The Capacity Analysis in the Secure Cooperative Communication System

Jong-Shin Chen[1], Cheng-Ying Yang[2], and Min-Shiang Hwang[3,4],
(Corresponding author: Min-Shiang Hwang)

Department of Information and Communication Engineering, Chaoyang University of Technology[1]
Taichung 41349, Taiwan, R.O.C.
Department of Computer Science, University of Taipei[2]
Taipei 10048, Taiwan, R.O.C.
Department of Computer Science and Information Engineering, Asia University[3]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University[4]
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Email: mshwang@asia.edu.tw)
(Invited Jan. 11, 2017)

Abstract

With the characteristic of spatial diversity and low cost, cooperative system is a tendency for the future communications. In the wireless communication system, there exist degradation factors such as signal fading, multipath transmission, signal inferences, bandwidth limitation and so on. In addition to these degradation factors, the wireless transmission is not a secure environment. The information might be leaked during the transmission. Currently, the issues of privacy and security have become increasingly important for the mobile users. Traditionally, the security scheme is applied to the higher network layer. Encryption can be complex and difficult without infrastructure. It is not suitable to apply to the equipment with low computing resources, such as Internet of Things (IoT) application. Within information theoretic security characterizes the fundamental ability of the physical layer to provide a secure transmission. Hence, this work concentrates on the secure cooperative communication system. Based on the Shannon third theorem on channel capacity, this work analyzes the secrecy capacity between the source station and the destination station. For a practical situation in the system, the scenario includes multiple source stations, multiple relay stations, multiple destination stations, and eavesdroppers. For the positive secrecy rate consideration, the maximum mutual information between the source station and the destination station and the minimum mutual information between the source station and the eavesdropper should be held. To ensure a secure communication, the derived theoretical solution could be applied to find the optimal relay assignment. Beyond the relay selection, some issues related to the secure cooperative communication are suggested for the future researches in the final.

Keywords: Internet of Things (IoT); Multiple Input Multiple Output (MIMO); Physical Layer Security; Secrecy Capacity; Secure Cooperative Communications; Shannon Third Theorem

1 Introduction

The wireless communications provide a number of multimedia services for the mobile users. However, there exist degradation factors, such as signal fading, multipath transmission, signal inferences, bandwidth limitation and so on because of the radio transmission. Under the condition of imitated transmission bandwidth, to improve system performance in the wireless systems could be a significant work. Especially, the spatial diversity techniques could be employed to improve the system performance [4, 7, 8, 11, 13]. For example, in the Multiple Input Multiple Output (MIMO) system, a spatial diversity gain is employed to improve the system performance. However, MIMO is with the high cost of hardware implementation because there are multiple antennas at both the transmitter and receiver [3, 7, 11]. Instead of MIMO technique, the cooperative communications with a relay channel increase the system capacity without extra antennas [8, 13].

Cooperative communication is an idea to employ the wireless channel to make communication nodes help each other to implement the communication process [11]. It benefits the wireless communication with the gain similar to that of MIMO. It improves the system capacity,

transmission speed, and system performance. On the other hand, it could reduce the power consumption at the communication ends to extend the lifetime of the system. It is suitable to provide the multimedia services for the mobile devices. In the cooperative communication systems, the relay station functions with a character of spatial diversity. Comparing with multiple carrier modulation schemes, the relay stations work as the receivers and the transmitters. The relay station not only forwards the transmitted information but also process the received signal. It provides a high throughput performance. The destination station could receive the information with a spatial diversity with employing the relay selection scheme. Even though the destination station has no multiple antennas, by employing the relay station as the virtual antenna, it increases the transmission data rate and provides a reliable channel capacity [7]. With a consideration of low cost, the cooperative communication system is a tendency in the future communications.

However, the wireless communication is not a secure environment for a highly private request. The issues of privacy and security have become increasingly important for the mobile users. Besides, security is the fundamental requirement for a personal communication. Secure communications enable the authenticated destination station could successfully receive the information from the source station. Also, it protects the transmitted information from the eavesdroppers to interpret. Traditionally, the secure communication depends on the cryptographic encryption at the application layer. The complex and difficult cryptography is the practical techniques without infrastructure for the secure communication in the presence of third parties [5, 10], i.e. eavesdroppers. The technique relates to construct and analyze the transmission protocols to overcome the influence of eavesdroppers to ensure the security constraints with confidentiality, integrity, and availability including authentication, and non-repudiation. Cryptographic encryption converts the meaningful information to be the apparent nonsense to avoid the eavesdroppers to release the desired and transmitted information. However, the encryption algorithms are developed based on the assumption of limited computational capability at the eavesdroppers [10]. Also, these encryptions assume there are a perfectly secret key management and the distribution scheme for the users. Hence, it is not practical for the wireless communication application. Especially, it is obvious for IoT application [19]. Besides, for the secure purpose, the social-aware networking has been proposed to the secure cooperative communication systems [6, 17]. The authentication protocol within the networking could be the preliminary limitation for access control scheme. Eventually, the secure communication could be hold based on the secrecy rate [9]. Hence, physical layer security has been proposed for this purpose [3, 5, 14, 20, 21].

In the cooperative communication system, the information is transmitted from the source station to the destination station with the help of relay stations [4]. Among the relay stations, the transmitted information is unwrapped in the presence of one or more eavesdroppers. The information could be eavesdropped from the source station or from the relay which the source station adopts in the cooperative communication. Hence, to provide a secure communication and service quality could become an important issue. In Section 2, the concept of the cooperative communication system is described and the quantity measurements of the information between the source station and the destination station are provided. Section 3 illustrates the analytical model for the secure communication and the theoretical requirement for the cooperative system is derived. Under the secure cooperative communication requirement, the constraint of the relay selection strategy is shown in Section 4. The conclusion and the further work suggestion are given in the final.

2 The Cooperative Communication

Similarly to the Multiple Input Multiple Output (MIMO) technique with a character of spatial diversity, the cooperative communication system uses single-antenna mobiles in a multi-user environment to share their antennas to create a virtual MIMO system and to improve the system performance. Basically, the concept of the cooperative communication is illustrated in Figure 1.

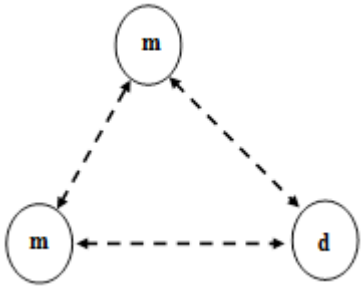


Figure 1: The concept of cooperative communication

In Figure 1, there are two mobile devices transmit the data to the same destination station simultaneously. Each device has its own antenna and cannot generate a spatial diversity. With the cooperation from the other device, it might be possible for one device to receive the other, the transmitted data can be forwarded with the same information to the destination station. One of these two mobile devices could be thought as the source station and the other is the corresponding relay station. With these three nodes, the source station, the relay station and the destination station, the capacity analysis of the cooperation communication system including these three nodes could be modeled as that in Figure 2.

In Figure 2, $h_{s,r}$ and $h_{r,d}$ denote as the channel response between source station to resource station and the

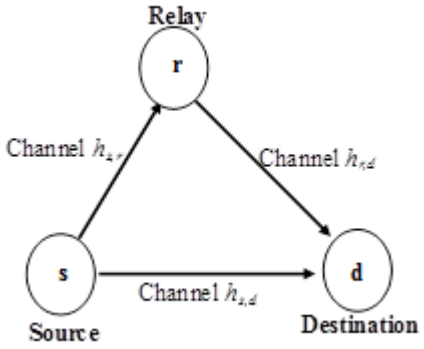


Figure 2: Analytical model for the cooperative communication

channel response between the resource station to destination station, respectively. The source station broadcasts the information to the destination station with both straight forward link and the assistant link with the relay station. This relay station might be another user in the system. The relay station functions as receiving the transmitted information from the source station and transmitting the information to the destination station. At the destination station, it multiple receives the information from the source station and the relay station. In the cooperative communication system, the destination station employs Maximal Ratio Combining (MRC) technique or Selective Combining (SC) technique to the received signals from the source station and the relay station [2]. It depends on the cooperative strategy used in the relay station. For example, in Amplify-and-Forward transmission mode, under AWGN channel, the maximize mutual information between the source and the destination becomes [18]:

$$I_{s,d} = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,d}|^2}{N_0} + \frac{1}{N_0}\frac{P_sP_r|h_{s,r}|^2|h_{r,d}|^2}{P_s|h_{s,r}|^2+P_r|h_{r,d}|^2+N_0}) \quad (1)$$

where P_s is the signal power from the source station, P_r is the signal power from the relay station, and $n_{s,r}$ and $n_{s,d}$ are AWGN with the variance N_0. In Fixed Decode-and-Forward transmission mode, under AWGN channel, the mutual information between the source and the destination becomes [16]

$$I_{s,d} = \min\{I_{s,r}, I_{r,d}\} \quad (2)$$

where

$$I_{s,r} = \frac{1}{2}\log_2(1+SNR_{s,r}) = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,r}|^2}{N_0})$$

and

$$I_{r,d} = \frac{1}{2}\log_2(1+SNR_{r,d}) = \frac{1}{2}\log_2(1+\frac{P_r|h_{r,d}|^2}{N_0}).$$

The system capacity depends on the maximum mutual information between the source station and the destination stations.

However, the wireless communication is not a secure environment. Within the theoretical information security characterizes [12], the fundamental ability of the physical layer provides a secure transmission. For example, channel coding and spread spectrum techniques provide secure communications. Hence, based on the Shannon third theorem on channel capacity, the secure communication could be hold based on the positive secrecy rate [1, 12]. The secrecy rate (i.e. secrecy capacity) of transmission is defined as the mutual information difference between the mutual information to the destination and that to the eavesdropper, i.e.

$$C_{s,d} = I_{s,d} - I_{s,e}. \quad (3)$$

3 The Secure Cooperative System

The secure cooperative system could be illustrated in Figure 3. There are a source station, a relay group, an eavesdropper group and a destination station in the system. In the system, the source station transmits the information. The information could be delivered directly to the destination station through the straightforward link between the source station and the destination. On the other hand, the information might be transmitted to the relay station and, then, delivered to the destination station with the help of the relay station. Similarly, the scenario of the information transmitted to the eavesdropper could be held in this wireless environment.

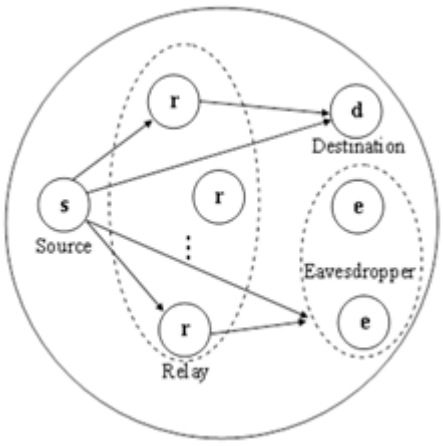
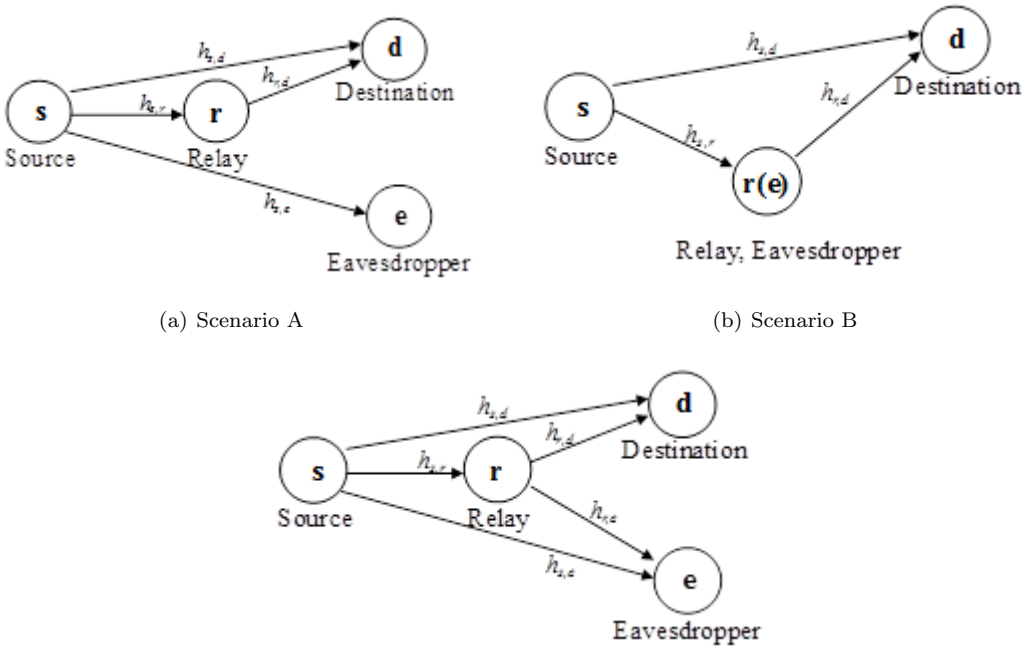


Figure 3: The cooperative communication environment

In order to consider the secure communication between the source station and the destination station, the location of the eavesdroppers could be considered with the following scenarios in Figure 4.

In Figure 4(a), the eavesdropper locates at the end communication link. The cooperative system employs



(a) Scenario A

(b) Scenario B

(c) Scenario C

Figure 4: The scenario for the location of eavesdroppers

the relay station to forward the information to the destination station. Hence, the mutual information between the source station and the destination could be obtained according to the previous theoretical derivation [16, 18]. Also, the mutual information between the source station and the eavesdropper could be obtained. The nodes in the cooperative communication system could work as the transmitter and receiver as that mentioned previously and each node could function as the relay station between the source station and destination station. Hence, in Figure 4(b), the relay could work as the eavesdropper to forward the information from the source station to the destination station. Similarly, the theoretical mutual information between the source station and the destination could be obtained according to the previous theoretical derivation. At the meantime, the analysis to mutual information between the source station and the eavesdropper could be considered as the case in Figure 4(a) with the same channel impulse response to the relay station, i.e. $h_{s,e} = h_{s,r}$. The case in Figure 4(b) could be considered as a special case of the scenario A. In Figure 4(c), the eavesdropper locates at the end communication link. With the different scenario to the scenario B, the relay station is not an eavesdropper and it forwards the transmitted information to the destination station. However, the eavesdropper receives the information from the source station and the relay station. For simplified analysis, the scenario C could be considered as the general case. For example, the situation in Figure 4(a) could be modified as that with the broken link between the relay station and eavesdropper in Figure 4(c). Hence, Figure 4(c) can be considered as the general situation for secure analysis and reshown in Figure 5.

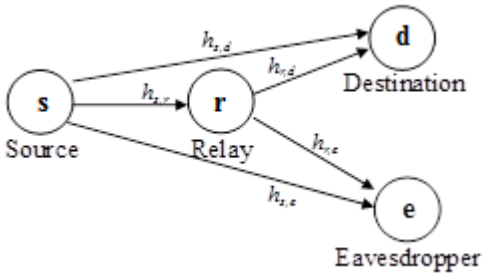


Figure 5: Analytical model for the secure cooperative communication

As the mentioned previously, for example, the maximize mutual information with AF mode between the source and the eavesdropper

$$I_{s,e} = \frac{1}{2}\log_2(1 + \frac{P_s|h_{s,e}|^2}{N_0} + \frac{P_r|h_{r,e}|^2}{N_0}) \quad (4)$$

Under the condition that the relay station could not decode the received signal correctly, the mutual information between the source station and the eavesdropper is

$$I_{s,e} = \frac{1}{2}\log_2(1 + \frac{P_s}{N_0}|h_{s,e}|^2). \quad (5)$$

The secrecy capacity of transmission is defined in Equation (3).

When the secrecy capacity is negative, the intercept event will be held and the eavesdropper could intercept the transmitted information successfully. Hence, the condition for a secure communication, the secrecy capacity $C_{s,d}$ should be positive. The maximum of secrecy capacity $C_{s,d}$ could be reached with maximizing the mutual information between the source station and the destination station and minimizing the mutual information between the source station and the eavesdropper. Hence, the relay selection strategy in the secure cooperative system could be employed with the concern of maximum the secrecy capacity in the system.

4 Relay Selection Strategy

For the relay selection, almost researchers concentrated on the situation that the single source station and discussed the relay assignment. However, in practical, there exist many source stations in the system. There are a lot of users requiring the relay stations to transfer the information. Based on this situation, relay selection should consider the multiple source stations, multiple relay stations and multiple destination stations in the system, as shown in Figure 6

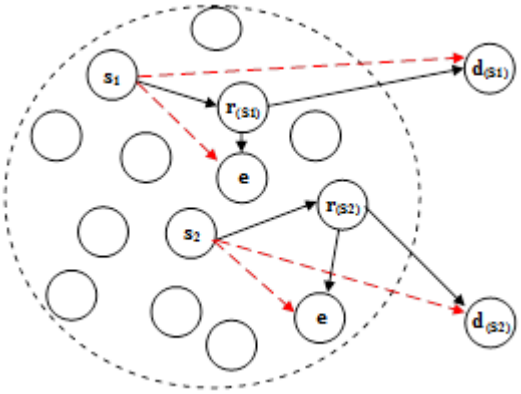


Figure 6: Fixed mode relay selection

The analysis to the relay selection is based on fixed mode in the cooperative communication system [16, 18]. It supposes that there are v nodes in the system and those nodes are denoted as set V. In the set V, there are k nodes as the source stations there are m nodes that could function as the source station and the relay station. These m nodes are denoted as set M. All the source stations are denoted as set S, i.e. $S \subseteq M$. $r(s)$ is defined as the set of the relay stations with forwarding the transmitted signal for the source station s. In this system, all source stations have their own destination stations. $d(s_i)$ represents the destination station for source station s_i. The destination station does not belong to set M. To analyze the secrecy capacity in the cooperative communications, initially, consider for the source station i transmits the information to the destination station d(si) with the relay station r_i. Under AWGN channel, for the example in AF mode, the mutual information between the source station i and the destination is described in Equation (1):

$$I_{s,d(s_i)} = \frac{1}{2}\log_2(1 + \frac{P_{s_i}|h_{s_i,d(s_i)}|^2}{N_0} + \frac{P_{r_i}||h_{r_i,d(s_i)}|^2}{N_0}).$$

Similarly, Equation (3) could be applied to DF mode if the relay station could correctly decode the transmitted signal and maximal ratio combining (MRC) strategy the equal gain for each forward link applied. However, if the relay station could not decode the transmitted signal correctly, Selective Combining (SC) strategy applied, the mutual information between the source station i and the destination is described in Equation (3) and could be rewritten as

$$I_{s_i,d(s_i)} = \frac{1}{2}\log_2(1 + \frac{P_{s_i}}{N_0}|h_{s_i,d(s_i)}|^2).$$

In the both modes, the mutual information between the source station and the eavesdropper is

$$I_{s_i,e} = \frac{1}{2}\log_2(1 + \frac{P_{s_i}|h_{s_i,e}|^2}{N_0} + \frac{P_{r_i}|h_{r_i,e}|^2}{N_0}).$$

The secrecy capacity in the cooperative system becomes

$$C_{s_i,d(s_i)} = I_{s_i,d(s_i)} - I_{s_i,e}.$$

To approach the maximal mutual information achieved in the system at the destination stations should consider the channel condition, under the situation of multiple source station, multiple relay stations, and multiple destination station environments. Hence, the relay selection strategy for secure cooperative communication could be developed based on the maximum mutual information between the source station i and the destination station, the minimum mutual information between the source station i and the eavesdropper and the positive secrecy capacity, i.e.

$$I_{s,d(s)} = \max_{r=(r_1,r_2,\cdots,r_k)\in R(s_1)\times R(s_2)\times\cdots\times R(s_k)} \sum_{i=1}^{k} I_{s_i,d(s_i)}$$

and

$$I_{s,e} = \min_{r=(r_1,r_2,\cdots,r_k)\in R(s_1)\times R(s_2)\times\cdots\times R(s_k)} \sum_{i=1}^{k} I_{s_i,e}$$

and, the positive secrecy capacity $C_{s_i,d(s_i)}$. Hence, the limitation to this problem could become

$$\begin{aligned} C &= \max \sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{i,j} C_{s_i,d(s_i)} \\ &= \sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{i,j} \cdot \{\max(I_{s,d(s)} - I_{s,e})\} \end{aligned}$$

under the conditions,

$$\begin{aligned} \sum_{i=1}^{k} \rho_{i,j} &\leq 1, \forall i = 1,2,\cdots,k, \quad \text{and} \\ \sum_{j=1}^{m} \rho_{i,j} &= 1, \forall j = 1,2,\cdots,m \end{aligned}$$

where $\rho_{i,j}$ is defined as the connection between the relay station i to the destination station j. Hence, how to choose the appropriate relay station i to approach the maximum mutual information becomes an important issue. The limitation for the relay selection strategy is with the above derivate equations.

5 Conclusion and Further Work

With the character of low cost, the cooperative system is a tendency for the future communications. For a practical situation in the cooperative system, the scenario includes multiple source stations, multiple relay stations, multiple destination stations, and eavesdroppers. This paper concentrates on the physical layer secure in the cooperative systems and develops the theoretical limitation for the relay assignment scheme. For the secrecy capacity in the system, it begins to analyze the theoretical mutual information between the source station and the destination station. The maximum mutual information could be achieved by the power management in the system. Also, it could be obtained with the appropriate relay selection strategy. On the other hand, in order to obtain the maximum the secrecy capacity, one possible solution is to achieve the minimum mutual information between the source station and the eavesdropper. To ensure the secure communication, based on the information theory, the secrecy capacity should be kept a positive value. By deriving the theoretical solution to the system performance in the secure cooperative system, this work applies the derived results to the considered environment to construct the optimal relay assignment scheme. By the way, the better relay selection strategy could be developed with maximizing the secrecy capacity in the system. Also, the effective relay selection algorithm could be developed in the future.

Other important issues to the secure cooperative communications including the power distribution, the coding schemes, the multiple access technique, and the transmission protocol and so on could be made further researches. Power control management is to find the appropriate power distribution among the relay stations. Obviously, it could be found in the theoretical mutual information analysis. Within the mathematical derivations, the transmitted power from the source station and the relay stations effects the system capacity. This power control issue for the relay stations could be included in the design to achieve the optimal throughput for the cooperative system. The coding schemes and multiple access techniques convert the desired information to be the nonsense data. It increases the secrecy capacity between the source station and the destination station to make sure the positive secrecy rate. These practical considerations and requirements on the system design could contribute to constructing a cooperative system as well as extensions to the fundamental idea of secure communication.

Acknowledgment

This research was partially supported by the Ministry Of Science and Technology, Taiwan (ROC), under contract no.: MOST 103-2632-E-324-001-MY3.

References

[1] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of 2006 IEEE International Symposium on Information Theory*, pp. 356–360, 2016.

[2] E. Beres and R. S. Adve, "Selection cooperation in multi-source cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 1, pp. 118–127, 2008.

[3] X. Chen, L. Lei, H. Zhang and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5135–5146, 2015.

[4] Y. Chou, J. Zhu, X. Wang and V.C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[5] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[6] X. Gu, L. Tang, and J. Han, "A social-aware routing protocol based on fuzzy logic in vehicular ad hoc networks," *Proceedings of 2014 International Workshop on High Mobility Wireless Communications (HMWC'14)*, pp. 12–16, 2014.

[7] L. Li, X. Zhou, H. Xu, G. Y. Li, D. Wang, and A. Soong, "Simplified relay selection and power allocation in cooperative cognitive radio systems," *IEEE Transactions on Wireless Communications*, vol. 10, no. 1, pp. 33–36, 2011.

[8] H. C. Lu and W. Liao, "Cooperative strategies in wireless relay networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 323–330, 2012.

[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[10] D. W. K. Ng, E. S. Lo and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp.4599–4615, 2014.

[11] A. Nosratinia, T. E. Hunter and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74–80, 2004.

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technology Journal*, vol. 29, pp. 656–715, 1949.

[13] K. Vardhe, D. Reynolds and B. D. Woerner, "Joint power allocation and relay selection for multiuser cooperative communication," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1255–1260, 2010.

[14] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 247–258, 2014.

[15] Y. Wang and G. Noubir, "Distributed cooperation and diversity for hybrid wireless networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 3, pp. 596–608, 2013.

[16] J. H. Wen, C. H. Chiang, Y. S. Lin, C. Y. Yang, "Performance evaluation for the cooperative communication systems in decode-and-forward mode with a maximal ratio combining scheme," *WSEAS Transactions on Communications*, vol. 13, pp. 424–429, 2014.

[17] F. Xia, L. Liu, J. Li, A. M. Ahmed, L. T. Yang and J. Ma, "BEEINFO: Interest-based forwarding using artificial bee colony for socially-aware networking," *IEEE Transactions on Vehicle Technology*, vol. 64, no. 3, pp. 1–11, 2014.

[18] C.Y. Yang, Y.S. Lin and M.S. Hwang, "Downlink relay selection algorithm for amplify-and-forward cooperative communication systems," in *Proceedings of 2013 Seventh International Conference on Intelligent, and Software Intensive Systems (CISIS'13)*, pp. 331–334, 2013.

[19] Z. K. Zhang, M. C. Y. Cho and S. Shieh, "Emerging security threats and countermeasures in IoT," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pp. 1–6, 2015.

[20] T. Zou, X. Wang and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[21] Y. Zou, J. Zhu, X. Wang and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

Biography

Jong-Shin Chen was born in 1972. He received the B.S. and Ph.D. degrees in computer science from Feng Chia University, Taiwan, in 1996 and 2003, respectively. Currently, he is an associate professor in the Department of Information and Communication Engineering, ChaoYang University of Technology, Taiwan. His research interests include big-data mining, capacity planning, and wireless networking.

Cheng-Ying Yang received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as an Associate Professor at Department of Computer Science, University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing and computer security.

Min-Shiang Hwang received the Ph.D. degree in computer and information science from the National Chiao Tung University, Taiwan in 1995. Dr. Hwang was the Chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2003. He was a distinguished professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). His current research interests include information security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 200+ articles on the above research fields in international journals.