitler üretilmektedir. JIKG'nin ilk dört adımı (1, 2, 3, 4) IKG algoritmasına benzerdir. Beşinci adımda, ilk olarak, anahtar bitleri, IKG'nin beşinci adımına benzer h_g alt bloğunun dizinlerinden üretilmektedir.

Sonrasında, alt blok ögesinin mutlak değerlerinin ortalaması, aşağıdaki gibi hesaplanmaktadır

$$av_g = \frac{\sum_{j=1}^{n} \lvert h_{g,j}\rvert}{n}$$

burada $g \in \{1, \ldots, G\}$ olmaktadır. Son olarak, h_g alt bloğunun her bir ögesi, gizli anahtar bitleri üretmek için ortalama, av_g ile karşılaştırılmaktadır. $\lvert h_{g,j}\rvert \geq av_g$ olması halinde, anahtar biti olarak 1 üretilmektedir, aksi takdirde 0 üretilmektedir. Bu nedenle, JIKG tabanlı yaklaşım, hem dizinlerden hem genliklerden yararlanılarak daha yüksek anahtar hızı oranı sağlamaktadır.

Örneğin, N = 128, $m_g = 2$, n = 4 olması durumunda ve arama Tablosu I kullanılarak, OFDM bloğu tarafından üretilen bitlerin toplam sayısı, JIKG algoritması için 192 olmaktadır.

Önerilen Algoritma 3: Sayı tabanlı anahtar üretimi (NKG)

IKG'nin anahtar hız oranını daha fazla geliştirmek için, ayrıca bir NKG yaklaşımı da önerilmektedir. NKG yaklaşımında, kanal kazançları, alt bloğun ortalamasının üzerinde olan çok taşıyıcılı bloğun her bir alt bloğundaki alt kanalların sayısı/sayımı, anahtar üretimi için kullanılmaktadır.

NKG'nin ilk dört adımı (1, 2, 3, 4) IKG algoritmasına benzerdir. Beşinci adımda, alt blok ögesinin mutlak değerlerinin ortalaması, aşağıdaki gibi hesaplanmaktadır

$$av_g = \frac{\sum_{j=1}^{n} |h_{g,j}|}{n}$$

Sonrasında, h_g alt bloğunun her bir ögesi, ortalama, av_g ile karşılaştırılmaktadır ve ortalamanın üzerinde olan alt taşıyıcıların sayısı, her bir alt taşıyıcı için sayılmaktadır. Son olarak, kanal kazançları, av_g üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına dayalı Tablo II kullanılarak meşru düğümlerde bir gizli anahtar üretilmektedir. Tablo II'deki birinci sütun, kanal kazançları, av_g üzerinde olan h_g alt bloğundaki en güçlü alt taşıyıcıları göstermektedir, ikinci sütun, bu alt taşıyıcıların sayısını göstermektedir ve üçüncü sütun ise bu dizinlere karşılık gelen üretilen anahtar bitlerini göstermektedir.

Örneğin, N = 128, n = 4 olması durumunda ve arama Tablosu II kullanılarak, OFDM bloğu tarafından üretilen bitlerin toplam sayısı, NKG algoritması için 64 olmaktadır.

Alt bloklar	Aktif alt taşıyıcıların sayısı	Anahtar bitleri
[$\|h_{g,1}\|$ 0 0 0]	{1}	[0 0]
[$\|h_{g,1}\|$ $\|h_{g,2}\|$ 0 0]	{2}	[0 1]
[$\|h_{g,1}\|$ $\|h_{g,2}\|$ $\|h_{g,3}\|$ 0]	{3}	[1 0]

$[\lvert h_{g,1}\rvert \ \lvert h_{g,2}\rvert \ \lvert h_{g,3}\rvert \ \lvert h_{g,4}\rvert]$	{4}	[1 1]

Tablo II: m= 2 BİTLERİ VE n=4'e YÖNELİK IKG ALGORİTMASINA İLİŞKİN ARAMA TABLOSU

NKG'nin anahtar hız oranını daha fazla geliştirmek için, alt kanalların sayısı, genlik/faz tabanlı anahtar üretimi yaklaşımı ile kullanılmaktadır. Örneğin, N = 128, n = 4 olması durumunda ve arama Tablosu II kullanılarak, bir OFDM bloğundaki genlik/faz tabanlı anahtar kullanımıyla birlikte NKG tarafından üretilen bitlerin toplam sayısı, 192 olmaktadır.

Önerilen Algoritma 4: Birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG)

NKG'nin anahtar hızını daha fazla arttırmak için, bir JNIKG yaklaşımı önerilmektedir. JNIKG yaklaşımında, bitler, alt taşıyıcıların genlikleri/fazlarıyla birlikte alt taşıyıcıların sayısı ve pozisyonları kullanılarak üretilmektedir.

JNKG'nin ilk dört adımı (1, 2, 3, 4) IKG algoritmasına benzerdir. Beşinci adımda, alt blok ögesinin mutlak değerlerinin ortalaması, aşağıdaki gibi hesaplanmaktadır

$$av_g = \frac{\sum_{j=1}^{n} \lvert h_{g,j}\rvert}{n}$$

Sonrasında, h_g alt bloğunun her bir ögesi, ortalama, av_g ile karşılaştırılmaktadır ve ortalamanın üzerinde alt taşıyıcıların sayısı, her bir alt taşıyıcı için sayılmaktadır. Son olarak, kanal kazançları, av_g üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına ve pozisyonlarına dayalı Tablo III kullanılarak meşru düğümlerde bir gizli anahtar bitleri üretilmektedir. Tablo III'ün birinci sütununun kanal kazançları ilgili alt bloğun ortalamasının üzerinde olan çok taşıyıcılı bloğun her bir alt bloğundaki alt taşıyıcıyı gösterirken, ikinci sütunun bunların sayısını gösterdiği unutulmamalıdır. Üçüncü sütun, sayı ile üretilen anahtar bitlerini gösterirken dördüncü sütun ise dizinlere karşılık gelen anahtar bitlerini göstermektedir.

Son olarak, h_g alt bloğunun her bir ögesi, gizli anahtar bitleri üretmek için ortalama, av_g ile karşılaştırılmaktadır. $|h_{g,j}| \geq av_g$ olması halinde, anahtar biti olarak 1 üretilmektedir, aksi takdirde 0 üretilmektedir. Bu nedenle, JIKG tabanlı yaklaşım, hem dizinlerden hem genliklerden yararlanılarak daha yüksek anahtar hızı oranı sağlamaktadır.

Örneğin, N = 128, n = 4 olması durumunda ve arama Tablosu III kullanılarak, OFDM bloğu tarafından üretilen bitlerin toplam sayısı, JINKG algoritması için 256 olmaktadır.

Kanal de-korelasyonu varsayımından dolayı, önerilen tüm algoritmalara yönelik meşru ve gayri meşru düğümlerde üretilen anahtar bitleri farklı olacaktır. Bunun nedeni, gayri meşru düğümün meşru düğüm ile aynı anahtar üretimini uygulamasına rağmen, meşru düğüme kıyasla farklı kanal yanıtlarından dolayı ortaya çıkan anahtar bitlerinin farklı olmasıdır.

Alt bloklar	Sayı	Sayıya göre anahtar	Dizinlere göre anahtar
$[\|h_{g,1}\|\ 0\ 0\ 0]$	1	[0 0]	[0 0]
$[0\ \|h_{g,2}\|\ 0\ 0]$	1	[0 0]	[0 1]
$[0\ 0\ \|h_{g,3}\|\ 0]$	1	[0 0]	[1 0]
$[0\ 0\ 0\ \|h_{g,4}\|]$	1	[0 0]	[1 1]
$[\|h_{g,1}\|\ \|h_{g,2}\|\ 0\ 0]$	2	[0 1]	[0 0]
$[h_{g,1}\ 0\ h_{g,3}\ 0]$	2	[0 1]	[0 1]
$[\|h_{g,1}\|\ 0\ 0\ \|h_{g,4}\|]$	2	[0 1]	[1 0]
$[\|h_{g,1}\|\ \|h_{g,2}\|\ 0\ 0]$	2	[0 1]	[1 1]
$[\|h_{g,1}\|\ \|h_{g,2}\|\ \|h_{g,3}\|\ 0]$	3	[1 0]	[0 0]
$[\|h_{g,1}\|\ 0\ \|h_{g,3}\|\ \|h_{g,4}\|]$	3	[1 0]	[0 1]
$[\|h_{g,1}\|\ \|h_{g,2}\|\ 0\ \|h_{g,4}\|]$	3	[1 0]	[1 0]

[0 $\|h_{\beta,2}\|$ $\|h_{\beta,3}\|$ $\|h_{\beta,4}\|$]	3	[1 0]	[1 1]
[0 0 0 0]	0	[1 1]	[0 0]
[0 0 $\|h_{\beta,3}\|$ $\|h_{\beta,4}\|$]	2	[1 1]	[0 1]
[0 $\|h_{\beta,2}\|$ $\|h_{\beta,3}\|$ 0]	2	[1 1]	[1 0]
[$\|h_{\beta,1}\|$ $\|h_{\beta,2}\|$ $\|h_{\beta,3}\|$ $\|h_{\beta,4}\|$]	4	[1 1]	[1 1]

TABLO III: n=4'e YÖNELİK JINKG ALGORİTMASINA İLİŞKİN ARAMA TABLOSU

Yukarıdaki bilgilere dayanarak, çok taşıyıcılı sistemlere yönelik yeni anahtar üretimine ilişkin yöntemler, aşağıda ayrıntılı olarak sunulmaktadır.

Buluş, dizin tabanlı anahtar üretimi (IKG) veya birleşik dizin tabanlı anahtar üretimi (JIKG) veya sayı tabanlı anahtar üretimi (NKG) veya birleşik sayı ve dizin tabanlı anahtar üretimi (JNIKG) dahil dört anahtar üretimi yöntemini mevcut buluşta önermektedir.

Ayrıntılar, aşağıdaki gibi özetlenebilmektedir:

Bir dizin tabanlı anahtar üretimi yöntemleri önerilmektedir ve burada yöntem, aşağıdakileri içermektedir;

1) Alice (meşru verici) ve Bob (meşru alıcı) tarafından **H** olarak, frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,
2) Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ile çarpılması ve ortaya çıkan vektör, $\boldsymbol{h_f}$ = diyagonal (**HR**) şeklinde verilebilmektedir,
3) Bütün $\boldsymbol{h_f}$ vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $\boldsymbol{h_f = [h_1, \ldots\ldots, h_G]}$, $\boldsymbol{h_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]}$, $\boldsymbol{G = N/n}$, ve $\boldsymbol{\beta \epsilon \{1, \ldots\ldots, G\}}$ olmaktadır,

4) Her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,j}|$ şeklinde hesaplanması, burada $h_{\beta,j}$, h_{β} alt bloğunun j'inci ögesi olmaktadır,

5) $|h_{\beta,j}|$ değerlerine dayanarak veya özellikle meşru düğümlerdeki alt taşıyıcıların sinyal-gürültü oranına (SNR) göre her bir h_{β} alt bloğundaki en güçlü alt taşıyıcıların sayısının m_{β} seçilmesi,

6) Son olarak, dizinlerin anahtar bitlerine olan pozisyonuna yönelik bir eşleme tablosu olan arama Tablosu I'e dayanarak anahtar bitlerinin üretilmesine yönelik seçilen alt taşıyıcıların pozisyonlarının/dizinlerinin kullanılması.

IKG'nin anahtar hızını daha fazla arttırmak için, bir JIKG yaklaşımı (yöntemi) olup;

1) Alice (meşru verici) ve Bob (meşru alıcı) tarafından herhangi düğümde **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,

2) Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ile çarpılması ve ortaya çıkan vektör, h_f = diyagonal (**HR**) şeklinde verilebilmektedir,

3) Bütün h_f vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesiyle burada $h_f = [h_1, \ldots\ldots, h_G]$, $h_{\beta} = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$ olmaktadır,

4) Her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,j}|$ şeklinde hesaplanması, burada $h_{\beta,j}$, h_{β} alt bloğunun j'inci ögesi olmaktadır,

5) Arama Tablosu I kullanılarak h_{β} alt bloğunun dizinlerinden anahtar bitlerinin üretilmesi

6) Alt blok ögesinin mutlak değerlerinin ortalamasının, aşağıdaki gibi hesaplanması:

$$av_{\beta} = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n} \quad \text{burada } \beta \epsilon \{1, \ldots\ldots, G\},$$

7) $|h_{\beta,j}| > av_\beta$ olması durumunda anahtar biti olarak 1 üretimi, aksi takdirde 0 üretimi olacak şekilde gizli anahtar bitleri üretmek amacıyla h_β alt bloğunun her bir ögesinin ortalaması, av_β ile karşılaştırılması.

IKG'nin anahtar hızını daha fazla arttırmak için, bir NKG yaklaşımı (yöntemi) olup;

1) Alice (meşru verici) ve Bob (meşru alıcı) tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanalı tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,
2) Herhangi düğümdeki elde edilen diyagonal kanal matrisinin (**H**) bir rastgele serpiştirici (**R**) ile çarpımı,
3) Bütün h_f vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $h_f = [h_1, \ldots\ldots, h_G]$, $h_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$ olmaktadır,
4) Her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,j}|$ şeklinde hesaplanması, burada $h_{\beta,j}$, h_β alt bloğunun j'inci ögesi olmaktadır,
5) Alt blok ögesinin mutlak değerlerinin ortalamasının hesaplanması, aşağıdaki gibidir:

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n},$$

6) Sonrasında, h_β alt bloğunun her bir ögesi, ortalama, av_β ile karşılaştırılmaktadır ve ortalamanın üzerinde alt taşıyıcıların sayısı, her bir alt taşıyıcı için sayılmaktadır.
7) Son olarak, kanal kazançları, av_β üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına/sayımına dayanarak arama Tablosu II kullanılarak meşru düğümlerde gizli anahtarın üretimi. Tablo II'nin birinci sütununun kanal kazançları ilgili alt bloğun ortalamasının üzerinde olan çok taşıyıcılı bloğun her bir alt bloğundaki alt taşıyıcıyı gösterirken, ikinci sütunun bunların sayısını gösterdiği ve üçüncü sütunun üretilen bitleri gösterdiği unutulmamalıdır.

NKG'nin anahtar hızını daha fazla arttırmak için, bir JNIKG yaklaşımı (yöntemi) sunulmaktadır;

1) Alice (meşru verici) ve Bob (meşru alıcı) tarafından **H** olarak frekans etki alanında herhangi düğümdeki kanal tahmin etmek amacıyla kanalın tutarlılık süresi içinde pilot sinyallerin birbirine gönderilmesi,
2) Herhangi bir düğümde elde edilen diyagonal kanal matrisinin (**H**), rastgele serpiştirici (**R**) ve h_f = diyagonal (**HR**) olarak elde edilen vektörün, çarpım,
3) Bütün h_f vektörünün, her bir alt bloktaki "n" ögeye sahip **G** alt bloklarına bölünmesi burada $h_f = [h_1, \ldots\ldots, h_G]$, $h_\beta = [h_{\beta,1}, \ldots\ldots, h_{\beta,n}]$, $G = N/n$, ve $\beta \epsilon \{1, \ldots\ldots, G\}$ olmaktadır,
4) Her bir alt bloğun ögelerinin mutlak değerlerinin, $|h_{\beta,j}|$ şeklinde hesaplanması, burada $h_{\beta,j}$, h_β alt bloğunun j'inci ögesi olmaktadır,
5) Alt blok ögesinin mutlak değerlerinin ortalamasının hesaplanması, aşağıdaki gibidir:

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n},$$

6) h_β alt bloğunun her bir ögesinin, ortalama, av_β ile karşılaştırılması ve ortalamanın üzerinde olan alt taşıyıcıların sayısı, her bir alt taşıyıcı için sayılmaktadır. Sonrasında, kanal kazançları, av_β üzerinde olan her bir alt bloktaki alt taşıyıcıların sayısına ve pozisyonlarına dayalı Tablo III kullanılarak meşru düğümlerde gizli anahtar bitleri üretilmektedir.
7) Son olarak, $|h_{\beta,j}| > av_\beta$ olması durumunda anahtar biti olarak 1 üretimi, aksi takdirde 0 üretimi olacak şekilde farklı alt taşıyıcıların genliklerinden gizli anahtar üretmek amacıyla h_β alt bloğunun her bir ögesinin ortalama, av_β ile karşılaştırması yapılmaktadır.

RIS destekli manipülasyon kullanılarak bahsi geçen yaklaşımlara (IKG, JIKG, NKG, ve JNIKG) yönelik önerilen geliştirme: RIS destekli yöntem, tüm yöntemlerin performansını arttırabilecek bir küçük uzantı veya eklenti olmaktadır. Bu, pilot sinyali iletimi esnasında olabilmektedir (bahsi geçen tekniklerin birinci adımı)

Genellikle, daha önceden açıklanan bir kanal tabanlı gizli anahtar üretimi yaklaşımları (IKG, JIKG, NKG ve JNIKG), özellikle uzun tutarlılık süresine sahip olunmasından dolayı kanalda çok fazla rastgelelik veya varyasyonun olmadığı statik ortamlar veya yetersiz saçılım bakımından çok zorlu bir görev olmaya devam etmektedir [9]. Daha az varyasyona sahip daha statik kanal, yeterli uzunluğa sahip şifreleme anahtarları üretmek için yeterli olmayabilmektedir. Günümüzde, akıllı ve kontrol edilebilir kablosuz ortam sağlama yetenekleri sayesinde yeniden yapılandırılabilir akıllı yüzey (RIS) çok fazla dikkat çekmiştir [10]. Ancak, kanal tabanlı anahtar üretimi bakımından kullanılmamıştır.

Buluşun önerilen fikri, kanal tabanlı anahtar bitlerinin rastgeleliğini geliştirmek için kanal manipülasyonu için RIS'in kullanılmasıdır. Daha spesifik olarak, RIS'teki her bir eleman, kanalın zenginliğinin arttırılması ve aynı zamanda Şekil 3'te sunulduğu gibi kanal tabanlı gizli anahtarın rastgeleliğinin arttırılması bakımından **pilot sinyal iletimi esnasında (bahsi geçen tekniklerin birinci adımı)** etkili kanalı manipüle etmek amacıyla rastgele faza ve/veya genliğe sahip gelen sinyali yansıtmak için kontrol edilecektir.

Buluş yapılandırılırken RIS; IKG, JIKG, NKG ve JNIKG yöntemlerinin ilk adımında kullanılmıştır.

Ayrıca, Bob ve Eve ile ilişkili kanal durumunda, RIS, vericiden alıcıya bir alternatif ve bağımsız yol sağlayarak güvenli anahtar üretimini sağlamak için kullanılacaktır.
Son olarak, anahtar üretimi ayrıca yetersiz saçılım ortamı durumunda RIS destekli işaret biçimlendirme kullanılarak; farklı işaretin genişliğine ve farklı işaretin yönelimlerine sahip farklı işaretler üreterek geliştirilebilmektedir. Önerilen kanal tabanlı manipülasyon ayrıca diğer algoritmalar için de kullanılabilmektedir.

REFERANSLAR

[1] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," IEEE Wireless Commun., vol. 26, no. 5, pp. 48–54, 2019.

[2] J. M. Hamamreh, E. Basar, and H. Arslan, “OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services,” IEEE Access, vol. 5, pp. 25 863–25 875, 2017.

[3] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” IEEE Commun. Magazine, vol. 53, no. 6, pp. 33–39, 2015.

[4] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in Proc. IEEE INFOCOM, April 2013, pp. 3048–3056.

[5] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 5, pp. 1484–1497, 2012.

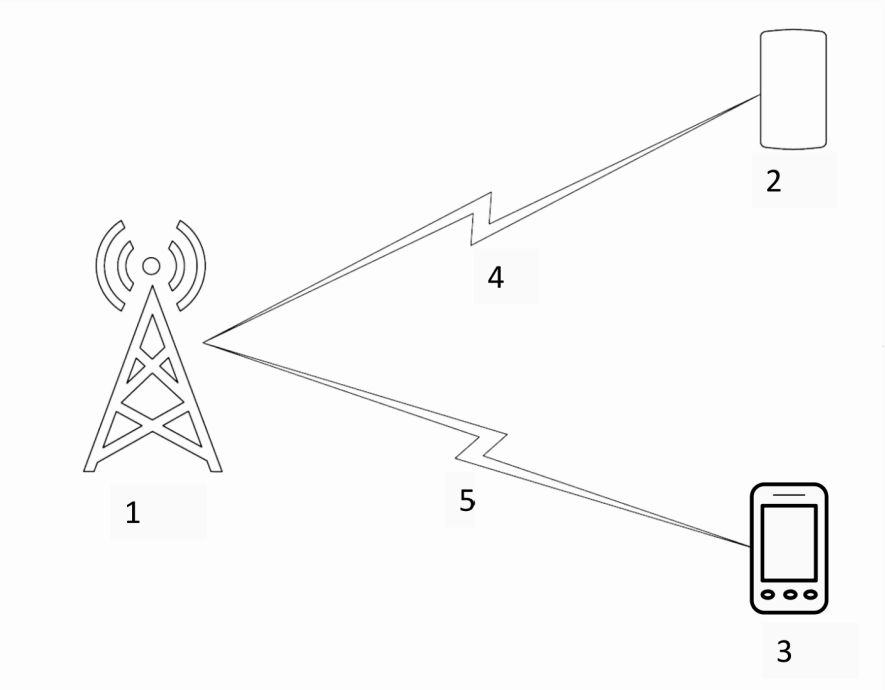
[6] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,” in Proc. IEEE INFOCOM, Apr 2011, pp. 1422–1430.

[7] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, “Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

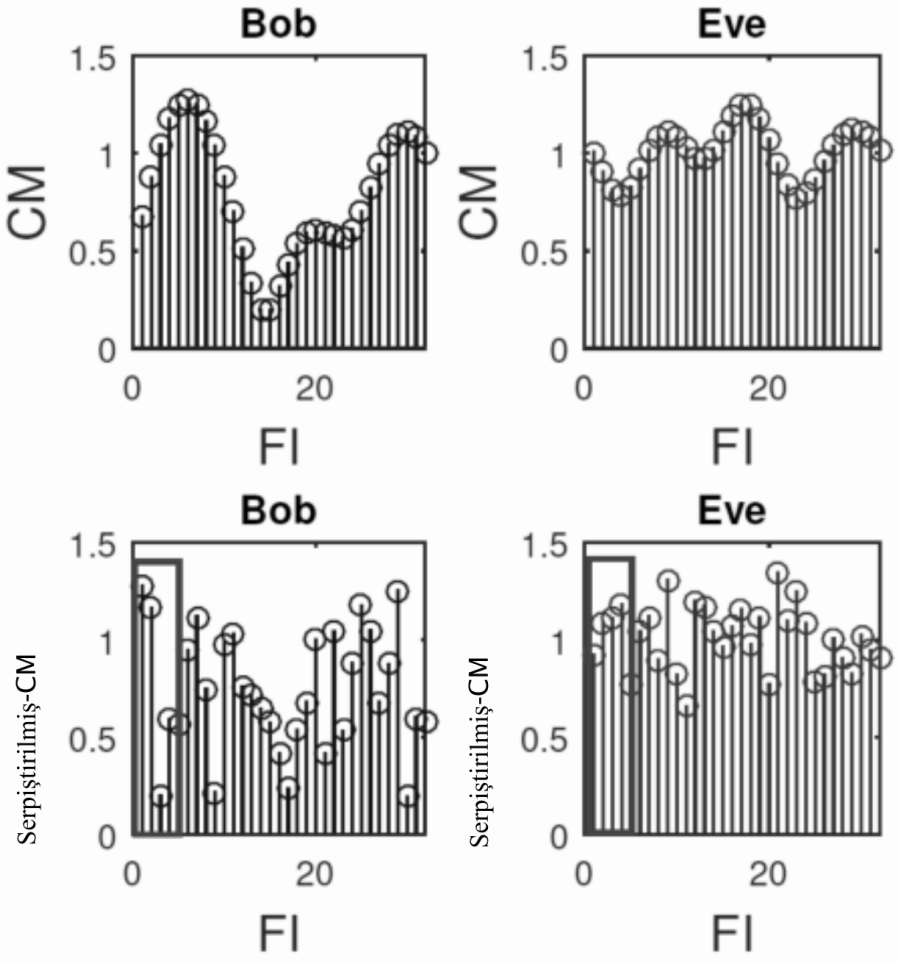
[8] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” IEEE Access, vol. 4, pp. 614–626, 2016.

[9] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1773–1828, 2019.

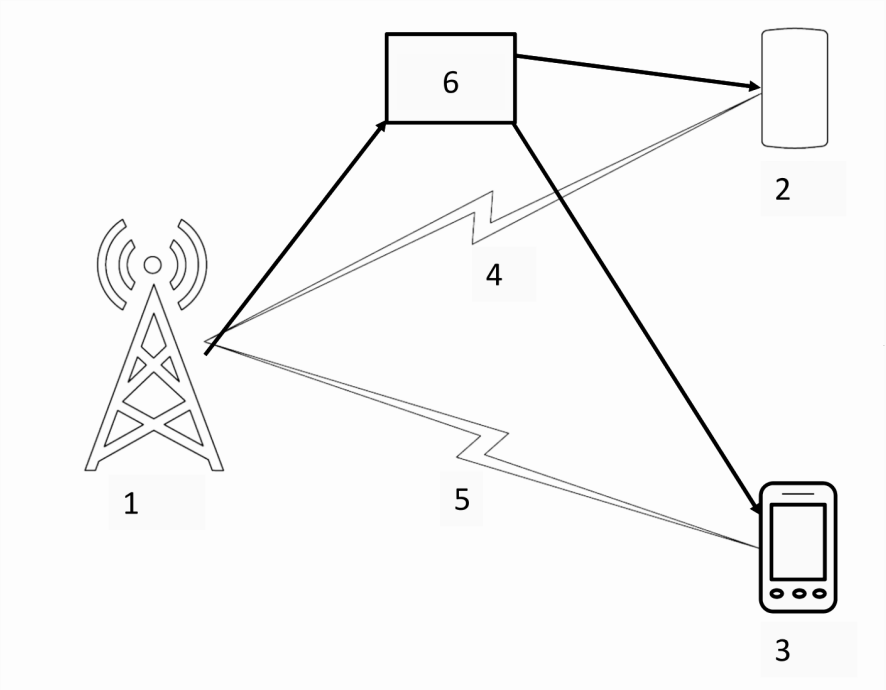
[10] A. Almohamad et al., "Smart and Secure Wireless Communications via Reflecting Intelligent Surfaces: A Short Survey," in IEEE Open Journal of the Communications Society, vol. 1, pp. 1442-1456, 2020, doi: 10.1109/OJCOMS.2020.302373



Şekil 1



Şekil 2



Şekil 3

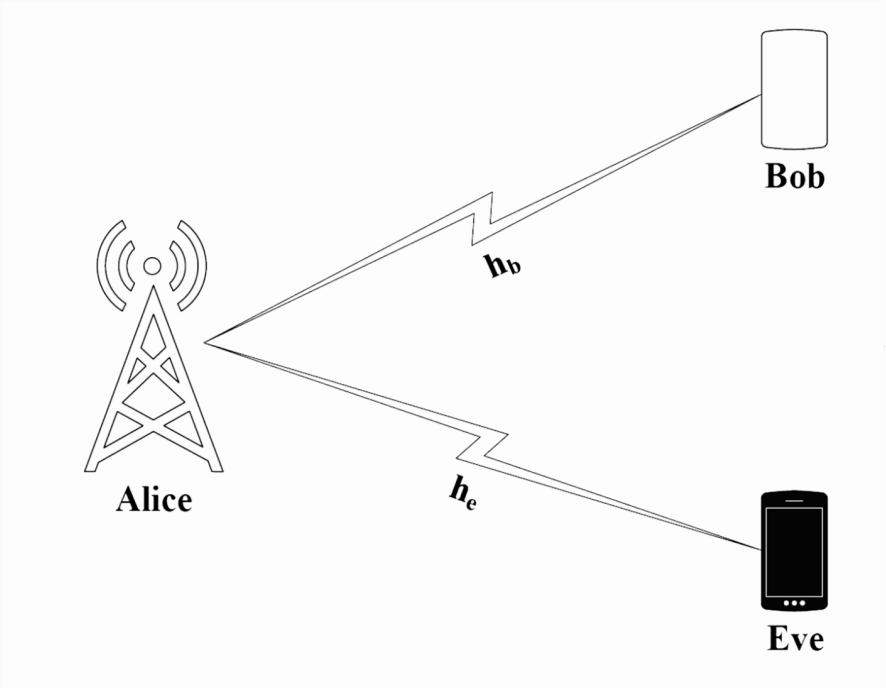


Figure 1

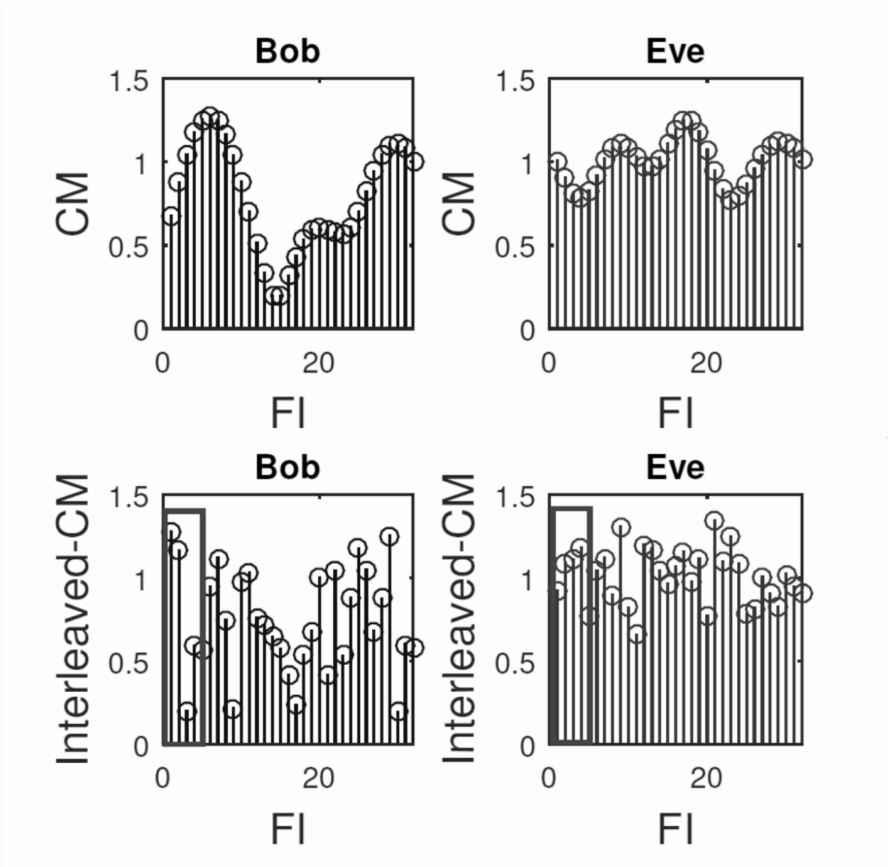


Figure 2

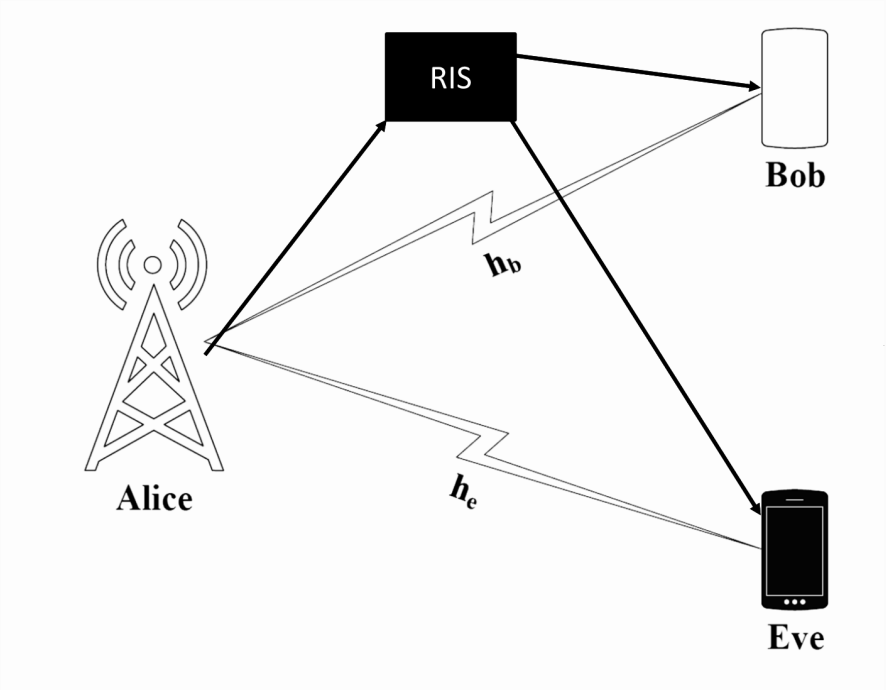


Figure 3