Journal of the Faculty of Engineering and Architecture of Gazi University 36:3 (2021) 1733-1745

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Ultimate secrecy in millimeter wave and terahertz communications

Ali Ekşim*, Tolga Demirci
Informatics and Information Security Research Center (TUBITAK-BİLGEM), 41470, Gebze, Kocaeli, Turkey

Highlights:

- The concept of ultimate secrecy in wireless communications is proposed
- Frequency ranges with the highest level of secrecy on millimeter wave and Terahertz bands and their level of communication secrecy are derived
- Point-to-point, cooperative and multi-hop channels were compared in terms of ultimate secrecy ranges

Keywords:

- Ultimate Secrecy
- Physical Layer Security
- Cooperative Communications
- Multi-hop Communications
- Wireless Communications

Article Info:

Research Article
Received: 12.12.2019
Accepted: 10.03.2021

DOI:

10.17341/gazimmfd.658438

Correspondence:

Author: Ali Ekşim
e-mail: ali.eksim@tubitak.gov.tr
phone: +90 262 648 1738

Graphical/Tabular Abstract

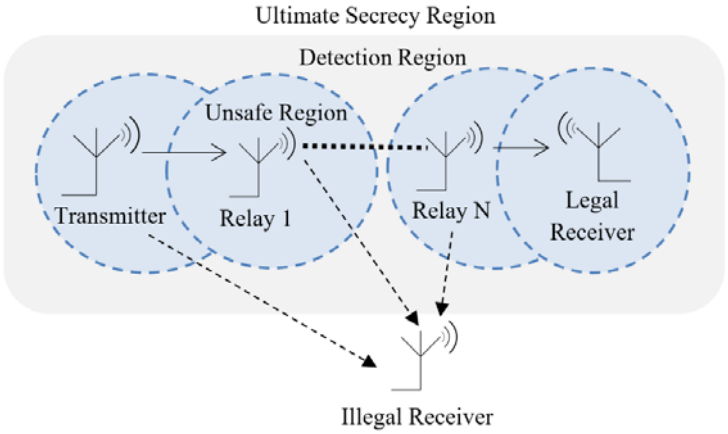


Figure A. The ultimate secrecy region of multi-hop communications is shown below.

Purpose:
Purpose of this study is to propose communication channel models and frequency bands that allow secure communication and save bandwidth for point-to-point, cooperative and multi-hop communication systems by using atmospheric attenuation properties of radio signals for millimeter wave and Terahertz bands.

Theory and Methods:
Atmospheric attenuation levels were calculated for ultimate secrecy and detection ranges of radio signals were calculated by determining the distance required for the signal to have power below the thermal noise power due to atmospheric attenuation. Calculations are done with point-to-point, cooperative and multi-hop channels. Commonly used physical layer security calculations are used to confirm the security properties of ultimate secrecy conditions.

Results:
Ultimate secrecy and detection ranges of radio signals were calculated all throughout the millimeter wave and Terahertz bands for the proposed three channel models. Secrecy ranges of cooperative and multi-hop channel are shown to be higher than point-to-point channel significantly. Number of hops is shown to be directly proportional to the range of ultimate secrecy and detection. Ultimate secrecy range is calculated to be below 7.5 km for millimeter wave band at 183 GHz and below 2 m for Terahertz band at 2899 GHz.

Conclusion:
In this work, it is shown that there are various frequency bands with high atmospheric attenuation in millimeter wave and Terahertz bands. This property is used to calculate secrecy ranges of point-to-point, cooperative and multi-hop communication channels. Calculated secrecy and detection ranges can be used to design secure and bandwidth efficient communication systems with the given frequency bands. For the three channel models, frequency bands with the highest secrecy can be used to attain secrecy and save bandwidth by frequency reuse. Determined frequency bands with low range of ultimate secrecy can be used in indoor and in-device communication systems with high demand of secrecy and bandwidth.

Journal of the Faculty of Engineering and Architecture of Gazi University 36:3 (2021) 1733-1745

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Milimetre dalga ve terahertz kablosuz haberleşmede mükemmel gizlilik

Ali Ekşim*, Tolga Demirci
Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK BİLGEM), 41470, Gebze, Kocaeli, Türkiye

ÖNEÇIKANLAR

- Kablosuz haberleşmede mükemmel gizlilik kavramı önerilmiştir
- Milimetre dalga ve Terahertz bantlarında en yüksek gizlilik düzeyine sahip frekans aralıkları ve bunların haberleşme gizliliği düzeyleri türetilmiştir.
- Noktadan noktaya, işbirlikli ve çok sekmeli kanallar mükemmel gizlilik aralıkları açısından karşılaştırıldı

Makale Bilgileri
Araştırma Makalesi
Geliş: 12.12.2019
Kabul: 10.03.2021

DOI:
10.17341/gazimmfd.658438

Anahtar Kelimeler:
Mükemmel gizlilik,
fiziksel katman güvenliği,
işbirlikli haberleşme,
çok sekmeli haberleşme,
kablosuz haberleşme

ÖZ

Bu çalışmada fiziksel katmanda haberleşme gizliliği çeşitli radyo frekansları için incelenmiştir. Milimetre dalga ve Terahertz bantlarında en yüksek seviye gizliliğe sahip frekans aralıkları ve bu aralıkların haberleşme gizliliği hesaplanmıştır. Kablosuz haberleşme için mükemmel gizlilik kavramı öne sürülmüştür. İşaret tespiti ve çözülmesi senaryoları için mükemmel gizlilik şartlarına uygun sönümleme çizgileri ve aralıkları 1 W-1000 W aralığındaki verici güçleri için hesaplanmıştır. Elde edilen sonuçlardan yola çıkılarak bant genişliği tasarruf etme yöntemi olan frekansı tekrar kullanma metodunun uygulanabileceği en yüksek potansiyele sahip frekans aralıkları hesaplanarak belirlenmiştir. Fiziksel katman gizliliği hesabı için yaygın olarak kullanılan ölçütler hesaplanmıştır. Yüksek sönümlemeye sahip frekanslar hesaplanarak bu frekanslarda işaretlerin tespit edilebileceği ve mükemmel gizliliğe sahip olduğu aralıklar tespit edilmiştir. Noktadan noktaya, işbirlikli ve çok sekmeli kanallar mükemmel gizlilik menzilleri bakımından karşılaştırılmıştır. Çok sekmeli kanallarda değişen sekme sayıları için mükemmel gizlilik menzilleri hesaplanmıştır ve sekme sayısı ile güvenlik ilişkisi gösterilmiştir. Mükemmel gizlilik menzili olarak milimetre dalga bandında 183 GHz'de 7,5 km ve Terahertz bandında ise 2899 GHz'de 2 m'nin altına indiği hesaplanmıştır. Bu sayede bina içi ve cihaz içi haberleşme (karttan karta veya çipten çipe haberleşme) gibi kısa menzilli haberleşme uygulamalarında yüksek güvenlik, aynı frekansı farklı yerlerdeki cihazlarda tekrar kullanma ve yüksek bant genişliği elde etmenin mümkün olduğu gösterilmiştir.

Ultimate secrecy in millimeter wave and terahertz communications

HIGHLIGHTS

- The concept of ultimate secrecy in wireless communications is proposed
- Frequency ranges with the highest level of secrecy on millimeter wave and Terahertz bands and their level of communication secrecy are derived
- Point-to-point, cooperative and multi-hop channels were compared in terms of ultimate secrecy ranges

Article Info
Research Article
Received: 12.12.2019
Accepted: 10.03.2021

DOI:
10.17341/gazimmfd.658438

Keywords:
Ultimate secrecy,
physical layer security,
cooperative communications,
multi-hop communications,
wireless communications

ABSTRACT

In this work, communication secrecy in the physical layer for various radio frequencies is examined. Frequency ranges with the highest level of secrecy on millimeter wave and Terahertz bands and their level of communication secrecy are derived. The concept of ultimate secrecy in wireless communications is proposed. Attenuation lines and ranges for both detection and ultimate secrecy are calculated for transmitter powers from 1 W to 1000 W. From results, frequency ranges with the highest potential to apply bandwidth saving method known as frequency reuse are devised. Commonly used secrecy benchmarks for the given conditions are calculated. Frequencies with the highest attenuation are derived and their ranges of both detection and ultimate secrecy are calculated. Point-to-point, cooperative and multi-hop channels are compared in terms of ultimate secrecy ranges. Multi-hop channel measurements are made with varying number of hops and the relation between the number of hops and communication security is examined. Ultimate secrecy ranges are calculated in millimeter wave band as under 7,5 kilometers for 183 GHz and in Terahertz band, under 2 meters for 2899 GHz. Therefore, for short-range wireless communication systems such as indoor and in-device communication systems (board-to-board or chip-to-chip communications), it is shown that millimeter wave and Terahertz bands can be used to reuse the same frequency in different locations with high security and high bandwidth.

*Sorumlu Yazar / Yazarlar / Corresponding Author / Authors: *ali.eksim@tubitak.gov.tr, tolga.demirci@tubitak.gov.tr /
Tel: +90 262 6481738

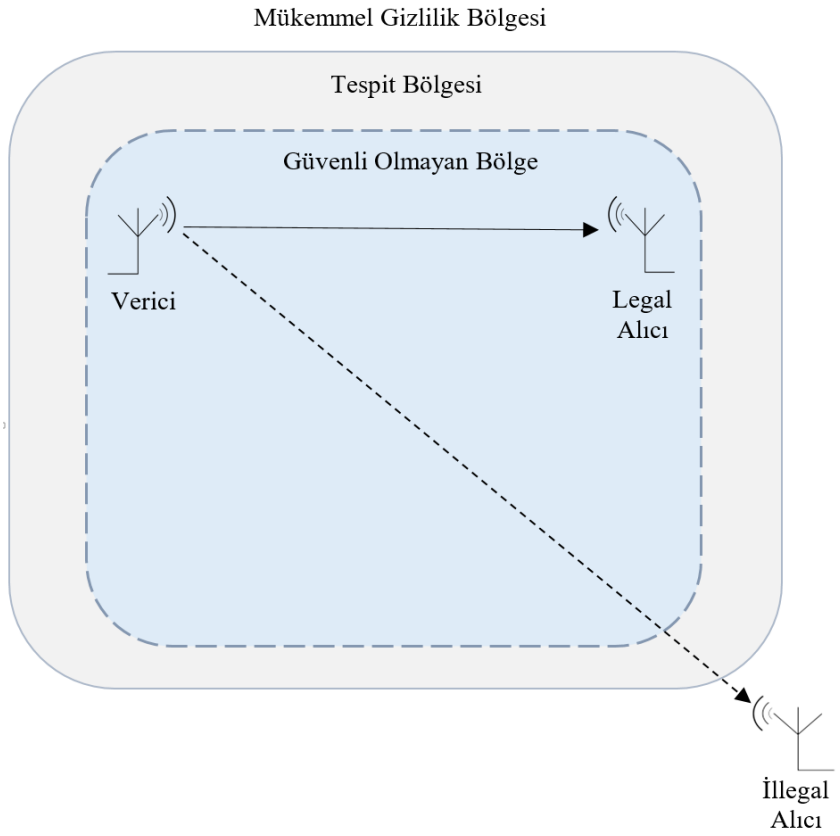
1. GİRİŞ (INTRODUCTION)

Kablosuz haberleşmede ve kablosuz yerel alan ağlarındaki yeni gelişmeler ile bant genişliğine ve haberleşme güvenliğine olan talep üstel olarak artmaktadır. Bant genişliği için spektrumdaki çoğu bant atanmış durumdadır ve kalan bantlar ise çok sınırlı ve yüksek bedele sahiptir. Bant genişliğinden tasarruf etmek için literatürde çeşitli çalışmalar bulunmaktadır. Bu probleme bir çözüm olarak uygulanan frekansı tekrar kullanma yöntemi, coğrafi bakımından birbirinden uzak olan kullanıcıların aynı frekans bantlarını kullanarak spektrumdan tasarruf etmesi şeklindedir [1]. Son yıllarda kablosuz haberleşme alanında yapılan çalışmalardan bazıları [17-20]'de verilmiştir. Diğer taraftan, haberleşme güvenliği ise kablosuz haberleşme sistemlerinin ışıma yapma doğasından ötürü önemli bir sorundur. Fiziksel katmanda haberleşme gizliliği kablosuz haberleşme sistemlerinde Shannon tarafından bilgi güvenliğinin tanımının [2] yapılmasından bu yana önemli bir konu olarak yer almaktadır. Yüksek katmanlarda kriptografinin kullanılarak güvenliğin elde edilmesi her zaman mümkün olmamaktadır. Bunun sebebi ise saldırılara açık olması, kanalın üst katmanlarının hatasız olma koşulu ve gizli anahtar saklama problemleridir [3]. Öte yandan, hızlı sönümlenen frekans bantları frekansların tekrar kullanılmasına olanak sağlamaktadır. Bu durum, farklı yerlerde bulunan çok sayıda kullanıcının aynı frekans bantlarını kullanmasını sağlayarak spektral verimi artırmaktadır. Bu çalışmada, milimetre dalga ve Terahertz bantlarında çalışan kablosuz haberleşme sistemlerinde atmosferik etkenlerin haberleşme gizliliği üzerine etkisini ve spektral tasarruf yöntemlerinin uygulanabilirliği hesaplanmaktadır. Atmosferik sönümlemenin haberleşme gizliliği üzerine etkisini belirleyebilmek için iki bölge tanımlanmıştır. Mükemmel gizlilik bölgesi, vericinin etrafında içerisinde işaretin çözülebildiği ve dışında işaretin çözülmesinin ve tespitinin mümkün olmadığı bölgedir. Bunu sağlamak için bu bölgenin dışında işaret-termal gürültü oranı 1 olmaktadır. Diğer bir bölge tanımı ise tespit bölgesidir. Tespit bölgesi, işaretin tespitinin mümkün olduğu ancak çözülmesinin mümkün olmadığı bölge olarak tanımlanmıştır. Radyo işaretlerinin atmosferik sönümlenmesinin hesabında atmosferik gazlardan su, oksijen ve azotun etkisi hesaba katılmıştır. Bu gazların varlığı frekans, sıcaklık, atmosferik basınç ve su buharı miktarına göre radyo işaretlerinde sönümlemeye yol açmaktadır. İşaretlerin atmosferik sönümlemesi en çok havadaki su buharı ve oksijenden kaynaklanmaktadır [6]. Atmosferik sönümleme milimetre dalga ve Terahertz bantları için [4]'de Annex-1'deki hesaplamalara göre varsayılan parametreler ile gerçekleştirilmiştir: 15°C sıcaklık, 1013,25 hPa atmosferik basınç ve 7,5 g/m^3 su buharı yoğunluğu. Toplam sönümleme Ω, su buharından kaynaklanan sönümleme (Ω_w) ile oksijenden kaynaklanan sönümleme (Ω_o)'ın toplamı olarak hesaplanmıştır (Eş. 1) [4].

$$\Omega = \Omega_w + \Omega_o \; dB/km. \quad (1)$$

Bu yöntemde sönümleme çizgileri tanımlanarak birbirleri üzerine eklenmektedir. Oksijen kaynaklı sönümleme için Debye modeli kullanılmıştır. Su buharı kaynaklı sönümleme için su bulut oluşumu ve bulut boyutu hesaba katılmıştır. Kablosuz haberleşmedeki önemli bir problem olan bant genişliğinin azlığına bir çözüm de spektrumda kullanılmayan yüksek frekansları kullanmaktır. Daha yüksek frekanslar kullanılarak daha yüksek bant genişlikleri daha kolay elde edilebilir. Yüksek frekanslar daha yüksek atmosferik sönümlemeye sahiptir. Bu yüzden frekansı tekrar kullanma yöntemini kullanmak ve yüksek haberleşme güvenliği elde etmek için daha fazla fırsat sağlamaktadır. Diğer taraftan fiziksel katman güvenliği, kablosuz haberleşme sistemlerinde önemli bir yere sahiptir. Daha güvenli haberleşme elde etmek, daha yüksek atmosferik sönümlemeye sahip frekansları kullanıp illegal dinlemeyi engelleyerek mümkündür. Radyo işaretlerinin atmosferik sönümlemesi literatürde çeşitli çalışmalarda incelenmiştir [4–7]. Ancak atmosferik sönümlemenin işaret gizliliğine olan etkisini inceleyen bilinen bir çalışma bulunmamaktadır. Bu çalışmada, radyo işaretlerinin milimetre dalga ve Terahertz bantları için fiziksel katman güvenliği hesaplamaları gerçekleştirilmiştir. Radyo işaretleri su ve oksijen kaynaklı sönümlemelere karşı açıktır [6]. Sönümlemenin derecesi ise International Telecommunication Union (ITU) tarafından hazırlanan öneri çalışmasında [4] verilen yöntemler ile hesaplanmıştır. Sonuç olarak bir işaretin fiziksel katman güvenliğinin kalitesi, verilen frekanstaki atmosferik sönümleme miktarı ile orantılıdır. Eğer atmosferik sönümleme, işaretin termal gürültü ile aynı seviyeye gelmesini sağlıyorsa bu işareti tespit etmek veya çözmek mümkün değildir. Sonuç olarak 1 THz'den sonra birçok frekans bandı için mükemmel gizlilik mesafesi 2 m'nin altındadır. Bu şartlarda işaretleri tespit etmek veya çözmek mümkün değildir çünkü işaret gürültü oranının düşüklüğünden dolayı işaret, termal gürültü ile karışmış durumdadır. Verici gücünü 1000 W'a kadar çıkarmak bile işaretin çözülebileceği mesafeyi önemli derecede arttıramamaktadır. Bu ise fiziksel katmanın güvenli olduğunu göstermektedir. Bu çalışmada, milimetre dalga ve Terahertz bantlarında çeşitli radyo frekansları için haberleşme gizliliğinin en yüksek seviyede olduğu frekanslar Şekil 1'de belirtilen bölgeler için belirlenmiştir.

Radyo işaretleri için atmosferik sönümleme milimetre dalga ve Terahertz bantları için [4]'de Annex-1'deki çalışmada verilen yöntemle hesaplanabilmektedir. Literatürde yaygın olarak kullanılan fiziksel katman güvenliği hesaplamaları olan gizlilik kapasitesi [8], gizlilik kesim olasılığı [11] ve kesinlikle pozitif gizlilik kapasitesi [10] hesaplanmıştır. Bu hesaplamalar bilgi kuramı yönünden fiziksel katman güvenliğini hesaplamada kullanılmaktadır. Hesaplamalar için [14]'teki çalışmalar temel alınarak [15]'teki sönümleme hesaplamaları dikkate alınmıştır. Çalışmadaki bölümlerin düzeni ise şu şekildedir: Bölüm 2.1'de işaretlerin atmosferik sönümlemesi açıklanmıştır ve milimetre dalga ve Terahertz bantları için atmosferik sönümlemeler hesaplanmıştır. Bölüm 2.2'de güvenli haberleşme sınırları ve mükemmel



Şekil 1. Noktadan noktaya haberleşme kanal modeli (Point-to-point communication channel model)

gizlilik ile işaret tespiti bölgelerinin menzilleri hesaplanmıştır. Milimetre dalga ve Terahertz bantlarında mükemmel gizlilik menzili en düşük olan en güvenli frekansların menzilleri tespit edilerek incelenmiştir. Bölüm 2.3'te fiziksel katman güvenliği hesaplamaları olan gizlilik kapasitesi, gizlilik kesim olasılığı ve kesinlikle pozitif gizlilik kapasitesi hesaplamaları mükemmel gizlilik durumu için hesaplanmıştır. Bölüm 3'te işbirlikli haberleşme kanalı için mükemmel gizlilik hesaplamaları yapılmıştır ve noktadan noktaya haberleşme kanalı ile mükemmel gizlilik menzilleri yönünden karşılaştırılmıştır. Bölüm 4'te ise çok sekmeli kanal için mükemmel gizlilik menzilleri hesaplanmıştır. Mükemmel gizlilik menzilleri çok sekmeli kanalların değişen sayıda sekme sayısı için hesaplanmıştır. Hesaplanan menziller milimetre dalga ve Terahertz bantları için noktadan noktaya haberleşme kanalı ile karşılaştırılarak sekme sayısının haberleşme gizliliğine olan etkisi gösterilmiştir. Bölüm 5'de ise çalışmadan elde edilen sonuçlar sunulmuştur.

2. NOKTADAN NOKTAYA KANAL MODELİ
(POINT-TO-POINT CHANNEL MODEL)

Noktadan noktaya haberleşme kanalı bir verici, bir legal alıcı ve bir illegal alıcıdan oluşmaktadır. Bu haberleşme kanalında işaretlerin atmosferik sönümlemesi çeşitli frekans bantlarında hesaplanmıştır. İşaretlerin tespitinin ve çözülmesinin mümkün olduğu menziller hesaplanmıştır. Elde edilen sonuçlardan yola çıkarak genel bir formül türetilmiştir. Literatürde yaygın olarak kullanılan haberleşme güvenliği hesaplamaları bu kanal için gerçekleştirilmiştir.

2.1. İşaretlerin Atmosferik Sönümlenmesi
(Atmospheric Attenuation of Signals)

Radyo işaretleri, atmosferik şartlarda sönümlemeye maruz kalmaktadır. Atmosferik sönümlemenin derecesi ise radyo işaretinin frekansına göre değişmektedir. Verilen frekans değerleri ve hava durumu şartlarında atmosferik sönümlemenin hesaplanması için [4]'teki Annex-1 kullanılmıştır. Milimetre dalga ve Terahertz bantları için atmosferik sönümleme Şekil-2'de verilmiştir. Şekil-2'den görülebildiği gibi belirli frekans aralıklarında sönümleme derecesi yüksektir; dolayısıyla işaretlerin tespit ve çözümleme menzilleri düşüktür. Buradan yola çıkarak bu frekans bantlarını kullanarak güvenli haberleşme elde etmek veya frekansı tekrar kullanma yöntemiyle bant genişliği tasarrufu yapmak mümkündür.

2.1.1. Güvenli Haberleşme Sınırları
(Secure Communication Boundaries)

İşaretin 1 Hz bant genişliğine sahip olduğu ve verici anteninin iletim gücü 30 dBm olan birim kazançlı bir anten olduğu varsayılmaktadır. Bu durumda ortam sıcaklığı 15°C için 204 dB'den fazla yol kaybına sahip işaretler termal gürültü seviyesine geleceği için tespiti ve çözümlenmesi

mümkün değildir. Deneysel çalışmalara göre termal gürültünün 3 dB üzerinde çözümlemek mümkün olmamakla beraber tespiti mümkün olmaktadır [7]. Bu yüzden bu şartlarda işaret tespiti için yol kaybının en fazla 201 dB olması gerekmektedir [4]. Buradan yola çıkarak haberleşmenin tamamen güvenli olduğu frekansları ve haberleşmenin güvenli olduğu bölgenin menzilini hesaplamak mümkündür. Milimetre dalga ve Terahertz bantları için mesafe başına düşen sönümleme miktarı eğrileri Şekil 2a ve Şekil 2b'de verilmiştir.

2.2. Mükemmel Gizlilik Hesaplamaları
(Ultimate Secrecy Calculations)

Bu çalışmadaki sistem, Şekil 1'de gösterildiği gibi bir verici, bir legal alıcı ve bir illegal alıcıdan oluşmaktadır. Mükemmel gizlilik bölgesi, vericinin etrafında işaretin tespitinin veya çözümlenmesinin mümkün olmadığı bölge olarak tanımlanmaktadır. İşaret-termal gürültü oranının 1'e eşit olması durumunda bu şartlar sağlanmaktadır. Tespit bölgesi ise vericinin etrafında işaretin tespitinin mümkün olduğu ancak çözümlenmesinin mümkün olmadığı bölge olarak tanımlanmaktadır. 1 W verici gücü ve 15°C sıcaklık ile alıcı-verici arası yol kaybının 204 dB'den fazla olması durumunda termal gürültüden dolayı işaretleri tespit etmek mümkün değildir [5]. Yol kaybı 204 dB'ye kadar ise işaretleri tespit etmek mümkün olmakla beraber çözümlemek mümkün olmamaktadır.

Deneysel bir çalışmaya göre bina içi bir çalışmada işaretlerin tespit edilemez duruma gelmeleri için alıcı-verici arası mesafenin 30 m olması veya aralarında bir kat bulunması yeterli olmuştur [12].

Bu sistemde verici ve alıcıların izotropik antene sahip oldukları varsayılmıştır. Termal gürültü (Eş. 2) [13],

$$N_T = -174\ dBm. \tag{2}$$

İzotropik anten kazancı (Eş. 3),

$$U_G = 0\ dBi. \tag{3}$$

Verici gücü (Eş. 4),

$$P_T = 30\ dBm. \tag{4}$$

İletim gücünün 1 W olduğu durumda mükemmel gizlilik ve işaret tespiti bölgelerinin menzilleri Şekil 3'te verilmiştir.

Tespit bölgesi ve mükemmel gizlilik bölgelerinin çok yakın olmasından dolayı iki bölgenin daha iyi ayırt edilebilmesi için 181-186 GHz ve 2895-2902 GHz aralığındaki menziller Şekil 4'te gösterilmiştir.

Benzer şekilde, verici güçleri 1W, 10 W, 100 W ve 1 kW için mükemmel gizlilik menzilleri Şekil 5'te verilmiştir. Dört ayrı güç seviyesinin menzillerinin ayırt edilebilmesi için 181-186 GHz ve 2897-2901 GHz bantlarında menzil eğrileri Şekil 6'da gösterilmiştir. Mükemmel gizlilik ve işaret tespiti için verilen verici güç değerlerinde gereken yol kayıpları (Eş. 5- Eş. 12) ise aşağıdaki gibidir.

Verici gücü 1 W için, $P_T = 30$ dBm,

$$L_{U_1W} = 174 + P_T = 204\ dB \tag{5}$$

$$L_{D_1W} = L_{U_1W} - 3\ dB = 201\ dB. \tag{6}$$

Tespit bölgesi sınırı termal gürültünün 3 dB üzeridir. Verici gücü 10 W için (P_T = 40 dBm),

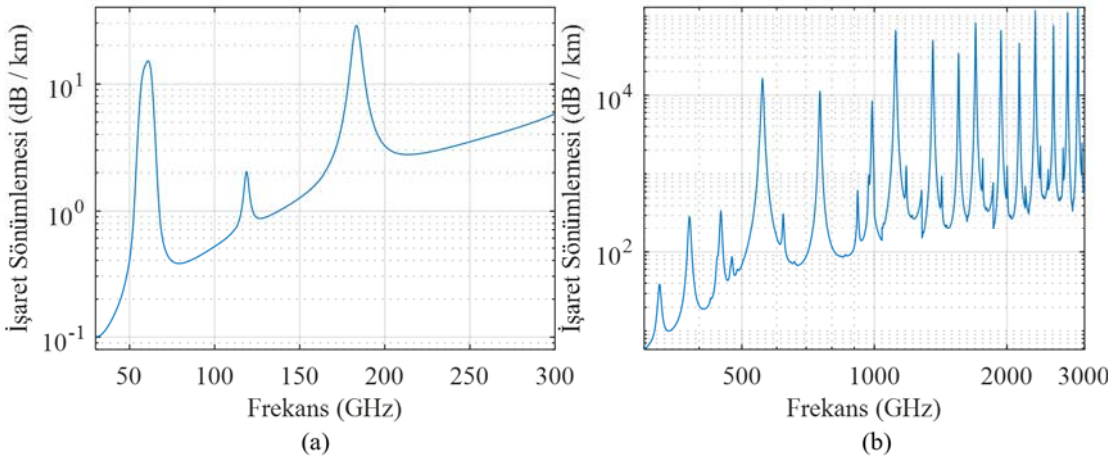
$$L_{U_{10}W} = 174 + P_T = 214\ dB. \tag{7}$$

$$L_{D_{10}W} = L_{U_{10}W} - 3\ dB = 211\ dB. \tag{8}$$

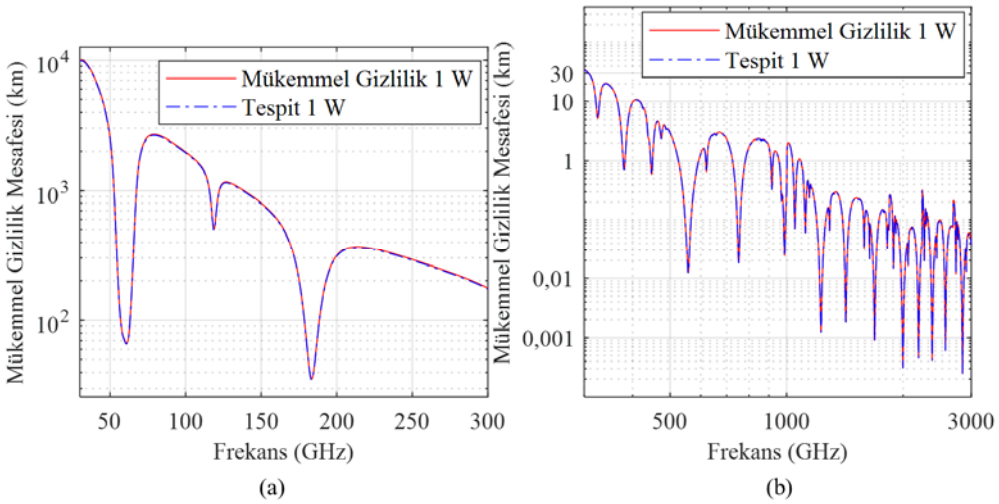
Verici gücü 100 W için ($P_T = 50\ dBm$),

$$L_{U_{100}W} = 174 + P_T = 224\ dB \tag{9}$$

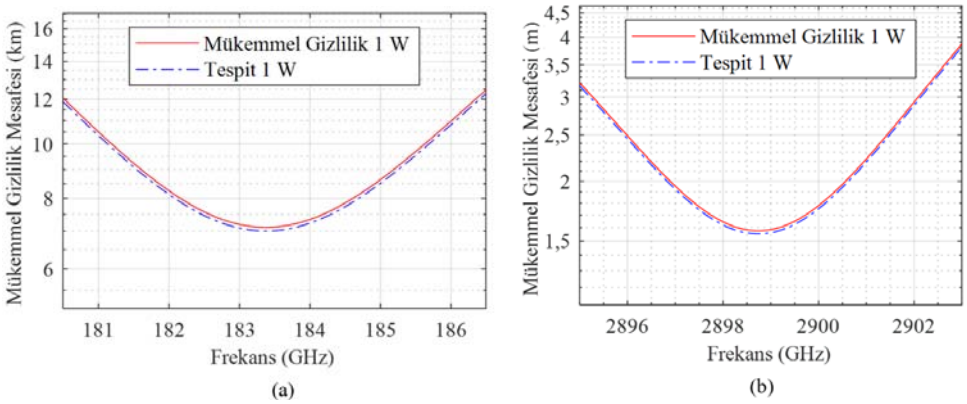
$$L_{D_{100}W} = L_{U_{100}W} - 3\ dB = 221\ dB. \tag{10}$$



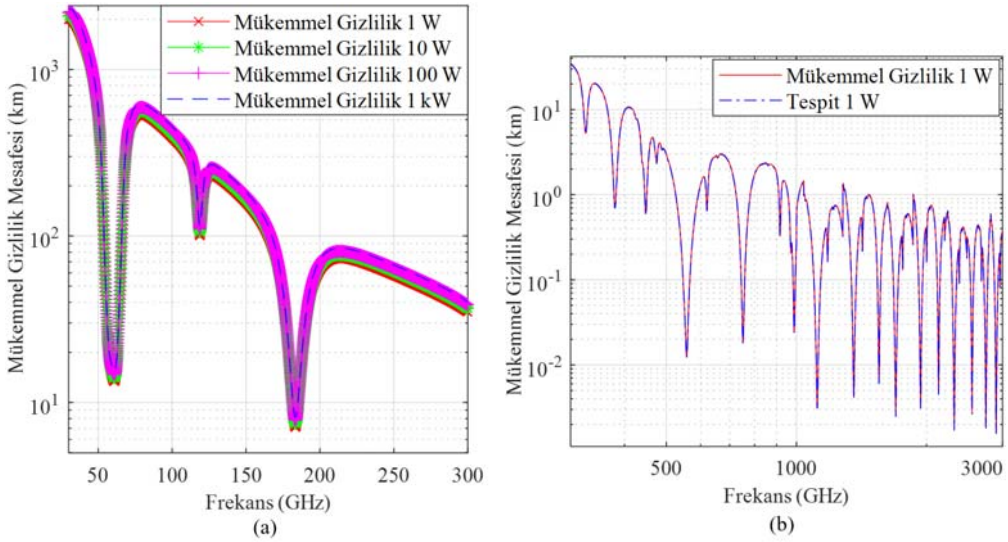
Şekil 2. Atmosferik sönümleme (a) Milimetre dalga bandı (b) Terahertz bandı
(Atmospheric attenuation (a) Millimeter wave band (b) Terahertz band)



Şekil 3. Noktadan noktaya haberleşme kanalında mükemmel gizlilik ve tespit mesafeleri (a) Milimetre dalga bandı (b) Terahertz bandı
(Ultimate secrecy and detection distances in the point-to-point communication channel (a) Millimeter wave band (b) Terahertz band)



Şekil 4. Mükemmel gizlilik ve tespit mesafeleri (a) 181-186 GHz bandı (b) 2895-2902 GHz bandı
(Ultimate secrecy and detection distances (a) 181-186 GHz band (b) 2895-2902 GHz band)



Şekil 5. Çeşitli verici gücü değerleri için mükemmel gizlilik mesafeleri (a) Milimetre dalga bandı (b) Terahertz bandı
(Ultimate secrecy distances for various transmitter power values (a) Millimeter wave band (b) Terahertz band)

Verici gücü 1 kW için (P_T = 60 dBm),

$$L_{U_{1\,kW}} = 174 + P_T = 234\ dB \quad (11)$$

$$L_{D_{1\,kW}} = L_{U_{1\,kW}} - 3\ dB = 231\ dB. \quad (12)$$

Tablo 1. Çeşitli verici güç değerleri için yol kayıpları
(Path losses for various transmitter power values)

Verici Gücü Watt (W)	İşaret tespiti için yol kaybı L_U (dB)	Mükemmel gizlilik için yol kaybı L_D (dB)
1	201	204
10	211	214
100	221	224
1000	231	234

Tablo 1'de çeşitli verici gücü değerlerinde mükemmel gizlilik ve işaret tespiti şartlarının sağlanması için gerekli yol kaybı değerleri verilmiştir. 1 W'dan 1000 W'a kadar, işaret tespiti ve mükemmel gizlilik bölgeleri için sönümleme çizgileri ve menzilleri hesaplanmıştır. Haberleşme gizliliği verici gücünün 1'den 1000 kata kadar değişmesine karşın çok az etkilendiği görülmektedir. Bu durum, sistemin gizliliğinin kararlılığını teyit etmektedir. Haberleşme sistemlerinde yüksek gizlilik elde etmek için bu şartlar kullanılabilmektedir. Örneğin, 28 GHz bandındaki deneysel bir çalışmada, hesaplanandan daha yüksek atmosferik sönümlemenin gerçekleştiği gözlemlenmiştir [7]. Çalışmada gösterildiğine göre işaretler, ITU'nun atmosferik sönümleme üzerine olan çalışmasındaki yöntem ile hesaplanan mesafelerden daha kısa olmaktadır [4]. İşaretler, hesaplanan sönümleme değerlerine karşın aynı binada farklı katlarda dahi tespit edilemez duruma gelmiştir. İşaretlerin menzilleri, engeller, nesneler ve insanlar gibi çevresel etkenlerden dolayı Şekil 3-Şekil 6'da gösterilen değerlerden daha düşük olmaktadır.

Mükemmel gizlilik için genelleştirilmiş formül (Eş. 13) [14], alıcı-verici arasındaki yol kaybı cinsinden aşağıdaki gibidir:

$$L_U \geq 174 + P_T + A_{G_T} + A_{G_R} - B. \quad (13)$$

Verilen ifadede A_{G_T} verici anten kazancı, A_{G_R} alıcı anten kazancı ve B işaretin bant genişliğidir. Bu eşitsizlikte, mükemmel gizliliği elde edebilmek için alıcı ile verici arasındaki yol kaybının, 0 dBi alıcı ve verici anten kazancı, 1 W verici gücü ve 1 Hz bant genişliği için 204 dB'ye eşit veya büyük olması gerekmektedir.

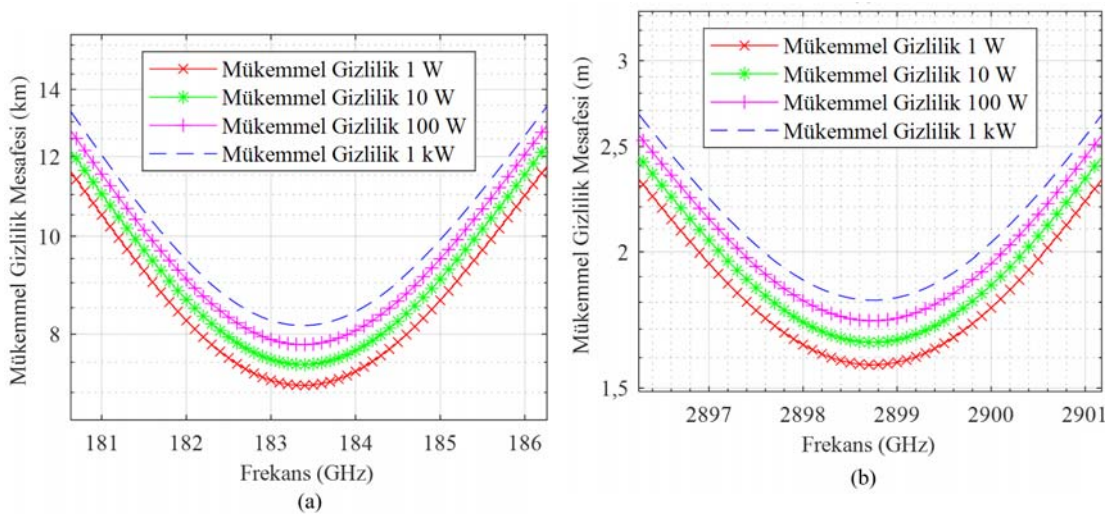
2.3. Fiziksel Katman Gizliliği (Physical Layer Security)

Bu bölümde literatürde yaygın olarak kullanılan bilgi kuramı temelli fiziksel katman gizlilik hesaplamaları verilen frekans ve mesafeler için hesaplanmıştır. Gizlilik, bir Wyner dinleme kanalı için yarı statik olarak tanımlanmıştır [9]. Bu modelde bir verici işareti iletmektedir ve legal alıcı ile illegal alıcılar işareti almaktadır. Legal alıcı ile verici arasındaki kanalın-gürültü gücü N_M, verici ile illegal alıcı arasındaki kanalın ise gürültü gücü N_W olup her iki kanal da toplamsal beyaz Gauss gürültüsü kanalıdır (AWGN). İletim gücü P_T olarak sınırlandırılmıştır. Bu parametrelere göre gizliliği sağlanan kanallar fiziksel katmanda güvenli olarak kabul edilmektedir. Bu, güvenliği elde etmek için kriptografik katmana olan ihtiyacı ortadan kaldırmaktadır. Kriptografik katmanlar hatasız üst katmana ihtiyaç duymaktadır, bu da maliyetli olmaktadır [12]. Bu sistemler saldırılara karşı açıktır ve çeşitli anahtar yönetimi problemleri mevcuttur [3]. Fiziksel katman gizliliğini tanımlamak ve hesaplamak için literatürde kullanılan çeşitli tanımlamalar mevcuttur.

2.3.1. Gizlilik kapasitesi (Secrecy capacity)

Gizlilik kapasitesi (Eş. 14) [8] aşağıdaki gibi tanımlanmıştır,

$$C_S = C_M - C_W. \quad (14)$$



Şekil 6. Çeşitli verici gücü değerleri için mükemmel gizlilik mesafeleri (a) 181-186 GHz bandı (b) 2897-2901 GHz bandı
(Ultimate secrecy distances for various transmitter power values (a) 181-186 GHz band (b) 2897-2901 GHz band)

Burada, temel kanalın gizlilik kapasitesi (Eş. 15)

$$C_M = \frac{1}{2}\log_2\left(1+\frac{P_T}{N_M}\right), \tag{15}$$

illegal kanalın gizlilik kapasitesi (Eş. 16)

$$C_W = \frac{1}{2}\log_2\left(1+\frac{P_T}{N_W}\right). \tag{16}$$

Mükemmel gizliliğe ulaşıldığında gizlilik kapasitesi C_U (Eş. 17),

$$C_U = C_M - C_W. \tag{17}$$

İletim gücünün 1 W olduğu varsayılmıştır. Mükemmel gizliliğe ulaşıldığında 204 dB'den fazla kayıp olmalıdır. (Eş. 15) ve (Eş. 16), (Eş. 17)'de yerine yazıldığında, sırayla (Eş. 18) ve (Eş. 19)'dan (Eş. 20) elde edilir.

$$C_U = \frac{1}{2}\log_2\left(1+\frac{1}{N_M}\right) - \frac{1}{2}\log_2\left(1+\frac{1}{N_W}\right) \tag{18}$$

$$C_U = \frac{1}{2}\left(\log_2\left(\frac{1+\frac{1}{N_M}}{1+\frac{1}{N_W}}\right)\right) \tag{19}$$

$$C_U = \frac{1}{2}\left(\log_2\left(\frac{\frac{N_M+1}{N_M}}{\frac{N_W+1}{N_W}}\right)\right). \tag{20}$$

Mükemmel gizlilik senaryosu için temel kanalın SNR'ı 1'e eşittir. Dolayısıyla, (Eş. 21) ve (Eş. 22) kullanilarak (Eş. 23) elde edilir.

$$N_M \ll N_W. \tag{21}$$

Dolayısıyla,

$$\frac{N_M}{N_W} \to 0. \tag{22}$$

$$C_u = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_W) & \gamma_M > \gamma_W \\ 0 & \gamma_M < \gamma_W \end{cases} \tag{23}$$

Legal alıcının SNR'ının (γ_M) illegal alıcının SNR'ından (γ_W) büyük olduğu varsayıldığı için gizlilik kapasitesi (Eş. 24),

$$C_u = \log_2\left(\frac{1+\gamma_M}{1+\gamma_W}\right). \tag{24}$$

Mükemmel gizlilik senaryosunda illegal alıcının SNR'ının 1'e eşit olduğu (0 dB) durum için (Eş. 25),

$$C_u = \log_2\left(\frac{1+\gamma_M}{2}\right). \tag{25}$$

Bu durumda gizlilik kapasitesi C_U, legal alıcının SNR'ından bağımsız olarak her zaman pozitiftir. Bu durumda pozitif gizlilik kapasitesi ile kanalın mükemmel gizlilik senaryosunda bilgi kuramı güvenliği bakımından güvenli olduğu sonucuna ulaşılmaktadır.

2.3.2. Gizlilik kesim olasılığı (Secrecy outage probability)

Gizlilik kesim olasılığı, anlık gizlilik kapasitesinin hedef bir gizlilik kapasitesinden az olması olasılığıdır $R_s > 0$ [8]. Gizlilik kesimi ana haberleşme kanalının illegal dinleyici kanalından fiziksel katman güvenliği yönünden daha kötü olduğunu göstermektedir.

$$P_o(R_s) = P(C_s < R_s) \tag{26}$$

ve

$$P_o(R_s) = 1 - \frac{\bar{\gamma}_M}{\bar{\gamma}_M + 2^{R_S}\bar{\gamma}_W}\exp\left(-\frac{2^{R_S}-1}{\bar{\gamma}_M}\right). \tag{27}$$

Mükemmel gizlilik senaryosu için illegal alıcının SNR değeri 1'e eşit olduğu durumda (0 dB), (Eş. 26) ve (Eş. 27)'den yararlanılarak gizlilik kesim olasılığı (Eş. 28),

$$P_o(R_s) = 1 - \frac{\bar{\gamma}_M}{\bar{\gamma}_M + 2^{R_S}}\exp\left(-\frac{2^{R_S}-1}{\bar{\gamma}_M}\right). \tag{28}$$

Mükemmel gizlilik senaryosu için gizlilik kesim olasılığı her zaman sıfır olmaktadır. Bu durum sınır değer olan R_s'e bağlı değildir çünkü illegal alıcının işaret-gürültü oranı 1'e eşittir. Sıfır gizlilik kesim olasılığı ile kanalın mükemmel gizlilik şartları altında tamamen güvenli olduğu ortaya çıkmaktadır.

2.3.3. Kesinlikle pozitif gizlilik kapasitesi (Strictly positive secrecy capacity)

Kesinlikle pozitif gizlilik kapasitesi (SPSC), anlık gizlilik kapasitesinin pozitif olma olasılığını ifade etmektedir [10]. SPSC nin matematiksel ifadesi (Eş. 29-30),

$$P_h(R_s) = P(C_s > R_S) \tag{29}$$

$$P_h(R_s) = \frac{\bar{\gamma}_M}{\bar{\gamma}_M + 2^{R_S}}\exp\left(-\frac{2^{R_S}-1}{\bar{\gamma}_M}\right). \tag{30}$$

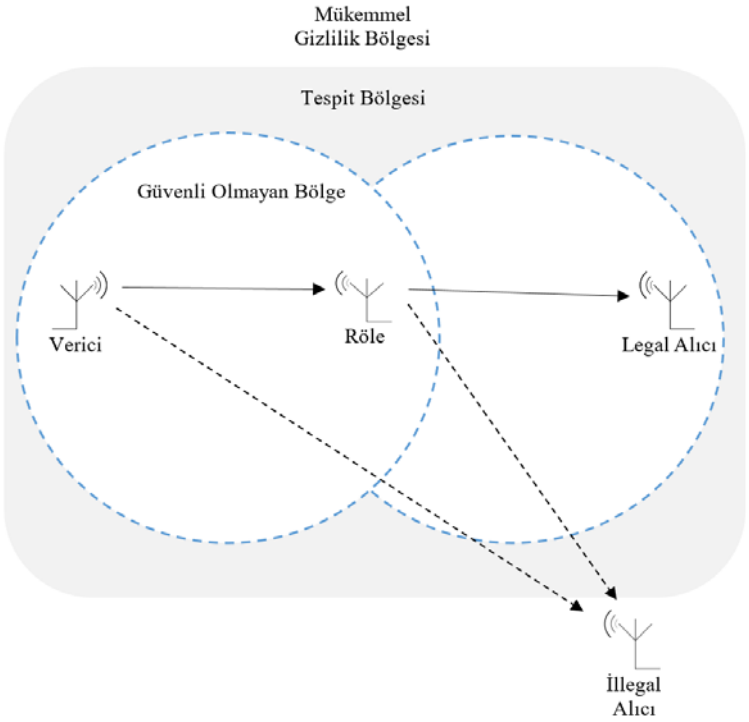
Kesinlikle pozitif gizlilik kapasitesi için, $R_S = 0$ ve legal alıcı, illegal alıcıya kıyasla yüksek SNR'a sahiptir ve illegal alıcının SNR değeri 1 veya daha düşüktür. Dolayısıyla SPSC ifadesi her zaman pozitif olmaktadır. Bu durumda kanalın bilgi kuramı bakımından güvenli olduğunu göstermektedir. Fiziksel katman güvenliği hesaplamalarına göre mükemmel gizlilik şartlarında haberleşme kanalının tamamen güvenliği olduğu sonucu ortaya çıkmaktadır. İllegal alıcının işaret-termal gürültü oranı 1'e eşit olduğunda haberleşme illegal alıcılara karşı tamamen güvenlidir.

3. İŞBİRLİKLİ HABERLEŞME KANAL MODELİ (COOPERATIVE CHANNEL MODEL)

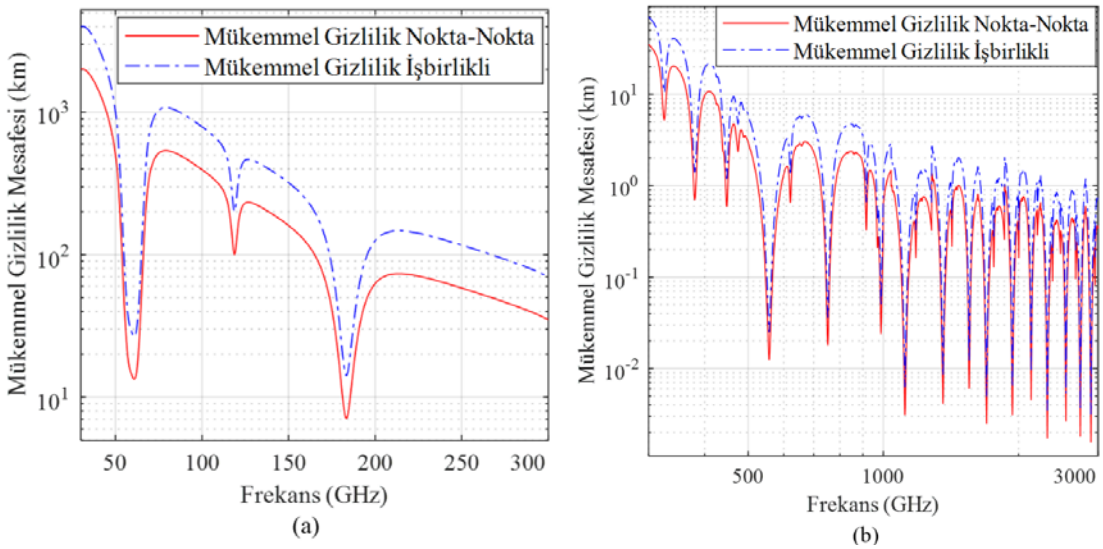
İşbirlikli haberleşme kanalı bir verici, bir legal alıcı, bir röle ve bir illegal alıcıdan oluşmaktadır. Bu haberleşme kanalında işaretlerin atmosferik sönümlemesi çeşitli frekans

bantlarında hesaplanmış, işaretlerin tespitinin ve çözülmesinin mümkün olduğu menziller ortaya konmuştur. Elde edilen sonuçlardan yola çıkarak genel bir formül türetilmiştir. Literatürde yaygın olarak kullanılan haberleşme güvenliği hesaplamaları noktadan noktaya haberleşme kanalında olduğu gibi işbirlikli kanalda da geçerlidir. Şekil 7'de işbirlikli haberleşme kanal modeli [16] gösterilmiştir.

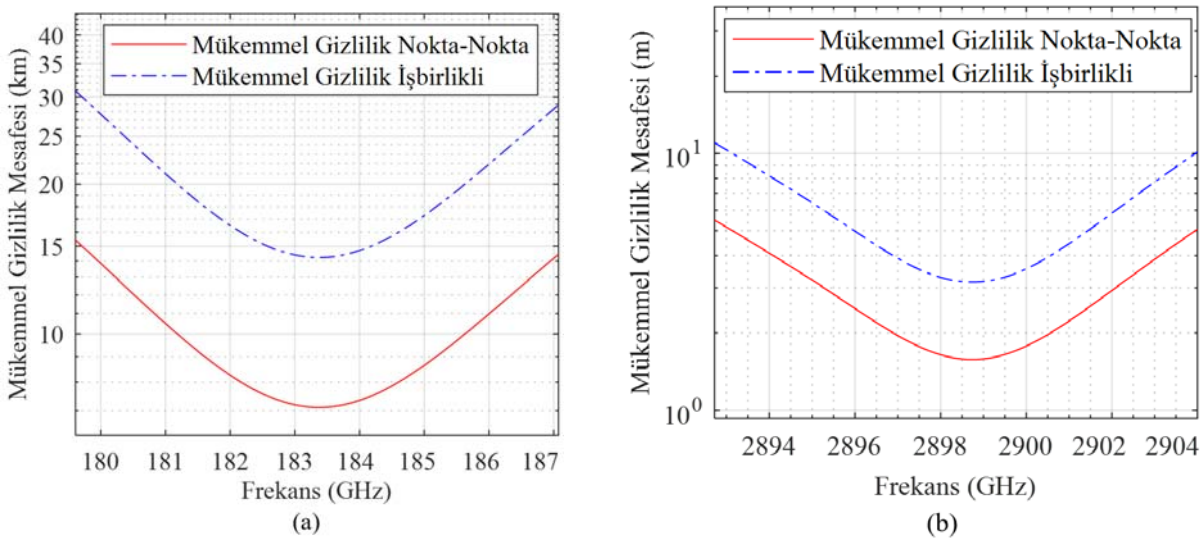
İşbirlikli haberleşme kanalında vericiden alınan işaret röle aracılığı ile alıcıya ulaşacağı için işaret normal durumda verici-röle-legal alıcı yolunu izlemesi gerekmektedir. Ancak illegal alıcının işareti alabilme durumu göz önüne alınırsa işaretin verici-illegal alıcı veya verici-röle-illegal alıcı yollarını izlemesi de mümkündür. Burada işaretin mükemmel gizlilik ve işaret tespiti menzillerini hesaplamak için sistemin en kötü güvenliğe sahip senaryosu dikkate alınırsa bu durumda işaretin mükemmel gizlilik ve tespit menzilleri aşağıdaki gibi hesaplanabilir: Vericinin mükemmel gizlilik menzili d_1, rölenin mükemmel gizlilik menzili d_2 olarak alınırsa sistemin mükemmel gizlilik menzili bu durumda $d_1 + d_2$ olmaktadır. İşbirlikli



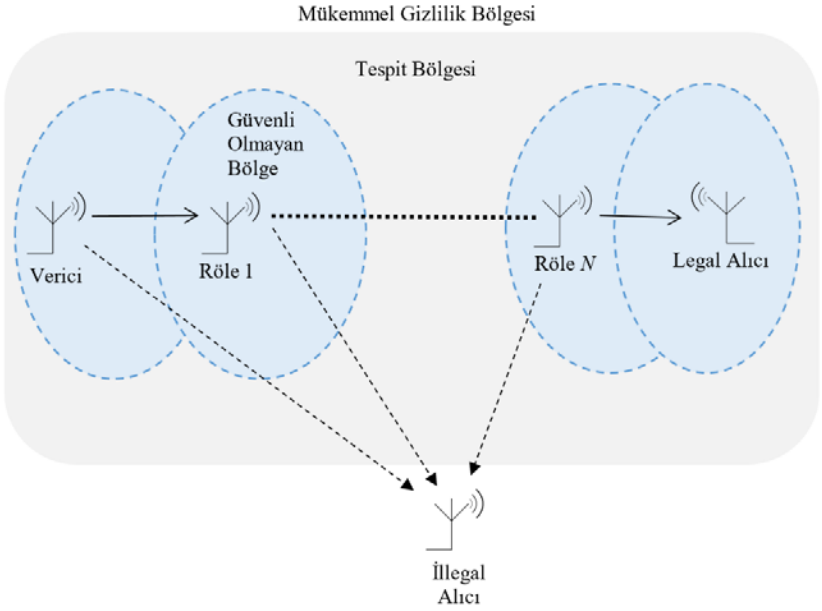
Şekil 7. İşbirlikli haberleşme kanal modeli (Cooperative communication channel model)



Şekil 8. İşbirlikli haberleşme kanalında mükemmel gizlilik ve tespit mesafeleri (a) Milimetre dalga bandı (b) Terahertz bandı (Ultimate secrecy and detection distances in the cooperative communication channel (a) Millimeter wave band (b) Terahertz band)



Şekil 9. İşbirlikli haberleşme kanalında mükemmel gizlilik ve tespit mesafeleri (a) Milimetre dalga 180-187 GHz bandı (b) Terahertz 2894-2904 GHz bandı (Ultimate secrecy and detection distances in the cooperative communication channel (a) Millimeter wave 180-187 GHz band (b) Terahertz 2894-2904 GHz band)

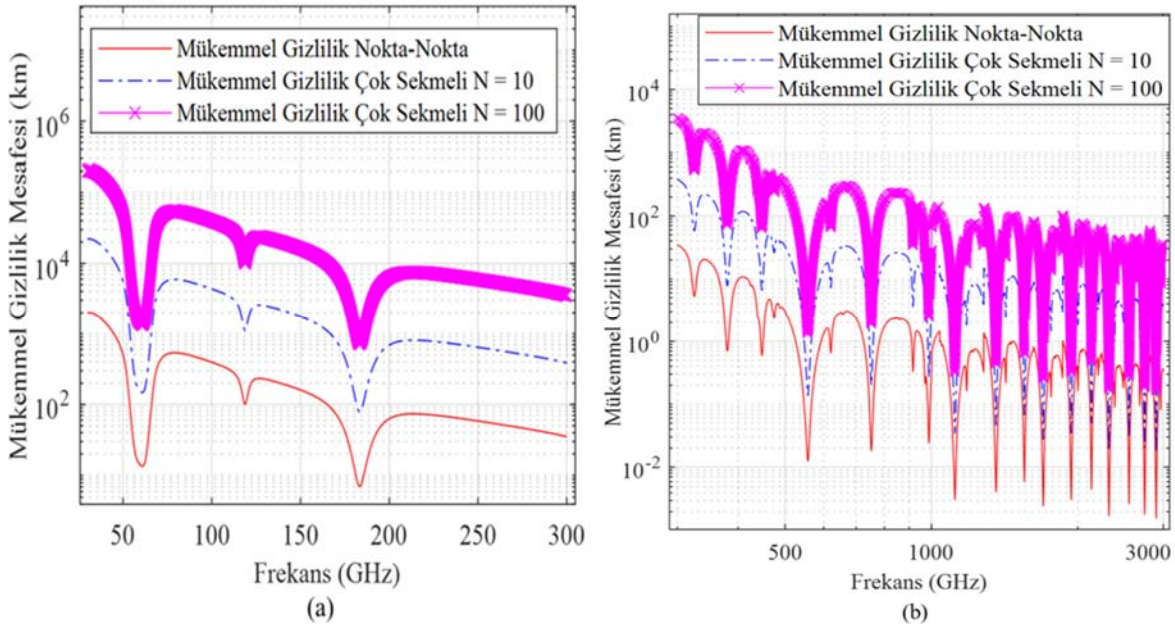


Şekil 10. Çok sekmeli kanal modeli (Multi-hop communication channel model)

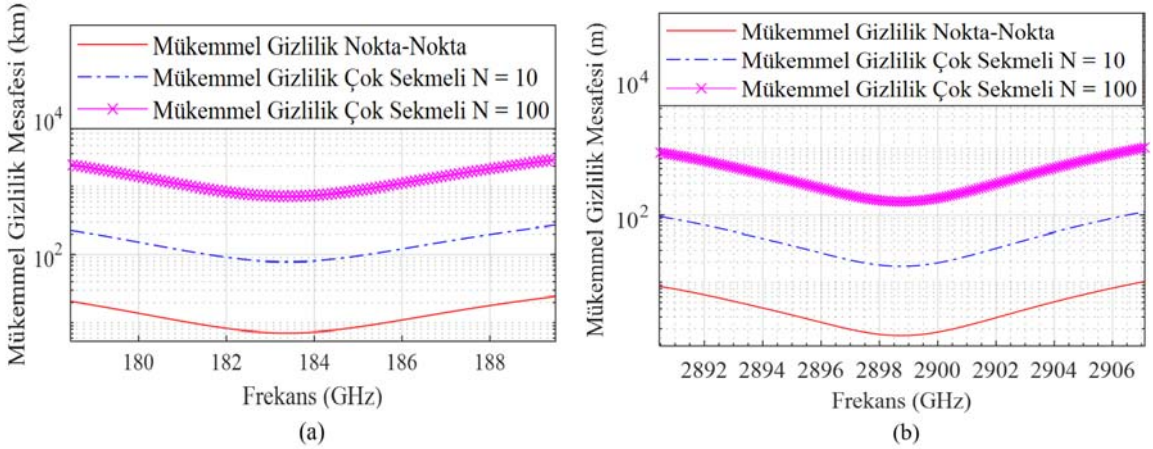
haberleşme kanalı için elde edilen bu sonuca göre mükemmel gizlilik ve tespit menzilleri noktadan noktaya haberleşme kanalı ile işbirlikli haberleşme kanalı için milimetre dalga ve Terahertz bantları için Şekil 8'deki gibi, 180-187 GHz ile 2894-2904 GHz aralığı için ise Şekil 9'daki gibi olmaktadır.

4. ÇOK SEKMELİ KANAL MODELİ
(MULTI-HOP CHANNEL MODEL)

Çok sekmeli haberleşme kanalı bir verici, bir legal alıcı, *N* tane röle ve bir illegal alıcıdan oluşmaktadır ve kanal modeli [16] Şekil 10'da gösterilmiştir. Bu haberleşme kanalında işaretlerin atmosferik sönümlemesi çeşitli frekans bantlarında hesaplanmış, işaretlerin tespitinin ve çözülmesinin mümkün olduğu menziller ortaya konmuştur. Elde edilen sonuçlardan yola çıkarak genel bir formül türetilmiştir. Literatürde yaygın olarak kullanılan haberleşme güvenliği hesaplamaları noktadan noktaya haberleşme kanalında olduğu gibi bu kanalda da geçerlidir. Çok sekmeli haberleşme kanalında vericiden alınan işaret *N* tane röle aracılığı ile alıcıya ulaşacağı için işaret normal durumda Verici-Röle 1-Röle 2- ... –Röle *N*-Legal Alıcı yolunu izlemesi gerekmektedir. Buna karşın illegal alıcının işareti alabilme senaryosunu göz önüne alınırsa işaretin Verici-İllegal Alıcı veya Verici-Röle-İllegal Alıcı yollarını izlemesi de mümkündür. Burada işaretin mükemmel gizlilik ve işaret tespiti menzillerini hesaplamak için sistemin en



Şekil 11. Çok sekmeli haberleşme kanalında mükemmel gizlilik ve tespit mesafeleri (a) Milimetre dalga bandı (b) Terahertz bandı (Ultimate secrecy and detection distances in the multi-hop communication channel (a) Millimeter wave band (b) Terahertz band)



Şekil 12. Çok sekmeli haberleşme kanalında mükemmel gizlilik ve tespit mesafeleri (a) Milimetre dalga 179-189 GHz bandı (b) Terahertz 2894-2904 GHz bandı (Ultimate secrecy and detection distances in the multi-hop communication channel (a) Millimeter wave 179-189 GHz band (b) Terahertz 2894-2904 GHz band)

kötü güvenliğe sahip senaryosu gözönüne alınırsa işaretin mükemmel gizlilik ve tespit menzilleri aşağıdaki gibi hesaplanabilir:

Vericinin mükemmel gizlilik menzili d, röle sayısı N olarak alınırsa sistemin mükemmel gizlilik menzili bu durumda $(N+1)d$ olmaktadır. Bu hesaplamaya göre çok sekmeli kanal modeli için sistemin mükemmel gizlilik ve tespit menzillerinin eğrileri aşağıdaki gibi olmaktadır. Bu örnekte röle sayısı 10 ve 100 olarak alınmıştır. İşbirlikli haberleşme kanalı için bu elde edilen sonuca göre mükemmel gizlilik ve tespit menzilleri, milimetre dalga ve Terahertz bantları için Şekil 11'deki gibi, 179-189 GHz ile 2894-2904 GHz aralığı için ise Şekil 12'deki gibi olmaktadır.

4. SONUÇLAR (CONCLUSIONS)

Bu çalışmada kablosuz haberleşme sistemlerinde bant genişliği azlığı ve haberleşme gizliliği problemlerine milimetre dalga ve Terahertz bantlarında atmosferik sönümleme yönünden bir çözüm sunulmuştur. Noktadan noktaya haberleşme kanalı, işbirlikli haberleşme kanalı ve çok sekmeli kanal modelleri için bant genişliği tasarrufuna izin veren çeşitli frekans bantları belirlenmiştir ve incelenmiştir. Aynı zamanda bu bantların haberleşme gizliliği özellikleri ve mükemmel işaret gizliliği ve işaret tespitinin gerçekleştiği bölgelerin menzilleri, işaret-termal gürültü oranının 1'e eşit olduğu durumlar hesaplanarak bulunmuştur. Vericinin bu menzillerinin alıcının

donanımından bağımsız olduğu gösterilmiştir. Verilen özelliklere sahip bir haberleşme kanalı bir Wyner dinleme kanalı tanımlanarak ve literatürdeki haberleşme gizliliği hesaplamaları kullanılarak haberleşmenin fiziksel katmanının güvenli olduğu gösterilmiştir. Frekansı tekrar kullanma yöntemi atmosferik sönümleme yönünden ele alınmıştır. Mükemmel haberleşme güvenliği frekansı tekrar kullanma yönteminin işlevselliğini sağlamaktadır. Bu şekilde birbirinden coğrafi yönden uzak olan birden fazla kullanıcının aynı frekansı kullanabilmesi sağlanmaktadır. Bu şekilde spektral verim arttırılabilmektedir. Radyo işaretlerinin milimetre dalga ve Terahertz bantlarında maruz kaldığı atmosferik sönümlemenin işaretlerin gizliliğinin üzerine olan etkisinden yola çıkarak mükemmel gizlilik tanımı yapılmıştır. Radyo işaretlerinin atmosferik gazlardan kaynaklı sönümlemesinin hesaplanmasında su buharı ve oksijenin etkisi hesaba katılmıştır. Sönümlemenin seviyesinin işareti termal gürültünün seviyesine getirecek düzeye gelmesi durumunda işareti tespit etmek veya çözümlemek mümkün değildir. Toplam sönümleme, su ve oksijenden kaynaklanan sönümlemenin toplamı olarak hesaplanmaktadır. Verici gücünün 1 W'dan 1000 W'a kadar olduğu durumda işaret tespiti ve mükemmel gizlilik bölgelerinin sönümleme eğrileri ve bu bölgelerin menzilleri hesaplanmıştır. Mükemmel gizlilik menzilleri işbirlikli haberleşme kanalı için hesaplanarak noktadan noktaya haberleşme kanalı ile gizlilik yönünden karşılaştırılmıştır. Çok sekmeli kanallar için mükemmel gizlilik menzilleri değişen sekme sayıları için hesaplanmıştır ve noktadan noktaya haberleşme kanalı ile karşılaştırılmıştır. Hesaplanan mükemmel gizlilik ve işaret tespiti bölge menzilleri açık işaret yolu olması durumu için hesaplanmıştır. Pratikte bu mesafeler engeller ve diğer çevresel etkenlerden dolayı daha küçük olarak gerçekleşmektedir. Ayrıca bant genişliği azlığı problemine bir çözüm olarak frekansların tekrar kullanılması yöntemi ile yapılan gizlilik hesaplamalarından faydalanılarak spektrumdan tasarruf edilebileceği sonucuna ulaşılmıştır. Spektrumda daha fazla bant genişliğine erişmek için kullanılmayan yüksek frekanslar kullanılabilmektedir. Sonuçlara göre 1 THz'den sonraki birçok frekans bandı için mükemmel gizlilik menzilinin 2 m'nin altında olduğu gösterilmiştir. Mükemmel gizlilik menzili milimetre dalga bandında 183 GHz'de 7,5 km ve Terahertz bandı 2899 GHz'de ise 2 m'nin altına inmektedir. Bu durumda işareti tespit etmek veya çözümlemek işaretin termal gürültü seviyesine düşmesinden dolayı mümkün değildir. Literatürde kullanılan fiziksel katman güvenliği hesaplamaları, mükemmel gizlilik durumu için hesaplanmıştır: Gizlilik kapasitesi, gizlilik kesim olasılığı ve kesinlikle pozitif gizlilik kapasitesi. Bu hesaplamalar ile mükemmel gizlilik şartlarının sağlandığı durumlarda fiziksel katman güvenliğinin tamamen sağlandığı teyit edilmiştir. İşaret-termal gürültü oranının 1'e eşit olduğu durumda herhangi bir illegal alıcının kanalı dinlemesi mümkün değildir. Haberleşme gizliliğinin verici gücünün 1 ile 1000 kat artırılmasına karşın pek etkilenmediği ortaya çıkmıştır. Bu da mükemmel gizlilik şartlarına sahip bir kanalın güvenli olduğunu teyit etmektedir. Bu yolla cihaz içi haberleşme (karttan karta veya çipten çipe haberleşme) ve bina içi haberleşme gibi kısa menzilli haberleşme uygulamalarında aynı frekansı farklı cihazlarda tekrar kullanmanın ve 2 m'nin altına kadar menzilde yüksek güvenlik ile yüksek bant genişliği elde etmenin milimetre dalga ve Terahertz bantlarında mümkün olduğu gösterilmiştir.

6. KAYNAKLAR (REFERENCES)

1. DiFonzo, D., Kreutel, R., Communications Satellite Antennas for Frequency Reuse, 1971 Antennas and Propagation Society International Symposium, Los Angeles CA-USA, 287- 290, 22-24 Eylül, 1971.
2. Shannon, C. E., Communication theory of secrecy systems, Bell Syst. Tech. J., 28, 656–715, 1949.
3. Pan, G., Tang, C., Zhang, X., Li, T., Weng, Y., Chen, Y., Physical-layer security over non-small-scale fading channels, IEEE Transactions on Vehicular Technology, 65 (3), 1326-1339, 2016.
4. International Telecommunication Union Attenuation by Atmospheric Gases. ITU-R Recommendation P.676-11, 2016.
5. Siles, G. A., Riera, J. M., Garcia-del-Pino, P., Atmospheric attenuation in wireless communication systems at millimeter and THz frequencies, IEEE Antennas and Propagation Magazine, 57 (1), 48-61, 2015.
6. Gibbons, C. Z., Zenithal attenuation due to molecular oxygen and water vapour, in the frequency range 3–350 GHz, Electronics Letters, 22 (11), 577-578, 1986.
7. Zhao, H. et al., 28 GHz Millimeter Wave Cellular Communication Measurements for Reflection and Penetration Loss in and Around Buildings in New York City, IEEE International Conference on Communications (ICC), 5163-5167, Budapeşte-Macaristan, 5163-5167, 9-13 Haziran, 2013.
8. Barros, J., Rodrigues, M. R. D., Secrecy Capacity of Wireless Channels, IEEE International Symposium on Information Theory, Seattle WA-USA, 356-360, 9-14 Temmuz, 2006.
9. Wyner, A. D., The wire-tap channel, The Bell System Technical Journal, 54 (8), 1355-1387, 1975.
10. Liu, X., Probability of strictly positive secrecy capacity of the rician-rician fading channel, IEEE Wireless Communications Letters, 2 (1), 50-53, 2013.
11. Lei, H., Zhang, H. Ansari, I. S. Gao, C. Guo, Y. Pan, G. Qaraqe, K. A., Performance analysis of physical layer security over generalized-K fading channels using a mixture gamma distribution, IEEE Communications Letters, 20 (2), 408-411, 2016.
12. Haneda, K. et al., Indoor 5G 3GPP-like Channel Models for Office and Shopping Mall Environments, IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur-Malezya, 694-699, 23-27 Mayıs, 2016.
13. Agilent Keysight Technologies, Fundamentals of RF and microwave noise figure measurements application note. https://www.keysight.com/zz/en/assets/7018-06808/application-notes/5952-8255.pdf?success=true. Erişim tarihi Şubat, 1, 2021.

14. Ekşim, A., Demirci, T., Ultimate Secrecy in Wireless Communications, 11th International Conference on Electrical and Electronics and Electronics Engineering (ELECO), Bursa-Türkiye, 682-686, 28-30 Kasım, 2019.
15. Tamosiunaite, M., Tamosiunas, S., Zilinskas, M., Valusis, G., Haidine A., Aqqal A., Broadband Communications Networks, IntechOpen, 978-1-78923-743-6, Rijeka-Hırvatistan, 2018.
16. Ekşim, A., Demirci, T., Ultimate Secrecy in Cooperative and Multi-hop Wireless Communications, 2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science, Roma-İtalya, 1-4, 2020, doi: 10.23919/URSIGASS49373.2020.9232409.
17. Ozgonul M, Seçmen M., Size-reduced printed log-periodic dipole antenna for wireless communication applications , Journal of the Faculty of Engineering and Architecture of Gazi University , 35 (3), 1631-1646, 2020.
18. Kanmaz M., Aydın M., Comparison of dv-hop based ındoor positioning methods in wireless sensor networks and new approach with k-means ++ clustering method , Journal of the Faculty of Engineering and Architecture of Gazi University, 34 (2), 975-986, 2019.
19. Ekşim A., Yetik H., Audio quality enhancement for ETSI TS 102 361 digital mobile radio standard compliant radios using volume optimization and better forward error correction scheme, Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (2), 665-674, 2018.
20. Yıldırım G., Tatar Y., Remote user supported IoT-WSN Laboratory and testbed platform: FiratWSN, Journal of the Faculty of Engineering and Architecture of Gazi University, 34 (4), 1831-1846, 2019.