ÖZET

GÜVENLİ HABERLEŞME YÖNTEMİ

Buluş, bir gizli anahtar üretim tekniğini içeren bir güvenli haberleşme yöntemi için bir yöntem sağlamayı hedeflemektedir. Kanal içine bir yapay bileşenin dahil edilmesiyle bir kanalın yönlendirilmesinden sonra, önerilen yöntemin yeniliği, kanal-uyumlu anahtarlar kullanılarak fiziksel katman güvenliğinin (PHY) geliştirilmesinden kaynaklanmaktadır. Bir uyumlu şekilde tasarlanan yapay bileşen, geçerli kullanıcı kanalı ile basamaklanmaktadır. Bir ortogonal frekans bölmeli çiftleme (OFDM) sisteminde, bir eşik değerden daha yüksek bir kanal alımına karşılık gelen alt taşıyıcılar anahtarların çıkartılması için seçilmektedir. Seçilen alt taşıyıcıların sayısı uyarlanır olduğundan dolayı, üretilen anahtar sekansların uzunluğu, ayrıca uyarlanır şekilde değişmektedir. Dolayısıyla, bir zaman bölmeli çiftleme (TDD) sisteminde kanal karşılıklılık özelliği kullanılabilmektedir.

(Şekil 3)

İSTEMLER

1. Güvenli bir haberleşme yöntemi olup, burada alıcı (B) kanal tahmini için bir referans sinyalini (s_{ref}) vericiye (A) göndermektedir ve burada N, karmaşık veri sembollerinin toplam sayısına karşılık gelmektedir; söz konusu yöntem, aşağıdaki adımları içermesi ile karakterize edilmektedir:

a. Verici (A) ve alıcı (B) arasında frekans seçici kanaldan m sayıda pik-noktaları dışında birinci m noktasının seçilmesi, burada noktalar alt taşıyıcılara karşılık gelmektedir ve burada $M < N$,

b. Seçilen m noktalarının kullanılmasıyla yapay bir kanalın,$F_b \in \mathbb{C}^{Nx1}$, oluşturulması,

c. $H_b = A_b \odot F_b$ olarak yapay kanal (F_b) ile alıcı (B) kanalının, $A_b \in \mathbb{C}^{Nx1}$ basamaklanmasıyla yeni bir kanalın, $H_b \in \mathbb{C}^{Nx1}$, oluşturulması,

d. Basamaklanan kanaldan, H_b, pik noktalarının seçilmesi,

e. Alımlarının bir ikili anahtarın üretilmesi için verici (A) ve alıcı (B) ile basamaklanan kanaldan pik noktalarına karşılık geldiği seçilen alt taşıyıcıların nicemlenmesi,

f. İkili anahtarın bir karmaşık anahtara dönüştürülmesi,

g. Karmaşık anahtarın N'nin en yakın çoğaltmasına yeniden biçimlendirilmesi.

2. Anahtarların çıkartılması için verici (A) tarafından dikkate alınan, alım kanalının (G) basamaklanan kanaldan, H_b, tüm frekans indislerinin (f) ortalama üstü alımı (G) olduğu, M sayıda pik-noktasının seçildiği, İstem 1'e göre güvenli haberleşme yöntemi.

3. Son anahtar bloğunun uzunluğunun N'den az olması durumunda, başlıktan anahtar numunelerinin karmaşık anahtarın yeniden biçimlendirilmesi için bir sonek olarak ilave edildiği, İstem 1'e göre güvenli haberleşme yöntemi.

4. Karmaşık anahtarın yeniden biçimlendirilmesinden sonra, iletilen sinyalin, x, $y_b = h_b * x + n_b$; olarak zaman-alan şifreli sembollere döngüsel sonekin (CP) uygulanmasıyla alıcıya (B) gönderildiği; y_b'nin alıcıda (B) alınan sinyal olduğu, h_b'nin zaman-alanda basamaklanan kanal olduğu ve n_b'nin alıcı (B) tarafında sıfır ortalamalı karmaşık toplanır beyaz Gauss gürültüsü (AWGN) olduğu, İstem 1'e göre güvenli haberleşme yöntemi.

TARİFNAME

GÜVENLİ HABERLEŞME YÖNTEMİ

Teknik Alan

Mevcut buluş, fiziksel katman güvenliğinin geliştirilmesine yönelik bir haberleşme yöntemi ile ilgilidir. Bu buluşta, bir kablosuz kanala bağlı olarak gizli anahtarların oluşturulmasına yönelik yeni bir yöntem önerilmektedir.

Önceki Teknik

Kablosuz iletimin yayın doğası, pasif bir gizli dinleyici varlığında geçerli verici ve alıcı arasındaki haberleşmeye yönelik hassasiyete neden olmaktadır. 5G'de ve kablosuz ağların haricinde büyük bir gelişme olduğundan, klasik şifreleme teknikleri güvenliğin garanti edilmesi için yeterince elverişli olmayabilmektedir. Rastlantısal kanalların karakteristiklerin kullanılmasıyla anahtarlar üreten teknikler, problemin üstesinden gelinmesi için geliştirilmelidir.

Ren K. ve ark (2011), Zeng K. (2015), Zhang J. ve ark. (2016) ve Hamamreh J. M. ve ark. (2018)'ı kapsayan çoğu çalışmaya göre, kanal-tabanlı güvenlik yöntemlerinin yenilikçi kavramının biri, geçerli verici ve alıcı arasında kanalın karakteristiklerinin ortaya çıkartılmasıyla gizli anahtarları üretirken, gizli veri içeriğine kulak misafirlerinin erişmesini önlemektedir. Badawy A. ve ark. (2016), kanal-tabanlı anahtar üretim tekniklerinin kanal karşılıklılığının varsayımına ağırlıklı olarak bağlı olduğunu belirtmektedir.

Zaman bölmeli çiftleme (TDD) haberleşme sisteminde, karşılıklılık özelliği, kanalın her iki ucunda aynı bağlantının gözlemlenmesinden dolayı geçerli taraflar için yüksek oranda yeniden biçimlendirilmiş anahtarların üretilmesine olanak sağlamaktadır. Ayrıca, Zhang J. ve ark. (2016), bir anahtar üretim sisteminin, rastlantısallığın performans ölçüleri, anahtar uyuşmazlık oranı (KDR), ve anahtar üretim oranının (KGR) düşünülmesiyle değerlendirilmelidir. Ayrıca, Zhang J., Marshall A. ve ark. (2016), üretilen bir anahtar sekansı için çok önemli bir karakteristik olarak rastlantısallığı kabul etmektedir.

Bir rastlantısal anahtar, pasif gizli dinleyici saldırıları varlığında güvenli bir şifrelemeyle ilgili sistem sağlayacaktır. KDR, toplam anahtarın uzunluğuna her geçerli taraf tarafından üretilen

anahtarlar arasında farklı bitlerin oranını göstermektedir. Buna ek olarak, KGR, her ölçümde üretilen anahtar bitlerinin niceliğini tanımlamaktadır.

Gizli anahtar üretiminde KGR'nin arttırılmasına yönelik, Li G. ve ark. (2016), OFDM tekniğinin kullanılması önermektedir. Yasal kullanıcı kanalının rastlantısallığının ortaya çıkartılması, Li G. ve ark. (2017)'de önerildiği gibi, anahtar kırılmasını zorlu hale getirmeye yönelik artan bir teknolojidir. Li G. ve ark. (2017) ve Patwari N. ve ark. (2010)'a göre, kanalın rastlantısallığının arkasındaki neden, haberleşme ortamında veya kanal içine yapay bileşenin dahil edilmesinde kullanıcının hareketi ve obje hareketleri olarak sunulabilmektedir.

Süzgeçler gibi yapay bileşenler kablosuz haberleşme sistemlerinde güvenliğin arttırılması için gerçekleştirilmektedir. Örneğin, Zhang J., Marshall A. ve ark. (2016)'da, bir alçak geçiren süzgeç, KDR'nin azaltılması ve sistemin SNR aralığının arttırılması için kullanılmaktadır, çünkü kanal ölçümlerinin çapraz korelasyonu gürültü ile çarpmaktadır. Ayrıca, Khiabani Y. S. ve ark. (2013)'de, bir birinci-dereceden sayısal süzgeç, hedef takımı içine otomatik tekrar talebi (ARQ) iletiminin eşleşmesi için gerçekleştirilmektedir. Diğer bir deyişle, Wu Y. ve ark. (2018)'de, m-pencereleri süzgeçleme yöntemi, çok bitli uyarlanır nicemleme şemasının düşük anahtar üretim tutarlılık olasılığına sahip olması için kullanılmaktadır. m-pencere süzgeçleme sisteminde, birden çok anahtar, aynı aralıkta bir anahtar bitinin üretilmesi için ortaya konulmaktadır ve m-penceler ile ön işlemleme kanal özdeğerleri anahtar uyum oranının arttırılmasına yardım etmektedir. Buna ek olarak, Patwari N. ve ark. (2010)'da, bir sonlu darbe yanıt uygulaması, Farrow süzgeci, bir fraksiyonel aradeğerleme süzgeci olarak gerçekleştirilmektedir. Buna ek olarak, bir alçak geçiren süzgeç, Zhang J. ve ark. (2015)'de gürültünün azaltılmasıyla kanalın karşılıklılığının geliştirilmesi için kullanılmaktadır. Bu çalışmada, alçak geçiren süzgeç geçerli verici ve alıcının kanal tahmini arasındaki korelasyonun geliştirileceği bir şekilde tahmin edilen kanalın yüksek frekanslı bileşenlerin baskılanması için tasarlanmaktadır. Alçak geçiren süzgeç sadece kanal karşılıklılığını arttırmamaktadır, aynı zamanda KDR'yi azaltmaktadır ve anahtar üretimine ulaşılmasını geliştirmektedir. Buna ek olarak, Fang S. ve ark. (2017) ve Fang S. (2018)'de, bir gecikme-ağırlıklı-toplam modülü kanal yönlendirmesi için kullanılmaktadır ve bu, bir sonlu darbe yanıt (FIR) süzgeci ile uygulanmaktadır. Orijinal iletilen sinyalin gecikmiş kopyaları, bir çokyolluluk kanalı ile sinyalin iletilmesi durumunda toplanmaktadır. Bununla birlikte, değinilen yöntemlerin bazıları, kaba kuvvet saldırısını kolay hale getirecek karmaşıklık ve uyarlanabilir olmaması gibi bazı dezavantajlara sahiptir.

Büyük ölçekli heterojen kablosuz ağ gibi sonraki ağlar için, anahtar yönetimi ve dağıtımı büyük sorunlardır. Bu, ULLRC, uzaktan cerrahi ve Nesnelerin İnterneti (IoT) gibi yenide kablosuz teknolojilerin desteklenmesi için sonraki ağlarda talepte bulunulacaktır. Ancak bu uygulamalarda kullanılan bu cihazlara sahip problemler aşağıdaki gibidir: bu tür teknolojiler için şifreleme-tabanlı teknikleri başarısız hale getiren güç-sınırlaması, gecikmeye-duyarlı ve işleme-kısıtlaması. Gelecek ağların, farklı güvenlik gerekliliklerine sahip çeşitli türlerde hizmetler ve senaryoların desteklenmesine gerek bulunmaktadır. Şifreleme-tabanlı yöntem senaryo spesifik güvenlik sağlayamamaktadır. Bu nedenlerden dolayı, anahtarlarının geçerli nodüllerde paylaşılması gerektiği konvansiyonel şifreleme-tabanlı güvenlik çözümlerine bağlı kalmadan güvenli haberleşme sağlanması çok önemlidir.

Önceki teknikte, CN104901795 sayılı patent dokümanı, kanal karakteristiklerine bağlı olarak bir fiziksel katman gizli anahtar çıkartma yöntemini açıklamaktadır. Bununla birlikte, bu dokümanda, alıcının, kanal tahmini için haberleşmeden önce vericiye bir referans sinyalini paylaştığı açıklanmamaktadır. Ayrıca, alt taşıyıcılara karşılık gelen, verici ve alıcı arasında frekans seçici kanaldan pik noktalarının, bir basamaklandırılmış kanalının oluşturulması için seçilmesi gerektiği açıklanmamaktadır.

Kısa Açıklama

Buluş, bir gizli anahtar üretim tekniğini içeren bir güvenli haberleşme yöntemi için bir yöntem sağlamayı hedeflemektedir. Kanal içine bir yapay bileşenin dahil edilmesiyle bir kanalın yönlendirilmesinden sonra, önerilen yöntemin yeniliği, kanal-uyumlu anahtarlar kullanılarak fiziksel katman güvenliğinin (PHY) geliştirilmesinden kaynaklanmaktadır. Bir uyumlu şekilde tasarlanan yapay bileşen, geçerli kullanıcı kanalı ile basamaklanmaktadır. Bir ortogonal frekans bölmeli çiftleme (OFDM) sisteminde, örneğin, bir eşik değerden daha yüksek bir kanal alımına karşılık gelen alt taşıyıcılar anahtarların çıkartılması için seçilebilmektedir. Seçilen alt taşıyıcıların sayısı uyarlanır olduğundan dolayı, üretilen anahtar sekansların uzunluğu, ayrıca uyarlanır şekilde değişmektedir. Dolayısıyla, bir zaman bölmeli çiftleme (TDD) sisteminde kanal karşılıklılık özelliği kullanılabilmektedir.

Önceki çalışmalardan farklı olarak, bu buluş, alıcının yeni oluşturulan kanalının yüksek oranda frekans seçici olduğunun ve bir eşik değerinden daha yüksek bir kanal alımına karşılık gelen alt taşıyıcıların sayısının arttırıldığının garanti edilmesi için bir yapay bileşenin dahil edilmesiyle yeni bir yöntemi açıklamaktadır. Yöntem, yeni tasarlanan yapay bileşen ile bir verici ve geçerli alıcı arasında kanalın basamaklandırılmasından sonra anahtarları doğal olarak çıkartmaktadır.

Yapay bileşen, seçilen alt taşıyıcılara karşılık gelen geçerli kullanıcı kanal değerlerinin kopyalarından oluşmaktadır. Buna ek olarak, anahtarlar geçerli kullanıcının basamaklandırılan kanalına bağlı olduğundan dolayı, bunların uzunluk ve değerlerinin, seçilen alt taşıyıcıların sayısına bağlı olarak uyarlanır bir şekilde değiştiğine değinilmesi önemlidir. Bu yüzden, gizli dinleyici, geçerli kullanıcıdan daha güçlü olması durumunda dahi verilerin şifresini çözememektedir.

Önerilen yöntem kablosuz sistemlerin fiziksel katman güvenliğini geliştirebilmektedir ve bu, geçerli nodüllerde anahtarlarının paylaşılmasının gerektiği konvansiyonel şifreleme-tabanlı güvenlik çözümlerine bağlı olmadan güvenli haberleşme sağlayabilmektedir. Bu algoritma ayrıca konvansiyonel yöntemlerde anahtar paylaşımı gibi fiziksel katman güvenliğindeki problemleri çözebilmektedir. Ayrıca, önerilen yöntem, kullanıcının kanalının rastlantısallığı arttırıldığında, Jiao L. ve ark. (2019)'da değinildiği gibi gizli anahtar üretim tekniğinde çok önemli sorunlar olan birlikte-konumlandırılan saldırılar ve yüksek geçici korelasyon gibi bazı problemlerin çözülmesine yönelik ümit verici bir yoldur.

Kısaca, önerilen algoritma, güçlü alt taşıyıcılardan (bir eşik değerden daha yüksek bir kanal alımına karşılık gelen alt taşıyıcılar) bitlerin çıkartılmasıyla daha güvenilir anahtar sağlayabilmektedir. Buna ek olarak, önerilen algoritma, anahtarın uyarlanır uzunluğunun sağlanmasıyla yüksek seviyede güvenli anahtar sağlayabilmektedir. Anahtarın uyarlanır uzunluğuna sahip olunmasıyla, gizli dinleyicinin anahtarı bulması çok zor ve verilerin şifresinin çözülmesi oldukça imkansızdır. Buna ek olarak, önerilen yöntem, bu paylaşımın bu anahtarın güvenli bir şekilde nasıl paylaşılacağı bakımından çok önemli olduğu geçerli nodüllerde gizli anahtarının paylaşılması gerektiği bu yöntemlerde güvenli çözümlere bağlı konvansiyonel yöntemlere bağlı kalmadan güvenli haberleşme garanti edilebilmektedir. Son olarak, önerilen yöntem esnek güvenliği garanti etmek üzere uygulanabilirdir.

Şekillerin Kısa Açıklaması

Şekil 1, bir pasif gizli dinleyici varlığında güvenli haberleşmeye yönelik önerilen sistem modelini göstermektedir.

Şekil 2 önerilen yöntemin OFDM alıcı-verici yapısını göstermektedir

Şekil 3, önerilen kanal-tabanlı anahtar üretim tekniğinin yapısını göstermektedir

Şekil 4a, alıcının kanalının frekans yanıt grafiğini göstermektedir

Şekil 4b, alıcının yeni oluşturulan kanalının frekans yanıt grafiğini göstermektedir

Şekil 5, sembol şifreleme için anahtarın yeniden şekillendirilmesine yönelik bir gösterimi göstermektedir

Referans Numaralarının Kısa Açıklaması

A. Verici
B. Alıcı
E. Gizli dinleyici
s_{ref}. Referans sinyali
h_b. Basamaklanan kanal
h_e. Gizli dinleyici kanalı
b_t. İletilen bitler
b_r. Alınan bitler
M. Modülasyon
DM. Demodülasyon
DC. Şifre çözme
K. Anahtar
S/P. Seriden paralele
P/S. Paralelden seriye
IFFT. Ters hızlı Fourier dönüşümü
FFT. Hızlı Fourier dönüşümü
CP. Döngüsel önek
CPR. Döngüsel önek giderilmesi
f. Frekans
G. Alım
KS. Anahtar akımı
N. Karmaşık veri sembollerinin toplam sayısı
EQ. Kanal dengelemesi
1. Alıcı kanalı
2. En yüksek M-tepe noktası seçimi
3. Yapay bir kanal yaratmak
4. Basamaklanmış kanal
5. Tepe noktaları seçimi
6. Niceleme
7. İkili anahtar
8. İkiliyi karmaşık anahtara dönüştürme

Ayrıntılı Açıklama

Şekil 1, bir pasif gizli dinleyici varlığında güvenli haberleşmeye yönelik önerilen sistem modelini göstermektedir. Özellikle, bir vericinin (A) amacı, gizli bir verinin gönderilmesi ve bir pasif gizli dinleyici (E) varlığında bir geçerli kullanıcı veya alıcı (B) ile gizlice haberleşilmesidir. Gizli dinleyicinin (E) hedefi, alındığı sinyallerin gözlemleri ile verici (A) ve alıcı (B) arasında haberleşme bağlantısından gizli veri içeriklerine erişilmesidir. Buna ek olarak, çoklu antenlere, daha iyi sinyal işleme becerilerine, daha fazla güce, donanım kapasitelerine, işleme kapasitesine, dağıtılmış alma kapasitesine ve çevrimdışı işlemeye sahip olunmasıyla alıcıdan (B) daha güçlü olmaktadır. Verici (A) tarafından konumlarının bilinmediği antenleri dağıtılmaktadır. Hem alıcının (B) hem de gizli dinleyicinin (E) kanallarının bağımsız olduğu ve birbiriyle korelasyon halinde olmadığı, yani gizli dinleyicinin (E) alıcıdan (B) en az yarım dalga boyu uzağında konumlandırıldığı varsayılmaktadır. Buna ek olarak, tüm alınan sinyaller, frekans seçici kanalı zayıflatan Rayleigh'ı deneyimlemektedir. Vericinin (A) bir zaman bölmeli çiftleme (TDD) sisteminde karşılıklılık özelliğinin kullanılmasıyla alıcının (B) kanal durum bilgisini (CSI) bildiği, ancak bunun pasif olmasından dolayı gizli dinleyici (E) kanalı hakkında herhangi bir bilgiye sahip olmadığı varsayılmaktadır. Bu yüzden, her iki kanal, vericiden alıcıya ve alıcıdan vericiye, Zhou X. ve ark. (2016)'de önerildiği gibi, korelasyon halinde olarak tahmin edildiği ve TDD modunda birbiri ile aynı olduğu varsayılmaktadır.

Önerilen haberleşme yönteminde, alıcı (B) kanal tahmini için bir referans sinyalini (s_{ref}) vericiye (A) göndermektedir. N'nin karmaşık veri sembollerinin toplam sayısına karşılık geldiği varsayıldığında; önerilen yöntem temel olarak aşağıdaki adımları içermektedir:

a. Verici (A) ve alıcı (B) arasında frekans seçici kanaldan m sayıda pik-noktalarının dışında birinci m noktasının seçilmesi, burada içindeki noktalar alt taşıyıcılara karşılık gelmektedir ve burada $M < N$,
b. Seçilen m noktalarının kullanılmasıyla yapay bir kanalın, $F_b \in \mathbb{C}^{Nx1}$, oluşturulması,
c. $H_b = A_b \odot F_b$ olarak yapay kanal ile alıcı (B) kanalının, $A_b \in \mathbb{C}^{Nx1}$ basamaklanmasıyla yeni bir kanalın, $H_b \in \mathbb{C}^{Nx1}$, oluşturulması,
d. Basamaklanan kanaldan, H_b, pik noktalarının seçilmesi,
e. Alımlarının bir ikili anahtarın üretilmesi için verici (A) ve alıcı (B) ile basamaklanan kanalından pik noktalarına karşılık geldiği seçilen alt taşıyıcıların nicemlenmesi,
f. İkili anahtarın bir karmaşık anahtara dönüştürülmesi,
g. Karmaşık anahtarın N'nin en yakın çoğaltmasına yeniden biçimlendirilmesi.

Tercih edilen bir yapılandırmada, kanal alımının (G) anahtarların çıkartılması için verici (A) tarafından düşünülen tüm frekans (f) indislerinin ortalama üstü kanal alımının (G) olduğu pik noktalarının sayısı (M) seçilmektedir.

Diğer yapılandırmada, son anahtar bloğunun uzunluğunun N'den daha az olduğu durumda, başlıktan anahtar numuneleri, karmaşık anahtarın yeniden biçimlendirilmesi için bir sonek olarak ilave edilmektedir.

Diğer bir yapılandırmada, karmaşık anahtarın yeniden biçimlendirilmesinden sonra, iletilen sinyal, x, $y_b = h_b * x + n_b$ olarak döngüsel önekin (CP) zaman-alan şifreli sembollere uygulanmasıyla alıcıya (B) gönderilmektedir, burada y_b, alıcıda (B) alınan sinyaldir, h_b, zaman-alanda basamaklanan kanaldır, ve n_b, alıcı (B) tarafında sıfır ortalamalı karmaşık toplanır beyaz Gauss gürültüsüdür (AWGN).

Örnek bir uygulama

Bu örnek uygulamada, ilk olarak alıcı (B) bir referans sinyalini (s_{ref}) kanal tahmini için vericiye (A) iletmektedir. Dolayısıyla, TDD modunda kanal karşılıklılık özelliğinin bir avantajı olarak, uydu yer bağı kanalı, Goldsmith A (2005) tarafından önerildiği gibi, yer-uydu bağından elde edilmektedir.

Önerilen yöntemin önerilen OFDM alıcı-verici yapısı Şekil 2'de gösterilmektedir. N'nin uzunluğuna sahip frekans-alan karmaşık veri sembolleri aşağıdaki gibi gösterilmektedir:

$$S = [S_1, S_2, \dots, S_N]$$

burada $S \in \mathbb{C}^{1xN}$. BPSK modülasyon kullanılarak elde edilen bu semboller, gizli dinleyici (E) varlığında alıcıya (B) verici (A) tarafından gönderilecektir.

Verilerin şifrelenmesi için bir gizli anahtar kullanılmaktadır. Vericideki bu anahtarın üretilmesi Şekil 3'te gösterilmektedir. Alıcı (B) tarafından deneyimlenen kanalın frekans yanıtı, $A_b \in \mathbb{C}^{Nx1}$ ile simgelenmektedir ve gizli dinleyici (E) tarafından, N'nin her birinin kanal uzunluğu olduğu $A_e \in \mathbb{C}^{Nx1}$ ile simgelenmektedir. N noktalarının dışında M seçilen alt taşıyıcılar ($M < N$), N'nin,$A_b = [A_{b_1}, A_{b_2}, \dots, A_{b_N}]^T$, olan alıcının (B) kanalının frekans yanıtından seçilmektedir. Kanal alımının tüm frekans indislerinin ortalama üstü alımı olduğu noktalara karşılık gelen bu M alt taşıyıcıları gizli anahtarların çıkartılması için verici (A) tarafından düşünülmektedir. Hem eşik değerinden daha yüksek bir kanal alımına karşılık gelen alt taşıyıcıların sayısının arttırılması hem de kanalın daha seçici olduğunun garanti edilmesi için, bir yapay kanal seçilen

M noktalarının kullanılmasıyla tasarlanmaktadır. Seçilen M frekans değerlerinde A_b değerleri, yapay kanalın uzunluğuna kadar kopyalanmaktadır, $F_b \in \mathbb{C}^{Nx1}$, alıcı (B) kanalının uzunluğuna, $A_b \in \mathbb{C}^{Nx1}$, eşittir. Alıcı (B) için yeni bir kanal, $\mathrm{H_b} \in \mathrm{C^{Nx1}}$, aşağıdaki gibi ifade edildiği üzere yapay kanal, $\mathrm{F_b} \in \mathrm{C^{Nx1}}$ ile alıcı (B) kanalının, $A_b \in \mathbb{C}^{Nx1}$, basamaklanmasıyla oluşturulmaktadır:

$$H_b = A_b \odot F_b$$

Kanal alım değerlerinin tüm değerlerin ortalama üstü alımının olduğu frekans indislerine karşılık gelen seçilen noktaların sayısı, Şekil 4a ve 4b'de gösterilmektedir. Şekil 4a'da gösterildiği gibi, alıcı (B) kanalının seçilen alt taşıyıcılarının sayısı emin bir şekilde anahtarların çıkartılması için çok azdır. Bu yüzden, verici (A), kanalın yönlendirilmesi için bir yapay bileşen ilave etmektedir. Dolayısıyla, Şekil 4b'de verilen basamaklanan kanalın seçilen parçalarının sayısı, Şekil 4a'da seçilen noktaların sayısından daha fazladır. H_b'nin alt taşıyıcılarının seçilmesinden sonra, alıcının (B) gelişmiş kanalı, bir anahtarın oluşturulması için verici (A) ve alıcı (B) ile nicemlenmektedir. Basamaklanan kanal alım ölçümleri, bölgeler içine eşit bir şekilde bölünmektedir ve her bölge alıcı (B) ve verici (A) ile çoklu bit nicemleme seviyelerine nicemlenmektedir. En yüksek pik noktalarının her biri, bir bit akımına karşılık gelmektedir. Bu yüzden, üretilen anahtarın uzunluğu, alıcı (B) basamaklanan kanalın seçilen pik noktalarının sayısına bağlıdır. Önerilen şifrelemenin sembol seviyesine bağlı olmasından dolayı, alıcı (B) için ikili anahtar, $B_b \in \{0, 1\}$, $i(2xB_b - 1)$ olarak bir karmaşık anahtara, C_b dönüştürülmektedir. Anahtarın uzunluğunun, sembollerin sayısından daha uzun olmasından dolayı, anahtar, sembollerin toplam sayısının, N, en yakın çoğaltmasına yeniden biçimlendirilmektedir.

Şekil 5'te görüldüğü gibi, bir uyarlanır uzunluğa sahip anahtar akım (KS), K_b, çoklu bloklar içine bölünmektedir ve her bloğun uzunluğu sembollerin sayısına, N eşit olmalıdır. Son anahtar bloğunun uzunluğunun N'den daha az olması durumunda, başlıktan anahtar numuneleri bir sonek olarak ilave edilmektedir. Anahtarın yeniden biçimlendirilmesinden sonra, bir verici (A) taraf, şifrelenmiş semboller, E_b, aşağıdaki gibi semboller, S, ile K_{b_i}'nin her anahtar bloğunun çoğaltılması olarak yazılabilmektedir:

$$E_b = K_{b_i} \odot S^T$$

burada i = 1, …, n ve n anahtar bloklarının sayısıdır. E_b, uzunluğun $(N \times n) \times 1$, şifrelenen sembollerinin bir vektörünün elde edilmesi için yeniden biçimlendirilmektedir. Uyarlanabilir uzunluğun iletilen sinyali, x, sembol arası ara yüzden (ISI) kaçınılması için zaman-alan şifreli sembollerine döngüsel önekinin (CP) uygulanmasından sonra alıcıya (B) gönderilmektedir. Alıcı (B) tarafında alınan sinyal, aşağıdaki tanımlanmaktadır:

$$y_b = h_b * x + n_b$$

burada h_b zaman-alanda alıcının (B) basamaklanan kanalıdır, x iletilen sinyaldir, ve n_b alıcıda (B) sıfır ortalamalı karmaşık toplanır beyaz Gauss gürültüsüdür (AWGN). x'in uzunluğu uyarlanır olduğundan dolayı, alınan sinyalin uzunluğu da, y_b, uyarlanabilirdir.

Döngüsel önekin (CP) giderilmesinden ve sonra zaman-alan alınan sinyalinde S/P dönüşümünün uygulanmasından sonra, y_b, alıcı sonuçlanan sinyal üzerinde FFT'yi kullanmaktadır. Bir sıfırdan zorlama kanalı dengeleme prosesi, daha iyi şifre çözümü için kanaldan gürültünün etkilerinin azaltılması için gerçekleştirilmektedir. Dolayısıyla, kanal eşitlenme prosesinden sonra alıcı (B) tarafındaki alınan sinyal, alınan sinyalin eleman-tarzı ile bulunmaktadır ve bunun kanalı aşağıdaki gibi ifade edilmektedir:

$$\widehat{Y_b} = Y_b \oslash H_b$$

Burada $\mathrm{H_b}$ alıcının (B) frekans-alanında basamaklanan kanalıdır ve Y_b, Şekil 2'de gösterilen S/P dönüşümünden sonra frekans-alan alınan sinyaldir. P/S dönüşümünden sonra, alıcı (B), kendi kanalından çıkartılan ve şifresi çözülmüş verinin aşağıdaki gibi gözlendiği anahtar akım (KS), $\mathrm{K_b}$, kullanılarak şifresi çözülmüş veri üretmektedir:

$$\widehat{X_b} = \widehat{Y_b} \oslash K_b$$

gizli dinleyici ayrıca iletilen sinyale, x, erişime sahiptir. Daha güçlü becerilere ve alıcıdan (B) daha hassas alıcıya sahip olmasına rağmen, kendi kanalından anahtarlarının üretilmesi için Şekil 2'de gösterildiği gibi alıcı (B) ile aynı adımları takip etmektedir. Gizli dinleyici (E) ayrıca alıcınınki (B) ile aynı şekilde bir yapay bileşeni tasarlamaktadır ve basamaklanan kanalın $\mathrm{H_e}$'nin elde edilmesi için, bunu kendi kanalı, A_e, ile basamaklamaktadır. Kanaldan yakalanan sinyal aşağıdaki gibi tanımlanmaktadır:

$$y_e = h_e * x + n_e$$

burada $\mathrm{h_e}$ zaman-alanda gizli dinleyici (E) basamaklanan kanaldır ve n_e gizli dinleyicinde (E) sıfır ortalamalı karmaşık AWGN'dir. Kanal dengeleme prosesinden sonra gizli dinleyicinde (E) alınan sinyal şu şekilde ifade edilmektedir:

$$\widehat{Y_e} = Y_e \oslash H_e$$

burada Y_e S/P dönüşümünden sonra frekans-alan alınan sinyaldir ve H_e gizli dinleyicinin (E) basamaklanan kanalıdır. Gizli dinleyici (E) anahtar, K_e, kullanılarak şifresi çözülmüş veriler üretmektedir, kendi kanalından çıkartılmaktadır ve şifresi çözülmüş veri aşağıdaki gibi ifade edilmektedir:

$$\widehat{X_e} = \widehat{Y_e} \oslash K_e$$

Hem alıcının (B) hem de gizli dinleyicinin (E), vericiden (A) alınan gizli verilerin şifresinin çözülmesi için Şekil 2'de gösterildiği gibi, aynı adımları takip etmektedir. Verici (A) alıcı (B) kanalından çıkartılan anahtarlar kullanılarak verileri ilettiğinden dolayı, alıcı (B), gizli dinleyici (E) varlığında bu sinyal emin bir şekilde alınabilmektedir. Gizli dinleyici (E) çoklu antenlere ve alıcıdan (B) daha fazla becerilere sahip olmasına rağmen, bunun içine bir yapay bileşenin ilave edilmesiyle kanalı manipüle edilmesinden sonra bunun kendi anahtarlarını çıkartması durumunda dahi verilerin şifresini doğru bir şekilde çözememektedir.

Referanslar

[1] K. Ren, H. Su, ve Q. Wang, “Secret key generation exploiting channel characteristics in wireless communications,” IEEE Wireless Commun., cil. 18, no. 4, ss. 6–12, 2011.

[2] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” IEEE Commun. Mag., cil. 53, no. 6, ss. 33–39, 2015.

[3] J. Zhang, T. Q. Duong, A. Marshall, ve R. Woods, “Key generation from wireless channels: Bir inceleme,” IEEE Access, cil. 4, ss. 614–626, 2016.

[4] J. M. Hamamreh, H. M. Furqan, ve H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” IEEE Commun. Surveys & Tut., 2018.

[5] A. Badawy, T. Elfouly, T. Khattab, C.-F. Chiasserini, A. Mohamed, ve D. Trinchero, “Robust secret key extraction from channel secondary random process,” Wireless Commun. Mob. Comp., cil. 16, no. 11, ss. 1389–1400, 2016.

[6] J. Zhang, A. Marshall, R. Woods, ve T. Q. Duong, “Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers,” IEEE Trans. Commun., cil. 64, no. 6, ss. 2578–2588, 2016.

[7] G. Li, A. Hu, L. Peng, ve C. Sun, “The optimal preprocessing approach for secret key generation from OFDM channel measurements,” IEEE Global Commun. Conf. (Globecom), 2016, ss. 1–6.

[8] G. Li, A. Hu, J. Zhang, ve B. Xiao, “Security analysis of a novel artificial randomness approach for fast key generation,” IEEE Global Commun. Conf. (Globecom), 2017, ss. 1–6.

[9] N. Patwari, J. Croft, S. Jana, ve S. K. Kasera, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” IEEE Trans. Mob. Comp., cil. 9, no. 1, ss. 17–30, 2010.

[10] Y. Wu, H. Xia, ve C. Cheng, “Improved mult-bit adaptive quantization algorithm for physical layer security based on channel charscteristics,” Int. Conf. Sys. Inf. (ICSAI), 2018, ss. 807–811.

[11] Y. S. Khiabani ve S. Wei, “ARQ-based symmetric-key generation over correlated erasure channels,” IEEE Trans. Inf. Forensics Sec., cil. 8, no. 7, ss. 1152–1161, 2013.

[12] J. Zhang, R. Woods, A. Marshall, ve T. Q. Duong, “An effective key generation system using improved channel reciprocity,” IEEE Int. Conf. Acoust., Speech Sig. Proc. (ICASSP), 2015, ss. 1727–1731.

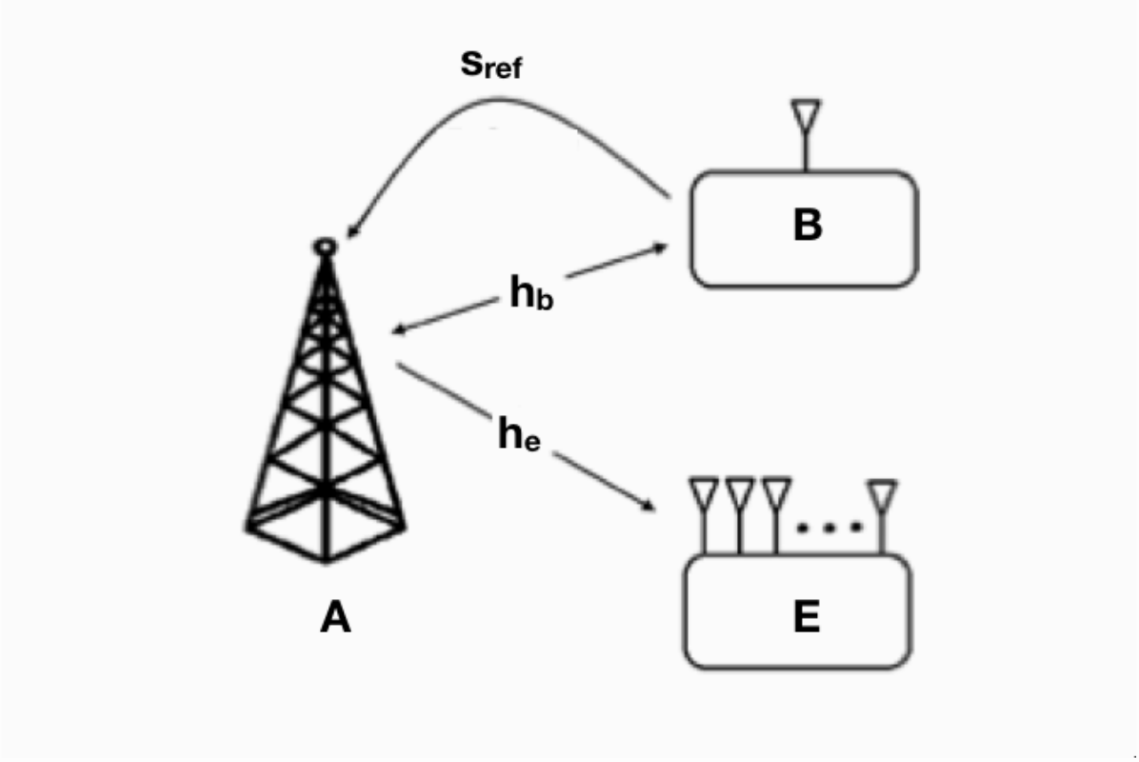
[13] S. Fang, I. Markwood, ve Y. Liu, “Manipulatable wireless key establishment,” IEEE Conf. Commun. Net. Sec. (CNS), 2017, ss. 1–9.

[14] S. Fang, “Channel camouflage and manipulation techniques in wireless networks,” PHD tezleri ve bitirme tezleri, 2018, https://scholarcommons.usf.edu/etd/7284.

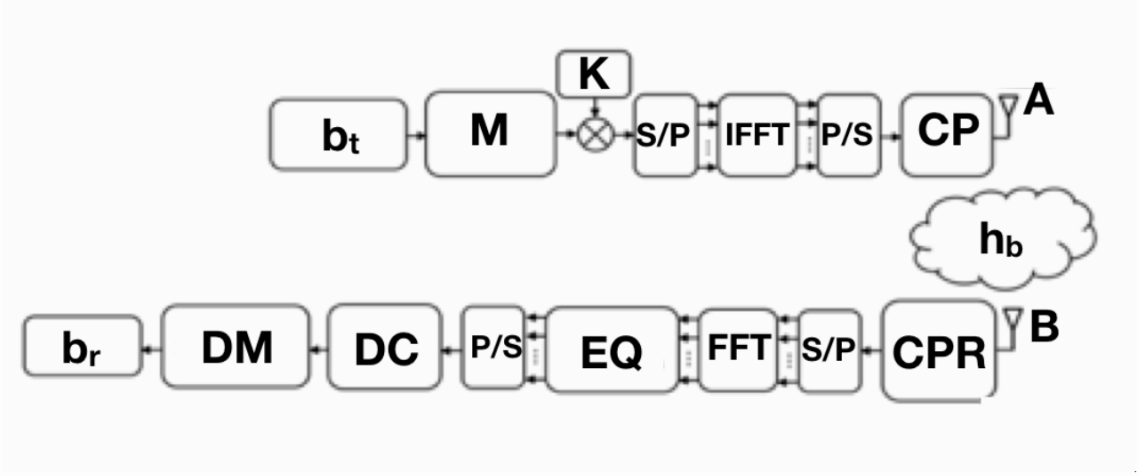
[15] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, ve K. Zeng, “Physical layer key generation in 5G wireless networks,” IEEE Wireless Commun. Mag., 2019.

[16] X. Zhou, L. Song, ve Y. Zhang, Physical Layer Security in Wireless Communications. CRC Baskı, 2016.

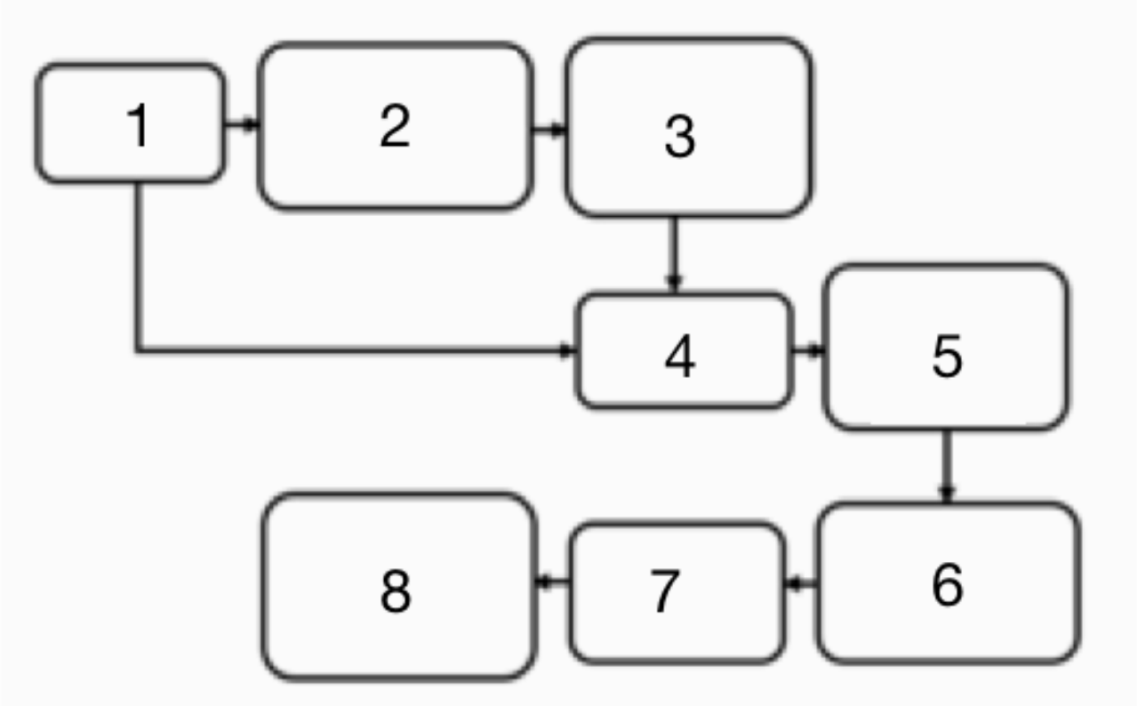
[17] A. Goldsmith, Wireless Communications. Cambridge University Baskı, 2005.



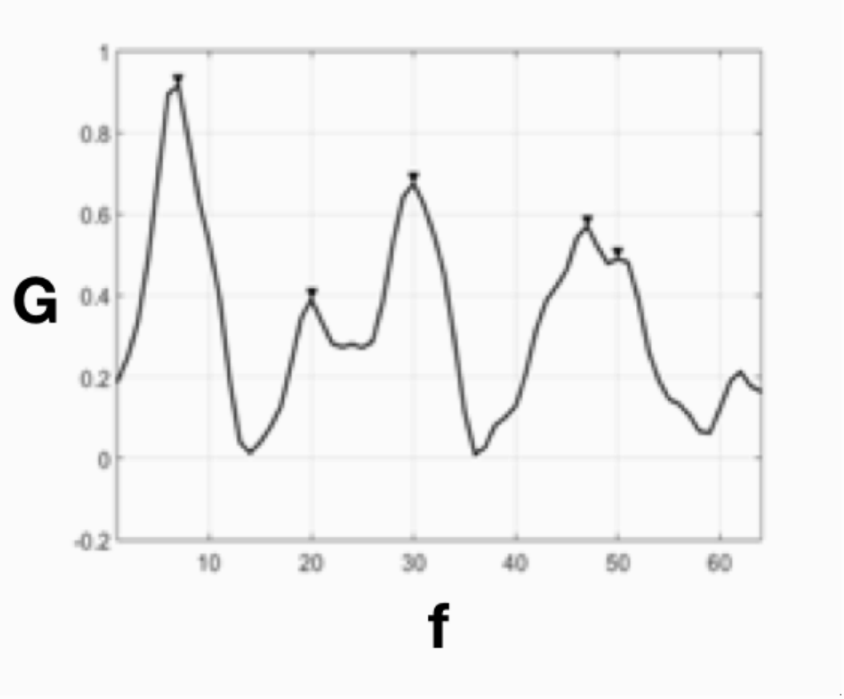
Şekil 1



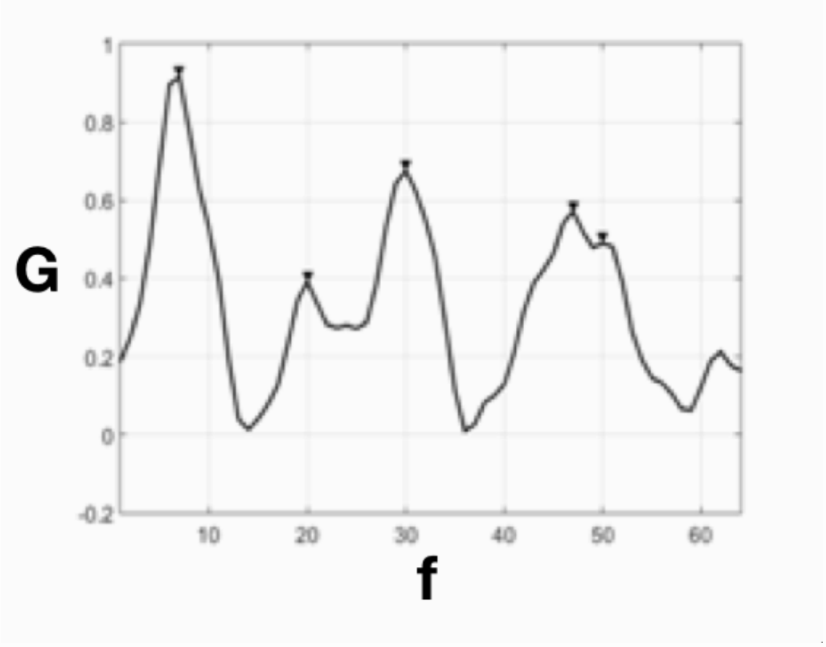
Şekil 2



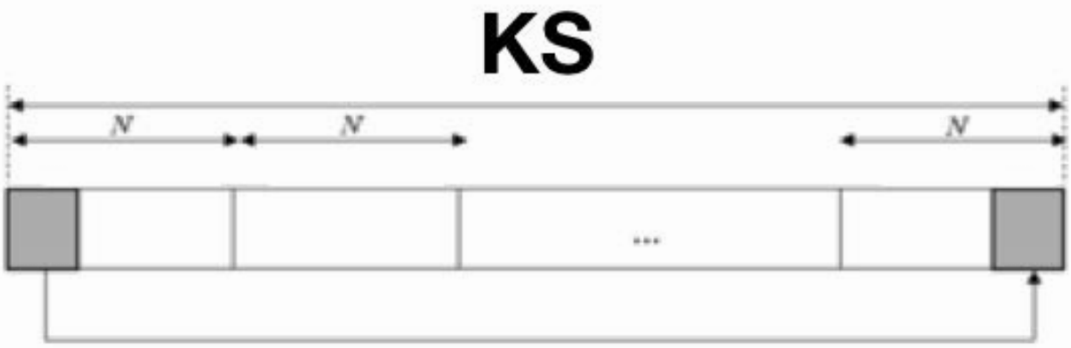
Şekil 3



Şekil 4a



Şekil 4b



Şekil 5