EPiC Series in Computing
Volume 58, 2019, Pages 144–154
Proceedings of 34th International Conference on Computers and Their Applications

EPiC Computing

Evaluation of Secrecy Rate in Cooperative Communication System

Cheng-Ying Yang[1], Hsin-Ying Liang[2,*]and Pin-Yen Huang[3]
[1] Department of Computer Science, University of Taipei, Taipei, Taiwan
[2] Dept. of Info. & Comm. Eng., Chaoyang University of Technology, Taichung, Taiwan
[3] Department of Computer Science, National Chengchi University, Taipei, Taiwan

Abstract

Cooperative system is a tendency for future communications because of its spatial diversity to improve the system performance. However, the security is a critical issue in the wireless application with a highly private request. Although the encryption schemes have been proposed to approach the secure purpose, those schemes need a lot of computing resource. It is not practical for the applications with limited computing ability, such as IoT. According to Shannon theory of perfect secrecy, the security could be implemented on the physical layer. Based on the positive secrecy rate, the evaluation of security, secure communication could be practical. This work concentrates on the theoretical solution to the secrecy rate in the AF mode cooperative communication system. Also, the numerical results with the proposed methodology are given. It shows the effects of eavesdropper could not affect the secure communication if the number of the eavesdropper is less than that of relays in the system. The appropriate relay assignment benefits the secure communication.

1 Introduction

Wireless communication networks play an important role in the smart city. It increases a lot of advanced services for life convenience. Although to access the wireless services is convenient, the degrading characteristics of radio transmission are signal fading, multipath transmission, signal inferences, bandwidth limitation and so on (Singh & Manu 2017). In order to combat the fading and increase the throughput, multiple-Input multiple-output (MIMO) that improves the system capacity, transmission speed and system performance has been realized as an effective scheme. However, MIMO employs multiple antennas at the transmitter and the receiver. MIMO has a high cost and could not be easily implemented because of physical size and power consumption (Chen, Lei, Zhang & Yuen 2015). Alternatively, similar to MIMO with the diversity gain, the cooperative communication is an idea to make communication nodes help each other to implement the communication process (Nosratinia,

*: Corresponding author

Hunter, & Hedayat 2004). Cooperative communication systems provide a high throughput performance compared with multiple carrier modulation schemes and MIMO schemes. The destination user could transmit data with a spatial diversity by employing the relay stations.

Comparing to MIMO systems, even though the destination user under the environment without multiple antennas, the cooperative communication system is still with the character of spatial diversity. By employing the relay station as the function of the antenna, it increases the transmission data rate and provides a reliable channel capacity (Chen, Yang, & Hwang 2017; Kramer, Gastpar, & Gupta 2005). Besides, the cooperative communication could reduce the power consumption at the communication ends to extend the lifetime of the system. It is suitable to provide 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 by employing the relay. 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 (Wang, & Noubir 2013). With consideration of low cost, the cooperative communication system is a tendency in future communications.

There are three transmission modes in cooperative communications. One is Amplify-and-Forward (AF) mode. Another is Decode-and-Forward (DF) mode and the other is Compress and Forward (CF) mode (Bletsas, Shin, & Win 2007). With AF mode, the transmitted signal could be amplified and retransmit to the destination. It is easy with low complexity. It could be applied to those short distance transmissions. With DF mode, the relay station decodes and demodulates the received signal and, then, recodes and modulates the signal to retransmit to the destination. With CF mode, the relay station does not have to decode the compressed signal. It uses the coding schemes to compress the received signal and retransmit to the destination. These cooperative communication systems could promote the system performance without the limitation of peer-to-peer transmission with an appropriate relay assignment (Yang, Lin & Wen 2014). Among these three transmission modes, AF mode is with low complexity to implement.

However, security is an important factor in the wireless application with a highly private request. The critical issues of privacy and security have become increasingly important for mobile users (Janani & Manikandan 2018; Rana & Sharma 2018). Especially, for banking and credit card transaction, security is an essential consideration for people to use the wireless application (Li, Hwang & Liu 2008; Li, Hwang & Chu 2009; Li & Hwang 2011; Lu, Wu & Yang 2015). Security becomes the fundamental requirement for personal communication. It enables the authenticated destination user could successfully receive the information from the source end (Ma, Han, Peng & Zhang 2018; Patel 2017). At the same time, it protects the transmitted information from the eavesdroppers. Conventionally, the security depends on the cryptographic encryption at the application layer. The complex and difficult cryptography is the practical techniques for secure communication. For example, RSA based asymmetric encryption and X.509 certifications were proposed for a two-way authentication security scheme (Chang & Hwang 1996; Deng, Huang & Qu 2017; Kothmayr, Schmitt, Hu, Brünig & Carle 2013; Sharma, Bala & Verma 2016). The authentication protocol that employs Elliptic Curve Qu-Vanstone (ECQV) implicit certificate scheme and Elliptic Curve Diffie-Hellman (ECDH) key exchange scheme has been proposed (Chiou, Ko & Lu 2018; Han, Xie & Liu 2017; Hou & Wang 2017; Hwang, Tzeng & Tsai 2004; Liu & Cao 2016; Porambage, Schmitt, Kumar, Gurtov & Ylianttila 2014; Teng & Li 2018; Tzeng & Hwang 2004). Cryptographic encryption converts the meaningful information to be the apparent nonsense to avoid the eavesdroppers to release the transmitted information. However, the encryption algorithms are developed based on the assumption of limited computational capability at the eavesdroppers (Ng, Lo & Schobe 2014). Moreover, there are perfectly secret key management and the distribution scheme for the users within these encryptions schemes. Hence, it is not practical for the real-time wireless application. For the Internet of things (IoT) application, the ability of computing is limited (Ma 2017; Tai & Chang 2017). Also, for the accessing internet, the authentication protocol within the networking could be the limitation because of less computing resource. Based on the secrecy rate, the secure communication, physical layer security, could be practical (Bloch & Barros 2011; Mukherjee, Fakoorian, Huang & Swindlehurst 2014; Shannon 1949; Zou, Zhu, Wang & Leung 2015).

Based on the maximum secrecy capacity, the analysis of AF mode cooperative communication system is proposed. It derives the relay assignment to maximize the overall secrecy rate. In the following section, the secure communication with Shannon theory is described. Also, the information in the cooperative system with AF transmission mode is derived. Based on the secure communication and AF mode cooperative system, the secure cooperative system model is proposed with the eavesdropper inside. In Section IV, the numerical results show the secrecy evaluation for the cooperative system with an exhaustive search mechanism. The conclusion of this work is given in the final.

2 Secure Cooperative Communication System

2.1 Secure Communication

Traditionally, secure communication employs authorization and authentication schemes to control system access. Moreover, in a wireless system, an encryption is added to the existed protocol to protect the eavesdropper to catch the transmitted signal and decode to be the transmitted information. Critically, for the purpose of information security, it is reasonable to adopt the secure scheme at each layer. However, the security mechanism could be implemented with an efficient cost consideration. According to Shannon theory of perfect secrecy (Shannon 1949), in Fig. 1, the security could be obtained if the entropy of the codeword is greater or equal to the transmitted information.

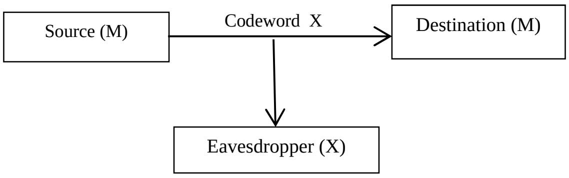

Fig. 1 A peer-to-peer communication with an eavesdropper

It leads to realizing the uncertainty of the transmitted codeword must be at least as larger as the uncertainty of information (Bloch & Barros 2011), i.e. positive secrecy rate (Barros & Rodrigues 2006),

$$C_{s,d} = I_{s,d} - I_{s,e} \quad (1)$$

where $C_{s,d}$ is the secrecy rate (i.e. secrecy capacity) of transmission is defined as the mutual information difference between the mutual information from the source to the destination and that from the source to the eavesdropper. $I_{s,d}$ and $I_{s,e}$ denote the information between the source and the destination and the information between the source and the eavesdropper, respectively. Under AGWN, the information between the source and the destination is

$$I_{s,d} = \frac{1}{2}\log_2(1 + SNR_{s,d}) \quad (2)$$

where $SNR_{s,d}$ is defined as the signal power to noise ratio between the source and the destination. Also, it could be represented as

$$I_{s,d} = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,d}|^2}{N_0}) \tag{3}$$

where P_s is the signal power from the source, $h_{s,d}$ is the channel response in AWGN with the variance N_0. Similarly,

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

where $h_{s,d}$ is the channel response. Hence, for a two-point communication, the secrecy rate could be found with the difference between Eq. (3) and Eq. (4).

2.2 Cooperative System

In the cooperative communication system, each station has a transmitter, a receiver, and an antenna. It assumes that each station could transmit and to receive signals simultaneously. Within Amplify-and-Forward (AF) mode, the transmitted signal could be amplified and retransmit to the destination. First, consider a single user in Fig. 2. $h_{s,d}$ denotes the channel response between the source station to destination station. Similarly, $h_{s,r}$ and $h_{r,d}$ represent the channel response between the source station and the relay station and the channel response between the relay station and the destination station, respectively. In Fig. 2, at the first time instant, the received signal at the relay station and destination station could be expressed in Eq. (5) and Eq. (6).

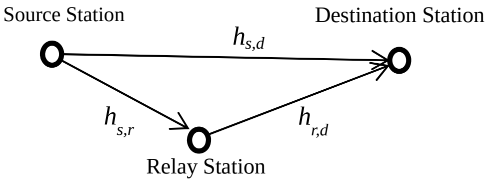

Fig. 2 A cooperative communication model

$$y_{s,r} = \sqrt{P_s}h_{s,r}x + n_{s,r} \tag{5}$$

and

$$y_{s,d} = \sqrt{P_s}h_{s,d}x + n_{s,d} \tag{6}$$

where P_s is the transmission power from the source station, $n_{s,r}$ and $n_{s,d}$ are AWGN with the variance N_0. Then, the relay retransmits the received signal. At the second time instant, at the destination station, the received signal has two components. One is from the source station and the other is from the relay station. With the processing of Maximal Ratio Combiner, the maximum SNR could be approached (Yang, Lin & Hwang 2013).

$$SNR_{\max} = \frac{P_s|h_{s,d}|^2}{N_0} + \frac{1}{N_0}\frac{P_sP_r|h_{s,r}|^2|h_{r,d}|^2}{P_s|h_{s,r}|^2 + P_r|h_{r,d}|^2 + N_0} \tag{7}$$

Then, the instantaneous mutual information, I_{AF}, between the source station and the destination station is

$$I_{AF} = \frac{1}{2}\log_2(1+SNR_{\max}) = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,d}|^2}{N_0}+\frac{1}{N_0}\frac{P_sP_r|h_{s,r}|^2|h_{r,d}|^2}{P_s|h_{s,r}|^2+P_r|h_{r,d}|^2+N_0}) \quad (8)$$

According to the above, the model of the secure cooper4ative communication system could be modeled in Fig. 3.

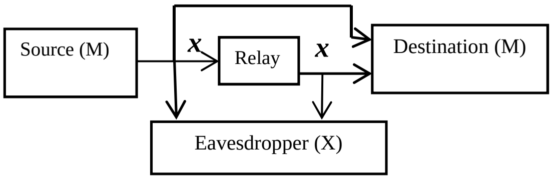

Fig. 3 Cooperative communication with an eavesdropper

In Fig. 3, the eavesdropper locates at the end communication link. Let $h_{s,r}$ and $h_{r,d}$ denote as the channel response between the source station and the relay and the channel response between the relay and the destination, respectively. The source station broadcasts the information to the destination station with both straightforward link and the assistant link with the relay station. This relay station might be another user in the system. The cooperative system employs the relay to forward the information to the destination. Hence, the mutual information between the source and the destination could be,

$$I_{s,d} = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,d}|^2}{N_0}+\frac{1}{N_0}\frac{P_sP_r|h_{s,r}|^2|h_{r,d}|^2}{P_s|h_{s,r}|^2+P_r|h_{r,d}|^2+N_0}) \quad (9)$$

where P_r is the signal power from the relay station and AWGN is with the variance N_0. Also, the mutual information between the source and the eavesdropper could be obtained.

$$I_{s,e} = \frac{1}{2}\log_2(1+\frac{P_s|h_{s,e}|^2}{N_0}+\frac{1}{N_0}\frac{P_sP_r|h_{s,r}|^2|h_{r,e}|^2}{P_s|h_{s,r}|^2+P_r|h_{r,e}|^2+N_0}) \quad (10)$$

The eavesdropper could be the relay itself. Then, the mutual information between the source and the eavesdropper becomes

$$I_{s,e} = \frac{1}{2}\log_2\left(1+\frac{P_s}{N_0}|h_{s,e}|^2\right) \quad (11)$$

The secrecy rate defined in Eq. (1). When the secrecy capacity is negative, the eavesdropper could intercept the transmitted information successfully. Hence, the condition for a secure communication, the secrecy rate, $C_{s,d}$, should be kept to be positive. The maximum of secrecy capacity $C_{s,d}$ could be reached by maximizing the mutual information between the source station and the destination station and minimizing the mutual information between the source station and the eavesdropper.

3 Secure Rate Evaluation

The secure rate evaluation is in the cooperative communication system based on fixed mode (Yang, Lin & Hwang 2013). It assumes 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**⊆**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 rate in the cooperative communications, initially, consider for the source station *i* transmits the information to the destination station $d(s_i)$ with the relay station r_i. Under AWGN channel, in AF mode, the secrecy capacity in the cooperative system becomes

$$C_{s_i,d(s_i)} = \max_{r=(r_1,r_2,\cdots r_k)\in R(s_1)\times R(s_2)\times\cdots\times R(s_k)} \left\{ I_{s_i,d(s_i)} - I_{s_i,e} \right\} \tag{12}$$

The maximal mutual information achieved at the destination stations should consider the channel condition, under the multiple source station, multiple relay station and multiple destination station environments. Hence, the secure rate analysis for the secure cooperative communication could be developed based on the maximum mutual information between the information from the source station *i* to the corresponding destination station and the information from the source station *i* to the eavesdropper *e*. In the meantime, the secrecy capacity should be larger than 0 in Eq. (12) for the security purpose, i.e. the positive secrecy capacity $C_{si,d(si)}$. Hence, the limitation of this problem could become

$$C = \max \sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{i,j} C_{s_i,d(s_i)} = \sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{i,j} \cdot \left\{ \max\left((I_{\mathbf{s,d(s)}}) - (I_{\mathbf{s,e}}) \right) \right\} \tag{13}$$

under the conditions,

$$\sum_{j=1}^{k} \rho_{i,j} \le 1, \forall i = 1,2,\cdots,k \tag{14}$$

And

$$\sum_{j=1}^{m} \rho_{i,j} = 1, \forall j = 1,2,\cdots,m \tag{15}$$

where $\rho_{i,j}$ is defined as the connection between the relay station *i* to the destination station *j*. In Eq. (14), for each destination, there is only one corresponding relay station connected to the destination station, $\rho_{i,j}$=1 when there is a connection between relay station *i* to destination station *j* and $\rho_{i,j}$=0 for other situations. In Eq. (15), for each relay, the relay station could connect at most one destination station only. To achieve the optimal solution to Eq. (13), the exhaustive search method could be employed.

4 Numerical Results

For In order to find the optimal solution for the relay mapping, the maximum secrecy rate, the exhaustive search method is used in this numerical experiment. With the exhaustive search method, the solution begins to calculate Eq. (15). First, for each relay station, calculate $|h_{s,ri}|^2$, $|h_{ri,dj}|^2$ and $|h_{s,e}|^2$. Then, calculate the maximum of ($I_{s,d(s)}$-$I_{s,e}$), recorded as $I_{M,N}$. $I_{M,N}$ denotes the secrecy rate from the source station to the destination station M with the relay station N , and $I_{M,N}$ is constructed in a matric $C_{si,d(si)}$,

$$C_{s_i,d(s_i)} = \begin{bmatrix} I_{1,1} & I_{1,2} & \cdots & I_{1,N} \\ I_{2,1} & I_{2,2} & \cdots & I_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ I_{M,1} & I_{M,2} & \cdots & I_{M,N} \end{bmatrix} \tag{16}$$

Finally, iterative calculate the (k, n combination for maximum value in Eq. (13) under the limitation of Eq. (14) and Eq. (15). The optimal mapping for the relay station and destination station could be found with calculation within C(k,n)·k! combinations. It is with high complicated computing to implement. In Fig. 4, the symbol opt(m, n) denotes there are m resource stations and n relays, with an exhaustive algorithm to determine the optimal relay assignment, in the cooperation system. It shows the system capacity of the cooperation system. With the increasing the number of relays and the optimal relay assignment, the capacity will approach the maximum.

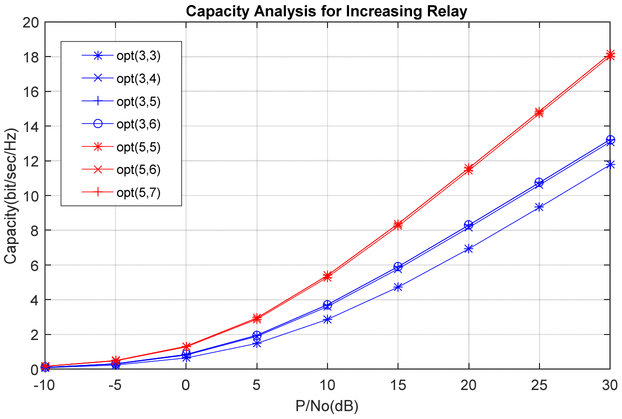

Fig. 4 System capacity of the cooperation system

In Fig. 5, it shows the capacity analysis, with the optimal relay selection, without any eavesdroppers in the cooperation system. Each relay receives the signal from the assigned source station and re-transmits the amplified to the destination station. With the appropriate relay assignment, more relay to choose, the more capacity to be achieved.

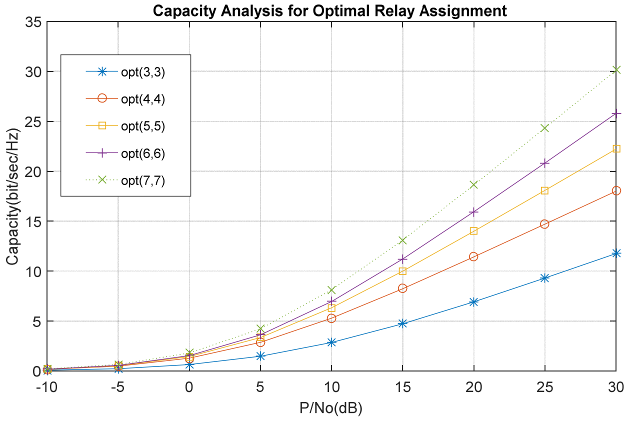

Fig. 5 System capacity of the cooperation system, *m*=*n*

In Fig. 6, the symbol opt(*m*,*n*,*o*) is used to describe there are *m* resource stations, *n* relays and o eavesdroppers in the system. It shows the secret rate increases when the SNR goes up. If there are eavesdroppers in the system, the secrecy capacity decreases when the number of eavesdropper increases.

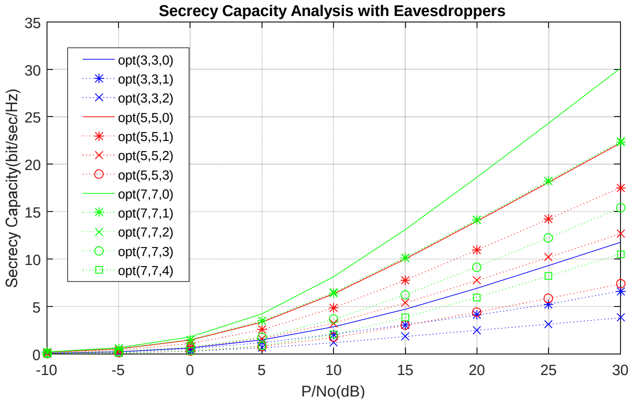

Fig. 6 Secrecy capacity of the system with eavesdroppers

The secrecy capacity analysis of the systems with two eavesdroppers is given in Fig. 7. It shows if the system has extra relays to reduce the degrading effects of eavesdroppers. The secrecy rate is lightly affected if the number of the relay is larger than the number of eavesdroppers. However, the secrecy rate is seriously decreasing when the number relay is less. For the decreasing secret rate, the difference between the number of relay and the number of the eavesdropper is the major degrading factor, but the ratio of relays and eavesdroppers is not. The relay mapping scheme could help to avoid the degrading effects of eavesdroppers and keep a positive secrecy capacity.

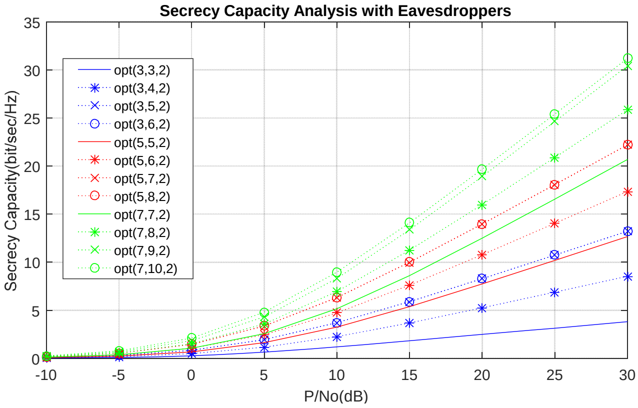

Fig. 7 Secrecy capacity of the system with two eavesdroppers

5 Conclusion

The cooperative system is a tendency for future communications because of low cost and low complexity. In this work, the theoretical solution for a secret AF mode cooperative communication has been proposed. According to Shannon theory, without the encryption, the physical layer could provide secure transmission. Hence, the mutual information is a major concern in this work. Secrecy rate is the evaluation of the secure communication between the source to the destination. However, the security situation might be interrupted by the negative secrecy rate. In order to provide secure communication, this work provides a relay mapping scheme to search the optimal assignment between the source and the relay. It begins to develop the theoretical limit for secure communication. Then, based on the positive secrecy capacity, the maximum secrecy rate is approached with an appropriate relay assignment. In the numerical experiment, the results show if the number of eavesdroppers is less than that of the sources, the secure communication still could work with a suitable relay assignment.

However, the calculation of the maximum secrecy rate is highly complicated. To develop an efficient algorithm to find a positive secrecy rate could be a research issue. The other issue on the power control at the relay station might be considered in the next research. While the eavesdropper has been detected, how to control the transmission power might be another feasible solution for the secret communication.

Acknowlegement

This research was partially supported by the Ministry Of Science and Technology, Taiwan (ROC), under contract no.: MOST 107-2221-E-845 -002 -MY3.

References

Barros, J., & Rodrigues, M. R. (2006, July). Secrecy capacity of wireless channels. *2006 IEEE International Symposium on Information Theory*. 356-360.

Bletsas, A., Shin, H., & Win, M. Z. (2007). Outage analysis for co-operative communication with multiple amplify-and-forward relays. *Electronics Letters*, 43(6), 51-52.

Bloch, M., & Barros, J. (2011). *Physical-layer security: from information theory to security engineering*. Cambridge University Press.

Chang, C. C., & Hwang, M. S. (1996). Parallel computation of the generating keys for RSA cryptosystems. *Electronics Letters,* 32(15), 1365-1366.

Chen, X., Lei, L., Zhang, H., & Yuen, C. (2015). Large-scale MIMO relaying techniques for physical layer security: AF or DF?. *IEEE Transactions on Wireless Communications*, 14(9), 5135-5146.

Chen, J. S., Yang, C. Y., & Hwang, M. S. (2017). The Capacity Analysis in the Secure Cooperative Communication System. *International Journal of Network Security,* 19(6), 863-869.

Chiou, S. Y., Ko, W. T., & Lu, E. H. (2018). A Secure ECC-based Mobile RFID Mutual Authentication Protocol and Its Application. *International Journal of Network Security,* 20(2), 396-402.

Deng, L., Huang, H., & Qu, Y. (2017). Identity Based Proxy Signature from RSA without Pairings. *International Journal of Network Security*, 19(2), 229-235.

Han, L., Xie, Q., & Liu, W. (2017). An Improved Biometric Based Authentication Scheme with User Anonymity Using Elliptic Curve Cryptosystem. *International Journal of Network Security*, 19(3), 469-478.

Hou, G., & Wang, Z. (2017). A Robust and Efficient Remote Authentication Scheme from Elliptic Curve Cryptosystem. *International Journal of Network Security,* 19(6), 904-911.

Hwang, M. S., Tzeng, S. F., & Tsai, C. S. (2004). Generalization of proxy signature based on elliptic curves. *Computer Standards & Interfaces*, 26(2), 73-84.

Janani, V. S., & Manikandan, M. S. K. (2018). An Outlook on Cryptographic and Trust Methodologies for Clusters Based Security in Mobile Ad Hoc Networks. *International Journal of Network Security*, 20(4), 746-753.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, 11(8), 2710-2723.

Kramer, G., Gastpar, M., & Gupta, P. (2005). Cooperative strategies and capacity theorems for relay networks. *IEEE Transactions on Information Theory*, 51(9), 3037-3063.

Li, C. T., & Hwang, M. S. (2011). A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks. *Information Sciences*, 181(23), 5333-5347.

Li, C. T., Hwang, M. S., & Liu, C. Y. (2008). An electronic voting protocol with deniable authentication for mobile ad hoc networks. *Computer Communications*, 31(10), 2534-2540.

Li, C. T., Hwang, M. S., & Chu, Y. P. (2009). An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks. *International Journal of Innovative Computing, Information and Control*, 5(8), 2107-2124.

Liu, L. H., & Cao, Z. J. (2016). A Note on" Efficient Algorithms for Secure Outsourcing of Bilinear Pairings". *International Journal of Electronics and Information Engineering,* 5(1), 30-36.

Lu, Y., Wu, X., & Yang, X. (2015). A secure anonymous authentication scheme for wireless communications using smart cards. *International Journal of Network Security,* 17(3), 237-245.

Ma, Y. (2017). NFC Communications-based Mutual Authentication Scheme for the Internet of Things. *International Journal Network Security*, 19(4), 631-638.

Ma, H., Han, X., Peng, T., & Zhang, L. (2018) Secure and efficient cloud data deduplication supporting dynamic data public auditing. *International Journal of Network Security,* 20(6), 1074-1084.

Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3), 1550-1573.

Ng, D. W. K., Lo, E. S., & Schober, R. (2014). Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer. *IEEE Trans. Wireless Communications*, 13(8), 4599-4615.

Nosratinia, A., Hunter, T. E., & Hedayat, A. (2004). Cooperative communication in wireless networks. *IEEE communications Magazine*, 42(10), 74-80.

Patel, D. (2017). Accountability in cloud computing by means of chain of trust dipen contractor. *International Journal of Network Security*, 19(2), 251-259.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014, April). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. *Wireless Communications and Networking Conference* (WCNC), 2014 pp. 2728-2733.

Rana A. & Sharma D. (2018). Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm. *International Journal of Electronics and Information Engineering*, 8(1), 1-8

Sharma, G., Bala, S., & Verma, A. K. (2016). An Improved RSA-based Certificateless Signature Scheme for Wireless Sensor Networks. *International Journal Network Security*, 18(1), 82-89.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, 28(4), 656-715.

Singh, R., & Manu, M. S. (2017). An Energy Efficient Grid Based Static Node Deployment Strategy For Wireless Sensor Networks. *International Journal of Electronics and Information Engineering*, 7(1), 32-40.

Tai, W. L., & Chang, Y. F. (2017). Comments on a Secure Authentication Scheme for IoT and Cloud Servers. *International Journal Network Security*, 19(4), 648-651.

Teng, L., & Li, H. (2018). A High-efficiency Discrete Logarithm-based Multi-proxy Blind Signature Scheme via Elliptic Curve and Bilinear Mapping. *International Journal of Network Security*, 20(6), 1200-1205.

Tzeng, S. F., & Hwang, M. S. (2004). Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem. *Computer Standards & Interfaces*, 26(2), 61-71.

Wang, Y., & Noubir, G. (2013). Distributed cooperation and diversity for hybrid wireless networks. *IEEE Transactions on Mobile Computing*, 12(3), 596-608.

Yang, C. Y., Lin, Y. S., & Hwang, M. S. (2013, July). Downlink relay selection algorithm for amplify-and-forward cooperative communication systems. *7th International Conference on Complex, Intelligent, and Software Intensive Systems* (CISIS) (pp. 331-334).

Yang, C. Y., Lin, Y. S., & Wen, J. H. (2014). Greedy Algorithm Applied to Relay Selection for Cooperative Communication Systems in Amplify-and-Forward Mode. *Journal of Electronic Science and Technology*, 12(1), 49-53.

Zou, Y., Zhu, J., Wang, X., & Leung, V. C. (2015). Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, 29(1), 42-48.