Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 15(1): 14-20, Mar. 2017 **Regular paper**

Survey on Physical Layer Security in Downlink Networks

Mohammed Adil Abbas, *Student Member, KIICE*, and Jun-Pyo Hong*, *Member, KIICE*

Department of Information and Communications Engineering, Pukyong National University, Busan 48513, Korea

Abstract

In this paper, we discuss physical layer security techniques in downlink networks, including eavesdroppers. The main objective of using physical layer security is delivering a perfectly secure message from a transmitter to an intended receiver in the presence of passive or active eavesdroppers who are trying to wiretap the information or disturb the network stability. In downlink networks, based on the random feature of channels to terminals, opportunistic user scheduling can be exploited as an additional tool for enhancing physical layer security. We introduce user scheduling strategies and discuss the corresponding performances according to different levels of channel state information (CSI) at the base station (BS). We show that the availability of CSI of eavesdroppers significantly affects not only the beamforming strategy but also the user scheduling. Eventually, we provide intuitive information on the effect of CSI on the secrecy performance by considering three scenarios: perfect, imperfect, and absence of eavesdropper's CSI at the BS.

Index Terms: Artificial noise, Beamforming, Downlink network, Physical layer security, Secrecy, Wiretap channel

I. INTRODUCTION

Because of the broadcasting nature of wireless communications, they are easier to attack than wired communications. Since the number of objects connected to the Internet is increasing rapidly and most connections rely on wireless communications, the demand for the security of private information is expected to be very high not only from academia but also from industry.

Traditionally, security was considered an issue related to cryptographic techniques in the upper network layers. The representative example is an example of data encryption based on a private code. Suppose that there are two terminals that have their own private code. Each terminal encrypts the message before transmission in order for the other legitimate terminal to get the message securely. In other words, the private code has to be known only to a pair of terminals for the secure communication between legitimate users. However, it is challenging to securely share the private code between the terminals, particularly in wireless networks.

The initial work on physical layer security was done by Shannon [1]. He invented the theoretical foundation of cryptography on the basis of information theoretic approaches. In [2], the researchers introduced the wiretap channel and derived its secrecy capacity by exploiting additional channel impairments to an eavesdropper. In particular, the basic wiretap channel consists of three terminals: transmitter (Alice), intended receiver (Bob), and eavesdropper (Eve) in Fig. 1. It was derived that Alice can forward a message to Bob with the positive rate while preventing Eve from extracting any information from the received signal only when the channel between Alice and Eve is a degraded version of that between Alice and Bob.

Received 06 January 2017, **Revised** 09 January 2017, **Accepted** 18 January 2017
***Corresponding Author** Jun-Pyo Hong (E-mail: jp_hong@pknu.ac.kr, Tel: +82-51-629-6227)
Department of Information and Communications Engineering, Pukyong National University, 45, Yongso-ro, Nam-gu, Busan 48513, Korea.

Open Access **http://doi.org/10.6109/jicce.2017.15.1.14** print ISSN: 2234-8255 online ISSN: 2234-8883

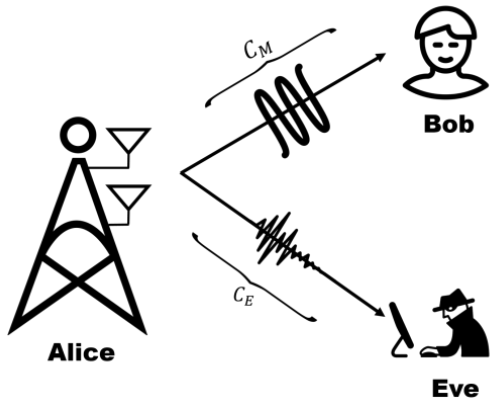

Fig. 1. Basic wiretap channel.

In the wiretap channel, the most used performance metric is the secrecy capacity, which is the maximum achievable rate without providing any information to eavesdroppers. In particular, with the additive white Gaussian noise channel assumption, the secrecy capacity of the basic wiretap channel can be expressed as follows:

$$C_S = [\log_2(1+\gamma_M) - \log_2(1+\gamma_E)]^+, \qquad (1)$$

where $[x]^+ = \max(x, 0)$, and γ_M and γ_E denote the signal-to-noise ratios (SNRs) of the main channel and the eavesdropping channel, respectively. From (1), we know that the secrecy capacity is the difference between the capacity C_M of the Alice–Bob link and the capacity C_E of the Alice–Eve link.

The rest of this paper is organized as follows: Section II introduces the physical layer security in the downlink networks consisting of a single base station and multiple users. In particular, subsection A discusses the transmission methods with the perfect channel state information (CSI) of the intended user at the base station, and subsection B discusses the transmission methods with the imperfect CSI. Finally, Section III concludes this paper.

II. PHYSICAL LAYER SECURITY IN DOWNLINK NETWORKS

A downlink network plays an important role in the current communication systems, such as cellular systems and wireless local area networks. Because of this network's importance in communication systems, there have been extensive works on increasing spectral efficiency in diverse types of downlink networks.

In a conventional downlink network consisting of a single base station and multiple receivers, the base station exploits the multi-antenna and the opportunistic receiver scheduling as the representative tools for improving the spectral efficiency. Further, in a downlink network including eavesdroppers, such tools are utilized not only for improving the achievable rate to an intended user but also for preventing eavesdroppers from extracting any information.

Fig. 2 illustrates a general system model of a downlink network with eavesdroppers. The network consists of a base station with M antennas, K legitimate users with $N_r$antennas, and N eavesdroppers with N_e antennas. The base station is assumed to know the perfect or imperfect CSI of K legitimate users but does not know the CSI of the eavesdroppers.

On the basis of the physical layer security concepts, positive secrecy can be achieved only when the main channel between the base station and the intended user is in a better condition than the eavesdropping channel between the base station and the eavesdroppers. However, because of the randomness of the channel condition, the main channel condition cannot always be better than the eavesdropping

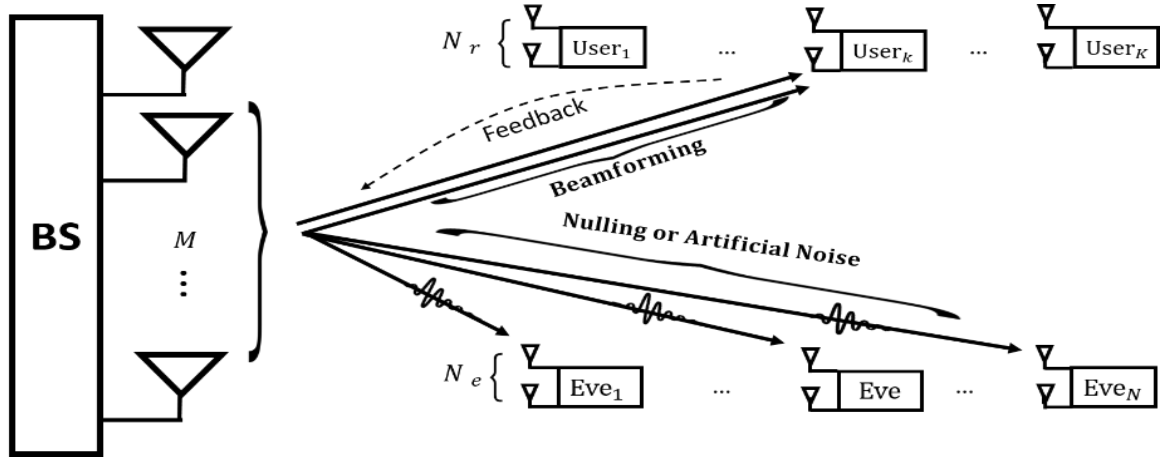

Fig. 2. Downlink network with eavesdroppers.

channel condition. Furthermore, some difficulties arise from the fact that the base station finds it difficult to obtain perfect CSI. In the following subsections, we will discuss the multi-antenna and user scheduling techniques for maximizing the secrecy performance to the availability of CSI at the transmitter.

A. Perfect CSI

In this subsection, we mainly focus on the transmission schemes exploiting the perfect CSI of the legitimate receivers for several types of eavesdroppers. Even though the perfect CSI is the ideal assumption because of the estimation error and feedback delay, it provides the performance upper bound and enables us to focus on the issues caused by eavesdroppers. Therefore, many works on physical layer security assume the perfect CSI of the legitimate users. The perfect CSI assumption enables the base station to enhance the secrecy rate (R_s) by adopting the transmission beam to the channel realizations and scheduling the user who has a good effective channel gain. Furthermore, it can be utilized for deciding the codeword length and the appropriate time to transmit data.

In a downlink network where all except the scheduled user are considered potential eavesdroppers, the best way to maximize the secrecy rate is to schedule the user who has the largest SNR if the base station is equipped with a single antenna. Then, the secrecy rate can be expressed by the difference between the achievable rate of the main link to the scheduled user and that of the link to the users who has the second largest SNR. With the opportunistic user scheduling at the base station, the secrecy rate of the network decreases with an increase in the number of users since the achievable rate of the link to the user with the second largest SNR converges to that to the scheduled user. Eventually, the secrecy rate becomes almost zero for a network with a large number of users [3].

1) Artificial Noise Transmission:

The multi-antenna at the base station provides additional degrees of freedom for enhancing the secrecy rate. It enables the base station not only to perform beamforming for forwarding the information signal but also to transmit the artificial noise for preventing eavesdroppers from extracting the information. The idea of utilizing artificial noise transmission was first introduced in [4, 5]. In other words, the transmit signal $\mathbf{x}_k$ for the user k is a linear combination of an information signal and artificial noise as follows:

$$\mathbf{x}_k = \sqrt{(1-\alpha)P}\,\boldsymbol{w}_k\, s + \sqrt{\alpha P}\,\boldsymbol{\eta}_k \ , \qquad (2)$$

where the transmit power $P = Tr[\mathbf{x}_k^H \mathbf{x}_k]$ and α denotes the power portion between the information signal and the noise. $\boldsymbol{w}_k \in \mathbb{C}^{M\times 1}$ represents the beamforming vector $||\mathbf{w}_k|| = 1$, which is given by $\boldsymbol{w}_k = \boldsymbol{h}_k^H / \|\boldsymbol{h}_k^H\|$; it is commonly known as maximum ratio transmission (MRT). $\boldsymbol{\eta}_k$ denotes the artificial noise vector that is designed to be orthogonal to the channel of the scheduled user but not the channels of the eavesdroppers. Hence, the noise vector ensures no channel degradation except the eavesdroppers' channels. When the base station knows the CSI of the links to legitimate users and has only the statistical knowledge of the link to the eavesdroppers, the secrecy rate of the network is heavily dependent on the types of eavesdroppers with respect to whether the eavesdroppers can share the received signal between them. The effect of information sharing on the performance is equivalent to that of multiple antennas at the base station on the performance. Since the mutual information between the base station and the eavesdroppers increase with an increase in the number of cooperating eavesdroppers, the base station in the case with information-sharing eavesdroppers is required for allocating more power on the artificial noise transmission than in the case with non-cooperating eavesdroppers. Furthermore, the secrecy rate decreasing speed with respect to the number of users monotonically increases with an increase in the number of information sharing eavesdroppers. In contrast, in the case of information non-sharing eavesdroppers, the non-adaptive equal power allocation between the information signal and the artificial noise achieves a secrecy rate performance comparable to the optimal power allocation [6].

Fig. 3 shows the gain of the artificial noise transmission against the conventional beamforming scheme, MRT. For a given target user, the achievable secrecy rate decreases with an increase in the number of eavesdroppers for all transmission scenarios. The transmission with MRT fails to achieve a positive secrecy rate if there are many eavesdroppers since there is a high probability for one or more eavesdroppers to have a channel similar to that of the intended user. However, an artificial noise transmission enables the base station to degrade the channel condition of the eavesdroppers and to achieve a non-zero secrecy rate, even for a large number of users [6].

If the objective of the downlink network is the maximization of the network security rate, we can consider opportunistic user scheduling to be an effective tool.

In conventional networks without any eavesdroppers, the base station schedules the user who has the largest channel gain for maximizing the network throughput. The network throughput increases with an increase in the number of users K, and it scales like $\log(\log K)$ for i.i.d. Rayleigh fading channel model. However, the opportunistic user scheduling rule and the corresponding secrecy rate characteristics are change significantly if the eavesdroppers are additionally

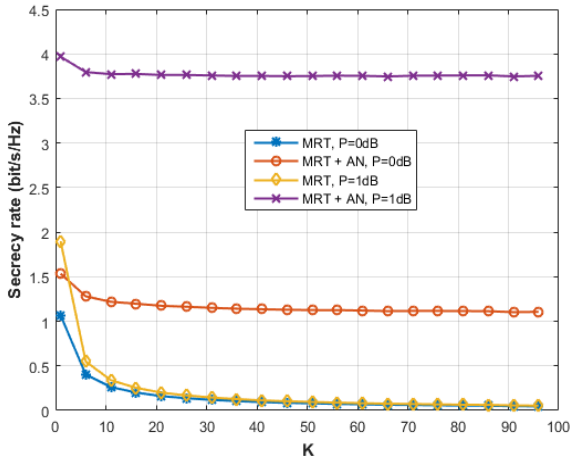

Fig. 3. Secrecy rate versus the number of eavesdroppers for equal power allocation [6].

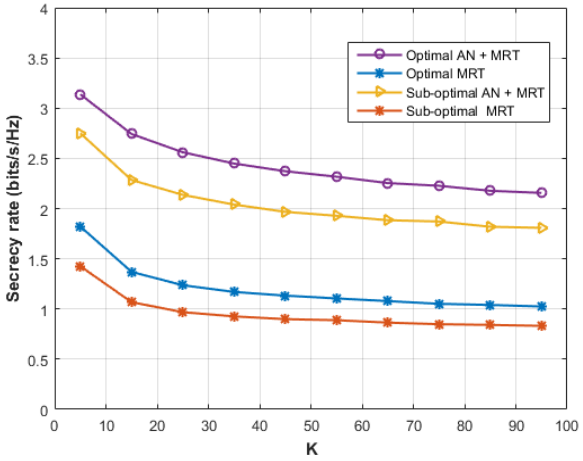

Fig. 4. Optimal and sub-optimal user scheduling.

considered in the network. In other words, the base station needs to take into account not only the CSI of the users but also the CSI of the eavesdroppers.

Fig. 4 shows the average network secrecy rate in a downlink network where there are K users and the global CSI is available at the base station. In this simulation, all except the scheduled user are considered to be potential eavesdroppers. The base station is required to schedule the users who have a high channel gain to the base station and a low channel gain between the base station and the eavesdroppers. In contrast to the throughput in the conventional downlink networks without eavesdroppers, the network secrecy rate is not a monotonic increasing function of K. This can be attributed to the fact that the increasing rate of the scheduled user's mutual information with respect to K is lower than that of the dominant eavesdropper's mutual information. The secrecy rates with optimal user scheduling, which takes into account both the main and the wiretap channel gains, are labeled "optimal" in Fig. 4. The secrecy rates with sub-optimal scheduling, which takes into account only the main channel gain, are labeled "sub-optimal" in Fig. 4.

It is impossible to guarantee a positive secrecy rate since there is always a positive probability that some of the eavesdroppers have a better channel condition than the scheduled user. In the slow fading channel, the codeword length is shorter than the channel coherence time. As an alternative performance metric for taking into account the failures in the secure communication, we can consider the outage secrecy capacity instead of the secrecy rate. The outage secrecy capacity is defined as the maximum secrecy rate while maintaining the secrecy outage probability below a certain value ε [6]. In contrast, in the fast fading channel where the codeword length is considerably longer than the channel coherence time, ergodic secrecy is a more appropriate performance metric [7].

When the base station has no CSI on the eavesdroppers, the secrecy rate for a given outage threshold ε is maximized with MRT and equal power allocation between the information signal and the artificial noise [8].

2) Zero Forcing Technique

The zero forcing (ZF) scheme that transmits the information signal in the orthogonal direction of the subspace spanned by the eavesdroppers' channels is an effective way to block the signal reception at the eavesdroppers. However, it basically requires an accurate CSI at the base station. When the CSI of both the users and the eavesdroppers is perfectly known to the base station with a sufficient number of transmit antennas, the ZF confidently delivers the message to the users with a relatively low interference level [9].

Further, when the eavesdroppers' CSI is not perfectly known to the base station or is partially available, the base station takes advantage of both the schemes. The ZF technique is used for maintaining the secrecy among the legitimate users and delivering the messages with the minimum interference and the artificial noise to confuse the eavesdroppers and enhance the secrecy. If the number of antennas at the eavesdropper is $N_e \leq M - K$, the base station can forward the information to any target user with a secrecy rate proportional to the transmit power even if no CSI of the eavesdropper is available except its statistical information. However, if the eavesdropper knows the global CSI and has a sufficient number of antennas to cancel out the artificial noise $N_e \geq M - K$, the secrecy rate becomes insensitive to the power increase and converges to a constant value for a large transmit power [10, 11].

Fig. 5 shows the impact of increasing N_e on the average secrecy rate. Even though the beamforming and the artificial noise transmission enhance the secrecy rate, it rapidly

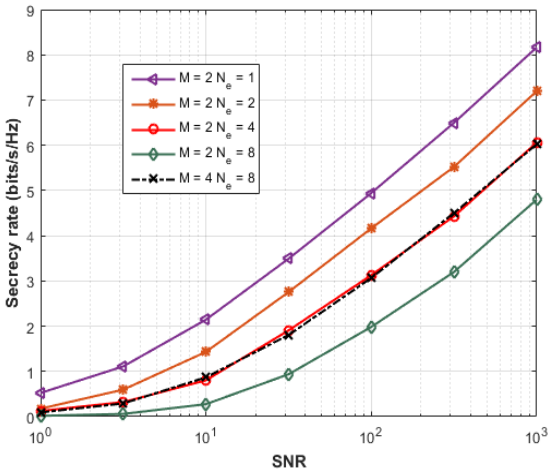

Fig. 5. Secrecy rate versus the number of antennas at eavesdropper N_e.

decreases with an increase in N_e.

In many scenarios, the base station is unable to obtain the CSI of the eavesdroppers since the eavesdroppers may not be willing to feedback their CSI. If the CSI of an eavesdropper is not available, the base station generates the beamforming vectors and schedules a user on the basis of only the CSI of the users, as in the case of a conventional network without any eavesdroppers [12].

3) Transmit Antenna Selection

Transmit antenna selection (TAS) is a simple transmission strategy that exploits a single radio frequency chain. Therefore, we can reduce the implementation cost, the computational complexity, and the hardware size. The base station selects the antenna that has a high main channel gain and low eavesdropping channel gains in order to maximize the secrecy rate with a single antenna. Because of the non-correlation between the channels of the intended user and the eavesdroppers, the secrecy rate increases monotonically with an increase in the number of antennas [13].

B. Imperfect CSI

In this subsection, we relax the perfect CSI assumption at the base station. In other words, there are some estimation errors at the CSI of the legitimate users. A perfect channel estimation is difficult to implement in practice since a better estimation requires more communication resources, such as time, bandwidth, and energy. There are several ways for the base station to track the CSI. In the time-division duplex (TDD) systems, the base station can estimate the CSI by using the channel reciprocity. In the frequency-division duplex (FDD) systems, the CSI is obtained from the feedback since there is no channel reciprocity. The imperfect CSI can be classified into three categories: deterministic imperfect instantaneous CSI, indeterministic imperfect instantaneous CSI, and statistical CSI [14].

The actual channel gain of the user k is represented by the sum of its estimation and estimation error $\mathbf{h}_k = \widehat{\mathbf{h}}_k + \mathbf{\Delta h}_k$. The estimation error $\mathbf{\Delta h}_k$ is unknown to the transmitter and is independent of the error estimated by the transmitter $\widehat{\mathbf{h}}_k$; the entries of both $\widehat{\mathbf{h}}_k$ and $\mathbf{\Delta h}_k$ are i.i.d. Gaussian random variables [15]. If there is an error in the CSI at the base station, it is impossible to perfectly align the beam vectors for the information signal and the artificial noise to the subspace spanned by the main channel and the null space of the main channel, respectively. Then, the received signal of the intended user is interfered by the artificial noise.

1) Artificial Noise Transmission

Let us consider the effect of imperfect CSI on the artificial noise transmission strategy. In a network where there is a single transmitter, a single legitimate receiver K = 1, and N non-cooperating eavesdroppers, the imperfect CSI affects the power allocation between the information signal and the artificial noise. As N_e increases, the power portion allocated to the artificial noise increases and converges to a fixed value at high SNR. In addition, as the estimation error increases, more power should be allocated to the artificial noise. This is because the channel estimation error degrades the information signal reception at the intended user but not at the eavesdroppers, and the effectiveness of the artificial noise on the eavesdroppers does not get degraded by the estimation error. Furthermore, since the artificial noise becomes a dominant factor for degrading the SNR at the intended user in a high SNR region, the secrecy rate converges to a fixed value with an increase in the SNR [11].

2) Zero Forcing Technique

For the scenario where $M > K$ and all except the scheduled user are considered the potential eavesdroppers, ZF is an effective way to block the signal reception at the eavesdroppers. However, it basically requires accurate CSI at the base station. As the magnitude of error in the CSI increases, the network secrecy rate decreases rapidly. As an alternative to mitigate the performance degradation from the imperfect CSI in the ZF, we can consider the regularized channel inversion (RCI). The RCI precoding matrix to deliver information $\mathbf{s} = [s_1, \ldots, s_K]^T$ is given by $\widehat{\mathbf{W}} = \widehat{\mathbf{H}}^H\left(\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H + \varphi\,\mathbf{I}\right)^{-1}$, where $\widehat{\mathbf{H}} = \left[\hat{\mathbf{h}}_1, \ldots, \hat{\mathbf{h}}_K\right] \in \mathbb{C}^{K\times M}$ denotes the channel matrix with errors. The regularization parameter φ controls the amount of interference introduced by one user to another. If the base station knows the perfect CSI of the users, RCI acts as ZF with $\varphi = 0$. In contrast, if there is imperfect CSI at the base station, RCI always outperforms ZF [11].

For $M > K$, nulling out the received signal at the

eavesdroppers with RCI is not always the best choice for maximizing the network secrecy rate. In some networks with non-cooperating eavesdroppers, an artificial noise transmission outperforms RCI even though it causes the artificial noise reception at the scheduled users because of the imperfect CSI [16].

3) Transmit Antenna Selection

When there is outdated CSI at the base station, the base station cannot achieve the diversity order proportional to the number of transmit antennas through TAS [17].

III. DISCUSSION AND CONCLUSIONS

In this paper, we introduced the work on physical layer security techniques in downlink networks including eavesdroppers. The multi-antenna and user techniques are considered to be the representative tools for improving the network secrecy rate. Although there has been extensive work on the wireless physical layer security technique, there are some topics that have not been clearly addressed.

In particular, most joint optimization problems associated with more than one physical layer security technique have not provided the information on optimal performance, for example, the joint optimization between transmission beamforming and user scheduling in the downlink network with potential eavesdroppers. Furthermore, there should be efforts to explore the commercial application of the physical layer security technique and implement the theoretical techniques in practical wireless systems.

ACKNOWLEDGMENTS

This work was supported by a 2015 Research Grant of Pukyong National University.

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[2] A. D. Wyner, “The wire-tap channel,” *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, “On the resilience of wireless multiuser networks to passive and active eavesdroppers,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1850-1863, 2013.

[4] R. Negi and S. Goel, “Secret communication using artificial noise,” in *Proceedings of IEEE Vehicular Technology Conference (VTC)*, Dallas, TX, 2005.

[5] R. Negi and S. Goel, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, 2008.

[6] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831-3842, 2010.

[7] X. Zhang, X. Zhou, and M. R. McKay, “On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170-2181, 2012.

[8] S. Gerbracht, Ch. Scheunert, and E. A. Jorswieck, “Secrecy outage in MISO systems with partial channel information,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704-716, 2012.

[9] G. Zheng, P. D. Arapoglou, and B. Ottersten, “Physical layer security in multibeam satellite systems,” *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 852-863, 2012.

[10] N. Li, X. Tao, and J. Xu, “Artificial noise assisted communication in the multiuser downlink: optimal power allocation,” *IEEE Communications Letters*, vol. 19, no. 2, pp. 295-298, 2015.

[11] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, “Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: ergodic secrecy sum rate and optimal power allocation,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7036-7050, 2016.

[12] I. Krikidis and B. Ottersten, “Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling,” *IEEE Signal Processing Letters*, vol. 20, no. 2, pp. 141-144, 2013.

[13] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372-375, 2012.

[14] B. He, X. Zhou, and T. D. Abhayapala, “Wireless physical layer security with imperfect channel state information: a survey,” 2013 [Internet], Available: https://arxiv.org/pdf/1307.4146.pdf.

[15] I. Telatar, “Capacity of multi- antenna Gaussian channels,” *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585-595, 1999.

[16] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, “QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach,” *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202-1216, 2011.

[17] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection,” *IEEE Communications Letters*, vol. 17, no. 5, pp. 864-867, 2013.

Mohammed Adil Abbas
received his B.Sc. degree from the School of Electronics and Communications Engineering, University of Baghdad, Iraq, in 2009. He is currently pursuing his master's degree at the School of Information and Communications Engineering, Pukyong National University, Korea. His research interests are in the area of cooperative communications and physical layer security.

Jun-Pyo Hong
received his B.Sc. in Electrical Engineering from Information and Communications University, Daejeon, Korea, in 2008, and his M.S. and Ph.D. in Electrical Engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2010 and 2014, respectively. He is currently Assistant Professor with Department of Information and Communications Engineering, Pukyong National University, Busan, Korea.