

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Vehicle Secrecy Parameters for V2V Communications

Na-Young Ahn and Dong Hoon Lee

Abstract

This paper studies the parameters affecting secrecy capacity in vehicle communication. The vehicle secrecy parameters largely include vehicle driving-related parameters, antenna-related parameters for transmitting and receiving signals, path-related parameters for indirect communication, and noise-related parameters using a fading channel. Although many researches have been conducted on antenna-related parameters and noise-related parameters considered in general wireless communication, relatively little research has been made on parameters caused by the vehicle itself. These vehicle secrecy parameters also imply that secrecy capacity can be varied by the user. In the future, this study will be a very informative topic when trying to perform vehicle communication while maintaining a certain level of security capacity. In the coming autonomous driving era, this research is very necessary and will help to carry out vehicle communications more safely.

Keywords: secrecy capacity, vehicle secrecy parameter, physical layer security, vehicle speed, antenna, relay, fading

1. Introduction

Vehicle-to-vehicle communication functionality is essential for general 5G communications [1, 2]. This functionality aims to achieve the safe operation of autonomous vehicles by sharing vehicle driving-related information, such as basic security messages (BSMs). To guarantee vehicle-to-vehicle functionality, security must be the foundation of design and privacy must be a priority. Previous studies have already made significant progress on security beyond the vehicular network layer [3, 4]. Yet, despite this, existing vehicle security schemes demonstrate insufficient computing power and large power consumption with respect to processing received or transmitted data from a large number of vehicles. To overcome these difficulties, researches on physical layer security [5–7] have attempted to develop secure data communication methods based on the physical properties of the wireless channel.

In information theory, channel (or Shannon) capacity is known as a maximal amount of information that can be transmitted through a wireless channel [8, 9]. In general, channel capacity is given as

$$C = W \log(1 + \text{SNR}), \quad (1)$$

where W is the channel bandwidth, and SNR is the signal-to-noise ratio. Secrecy capacity denotes the channel capacity of a legitimate channel less the channel

capacity of a wiretap channel. That is, secrecy capacity is a maximum data rate that is achievable between the legitimate TX-RX pair, subject to the constraints on information attainable by an unauthorized receiver [10]. For a Gaussian wiretap channel, secrecy capacity C_s is:

$$C_s = \frac{1}{2} \log \left(1 + \frac{P}{N_m} \right) - \frac{1}{2} \log \left(1 + \frac{P}{N_w} \right), \quad (2)$$

where P is the transmitter's power, N_m is the receiver's noise, and N_w is the eavesdropper's noise.

Secrecy capacity means an entropy that can conceptually transmit secrets securely without taps. It is a value obtained by subtracting the channel capacity for performing illegal communication from the channel capacity for performing mathematically legitimate communications? In information theory, channel capacity is the maximum rate that can be transmitted without error. Thus, the unit of secrecy capacity is bits/sec/Hz. Could this concept be meaningful in vehicle communication? We are asking questions, and so on. Nobody knows the existence of wiretapping. In vehicle communication, valid data are transmitted over the air in four directions, and anyone can obtain it if desired. Even if it is encrypted, the existence of a quantum computer makes it possible for this threat to cause serious problems. We naturally cannot but consider wireless channels, but protected channels, in vehicular communications. So how can we protect wireless channels, but secure channels from eavesdroppers? The answer is physical layer security. Therefore, research on modeling for vehicle communications is inevitable.

Secrecy capacity can be controlled in real time. The parameters affecting these security capacities are classified as follows: vehicle-related parameters, antenna-related parameters, communication path-related parameters, and noise-related parameters.

2. Vehicle-related parameters

Vehicle-related parameters are very important for vehicle accidents and physical safety as parameters related to the operation of the vehicle while driving. The vehicle-related parameters include speed of the autonomous vehicle, the response time, etc., as mentioned by Ahn et al. [11].

2.1 Vehicle speed

It is generally assumed that secrecy capacity will be increased according to the vehicle speed. For example, it is assumed that there will be a difference in eavesdropping data transmitted from a vehicle running at low speeds and eavesdropping data transmitted from vehicles running at high speeds. Considering the Doppler effect, there is a theoretical study on this [12]. Chopra et al. suggested that as the vehicle speed increases, the eavesdropper is less likely to succeed in eavesdropping [12].

Chopra has announced that as speed of the vehicle increases, the probability of an attacker's success gradually decreases, referring to **Figure 1**. A common guess is that you will get your hands on these results. SNR value for speed is drastically reduced according to the effects of beam merge and Doppler shift, and the probability of success of the eavesdropper is expected to sharply decrease (**Figure 1**).

However, this is related to naive wireless communication, and it is difficult to apply it to a vehicle in operation. As mentioned in the previous section, the

autonomous vehicle speed is closely related to the safety distance, and the safety distance eventually affects the channel capacity between vehicles. According to my modeling and simulation results, as the vehicle speed increases, secrecy capacity becomes rather small.

Ahn et al. concluded that vehicle speed is closely related to the safety distance to prevent impulsiveness, and this safety distance ultimately affects secrecy capacity, resulting in a close relationship between vehicle speed and secrecy capacity, referring to **Figure 2**. The result was, surprisingly, that the faster the vehicle speed was, the less secrecy capacity was increased, rather than increasing (**Figure 2**) [11].

Some say that secrecy capacity will increase with speed of the vehicle, and others say that secrecy capacity will be reduced depending on speed of the vehicle. Who is wrong and who is right? I think that these results are derived from the fact that the definition of secrecy capacity for vehicles has not been established. In addition, it is presumed that there is a totally different answer depending on the setting, whether or not the eavesdropper is present, whether the eavesdropper is moving, and the information of the eavesdropper. It means that this lack of research on secrecy capacity in vehicle communication.

So, what information do these facts give us? The relationship between vehicle speed and secrecy capacity is simply not defined. Nevertheless, there is a connection between speed of the vehicle and secrecy capacity. The important thing is that you can control secrecy capacity at the speed of the vehicle.

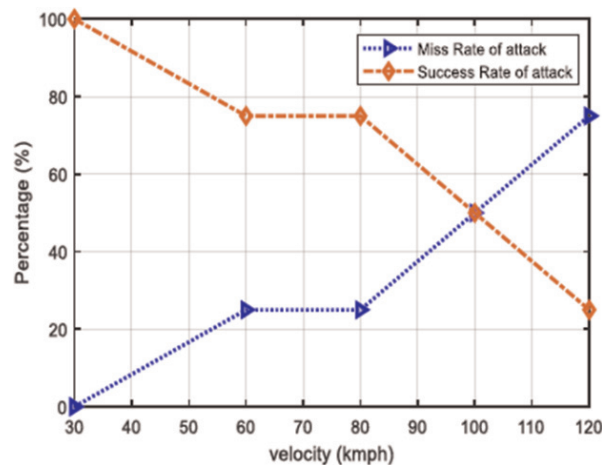


Figure 1.
Percentage of miss/success rate of attack for eavesdroppers according to different velocities of user [12].

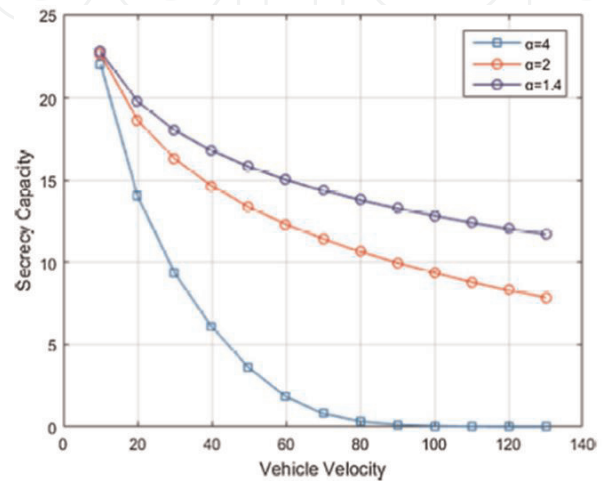


Figure 2.
The relationship of secrecy capacity according to speed of vehicle [11].

2.2 Vehicle system parameter

What do the system parameters of the car mean? System parameters are an important factor in determining the collision distance between vehicles. For example, response time has a significant impact on break distance. The break distance is proportional to the safety distance. The response time will eventually affect the safety distance, and this safety distance will eventually affect secrecy capacity.

The faster the response time from one vehicle to the reception and processing of signals from other vehicles, the sooner it is expected to help secure safety. If you think about it, it would be better to respond quickly to ensure safety. In fact, in my simulation results, it was confirmed that the shorter the response time, the greater secrecy capacity. However, this cannot be the correct answer in a real environment. Why? What is the purpose of using secure capacity? Its purpose is to ensure the safety of communication from any eavesdropper.

In order to secure the communication, the encryption method is basically used in vehicle communication. There is a difference between the response time using an encryption scheme and the response time without an encryption scheme. For security, encryption will be used, and if encryption is used, response time will naturally be longer. This long response time will eventually lead to a reduction in secrecy capacity.

To summarize, in order to achieve security based on physical layer security, a short response time is advantageous. On the other hand, to achieve application layer security, response time is inevitably long. The trade-off between physical layer security and application security is inevitable.

In any case, it is important to note that secrecy capacity is closely related to the response time of the system. In addition, it is generally possible to select the relevant mode whether or not to apply application security in the vehicle system. This means that the response time associated with secrecy capacity is not fixed but selectable by the user. The conclusion is that secrecy capacity is controllable according to the selected response time.

2.3 Speed limit

Does the law govern secrecy capacity? That is right. All vehicles that drive on the road must be moving in compliance with speed limit. I have conceptually presented and calculated secrecy capacity of a rolling car at the intersection. The conclusion was not beyond the expected range. It has been confirmed that as speed limit increases, secrecy capacity decreases. If you comply with vehicle regulations, your secrecy capacity will remain constant. In the real world, however, there is no vehicle that keeps the law. Are these only vehicle-related parameters?

3. Antenna-related parameters

Antenna beam radiation technology has been studied variously for physical layer security in wireless communication. Examples include transmission power allocation, artificial noise generation, jamming, and beam direction determination.

3.1 Transmission power

According to my confirmation, secrecy capacity changes according to the transmission power. For example, it has been confirmed that secrecy capacity is increased so that the transmission power can be increased. Then, in order to vary

secrecy capacity, it is necessary to check whether the intensity of the transmission power can be controlled in real time. However, there have been many researches on adaptive transmission power control in view of power consumption [13, 14]. The study of the majority of adaptive transmit power control aims at minimizing power consumption and storing energy. It is known that transmission power control is possible although the purpose is different. This means that secrecy capacity can be controlled in real time through transmission power control.

3.2 Beamforming

Beamforming technology is a very old technology of physical layer security. By forming a beam to be transmitted to the target device, the attack opportunity itself is deprived of an attacker having malicious purpose in the other direction. Recently, a technique for maximizing secrecy capacity using beamforming has been disclosed [15]. 3D beamforming technology is introduced beyond 2D to increase secrecy capacity [16, 17].

3.3 Artificial noise/jamming

A method for increasing secrecy capacity using artificial noise or jamming is disclosed [18, 19]. The jamming strategy is to send an artificial noise signal to the eavesdropper to effectively reduce their channel quality from correct reception. If an artificial noise signal is aimed at an eavesdropper, the quality of the eavesdropper's channel may be degraded. According to the eavesdropping channel model, a complete secret can be achieved if the eavesdropper's channel state is worse than a certain level, i.e., the legitimate receiver's channel state. Thus, radio interference can be a practical physical layer-based security measure, especially if the transmitted information needs to be protected from unintentional manual eavesdroppers.

3.4 Antenna gain

The size and shape of the small antenna will change the effective area of the antenna and the power output of the receiver antenna will be changed to affect SNRs. To obtain an antenna gain G , a relatively small antenna is needed at high frequencies [20, 21],

$$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f^2 A_e}{C^2}, \quad (3)$$

where A_e is the effective area, f is the carrier frequency, C is the speed of light, and λ is the carrier wavelength. As can be seen from the equation, if the effective area of the receiving antenna is increased, SNR value can be improved. Increasing the carrier frequency of the transmitter can improve SNR value.

3.5 Array antenna

The array antenna disperses the incident laser beam into the respective antenna elements through a plurality of directional couplers, modulates the phase or frequency of the dispersed laser beam, and adjusts the traveling direction of the output laser beam [22]. In general, the array antenna can vary the elevation angle and the azimuth angle of the beam. What this means is that the host vehicle can concentrate and transmit the beam to a specific target vehicle [23, 24]. Naturally, secrecy capacity can be improved as compared with not. In order to keep secrecy capacity

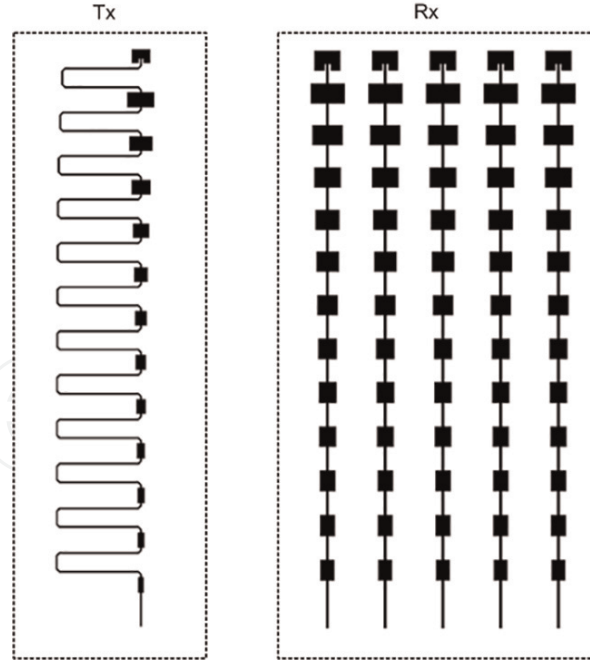


Figure 3.
Array antenna for vehicles.

of the vehicle above a certain value, this characteristic of the array antenna can be used. For example, when secrecy capacity of the vehicle is below a certain value, secrecy capacity can be increased by controlling the phase/frequency of the array antenna.

Referring to **Figure 3**, the array antenna includes a transmitter Tx having a snake feed line structure composed of a plurality of antennas and a receiver Rx having a structure of a plurality of lines composed of a plurality of antennas. Each antenna of Tx and Rx may be implemented in a microstrip structure.

4. Path-related parameters

4.1 Relay communication

As described above, secrecy capacity decreases as the vehicle speed increases. Decreased secrecy capacity as the vehicle speed increases can be compensated by a cooperative relay communication. In V2V communication, secrecy capacity can be improved by adoption at one relay R between the host vehicle A and the target vehicle B. In a general, secrecy capacity of a cooperative relay communication is higher than that of the direct communication without a relay [25–28]. For simplicity of the analysis of secrecy capacity, we assume that the system model comprises one relay R between the host vehicle A and the target vehicle B, as shown in **Figure 4**.

Channel capacity of the legitimated channel is expressed as:

$$C_1(A, B) = W \log_2 \left(1 + \left(\frac{P_A h_{AB}}{P_R h_{RB} + \sigma_B^2} \right) \right), \quad (4)$$

where P_A and P_R are the transmission powers of the host vehicle A and the relay R, respectively; h_{AB} is the channel gain between the host vehicle A and the target vehicle B; h_{RB} is the channel gain between the relay R and the target vehicle B; σ_B^2 is an additive white Gaussian noise at the target vehicle B; and W is a bandwidth.

And channel capacity of the wiretap channel is given by:

$$C_2(A, E) = W \log_2 \left(1 + \left(\frac{P_A h_{AE}}{P_R h_{RE} + \sigma_E^2} \right) \right), \tag{5}$$

where h_{AE} is the channel gain between vehicle A and eavesdropper E, and σ_E^2 is the additive white Gaussian noise at vehicle B. Then, secrecy capacity with the cooperative relay communication is denoted by

$$C_R = W \left[\log_2 \left(1 + \left(\frac{P_A h_{AB}}{P_R h_{RB} + \sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{P_A h_{AE}}{P_R h_{RE} + \sigma_E^2} \right) \right) \right]. \tag{6}$$

Figure 5 shows secrecy capacity with and without the relay R. Referring to **Figure 5**, we can see that the relay R helps to improve secrecy capacity in total. We confirmed that V2V communication using the relay may enhance secrecy capacity. The relationship between the existence of the relay and secrecy capacity can be summarized as shown in **the following table, Table 1**.

As described above, when relay communication is performed, an improvement in secrecy capacity is basically expected as compared with the case where relay communication is not performed. For this reason, relay communication is basically installed in vehicle communication. However, relay communication still has the issue of relay selection and communication rejection of relay object. The important

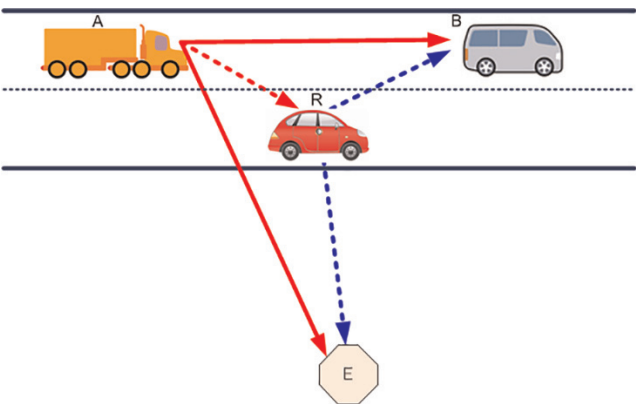


Figure 4.
System model with a relay between vehicle A and vehicle B.

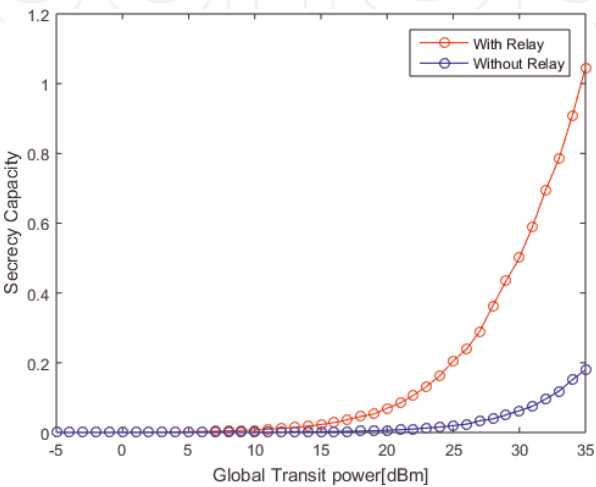


Figure 5.
Secrecy capacity variance according to relay existence [11].

Relay	Off	Down	Secrecy capacity
	On	Up	

Table 1.
Relationship between the relay mode and secrecy capacity [11].

thing is that the choice of relay communication can be a factor enough to be a variable factor of secrecy capacity.

4.2 RSU-assisted communication

When direct communication is not possible, Road Side Unit (RSU) can be used for vehicle communication [29–31]. RSU can be used to deliver a message from one vehicle to another. Here, the other vehicle may be an unspecified number, usually according to the broadcast message. Therefore, since the target vehicle cannot be specified, it is logically difficult to define secrecy capacity. At the same time, however, the presence of eavesdroppers is also unspecific, so secrecy capacity is expected to increase. When direct vehicle communication is not possible, indirect vehicle communication via RSU can be achieved. For example, when serious defects in secrecy capacity are found or expected, indirect vehicle communication via RSU may be required. When secrecy capacity control is not possible, that is, vehicle communication using RSU can be used last.

5. Noise-related parameters

Will noise-related parameters affect secrecy capacity? According to the concept of secrecy capacity, noise is of course a big influence. However, the problem is whether such noise is controllable in communication. Although it is a technology related to noise removal in other fields, wavelet transform is used to reduce power analysis attacks by removing noise [32–34]. Preventing DPA through wavelet transform is basically data modulation to ensure the randomness of transmitted data. However, the concern of noise related to secrecy capacity is not data modulation, but an issue related to the environment of the channel being transmitted. Is there a technique to eliminate or reduce channel noise, even if there is a technique to increase the noise of the channel? Although there is a technique of relatively increasing or decreasing the size of a signal, there is no technique for reducing or eliminating the absolute amount of noise.

However, it cannot be said that at some point the noise of the channel becomes the noise of the channel at another point. This suggests that the channel noise at another point in time may be changed depending on the channel noise at a certain point in time. Recently, research has been introduced to improve the characteristics of a wireless signal by reducing channel noise using adaptive equalization/filter algorithms [35, 36].

5.1 Additive white Gaussian noise channel

The channels used in communication are classified into various channels according to the noise component existing in the medium in which the signal is moving, not the medium itself. There are a lot of kinds of noise in the air, and because these noises occur at all frequencies, this noise is called white noise. The visible light, which is a type of electromagnetic wave with high frequency, has

a different color depending on the frequency, but it is attached as if noise of various frequencies is gathered like a white color when a plurality of colored light is overlapped.

Additive White Gaussian Noise (AWGN) channel is the most common type of channel, and is a channel that produces even noise across the entire frequency band. AWGN is a random noise without any special peripheral elements. This channel only contains the sum of the white noise. Here white noise follows Gaussian density. The corresponding probability density function $p(x)$ is expressed by the following equation [37, 38]:

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x - \mu)^2}{2\sigma^2}\right), \quad (7)$$

where μ is the mean, σ is the standard deviation, and σ^2 is the variance.

5.2 Rician fading channel

In a wireless channel environment, when the direct wave (line-of-sight) mainly appears in an environment such as a room dominated by a reflected wave, the probability distribution characteristic of the radio reception signal shows a Rician distribution [39, 40]. Rician probability density function $p(x)$ is expressed by the following equation:

$$p(x) = \frac{x}{\sigma^2} \exp\left(-\frac{(x^2 + A)^2}{2\sigma^2}\right) I_0\left(\frac{Ax}{\sigma^2}\right), \quad A \geq 0, \quad (8)$$

where σ^2 is the variance of the received total reflected power, that is, the multipath signal, A is the magnitude of line of sight (LOS) or dominant component, and I_0 is the zero-order transformed Bessel function.

5.3 Rayleigh fading channel

Rayleigh distribution is a stochastic model that shows the statistical time-varying characteristics of the envelope of random amplitudes of the received signal by independent quadrature components (such as in-phase and quadrature) or multiple multipath signals when the indirect wave (reflected wave, etc.) predominates over the direct channel in the wireless channel environment [41–43].

Rician factor K is dominant for multipath power (σ^2), and the ratio of the minute power ($A^2/2$) is represented by $K = A^2/2\sigma^2$. When $K = 0$, the Rician distribution is a Rayleigh distribution. Rayleigh probability density function $p(x)$ is expressed by the following equation:

$$p(x) = \frac{x}{\sigma^2} \exp\left(-\frac{x^2}{2\sigma^2}\right) I_0\left(\frac{Ax}{\sigma^2}\right), \quad A \geq 0. \quad (9)$$

5.4 Nakagami fading channel

The multipath fading phenomenon of signals in wireless mobile communication is a very important problem. In modeling such a fading channel, a Nakagami fading model is known to be fit and theoretically suitable. The Nakagami fading model has the following probability density function for the envelope of the signal [44–47]:

$$p(x) = \frac{2m^m x^{2m-1}}{\Gamma(m)\Omega^m} \exp\left(-\frac{mx^2}{\Omega}\right), x \geq 0, \quad (10)$$

where x is the size of the Nakagami fading signal, Ω is the mean square value of x , $\Gamma(m)$ is the gamma function, and m is the rate of the modality, which determines the shape of the distribution and is a fading index that indicates the degree of fading. When $m = 1$, Rayleigh distribution is obtained. When $m = 0.5$, Gaussian distribution is gained.

Generally, selective diversity is used to reduce the influence of fading. The selection diversity is a method of selecting the largest signal among the signals received through the multipath. If the signal received at the k -th receiving end is the largest, the received signal can be represented by a sinusoidal wave:

$$y_k(t) = u_k \exp(j2\pi f_0 t), \quad (11)$$

where u_k is the magnitude of the k -th received signal envelope and f_0 is the carrier frequency. Therefore, the average power of the received signal is $u_k^2/2$. Assuming that the average noise power is N , the SNR value of the signal received at the k -th receiving end is as follows.

$$\gamma_k = \frac{u_k^2}{2N}, \quad (12)$$

Therefore, the probability density function for SNR of the k -th receiver experiencing Nakagami fading is expressed by the following equation.

$$p_\gamma(\gamma) = \frac{m_k^{m_k} \gamma_k^{m_k-1}}{\Gamma(m_k) \gamma_0^{m_k}} \exp\left(-\frac{m_k \gamma_k}{\gamma_0}\right), \gamma \geq 0, \quad (13)$$

where γ_k is the SNR value of the k -th receiver, γ_0 is the average SNR value in the presence of fading, and m_k is the SNR value of the k -th receiver. The probability distribution function is the integral of the probability density function:

$$P_\gamma(\gamma) = \int_0^\gamma \left(\frac{m_k^{m_k} \gamma_k^{m_k-1}}{\Gamma(m_k) \gamma_0^{m_k}} \exp\left(-\frac{m_k \gamma_k}{\gamma_0}\right) \right) dx, \gamma \geq 0, \quad (14)$$

Assuming that all receivers are independent of each other, the probability that SNR value of the signal received after the selective combining is less than x is expressed by the following equation:

$$P_r(\gamma_{sc} \leq x) = \prod_{k=1}^D P_r(\gamma_k \leq x), \quad (15)$$

where γ_{sc} is the SNR value after selective combining and D is the number of receivers. Assuming that the average SNR value and the fading parameter m_k are the same at each receiving end, the SNR value of the received signal has the same probability distribution. Therefore, the SNR value of the signal received is expressed by:

$$P_{\gamma,sc}(x) = [P_r(\gamma_k \leq x)]^D = [P_r(x)]^D, \quad (16)$$

As a result, the probability density function for SNR of the received signal after selective combining is expressed by the following equation as a differential value of Eq. (16):

$$P_{\gamma,sc}(\gamma) = D [P_{\gamma}(\gamma)]^{D-1} P_{\gamma}(\gamma). \quad (17)$$

If the number of antennas of the receiver is larger than that of the transmitter, the signal with the highest SNR among the signals of the multipath can be used or the signal can be combined. If the number of antennas of the transmitter is larger than that of the receiver, beamforming can increase the SNR value obtained by the receiver. The number of antennas D of the receiving end may affect the SNR value.

6. Conclusions

We studied vehicle-related parameters that affect secrecy capacity of vehicle communication, such as vehicle speed, response time, and speed limit. When considering the Doppler effect according to the speed of the vehicle, secrecy capacity is studied to be proportional to the speed, but when considering the safety distance of autonomous driving, secrecy capacity is inversely proportional to the speed of the vehicle. In general, the relationship between secrecy capacity according to the antenna-related parameters, beamforming, jamming, the size of the antenna, and the number of antennas was also discussed. We also looked at increasing secrecy capacity in indirect communication through relays rather than direct communication, and improving security through assistive devices. Finally, we examined how the noise-related parameters according to the fading model influence secrecy capacity. In conclusion, it was confirmed that various vehicle secrecy parameters exist in vehicle communication, and these parameters can be changed by a user. This makes it possible for us to be able to communicate with the vehicle later, while maintaining a certain level of security. It is expected that the road to secure the security of the vehicle radio channel used for these vehicle secrecy parameters will begin not long.

Acknowledgements


We sincerely appreciate Professor S.J. Oh for teaching physical layer security.

Author details

Na-Young Ahn and Dong Hoon Lee*
 The Graduate School of Information Security at Korea University, Seoul, Korea

*Address all correspondence to: donghlee@korea.ac.kr

IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Sun L, Du Q. Secure data dissemination for intelligent transportation systems. In: *Secure and Trustworthy Transportation Cyber-Physical Systems*, Springer Briefs in Computer Science. 2017. pp. 99-140
- [2] Camacho F, Cárdenas C, Muñoz D. Emerging technologies and research challenges for intelligent transportation systems: 5G, HetNets, and SDN. *International Journal on Interactive Design and Manufacturing*. 2018;**12**(1): 327-335
- [3] Whyte W, Weimerskirch A, Kumar V, Hehn T. A security credential management system for V2V communications. In: *2013 IEEE Vehicular Networking Conference (VNC)*. 2013
- [4] Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*. 2017;**4**(6):1832-1843
- [5] Liang L, Peng H, Li GY, Shen XS. Vehicular communications: A physical layer perspective. *IEEE Transactions on Vehicular Technology*. 2017;**66**(12): 10647-10659
- [6] Han D, Bai B, Chen W. Secure V2V communications via relays: Resource allocation and performance analysis. *IEEE Wireless Communications Letters*. 2017;**6**(3):342-345
- [7] Eltayeb ME, Choi J, Al-Naffouri TY, Heath RW Jr. Enhancing secrecy with multi-antenna transmission in millimeter wave vehicular communication systems. *IEEE Transactions on Vehicular Technology*. 2017;**66**(9):8139-8151
- [8] Available from: https://en.wikipedia.org/wiki/Information_theory
- [9] Bloch M, Barros J, Rodrigues MRD, McLaughlin SW. Wireless information-theoretic security. *IEEE Transactions on Information Theory*. 2008;**54**(6): 2515-2534
- [10] Zou Y, Zhu J, Wang X, Leung VCM. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*. 2015;**29**(1):42-48
- [11] Ahn NY, Lee DH, Oh S-J. Vehicle communication using secrecy capacity. In: Kapoor S, Arai K, Bhatia R, editors. *Proceedings of the Future Technologies Conference (FTC) 2018 - Volume 2, Advances in Intelligent Systems and Computing*. Vol. 881. Switzerland: Springer Verlag. 2019. pp. 158-172. Available at: https://doi.org/10.1007/978-3-030-02683-7_13
- [12] Chopra G, Jha RK, Jain S. Novel beamforming approach for secure communication in UDN to maximize secrecy rate and fairness security assessment. *IEEE Internet of Things Journal*. 2019;**6**(4):5935-5947
- [13] Lin S, Zhang J, Zhou G, Gu L, Stankovic JA, He T. Adaptive transmission power control for wireless sensor networks. In: *Proc. 4th Int. Conf. Embedded Netw. Sensor Syst.* 2006. pp. 223-236
- [14] Zareei M, Vargas-Rosales C, Villalpando-Hernandez R, Azpilicueta L, Anisi MH, Rehmani MH. The effects of an adaptive and distributed transmission power control on the performance of energy harvesting sensor networks. *Computer Networks*. 2018;**137**:69-82
- [15] Nandan N, Majhi S, Wu H. Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming.

IEEE Transactions on Wireless Communications. 2018;17(8):5327-5337

- [16] Yaacoub E, Al-Husseini M, Chehab A, Abualsaud K, Khattab T, Guizani M. 3D beamforming with massive cylindrical arrays for physical layer secure data transmission. *IEEE Communications Letters*. 2019;23(5): 830-833
- [17] Cho S, Chen G, Coon JP. Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems. *IEEE Transactions on Information Forensics and Security*. 2019;14(10):2633-2648
- [18] Wang S, Jiang X-Q, Wang P, Zhu Y. An artificial noise assisted secrecy-enhancing scheme for space-time shift keying systems. *Physical Communication*. 2019;35:100693
- [19] Huo Y, Tian Y, Ma L, Cheng X, Jing T. Jamming strategies for physical layer security. *IEEE Wireless Communications*. 2018;25(1):148-153
- [20] Compston AJ, Fluhler JD, Schantz HG. A fundamental limit on antenna gain for electrically small antennas. In: 2008 IEEE Sarnoff Symposium; Princeton, NJ. 2008. pp. 1-5
- [21] Hong T, Liu C, Kadoch M. Machine learning based antenna design for physical layer security in ambient backscatter communications. *Wireless Communications and Mobile Computing*. 2019:4870656
- [22] Trichili A, Park K, Zghal M, Ooi BS, Alouini M. Communicating using spatial mode multiplexing: Potentials, challenges and perspectives. *IEEE Communication Surveys and Tutorials*; 2019:1
- [23] Inomata M, Imai T, Kitao K, Okumura Y, Motoharu S, Takatori Y.

Radio propagation prediction for high frequency bands using hybrid method of ray-tracing and ER model with point cloud of urban environments. In: *IET Conference Proceedings*. 2018

- [24] Guntupalli AB, Wu K. 60 GHz circularly-polarized smart antenna system for high throughput two-dimensional scan cognitive radio. In: 2013 IEEE MTT-S International Microwave Symposium Digest (MTT); Seattle, WA. 2013. pp. 1-3
- [25] Sun L, Ren P, Du Q. Distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks. *EURASIP Journal on Wireless Communications and Networking*. 2014;1:1-11
- [26] Zheng T, Wang H, Huang R, Mu P. Adaptive DF relaying transmission for security. In: 2015 IEEE Globecom Workshops (GC Wkshps); San Diego, CA. 2015. pp. 1-6
- [27] Han D, Bai B, Chen W. Secure V2V communications via relays: Resource allocation and performance analysis. *IEEE Wireless Communications Letters*. 2017;6(3):342-345
- [28] Chen JS, Yang CY, Hwang MS. The capacity analysis in the secure cooperative communication system. *International Journal of Network Security*. 2017;19(6):863-869
- [29] Wu Y et al. Secrecy-driven resource management for vehicular computation offloading networks. *IEEE Network*. 2018;32(3):84-91
- [30] Wang J, Liu J, Kato N. Networking and communications in autonomous driving: A survey. *IEEE Communication Surveys and Tutorials*. 2019;21(2): 1243-1274
- [31] Wang L, Liu X. NOTSA: Novel OBU with three-level security architecture

for internet of vehicles. *IEEE Internet of Things Journal*. 2018;5(5):3548-3558

[32] Pelletier H, Charvet X. Improving the DPA Attack Using Wavelet Transform; 26-29 September 2005. Honolulu, Hawaii, USA: NIST's Physical Security Testing Workshop; 2005

[33] Ai J, Wang Z, Zhou X, Ou C. Improved wavelet transform for noise reduction in power analysis attacks. In: 2016 IEEE International Conference on Signal and Image Processing (ICSIP); Beijing. 2016. pp. 602-606

[34] Dong X et al. A wavelet-based power analysis attack against random delay countermeasure. In: 2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST); Hong Kong. 2018. pp. 19-24

[35] Martinek R, Vanus J, Bilik P, Al-Wohaishi M, Zidek J, Wen H. The implementation of equalization algorithms for real transmission channels. In: 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings; Taipei. 2016. pp. 1-6

[36] Martinek R et al. Modelling of wireless fading channels with RF impairments using virtual instruments. In: 2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON); Clearwater, FL. 2016. pp. 1-6

[37] Shu Z, Yang Y, Qian Y, Hu RQ. Impact of interference on secrecy capacity in a cognitive radio network. In: 2011 IEEE Global Telecommunications Conference—GLOBECOM 2011; Kathmandu. 2011. pp. 1-6

[38] Yacoub MD. The α - μ distribution: A physical fading model for the Stacy distribution. *IEEE Transactions on Vehicular Technology*. 2007;56(1):27-34

[39] Qu S, Fleisher SM. Double differential MPSK on the fast Rician fading channel. *IEEE Transactions on Vehicular Technology*. 1992;41(3): 278-295

[40] Hua Y, Wang Y. On the saturate throughput of IEEE 802.11 DCF with capture effect in Rician fading channel. In: 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing; Dalian. 2008. pp. 1-4

[41] Donald AMM, Olivier JC. A comparative study of deterministic and stochastic sum-of-sinusoids models of Rayleigh-fading wireless channels. In: 2007 IEEE Wireless Communications and Networking Conference, Kowloon. 2007. pp. 2027-2031

[42] Afzal A, Hassan SA. A stochastic geometry approach for outage analysis of ad hoc SISO networks in Rayleigh fading. In: 2013 IEEE Global Communications Conference (GLOBECOM); Atlanta, GA. 2013. pp. 336-341

[43] Feng Q, Li W, Huang L. Analysis of spontaneous Raman and Rayleigh scatterings in distributed Fiber Raman amplification systems based on a random distribution model. *IEEE Photonics Journal*. 2017;9(6):1-8. Art No. 7205008

[44] Abbas SA, Sheikh AU. A geometric theory of Nakagami fading multipath mobile radio channel with physical interpretations. In: Proceedings of Vehicular Technology Conference. Vol. 2. Atlanta, GA, USA: VTC; 1996. pp. 637-641

[45] Zhang QT. A generic correlated Nakagami fading model for wireless communications. *IEEE Transactions on Communications*. 2003;51(11): 1745-1748

[46] Lu J, Han Y. Application of multipath shape factors in Nakagami-m fading channel. In: 2009 International Conference on Wireless Communications & Signal Processing; Nanjing. 2009. pp. 1-4

[47] Nguyen T, Tran X. Performance of cooperative NOMA system with a full-duplex relay over Nakagami-m fading channels. In: 2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom); Hanoi, Vietnam. 2019. pp. 130-134