ÖZET

SİNYAL İLİŞKİSİNE DAYALI FİZİKSEL KATMAN KİMLİK DOĞRULAMA VE GÜVENLİK YÖNTEMİ

Buluş, kullanıcılara hizmet sağlayan bir sistemin, hizmet kalitesini ve güvenliğini sağlayabilmek adına, yasal kullanıcıları tanımlayan ve yasal olmayan olarak isimlendirilen olası kötü niyetli kullanıcıları tespit eden sinyal ilişkisine dayalı bir fiziksel katman doğrulama ve güvenlik yöntemi ile ilgilidir.

(Şekil 1)

İSTEMLER

1. Kullanıcılara hizmet sağlayan bir sistemin, yasal kullanıcıları tanımlayan ve yasal olmayan niyetli kullanıcıları tespit eden sinyal ilişkisine dayalı bir fiziksel katman doğrulama ve güvenlik yöntemi olup, **özelliği;**

- eğitim verileri (A) modüle edilerek T_X eğitim sembollerinin (B) oluşması (101),
- T_X eğitim sembollerinin (B) kablosuz bir kanaldan geçirilip gürültü eklenmesiyle R_X eğitim sembollerinin (C) elde edilmesi (102),
- alınan R_X eğitim sembolleri (C) ile T_X eğitim sembollerinin (B) yasal alıcı tarafından depolanması,
- güvenirliğini tespit edilmek istenen R_X (r_A) sembollerin tahmin edilmesi için,
    - o R_X eğitim sembolleri (C) ve T_X eğitim sembolleri (B) ile pilot sembolleri ve interpolasyon kullanılarak kanal tahmini yapılması (103)
    - o test verileri (E) modüle edilerek T_X test sembollerinin elde edilmesi (104),
    - o tahmin edilmiş yasal kullanıcı kanal (D) ve test aşamasında bilinen T_X test sembolleri (F) kullanılarak Minimum Ortalama Karesel Hata sinyal bulma algoritması ile güvenirliği tespit edilmek istenen R_X (G) sembollerinin tahmin edilmesi (106)
- alınan R_X (G) ve tahmin edilen R_X (H) semboller hipotez testi yapılması (107),
- hipotez testi sonucunda alınan R_X (G) ve tahmin edilen R_X (H) semboller arasındaki fark belirli bir eşik değerinin altındaysa kullanıcının yasal, üstünde ise kullanıcı yasal değil olarak belirlenmesi (I)

işlem adımlarını içermesidir.

2. Kullanıcılara hizmet sağlayan bir sistemin, yasal kullanıcıları tanımlayan ve yasal olmayan niyetli kullanıcıları tespit eden sinyal ilişkisine dayalı bir fiziksel katman doğrulama ve güvenlik yöntemi olup, **özelliği;**

- eğitim verileri (A) modüle edilerek T_X eğitim sembollerinin (B) oluşması (101),

- T_X eğitim sembollerinin (B) kablosuz bir kanaldan geçirilip gürültü eklenmesiyle R_X eğitim sembollerinin (C) elde edilmesi (102),

- alınan R_X eğitim sembolleri (C) ile T_X eğitim sembollerinin (B) yasal alıcı tarafından depolanması,

- güvenirliğini tespit edilmek istenen R_X (r_A) sembollerin tahmin edilmesi için,

    - T_X eğitim sembolleri (B) ve R_X eğitim sembolleri (C) kullanılarak makinenin eğitilmesi (108),

    - test verilerinin (E) modüle edilmesi (104),

    - T_X test sembolleri, eğitilmiş makinede girdi olarak kullanılarak, güvenirliği tespit edilmek istenen R_X (G) sembollerinin tahmin edilmesi (109),

- alınan R_X (G) ve tahmin edilen R_X (H) semboller hipotez testi yapılması (107),

- hipotez testi sonucunda alınan R_X (G) ve tahmin edilen R_X (H) semboller arasındaki fark belirli bir eşik değerinin altındaysa kullanıcının yasal, üstünde ise kullanıcı yasal değil olarak belirlenmesi (I)

işlem adımlarını içermesidir.

TARİFNAME

SİNYAL İLİŞKİSİNE DAYALI FİZİKSEL KATMAN KİMLİK DOĞRULAMA VE GÜVENLİK YÖNTEMİ

Teknik Alan

Buluş, kullanıcılara hizmet sağlayan bir sistemin, hizmet kalitesini ve güvenliğini sağlayabilmek adına, yasal kullanıcıları tanımlayan ve yasal olmayan olarak isimlendirilen olası kötü niyetli kullanıcıları tespit eden sinyal ilişkisine dayalı bir fiziksel katman doğrulama ve güvenlik yöntemi ile ilgilidir.

Tekniğin Bilinen Durumu

Günümüzde kablosuz haberleşme sistemleri sivil ve askeri uygulamalarda sıklıkla kullanılmış ve hayatımızın önemli bir parçası haline gelmiştir. Bu doğrultuda, insanlar kredi kartı işlemleri, enerji fiyatlandırması, e-sağlık verileri, komut ve kontrol mesajları [1] gibi özel bilgilerini iletmek için kablosuz ağları kullanmaktadırlar. Fakat kablosuz iletişimin yayın yapısından dolayı, yasal olmayan bir düğüm, yasal olan kullanıcılar arasındaki iletişimi dinlemeye çalışabilir (eavesdropping), iki yasal kullanıcı arasında iletilmekte olan mesajı değiştirebilir (spoofing) ve yasal olan kullanıcılar arasındaki iletişimi bozmak için kasıtlı girişim oluşturabilir (jamming). Bu nedenlerden ötürü, güvenlik, kablosuz ağlar için kritik bir konudur [2].

Kablosuz ağların güvenliği, genellikle kriptografi gibi üst katman teknikleriyle sağlanır. Fakat hesaplama ve bant genişliği kaynakları sınırlı olduğunda, şifreleme tekniklerinin uygulanması oldukça zordur. Ayrıca, kriptografi tabanlı metotlar servis odaklı ve kullanıcı merkezli güvenlik garantisi sağlayamamaktadır [3]. Bu gibi sınırlamalar nedeniyle, son zamanlarda fiziksel katman güvenliği (PLS) [4] büyük ilgi görmüştür. Yukarıda anlatılan saldırılardan, iki yasal kullanıcı arasındaki iletilen mesajı değiştirebilen spoofing saldırısı, yasal kullanıcılar arasındaki iletişimin güvenliği açısından büyük tehlike oluşturmaktadır. Bu saldırı yöntemini önlemek için özellikle, fiziksel katman doğrulama (PLA), en güçlü fiziksel katman güvenlik tekniklerinden biridir. Bu doğrultuda, literatürde gizlilik kapasitesi (secrecy capacity), kanal tabanlı kimlik doğrulama (channel based authentication), radyo frekansı tanıma (RF recognition) ve kablolu dinleme koduna dayalı kimlik doğrulama (wiretap code-based authentication) gibi çeşitli PLA çalışmaları yer almaktadır [5]. Literatürdeki birçok PLA çalışması spoofing saldırılarını önlemek için yasal alıcı-verici

arasındaki kanalı ele almaktadır. Çünkü kanal tabanlı PLA tekniklerinin, kanalın taklit edilmesi zorluğu, uygulama kolaylığı ve bir saldırı tespit edildiğinde imzayı ayarlama kolaylığı gibi avantajları bulunmaktadır [6].

Kanal bazlı PLA çözümlerinde, spoofing saldırılarına karşı sinyallerin genlik, faz, çok yollu gecikme bilgileri kullanılmaktadır. [7] numaralı yayında, kanalın güç gecikme profili (PDP), spoofing saldırı tanımlamasını gerçekleştirmek için kullanılmıştır. Bu yöntemde yasal kullanıcının alıcıya spooferdan daha yakın olduğu kabul edilmiştir. Fakat bazı durumlarda saldırgan yerini alıcıya, yasal kullanıcıdan daha yakın olacak şekilde değiştirebilir ve algoritmanın çalışmamasına neden olabilir.

Bazı kanal tabanlı PLA uygulamalarında kanal impuls cevabı (CIR)'dan yararlanılarak oluşturulmuş çözümler önerilmektedir. Bu yöntemlerde yasal kullanıcı bir mesaj gönderdiğinde, alıcı bağlantı (kanal) tahminini gerçekleştirir ve referans bağlantı imzası olarak atar. Yasal olmayan kullanıcı mesaj gönderdiğinde, bu kullanıcı farklı bir yerde bulunduğundan yasal verici kullanıcı bağlantısından farklı olacaktır. Spooferın link imzası referansla karşılaştırıldığında, alıcı sinyalin yasal vericiden iletilmemesine karar verir ve reddeder. Fakat, bu yöntemlerde, bağlantı imzaları, kanal impuls yanıtından (CIR) elde edildiğinden, vericinin yerindeki değişiklik, CIR'da, dolayısıyla bağlantı imzalarında da değişime yol açacaktır. Bu sebeple, bu metotlar kanala bağımlı güvenlik çözümleri vericinin statik olduğu durumlar için önerilmiş ve hareketlilik durumu incelenmemiştir. Bu problemi çözmek için [8] numaralı yayında, zamana bağlı değişen kanallar için kanal frekans cevabını (CFR) kullanımını önerilmiştir. Bu yöntemler yasal kullanıcıların tanımlanması, aday kullanıcının kanalının gözlemlenmesine ve sistem tarafından önceden bilinen yasal kullanıcı kanalları ile karşılaştırarak adayın yasal olup olmadığına karar verilmesine dayanmaktadır. Ancak, mevcut kanal tabanlı fiziksel katman kimlik doğrulama tekniklerinin bazı dezavantajları vardır. İlk olarak, mevcut yöntemlerde kullanıcının yasal olup olmadığı kararı, eğitim ve test aşamalarını içeren her bir doğrulama prosedürü için kanal bilgisi tahmin edilerek verilmektedir. Test aşamasında da tekrardan kanalın tahmin edilmesi, kullanılan pilot sayısını artırmakta ve spektral verimliliği azaltmaktadır. İkinci olarak, gerçek zamanda kanaldaki tap sayısı tam olarak bilinmemektedir. Bu yüzden kanal modellenirken gerçek tap sayısından az veya fazla olacak şekilde kanal modellenebilmektedir. Kanalın gerçekte olduğundan daha az tap sayısı kullanılarak modellenmesi kanal tahmin kalitesini çok fazla düşürmektedir. Çünkü bazı taplar hakkında hiçbir bilgi verilmemektedir. Bu yüzden kanalın olduğundan daha fazla tap sayısı ile modellenmesi kanalın daha az tap sayısı ile modellenmesine göre

daha fazla kabul gören bir yaklaşımdır. Yine mevcut uygulamada, kanal tabanlı fiziksel katman kimlik doğrulama algoritmaları iki kanal arasındaki farka hipotez testi kullanarak bakılmaktadır. Kanal tap sayısı artırıldığında, fazla olan taplar doğrudan gürültülü bilgi içerecektir ve kimlik doğrulama başarısı düşecektir.

Sonuç olarak, yukarıda anlatılan olumsuzluklardan dolayı ve mevcut çözümlerin konu hakkındaki yetersizliği nedeniyle ilgili teknik alanda bir geliştirme yapılması gerekli kılınmıştır.

Buluşun Amacı

Buluş, mevcut durumlardan esinlenerek oluşturulup, yukarıda belirtilen olumsuzlukları çözmeyi amaçlamaktadır.

Bu buluşun amacı, detaylı bir kanal tahmini işlemi gerçekleştirmeye gerek kalmadan kullanıcı kimlik doğrulamasını yapabilmektir.

Buluşun diğer bir amacı, daha az sayıda pilot kullanılmasıyla kullanıcı kimlik doğrulaması için etkili ve hızlı bir teknik ortaya koymaktır. Hız, farklı kullanıcı sayıları ve türlerinde beklenen artışla birlikte 5G ve ötesi fiziksel katman güvenliği için önemli bir gerekliliktir.

Buluşun diğer bir amacı, kanal test aşamasında tekrar tahmin etmeye gerek kalmadan yasal kullanıcıların kanallarının dolaylı olarak tanımlamasına ve spektral verimlilik artmasını sağlamaktır. Kanalın test aşamasında fiziksel katman güvenliği için tahmin edilmemesi, test aşamasında kullanılacak olan pilot sayısını azaltmaktadır. Kullanılan pilot sayısındaki bu azalma doğrudan spektral verimliliğin artmasını sağlamaktadır.

Buluşun diğer bir amacı, kanalın olduğundan daha fazla tap sayısı ile modellenmesi durumunda avantaj sağlamaktır.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen şekiller ve bu şekillere atıflar yapılmak suretiyle yazılan detaylı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle değerlendirmenin de bu şekiller ve detaylı açıklama göz önüne alınarak yapılması gerekmektedir.

Buluşun Anlaşılmasına Yardımcı Olacak Şekiller

Şekil 1, buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin MMSE yöntemi ile uygulanmasının eğitim aşaması akış diyagram görünümüdür.

Şekil 2, buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin MMSE yöntemi ile uygulanmasının test aşaması akış diyagram görünümüdür.

Şekil 3, buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin ML yöntemi ile uygulanmasının eğitim akış diyagram görünümüdür.

Şekil 4, buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin ML yöntemi ile uygulanmasının test akış diyagram görünümüdür.

Parça Referanslarının Açıklanması

A. Eğitim verileri

B. T_X eğitim sembolleri

C. R_X eğitim sembolleri

D. Tahmin edilmiş yasal kullanıcı kanalı

E. Test verileri

F. T_X test sembolleri

G. R_X test sembolleri

H. Tahmin edilmiş test sembolleri (r_A)

I. Hipotez testi sonucunda alınan R_X (G) ve tahmin edilen R_X (H) semboller arasındaki fark belirli bir eşik değerinin altındaysa kullanıcının yasal, üstünde ise kullanıcı yasal değil olarak belirlenmesi

101. Eğitim verileri modüle edilerek T_X eğitim sembollerinin oluşması

102. T_X eğitim sembollerinin (B) kablosuz bir kanaldan geçirilip, gürültü eklenmesiyle R_X eğitim sembollerinin (C) elde edilmesi

103. R_X eğitim sembolleri (C) ve T_X eğitim sembolleri (B) ile pilot sembolleri ve interpolasyon kullanılarak kanal tahmini yapılması

104. Test verileri (E) modüle edilerek T_X test sembollerinin (F) elde edilmesi

105. T_X test sembollerinin (F) yasallığı test edilmek istenilen kablosuz kanalından geçirilip, gürültü eklenmesiyle R_X test sembollerinin (G) elde edilmesi

106. tahmin edilmiş yasal kullanıcı kanal (D) ve test aşamasında bilinen T_X test sembolleri (F) kullanılarak Minimum Ortalama Karesel Hata sinyal bulma algoritması ile güvenirliği tespit edilmek istenen R_X (G) sembollerinin tahmin edilmesi

107. alınan R_X (G) ve tahmin edilen R_X (H) semboller hipotez testi yapılması

108. T_X (B) ve R_X (C) eğitim sembolleri kullanılarak makinenin eğitilmesi

109. Tx test sembolleri (F) eğitilmiş makinede kullanılarak, güvenirliği tespit edilmek istenen R_X test sembollerinin (G) tahmin edilmesi

Buluşun Detaylı Açıklaması

Bu detaylı açıklamada, buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin tercih edilen yapılanmaları, sadece konunun daha iyi anlaşılmasına yönelik olarak açıklanmaktadır.

Buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yöntemi iki farklı metot kullanarak önerilmiştir.

Buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yöntemi için önerilen MMSE'ye dayalı metodun eğitim ve test aşaması sırasıyla Şekil 1 ve Şekil 2'de görülmektedir.

Buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yöntemi için önerilen ML'ye dayalı metodun eğitim ve test aşaması sırasıyla Şekil 3 ve Şekil 4'te görülmektedir.

Buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin MMSE metodu için önerilen işlem adımları şu şekildedir:

- Şekil 1'de görüleceği üzere, önce eğitim verileri (A) modüle edilmekte ve T_X eğitim sembolleri (B) oluşmaktadır. Sonra T_X eğitim sembolleri (B) kanaldan geçirilmektedir ve dış etkenlerden dolayı sembollere gürültü eklenmektedir. (102) Böylece R_X eğitim sembolleri (C) elde edilir.

- Alıcı tarafında R_X eğitim sembolleriyle (C) belirtilen alınan sinyal semboller ile T_X eğitim sembolleri (B) yasal alıcı tarafından depolanır.

- Depolanan R_X eğitim sembolleri (C) ve T_X eğitim sembolleri (B) ile pilot sembolleri/veri yönelimli izleme ve interpolasyon [9] kullanılarak kanal tahmin edilir ve tahmin edilmiş kanal (D) bilgisi sonradan kullanılmak üzere depolanır. (103)

- Test verileri (güvenirliği tespit edilmek istenen veriler) eğitim verileri (E) gibi T_X test sembolleri (F) ve R_X test sembolleri (G) olacak şekilde oluşturulur. (104)

- Tahmin edilmiş kanal (D) ve test aşamasında bilinen T_X test sembolleri (F) kullanılarak Minimum Ortalama Karesel Hata (MMSE) sinyal bulma algoritması ile güvenirliği tespit edilmek istenen R_X (G) sembolleri tahmin edilir. (106)

- Doğrulama yapılabilmesi için alınan R_X (G) ve tahmin edilen R_X (H) sembollere dayanarak gelen sembollerin güvenilir olup olmadığı tespit edilmektedir. Bunun için önceki birçok doğrulama çalışmasında olduğu gibi hipotez testi [10-11] kullanılır.

- Bu hipotez testinde alınan R_X (G) ve tahmin edilen R_X (H) semboller arasındaki fark belirli bir eşik değerinin altındaysa kullanıcı yasal, üstünde ise kullanıcı yasal değil olarak belirlenir. Bu şekilde fiziksel katman doğrulama tamamlanmış olunur.

Buluşa konu olan sinyal ilişkisine dayalı fiziksel katman kimlik doğrulama ve güvenlik yönteminin ML metodu için önerilen işlem adımları şu şekildedir:

- Şekil 3'te görüleceği üzere, önce eğitim verileri (A) modüle edilmekte ve T_X eğitim sembolleri (B) oluşmaktadır. Sonra T_X eğitim sembolleri (B) kanaldan

geçirilmektedir ve dış etkenlerden dolayı sembollere gürültü eklenmektedir. Böylece R_X eğitim sembolleri (C) elde edilir.

- Elde edilen T_X eğitim sembolleri (B) giriş, R_X test sembolleri (C) ise çıkış olacak şekilde makine eğitilir (108). Eğitim sonucunda makine gelecek T_X verilerine göre güvenirliği tespit edilmek istenen R_X (G) sembollerinin tahmini yapabilmektedir.

- Doğrulama yapılabilmesi için alınan R_X (G) ve tahmin edilen R_X (H) sembollere dayanarak gelen sembollerin güvenilir olup olmadığı tespit edilmektedir. Bunun için yukarıda anlatılan hipotez testi yapılır (107).

- Bu hipotez testinde alınan R_X (G) ve tahmin edilen R_X (H) semboller arasındaki fark belirli bir eşik değerinin altındaysa kullanıcı yasal, üstünde ise kullanıcı yasal değil olarak belirlenir. Bu şekilde fiziksel katman doğrulama tamamlanmış olunur.

Referanslar

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,”IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp.679–695, Apr. 2018.

[2] 5G vision,” White Paper, 5G-PPP, Feb. 2015.

[3] L. Sun and Q. Du, “A Review of Physical Layer Security Techniques for Internet of Tings: Challenges and Solutions,” Entropy, vol. 20, no. 10, p. 730, 2018.

[4] Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wireless Commun. vol. 18, no. 2, pp. 66–74, Apr. 2011.

[5] Y. Liu, H. Chen, and L. Wang, “Physical layer security for next-generation wireless networks: Theories, technologies, and challenges,” IEEE Commun. Surveys Tuts., vol. 19, no. 1, pp. 347–376, First quarter 2017.

[6] C. Pei, “Channel-based physical layer authentication,” Master’s thesis, University of Waterloo, Waterloo, 2014.

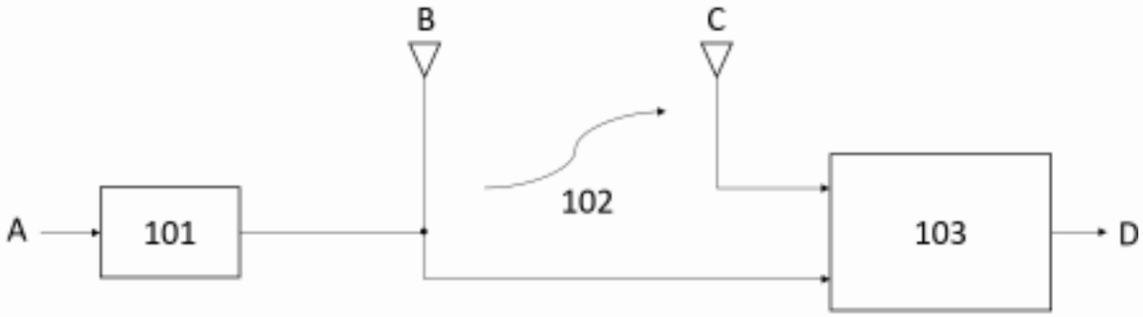
[7] M. Yilmaz and H. Arslan, “Impersonation attack identification for secure communication,” in IEEE Globecom Workshops (GC Wkshps), Dec 2013, pp. 1275–1279

[8] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, “Channel-based spoofing detection in frequency-selective rayleigh channels,” IEEE Trans. Wireless Commun., vol. 8, pp. 5948–5956, December 2009

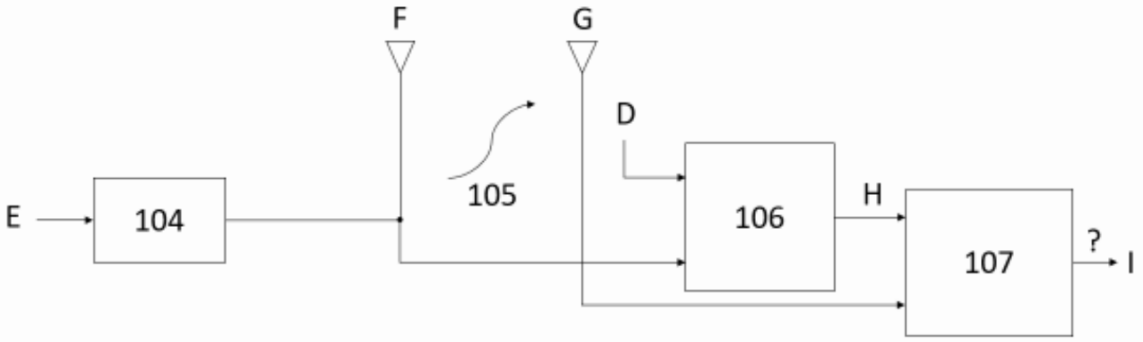
[9] H. Arslan and G. E. Bottomley, “Channel estimation in narrowband wireless communication systems,” Wireless Commun. And Mobile Comput., vol. 1, no. 2, pp. 201–219, 2001.

[10] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, “Channel-based physical layer authentication,” in Proc. GLOBECOM, Dec 2014, pp. 4114–4119.

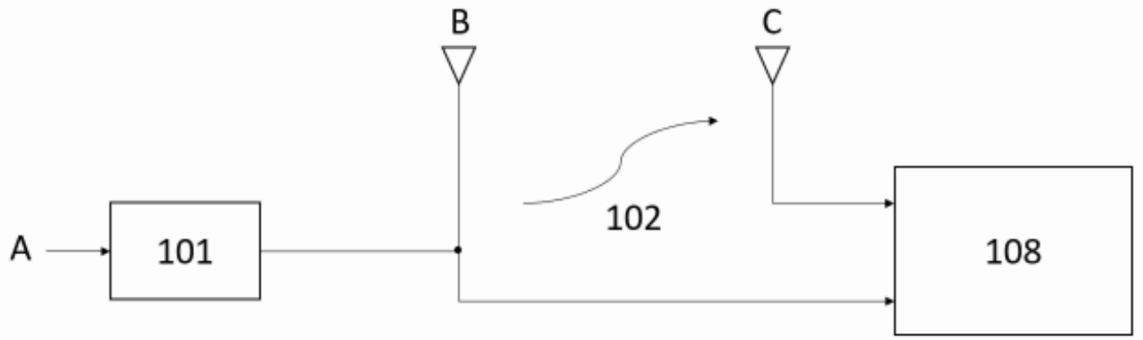
[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Fingerprints in the ether: Using the physical layer for wireless authentication,” in Proc. ICC, June 2007, pp. 4646–4651.



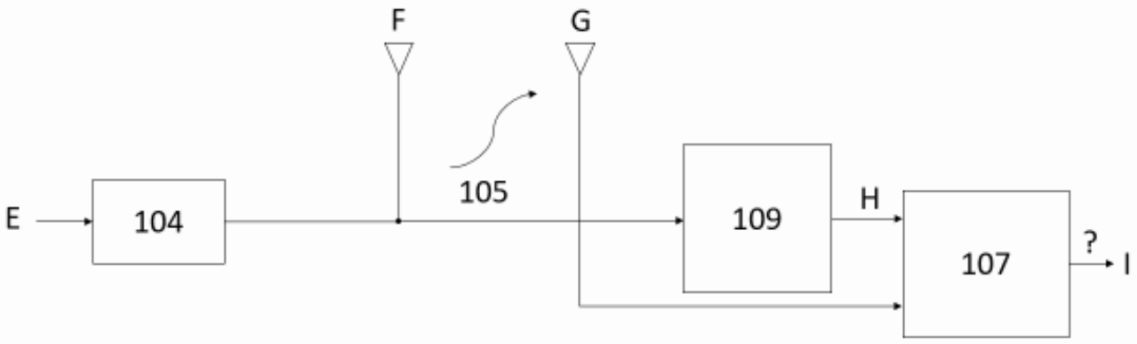
Şekil 1



Şekil 2



Şekil 3



Şekil 4