Greedy Algorithm Applied Secrecy Rate Analysis in the Cooperative Communication

Jong-Shin Chen¹, Shu-Chen Chang², Pin-Yen Huang³ and Cheng-Ying Yang⁴,*

¹ Dept. of Information and Communication Engineering, Chaoyang University of Technology, Taiwan
² Department of Business Administration, National Formosa University, Taiwan
³ Department of Computer Science, National Chengchi University, Taipei, Taiwan
⁴ Department of Computer Science, University of Taipei, Taipei, Taiwan

Abstract - Cooperative communication is the future tendency because of low cost. Three fundamental schemes including Amplify-and-Forward (AF) mode, Decode-and-Forward (DF) mode and Compress and Forward (CF) mode could be employed. In the system, relays play the role to transmit the delivered signal to the destination. However, there might be the eavesdroppers pretend the relay to snip the message. Currently, privacy and security are highly requested in the communication. Hence, the secrecy protection becomes important. Traditionally, the complex encryption scheme would be applied but it is not practical to apply to the equipment with low computing resources. According to Shannon Theory, positive secrecy rate could support secure communications. Maximum secrecy rate is the initial step to analyze the possible secure communication in the cooperative system. The exhaustive method to find the extreme secrecy rate in the system could be realized. However, time efficiency is not considerable. In order to reduce the computational complexity, a greedy algorithm might provide an acceptable solution to approach the purpose of analysis. In this work, the DF mode cooperative mode is adopted for analysis with a greedy algorithm. The result shows the effects of eavesdropper are not significant if the destination station select the strong signal from legitimate stations.

Keywords: secrecy rate, encryption, greedy algorithm, Cooperative communication, DF mode

1 Introduction

Wireless networks provide a variable multimedia service. The throughput was 96 EB very month in 2016. It could be expected to increase to 278 EB in 2021. Also, mobile communication could occupy 63% of the throughput on the internet [1]. Hence, wireless networks play an important role in future communication. To access the wireless services is convenient for mobile users, but the degradation characteristics of signal fading, multipath transmission, signal inferences, bandwidth limitation and so on degrade the system performance. Under the limitation of transmission bandwidth, to improve system performance in the wireless systems becomes important. Employing spatial diversity could be the solution to improve system performance [2]-[3]. To combat the fading, with the spatial diversity, Multiple-Input Multiple-Output (MIMO) improving the system capacity, transmission speed and system performance have been an effective scheme. However, because of high-cost consideration, using multiple antennas at the transmitter and the receiver, MIMO could not be easily implemented [4]. Similar to MIMO, cooperative communication with diversity gain is a solution to increase the system performance [5]. In the cooperative communication systems, the relay plays with a character of spatial diversity. Not only forwarding the transmitted data but also processing the received data, the relay provides a high throughput performance. The destination station could receive data with spatial diversity. Although the destination station has no multiple antennas, it increases the transmission data rate and provides a reliable channel capacity [6].

For the transmission, there are Amplify-and-Forward (AF) mode, Decode-and-Forward (DF) mode and Compress and Forward (CF) mode in the cooperative communication system [7]. AF mode provides low complicated hardware and is easy to be implemented. In DF mode, the relay decodes and demodulates the received signal, and then recodes and modulates the signal to retransmit to the destination. DF mode could have benefits on the coding gain. The relay station does not have to decode the compressed signal in CF mode. The transmission mode uses the coding schemes to compress the received signal and transfer the signal to the destination station. However, wireless communication is not a secure environment. Privacy and security have become increasingly important. The purpose of secure communications is to enable the authentic destination could successfully receive the information from the source station without any information leaking. Traditionally, the security depends on the cryptographic encryption at the application layer. The complex and difficult cryptography is practical. For example, RSA based asymmetric encryption and X.509 certifications were proposed for a two-way authentication security scheme [8]. Cryptographic encryption converts meaningful information to be the apparent nonsense to avoid the eavesdroppers to release the transmitted information.
However, the encryption algorithms assume the limited computational capability at the eavesdroppers and there are perfectly secret key management and the distribution scheme. For the real-time wireless application, it is not practical. For the accessing internet, the authentication protocol within the networking could be the limitation because of less computing resource. For secure communication, physical layer security is proposed [9].

In the cooperative communication system, the transmitted information is unwrapped in the environment with eavesdroppers. The information could be snooped from the source station or from the relay which the source station adopts. Also, the relay might be the eavesdropper. Hence, the relay selection strategy could be a critical scheme. It depends not only on the mutual information between the source station and the destination station but also on the secrecy rate between the source station and the destination station. To approach the secure cooperative communication between the source station and the destination station, the relay selection algorithm should base on the analysis of the positive secrecy rate [4][10]. Based on the maximum secrecy rate, the analysis of cooperative communication system is proposed. In the following, the cooperative communication system model is described with a theoretical performance evaluation. In section 3, the maximum secrecy rate is analyzed under the condition of the wiretap channel model. In Section 4, the numerical results show the secrecy evaluation for the cooperative system. The conclusion is given in the final.

2 Cooperative Communication System

The cooperative communication system could be illustrated in Fig. 1.

The system includes source stations, a relay group, an eavesdropper group and a destination station. In the system, the source station transmits the information. The information could be delivered directly to the destination through the transmission link between the source station and the destination. Also, the information might be transmitted to the relay station and, then, delivered to the destination station with the help of the relay. Consider a single user environment, as shown in Fig. 2. $h_{sr}$ is denoted as the channel response between the source station to destination station. $h_{sr}$ and $h_{rd}$ are denoted as the channel response between source station to the relay and the channel response between the relay to the destination station, respectively.

\[
y_{sr} = \sqrt{P_s} h_{sr} x + n_{sr} \quad (1)
\]

\[
y_{sd} = \sqrt{P_r} h_{rd} x + n_{sd} \quad (2)
\]

where $P_s$ is the signal power from the source station, $x$ is the transmitted coded signal from the source station, and $n_{sr}$ and $n_{sd}$ are AWGN with the variance $N_0$. The relay retransmits the coded signal to the destination station. At the second time, the received signal, from the relay station, at the destination station is

\[
y_{rd} = \sqrt{P_r} h_{rd} \tilde{x} + n_{rd} \quad (3)
\]

where $\tilde{x}$ is the decoded signal and $n_{rd}$ is AWGN with the variance $N_0$. The decoded signal $x$ should be the same as the one transmitted from the source station. Or, it will cause a catastrophic error. Hence, eq. (3) could be written as

\[
y_{rd} = \sqrt{P_r} h_{rd} x + n_{rd} \quad (4)
\]

In a normalized channel, the mutual information between the source station and the destination station could be evaluated by

\[
I_{sd} = \frac{1}{2} \log_2 \left( 1 + \frac{P_r}{N_0} |h_{rd}|^2 \right) \quad (5)
\]

Also, the mutual information between the relay and the destination station could be evaluated by

\[
I_{rd} = \frac{1}{2} \log_2 \left( 1 + \frac{P_r}{N_0} |h_{rd}|^2 \right) \quad (6)
\]
if the signal power transmitted at the relay is kept as $P_r$. Hence, for the single user, the minimum mutual information between the source station and the destination station could be

$$I_{DR} = \min(I_{s,d}, I_{r,d}) \quad (7)$$

Similarly, the scenario of the information transmitted to the eavesdropper could be held in this wireless environment as shown in Fig. 1. The leaked information to the eavesdropper under AWGN is

$$I_{se} = \frac{1}{2} \log_2 \left(1 + \frac{P_r}{N_0} h_{se}^2 \right) \quad (8)$$

### 3 Secrecy Rate Analysis

In the cryptanalysis, it assumes the eavesdropper could access the complete message from the source, i.e. the received message at the destination is the same as that received at eavesdropper. However, the wiretap channel model [12] depicts an entire communication system from the source to the destination. The message sent from the source through the main channel to the destination. On the other hand, the transmitted message is received by the eavesdropper via the wiretap channel, as shown in Fig. 3. For the physical-layer security, the wiretap channel model could be modified with coding scheme. In the cryptanalysis, the encrypted message is known by the eavesdropper. However, in the wiretap channel model, the error-free encrypted message known by the eavesdropper is a special case of the consideration because the physical-layer security is gained by the channel characteristics, such as noise.

![Fig. 3 Wiretap channel model for the communication](image)

According to Shannon theorem [13], a secure communication achieves not only an arbitrarily low error probability but also security against the attackers. Hence, in the wiretap channel model, the secrecy rate is defined based on the previous two purposes [14].

$$C_s = \max_{\rho(i)} I(X;Y | Z) = \max_{\rho(i)} \left( I(X;Y) - I(X;Z) \right)$$

$$\geq \max_{\rho(i)} I(X;Y) - \max_{\rho(i)} I(X;Z) \quad (9)$$

This equation provides a valuable point for secure communication, i.e. the positive secrecy capacity could have security against the eavesdropper. It might be held because of the quality of the main channel.

In eq. (9), secrecy rate $C_s$ should be positive for secure communication. It means that the channel capacity between the source to the destination must be larger than that between the source to the eavesdropper.

$$C_s = \max_{\rho(i)} I(X;Y) = \max_{\rho(i)} I_{DR} \quad (10)$$

and

$$C_e = \max_{\rho(i)} I(X;Z) = I_{se} \quad (11)$$

For simplification, in this work, the relay could connect at most one destination station only. Also, the eavesdropper is assumed as the relay at the end of the communication. AWGN channel is assumed in both the main channel and the wiretap channel,

$$I_{se} = I_{sr} = \frac{1}{2} \log_2 \left(1 + \frac{P_r}{N_0} h_{sr}^2 \right) \quad (12)$$

Under the above situation, considering each destination station received the signal from one relay station only, this work intends to find the pairs to match these $N$ destination stations and the corresponding $M$ relay stations. Hence, the total secrecy rate becomes

$$C_{\text{total}} = \max_{\rho(i)} \sum_{j=1}^{N} \rho_{ij} \cdot C_{s,ij} \quad (13)$$

under the conditions

$$\sum_{j=1}^{N} \rho_{ij} = 1, \forall j = 1,2,\ldots,N \quad (14)$$

and

$$\sum_{i=1}^{M} \rho_{ij} \leq 1, \forall i = 1,2,\ldots,M \quad (15)$$

$\rho_{ij}$ is defined as the connection between relay station $i$ to destination station $j$.

### 4 Numerical Results

With the exhaustive search method, the algorithm should begin to calculate eq. (13). First, for each relay station, calculate eq. (10) and eq. (12), respectively. Second, calculate $C_{s,ij}$ and recode in an $M \times N$ array such as...
Third, iterative calculate the \((i, j)\) combination for maximum value in the 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 combinations.

The computation is with high complicated computing to implement if there are large \(M\) and \(N\). Especially, the computing complexity is high for the burst traffic arriving. In order to reduce the computational complexity, a greedy algorithm could be applied. The benefit of greedy algorithm is that the solutions can be straightforward and easy to understand [15]. The applied greedy algorithm could be modified from the exhaustive search method.

Step 1, calculate \(C_d\) and \(C_e\) for all relay stations.
Step 2, create an \(M \times N\) array, calculate \(C_{s,ij}\) and recode in the array.
Step 3, according to the created array, assign the maximum value of \(C_{s,ij}\) to the pair of relay station \(i\) and destination station \(j\). Randomly, choose one of maximum value to assign if there more than one maximum value appeared. Record the pair \((i,j)\) to represent the \(i\)th relay station is assigned to sever the \(j\)th destination station. At the meantime, corresponding to the chosen cell, delete all other row cells in the array. It means the chosen relay station could not serve for other destination stations. Similarly, corresponding to the chosen cell, delete all other column cells in the array. It means the chosen destination is served by one relay station only. Then, a new reduced matrix is created.
Step 4, Repeat step 3 till finishing the assignment work.
Step 5, according to the pair assignment, calculate the total secrecy rate \(C_{s,\text{total}}\).

In the numerical experiment, the symbol \((N,M,E)\) shown in Fig. 4 represents that there are \(N\) source stations, \(M\) relays and \(E\) eavesdroppers. In this result, it is clear to illustrate in DF mode cooperative communication, the effects of relay assistance to forward the transmitted signal could not be significant. The communication between the source and the destination could still be connected with the legitimate stations.

5 Conclusions

The cooperative system is a tendency for the future wireless communications because of low cost. In this work, the solution for a secret DF mode cooperative communication has been proposed. According to Shannon theory, the physical layer could provide a secure transmission if there exists a positive secrecy rate. Hence, secrecy rate computation is a major concern in this work. The maximum secrecy rate is highly complicated. To develop an efficient algorithm to find a positive secrecy rate could be a research issue. This work adopts greedy algorithm for search the relay mapping. In the numerical results, the effects of eavesdropper is not serious in the cooperative system. 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.

Acknowledgment

This research was partially supported by the Ministry Of Science and Technology, Taiwan (ROC), under contract no.: MOST 107-2221-E-845 -002 -MY3 and MOST 107-2221-E-845-001 -MY3.

References


A.D. Wyner, “The wire-tap channel,” Bell system technical journal, Vol. 54(8), pp. 1355-1387, 1975

