Ultimate Secrecy in Cooperative and Multi-hop Wireless Communications

Ali Ekşim and Tolga Demirci
Center of Research for Advanced Technologies of Informatics and Information Security, TUBITAK BİLGEM, Gebze, Kocaeli, 41700, Turkey, https://bilgem.tubitak.gov.tr/en

Abstract

In this work, communication secrecy in cooperative and multi-hop wireless communications for various radio frequencies are examined. Attenuation lines and ranges of both detection and ultimate secrecy regions were calculated for cooperative communication channel and multi-hop channel with various number of hops. From results, frequency ranges with the highest potential to apply bandwidth saving method known as frequency reuse were determined and compared to point-to-point channel. Frequencies with the highest attenuation were derived and their ranges of both detection and ultimate secrecy are calculated. Point-to-point, cooperative and multi-hop channels were compared in terms of ultimate secrecy ranges. Multi-hop channel measurements were made with different number of hops and the relation between the number of hops and communication security is examined. Ultimate secrecy ranges were calculated up to 1 Terahertz and found to be less than 13 meters between 550-565 GHz frequency range. 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 various bands in the Terahertz band can be used to reuse the same frequency in different locations to obtain high security and high bandwidth.

1. Introduction

Recent developments in wireless communications such as wireless local area networks (W-LAN), low power wide area networks (LPWAN), Internet of Things (IoT) and fifth generation cellular communication systems (5G) resulted in exponentially more demand of bandwidth and security. IoT networks with massive number of sensors and units require very high data rates and security to maintain systems such as smart building, smart cities, automotive, healthcare, smart grid, logistics, agriculture, manufacturing, smart retail and wearables. As for bandwidth, most frequency bands in the spectrum have been licensed and remaining bands are very limited and costly. There have been various approaches to use the limited available bandwidth more efficiently. One approach is frequency reuse, which is the allocation of identical frequencies for users that are geographically separated [1]. On the other hand, communication security is an important issue due to broadcast nature of wireless communications. Communication secrecy in the physical layer has been a leading topic in wireless communications since the first definition of information theoretical security by Shannon [2]. Using cryptography to attain security in the upper layer is not always feasible due to susceptibility to attacks, requirement for the upper layer of the channel to be error free and secret key management issues [3]. On another note, fast fading frequency bands allow frequency reuse by allowing multiple users in different locations to use the same frequency and to increase spectral efficiency. This work presents a definition and an application on propagation effects of secrecy properties of communication systems within the frequency range 1-1000 GHz. To determine the effect of atmospheric attenuation on secrecy, two regions are defined. Ultimate secrecy region is defined as the region around the transmitter which decoding or detecting the signal is impossible. This is achieved when signal to thermal noise power ratio is 1. The other region is defined as detection region which detection of the signal is possible but decoding is impossible. At [4], communication secrecy is examined from perspective of atmospheric attenuation in point-to-point channel. In this work, communication secrecy is studied in cooperative and multi-hop wireless communications. Atmospheric attenuation caused by water vapor and oxygen for 1-1000 GHz is calculated from Annex-1 of [5] with the default parameters: 15°C of temperature, 1013.25 hPa of atmospheric pressure and 7.5 g/m^3 of water vapor content level [6].

It is possible to have more secure communication by using frequencies with higher atmospheric attenuation levels and signals which can be secured from eavesdropping. Atmospheric attenuation of radio signals has been examined in various studies [5–7]. However, there is no known study available regarding the effects of atmospheric attenuation. This work aims to derive physical layer security levels of radio signals from atmospheric attenuation in 1-1000 GHz frequency region. Level of atmospheric attenuation of signals is derived from recommendation by International Telecommunication Union (ITU) in [5]. It is deduced that the quality of physical layer security of signals are proportional to the level of attenuation for equal distances and frequencies. If the level of attenuation is enough to get the signal down to the same level as thermal noise then it is impossible to detect or decode the signal. From results, it can be concluded that for almost every frequency above 400 GHz, range of ultimate secrecy is below 10 km which provides perfect communication security inside the area in this radius. It is impossible to detect or decode the signal due to low signal-to-noise ratio (SNR) in which the signal is mixed with the thermal noise. This shows that the physical layer of the system is perfectly secure.

Point-to-point system model is illustrated in Figure 1 for defined secrecy regions. In Figure 2, total atmospheric attenuation of radio signals per km for 1-1000 GHz range is given.

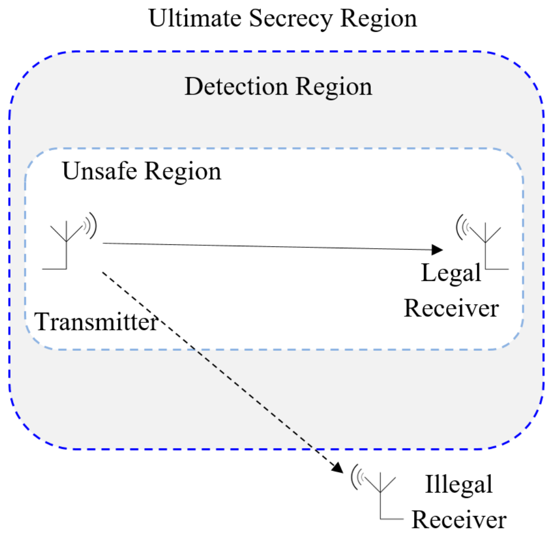

Figure 1. Point-to-point communication channel model.

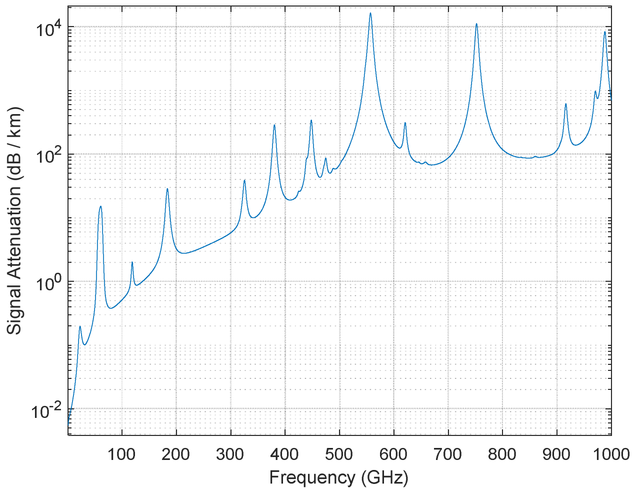

Figure 2. Total atmospheric attenuation of radio signals per km for 1-1000 GHz range.

Generalized formula for ultimate secrecy [4] with respect to path loss between transmitter and illegal receiver,

$$L_U \geq 174 + P_T + A_{G_T} + A_{G_R} - B \tag{1}$$

where A_{G_T} is the transmit antenna gain, P_T is the transmit power, A_{G_R} is the receive antenna gain and B is the signal bandwidth. In this inequality, to attain ultimate secrecy, path loss between receiver and transmitter must be higher or equal to 204 dB for 0 dBi receiver and transmitter antenna gain and 1 W transmit power with 1 Hz bandwidth.

The organization of this paper is as follows: In section 2, secure communication boundaries and ranges of ultimate secrecy and detection regions for cooperative communication channel is calculated. In section 3, multi-hop communication secrecy levels are calculated. In section 4, the work is concluded and summary of the work is presented.

2. Cooperative Channel Model

The cooperative communication channel comprises a transmitter, a legal receiver, a relay and an illegal receiver. The atmospheric attenuation of the signals in this communication channel is calculated in various frequency bands. Ranges for detecting and decoding the signals are calculated. The communication security calculations commonly used in the literature are valid for the cooperative channel as well as the point-to-point communication channel. Figure 3 shows the cooperative communication channel model.

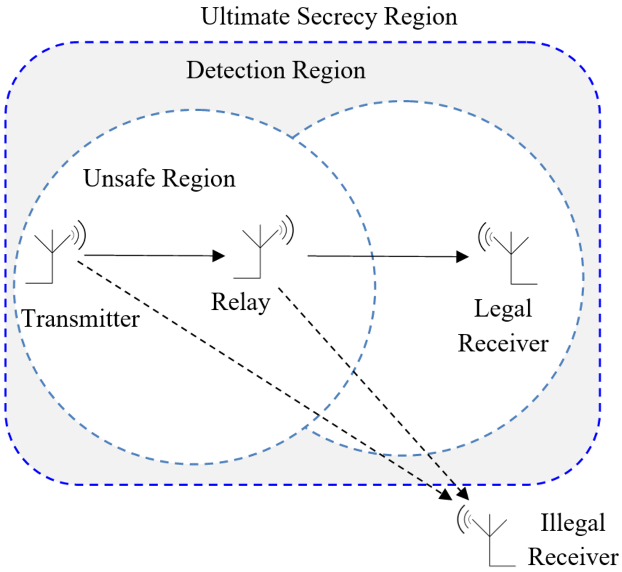

Figure 3. Cooperative communication channel model.

Since the signal received from the transmitter in the cooperative communication channel will reach the receiver through the relay, the signal should normally follow the transmitter-relay-legal receiver path. However, if the illegal receiver is able to receive the signal, it is also possible for the signal to follow the transmitter-illegal receiver or transmitter-relay-illegal receiver paths. To evaluate ultimate secrecy, the worst-case scenario of the cooperative communication channel is taken into account. The transmitter's ultimate secrecy range is d_1 and ultimate secrecy range of the relay is d_2, ultimate secrecy range of the system becomes $d_1 + d_2$. According to this result obtained for the cooperative communication channel, ultimate secrecy ranges are depicted in Figure 4 in which detection and ultimate secrecy for point-to-point and cooperative communication channel for Terahertz band are shown. Ultimate secrecy distances of the band with the minimum secrecy distance in Terahertz band which is 550-565 GHz band are shown in Figure 5.

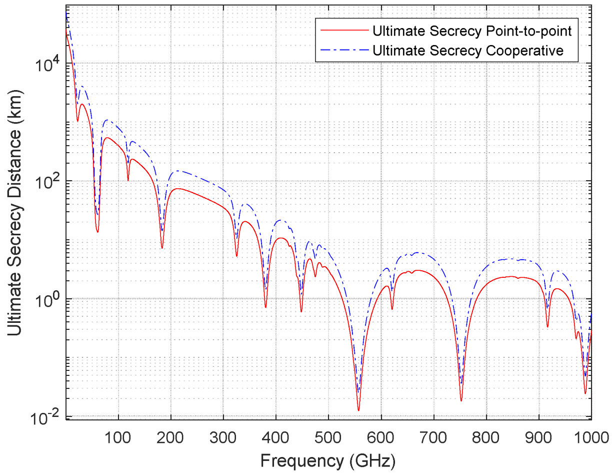

Figure 4. Ultimate secrecy ranges of point-to-point and cooperative communication channel.

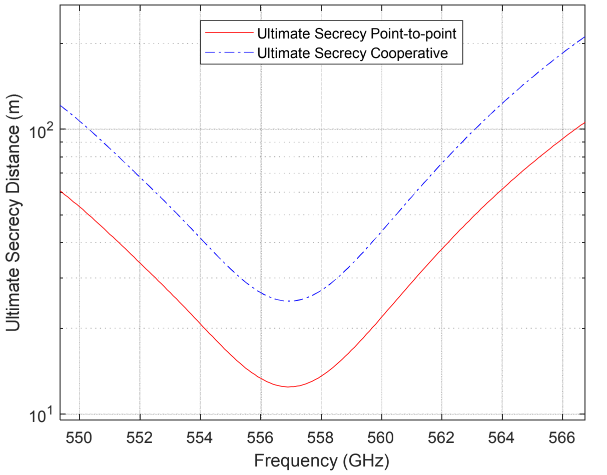

Figure 5. Ultimate secrecy ranges of point-to-point and cooperative communication channel for 550-565 GHz band.

3. Multi-hop Channel Model

The multi-hop communication channel consists of a transmitter, a legal receiver, N relays and an illegal receiver. The multi-hop channel model is given in Figure 6.

Since the signal received from the transmitter in the multi-hop communication channel will reach the receiver through N relays the signal should normally follow the path of Transmitter-Relay 1-Relay 2- ... – Relay N-Legal Receiver. To calculate ultimate secrecy, the worst-case scenario of the multi-hop communication channel is taken into account. The longest ultimate secrecy range of one hop is d and the number of relays is N, then the ultimate secrecy range of the system is $(N+1)d$. According to this calculation, the curves of the system's ultimate secrecy ranges for the multi-hop channel model are calculated.

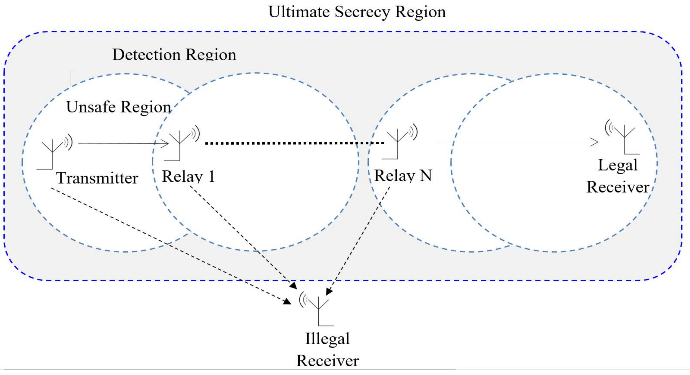

Figure 6. Multi-hop communication channel model.

According to this result, ultimate secrecy ranges for the cooperative communication channel are as shown in Figure 7 for 1-1000 GHz frequency band, and in Figure 8 for 550-565 GHz frequency band which has the minimum secrecy range in Terahertz band for the number of hops are 10 and 100.

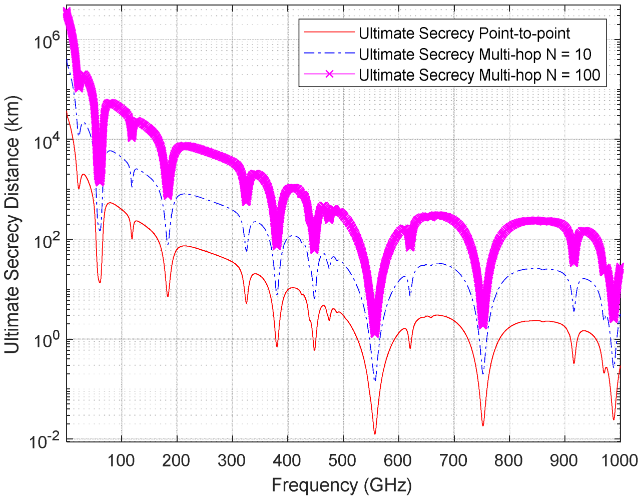

Figure 7. Ultimate secrecy ranges of multi-hop channel

Ultimate secrecy ranges are highly dependent on number of hops in the channel. Increasing number of hops causes a wider ultimate secrecy range.

4. Conclusions

In this study, a solution to the problems of bandwidth and communication confidentiality in wireless communication systems in terms of atmospheric attenuation in 1-1000 GHz frequency band is presented. Various frequency bands that allow bandwidth savings for point-to-point communication channel, cooperative communication channel and multi-hop channel models have been identified and examined. At the same time, the communication confidentiality

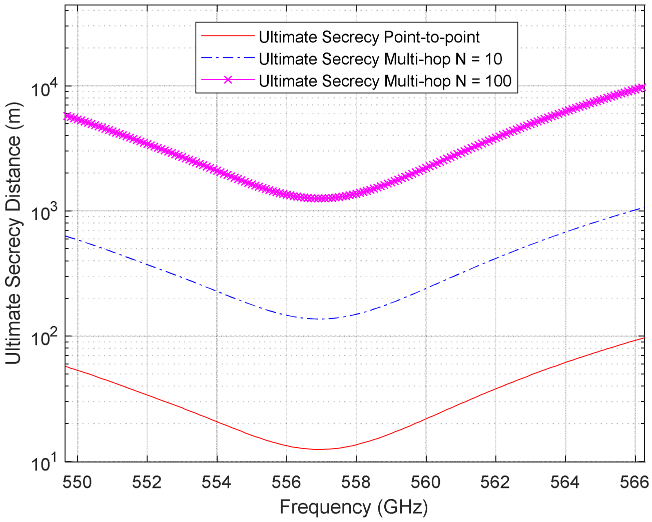

Figure 8. Ultimate secrecy ranges of multi-hop channel for 550-565 GHz band.

characteristics of these bands and the range of the areas where the signal detection is possible are realized by calculating the conditions where the signal-to-thermal noise ratio is equal to 1. It has been shown that the ultimate secrecy ranges of the transmitter are independent of the equipment of the receiver. Ultimate secrecy ranges are calculated for the cooperative communication channel and compared with the point-to-point communication channel in terms of confidentiality. Ultimate secrecy ranges for multi-hop channels were calculated for varying hop counts and compared with a point-to-point communication channel. The derived ultimate secrecy and detection zone ranges have been calculated for the presence of an open beacon path. In practice, these distances are smaller due to obstacles and other environmental factors. As a result, it is concluded that the spectrum can be saved by making use of the privacy calculations made by reusing the frequencies as a solution to the bandwidth shortage problem. The ultimate secrecy range is less than 13 m at 550-565 GHz in the Terahertz band for point-to-point channel, 26 m for cooperative channel and 1.3 km for 100-hop channel. In this case it is not possible to detect or decode the signal because the signal falls below to the thermal noise level. The physical layer security calculations used in the literature have been calculated for ultimate secrecy. If the signal-to-noise ratio is equal to 1, it is not possible for any illegal receiver to listen to the channel [4]. This confirms that a channel with ultimate secrecy requirements is met. In this way, it is possible to use the same frequency bands for devices located at different locations in communication systems with very high demand of bandwidth and security. Real world application of this study can be IoT network systems with applications such as, smart grid, smart cities, health, manufacturing, transportation, energy and government; short range communication applications such as in-device communication (card-to-card or chip-to-chip communication) and indoor communication in different devices. In order to achieve high security with a range of less than 13 m and high bandwidth and secure communication at Terahertz band can be obtained under these conditions.

5. References

1. D. DiFonzo, and R. Kreutel, “Communications satellite antennas for frequency reuse,” 1971 Antennas and Propagation Society International Symposium, Los Angeles, CA, USA, 1971, pp. 287- 290.

2. C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, **28**, pp. 656–715, 1949.

3. G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng’ and Y. Chen, “Physical-Layer Security over Non-Small-Scale Fading Channels,” *IEEE Transactions on Vehicular Technology*, **65**, 3, March 2016.

4. A. Ekşim, and T. Demirci, “Ultimate Secrecy in Wireless Communications,” 11th International Conference on Electrical and Electronics and Electronics Engineering ELECO, Bursa, Nov. 2019.

5. Attenuation by Atmospheric Gases, “International Telecommunication Union ITU-R Recommendation P.676-11, 2016.

6. 5. G. A. Siles, J. M. Riera’ and P. Garcia-del-Pino, “Atmospheric Attenuation in Wireless Communication Systems at Millimeter and THz Frequencies,” *IEEE Antennas and Propagation Magazine*, **57**, 1, pp. 48-61, Feb. 2015.

7. C. J. Gibbons, “Zenithal attenuation due to molecular oxygen and water vapour, in the frequency range 3-350 GHz,” *Electronics Letters*, **22**, 11, pp. 577-578, 22 May 1986.