Benefits of Compute-and-Forward in Throughput, Energy, and Security

Ren, Zhijie

DOI
10.4233/uuid:56ffa114-02a7-48f7-b6d2-4d663366f3ab

Publication date
2016

Document Version
Final published version

BENEFITS OF COMPUTE-AND-FORWARD IN THROUGHPUT, ENERGY, AND SECURITY

BENEFITS OF COMPUTE-AND-FORWARD IN THROUGHPUT, ENERGY, AND SECURITY

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. ir. K.C.A.M. Luyben,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op maandag 4 juli 2016 om 15:00 uur

door

Zhijie REN

Master of Science in Electrical Engineering,
Delft University of Technology,
geboren te Beijing, China.

Dit proefschrift is goedgekeurd door de

Promotor: Prof. dr. M. C. Gastpar
Copromotor: Dr. ir. J. H. Weber

Samenstelling promotiecommissie:

Rector Magnificus,	voorzitter
Prof. dr. M. C. Gastpar	Technische Universiteit Delft, promotor
Dr. ir. J. H. Weber	Technische Universiteit Delft, copromotor
Onafhankelijke leden:	
Prof. dr. ir. K. I. Aardal	Technische Universiteit Delft
Prof. dr. ir. J. van den Berg	Technische Universiteit Delft
Prof. dr. A. Yener	Pennsylvania State University
Dr. ir. F. M. J. Willems	Technische Universiteit Eindhoven
Prof. dr. ir. R. L. Lagendijk	Technische Universiteit Delft, reservelid
Overige leden:	
Dr. ir. J. Goseling,	Universiteit Twente

Dr. ir. J. Goseling heeft in belangrijke mate aan de totstandkoming van het proefschrift bijgedragen.

This work is supported by ERC Starting Grant 259530-ComCom.

Keywords: Network Coding, Compute-and-forward, Information Theoretical Security

Printed by: Ipskamp Printing

Front & Back: Inspired by the paintings of Piet Mondriaan and the spirit of the digital world. The binary codewords are the ASCII representations of the title and the name of the author.

ISBN 978-94-6186-674-5

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

CONTENTS

SUMMARY

Compute-and-forward (CF), also known as reliable physical layer network coding, is a novel technique which allows the terminals in wireless networks to decode linear combinations of the messages after receiving a superimposed signal of these messages in the physical layer. It has already been shown that CF can benefit wireless networks in many aspects. In particular, since it turns the superposition of multiple wireless signals, which is traditionally considered as a collision, into useful information, it significantly boosts the throughput and reduces the energy consumption by reducing the number of transmissions and receptions required in wireless networks. Moreover, in security aspect, CF can also be used to improve the rate of a secure transmission approach called cooperative jamming. In this thesis, we extensively study the benefits of CF in the aspects of throughput, energy consumption, and security in various unicast networks.

Firstly, we focus on the throughput benefit of CF for multiple unicasts, which is defined as the ratio of the achievable common rate of CF based schemes and the corresponding rate of the traditional schemes. It is proved that the throughput benefit is upper bounded by $3K$ in any network, in which K is the number of the unicast sessions. Also, example networks in which CF has a throughput benefit of at least $K/2$ are given. In particular, the throughput benefit of CF in line networks is extensively studied, where upper bounds and lower bounds of the throughput benefit are given for both centralized and decentralized scheduling cases.

Next, it is proved that the energy benefit of CF, defined similarly to the throughput benefit of CF, is upper bounded by $\min(\bar{d}, K, 12\sqrt{K})$, where $\bar{d}$ is the average distance of the sessions. Moreover, it is shown that the energy benefit in many specific networks is upper bounded by some constants. In line networks and hexagonal lattice networks, CF based transmission schemes are given which achieve the upper bounds in some cases.

Finally, the problem of the information theoretically secure transmission on the two-hop channel with an untrusted relay is considered. Two secure transmission schemes based on the novel scaled CF technique are proposed, which outperform all other existing secure transmission schemes and achieve the upper bound for many different power configurations. Moreover, it is shown that our schemes can also achieve a relatively high secrecy rate in the two-hop channel with an external eavesdropper.

SAMENVATTING

Compute-and-forward (CF), ook bekend onder de naam 'reliable physical layer network coding', is een nieuwe techniek die het mogelijk maakt dat toestellen in draadloze netwerken lineaire combinaties van de berichten decoderen na ontvangst van een gesuperponeerd signaal van deze berichten in de physische laag. Het is reeds aangetoond dat CF draadloze netwerken in vele opzichten voordeel kan bieden. Aangezien het de superpositie van meerdere draadloze signalen, hetgeen traditioneel als een conflict wordt beschouwd, omzet in nuttige informatie, geeft het de doorvoersnelheid een significante impuls en reduceert het het energiegebruik door het terugbrengen van het aantal verzendingen en ontvangsten in draadloze netwerken. Vanuit securiteitsoogpunt kan CF bovendien worden gebruikt om de snelheid te verbeteren van een veilige transmissiebenadering genaamd 'cooperative jamming'. In dit proefschrift bestuderen we uitgebreid de voordelen van CF met betrekking tot de aspecten doorvoersnelheid, energiegebruik en securiteit in diverse unicast-netwerken.

Ten eerste richten we ons op het snelheidsvoordeel van CF in het geval van meerdere unicast-sessies, gedefinieerd als de verhouding tussen de behaalbare gezamenlijke snelheid van CF-gebaseerde systemen en de vergelijkbare snelheid van traditionele systemen. Er wordt bewezen dat dit voordeel ten hoogste $3K$ is voor elk netwerk, waarbij K het aantal unicast-sessies is. Tevens worden voorbeelden gegeven van netwerken waarvoor CF een voordeel van tenminste $K/2$ heeft. In het bijzonder wordt het snelheidsvoordeel van CF voor lijnnetwerken uitgebreid bestudeerd, waarbij boven- en ondergrenzen worden gegeven voor zowel centraal als decentraal georganiseerde schema's.

Vervolgens wordt bewezen dat het energievoordeel van CF, op soortgelijke manier gedefinieerd als het snelheidsvoordeel, naar boven wordt begrensd door $\min(\bar{d}, K, 12\sqrt{K})$, waarbij $\bar{d}$ de gemiddelde afstand van de sessies is. Bovendien wordt aangetoond dat het energievoordeel voor veel specifieke netwerken naar boven wordt begrensd door een constante. Voor lijnnetwerken en hexagonale lattice-netwerken worden CF-gebaseerde systemen gegeven die in enkele gevallen de bovengrenzen behalen.

Tenslotte wordt het probleem beschouwd van informatietheoretisch veilige transmissie over een 2-hop-kanaal met een niet-vertrouwd tussenstation. Twee veilige transmissiesystemen gebaseerd op de nieuwe geschaalde CF-techniek worden voorgesteld, die beter presteren dan alle bestaande veilige transmissiesystemen en de bovengrenzen behalen voor vele verschillende vermogensconfiguraties. Bovendien wordt aangetoond dat onze veilige systemen een relatief hoge snelheid behalen voor een 2-hop-kanaal met een externe afluisteraar.

1

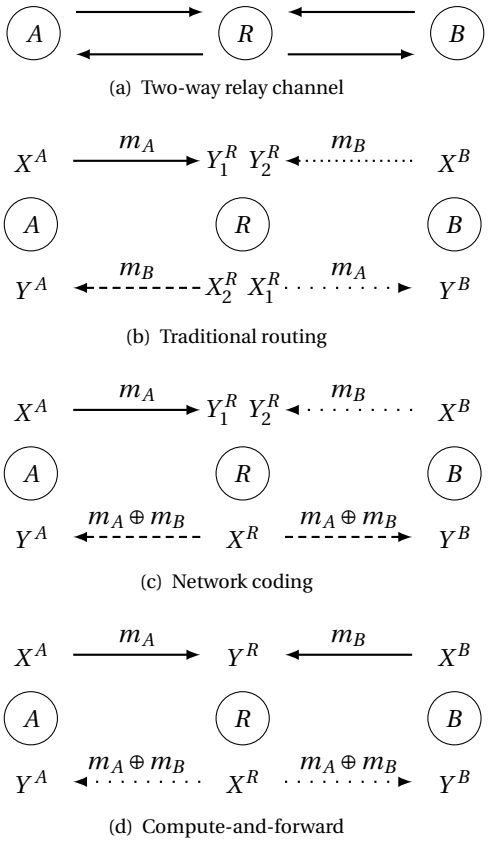
INTRODUCTION

At the beginning of this century, the concepts of network coding (NC) [1] opened up a new horizon in wireless communication. Traditionally, broadcast and superposition, the two characteristic features of wireless networks, are not well exploited. Broadcast messages sometimes are not useful for all receivers and the superposition of multiple messages is considered as a collision. NC, the technique that allows a node to combine and compute messages before transmission, exploits these two features of wireless networks and improves the performance in many aspects compared to the traditional methods. Firstly, broadcast can be useful for multiple destinations if a linear function of multiple messages is transmitted. More recently, an advanced NC technique called compute-and-forward (CF) [29] also exploits superposition. It allows wireless terminals to directly and reliably decode linear functions of multiple messages from different sources when receiving their physically superimposed signals.

In this thesis, we study the improvement brought by CF technique in three aspects: throughput, energy, and security.

1.1. TWO-WAY RELAY CHANNEL

Two-way relay channel (TWRC), as shown in Fig. 1.1(a), is a classical wireless channel model in which nodes A, B, and R are wireless terminals and A and B want to exchange information. Node R is used to relay the messages since A and B cannot receive the transmissions from each other directly. Albeit the simpleness, the TWRC reflects many practical wireless networks, e.g., cellular networks with cell phones A and B and base station R. Here, we use this channel to give conceptual ideas of why and how these three aspects can benefit from applying CF. We assume that the channel has additive white Gaussian noise (AWGN) and the amount of time needed to reliably transmit a length-N binary sequence is 1 time slot. Also, assume that all three nodes apply half-duplex, which means that they cannot transmit and receive at the same time.



(a) Two-way relay channel

(b) Traditional routing

(c) Network coding

(d) Compute-and-forward

Figure 1.1: Various transmission schemes on the two-way relay channel. In figure (b)- (d), Different types of lines are used to represent different time slots.

1.1.1. THROUGHPUT BENEFIT

Firstly, consider a traditional point-to-point based routing scheme (Fig. 1.1(b)). In the first time slot, node A transmits the message to R. Node R forwards this message to node B in the second time slot. Then, symmetrically, the message from node B is transmitted to node A in the third and fourth time slots. The rate for the transmissions of both directions is $1/4$ message per time slot. This is the best rate that can be achieved by the traditional point-to-point based approach because the relay R cannot transmit and receive at the same time due to half-duplex, cannot send a message to multiple receivers simultaneously, and cannot receive two messages simultaneously since two wireless signals will collide.

This rate can be improved to $1/3$ by using NC with broadcast (Fig. 1.1(c)). In the first two time slots, nodes A and B transmit to node R, respectively. Then node R computes $X_R = m_A \oplus m_B$ and broadcasts it in the third time slot simultaneously to A and B. Both A and B can decode their desired messages since they know their own messages, e.g., nodes A can decode m_B by computing $m_B = X_R \oplus m_A = (m_A \oplus m_B) \oplus m_A$.

CF, sometimes called reliable physical layer network coding (PLNC), is a technique which also exploits the superposition of the signals of multiple messages in the physical layer. More specifically, if nodes A and B transmit their messages simultaneously, node R can reliably decode $m_A \oplus m_B$ instead of considering the reception as a collision (details will be specified in Chapter 2). Then, in the second time slot, the relay R broadcasts $m_A \oplus m_B$ and nodes A and B can decode their desired messages in the same fashion as NC. This scheme is shown in Fig. 1.1(d). In this case, the transmit rate of both directions is 1/2, which is two times as much as the rate of traditional routing.

1.1.2. ENERGY BENEFIT

The same TWRC and the three schemes are compared in a different aspect: the energy consumption. Nowadays, many of the wireless terminals are battery-driven, energy-sensitive equipments, such as cell phones, wireless sensors, laptops, tablets, etc. Here, assume that transmitting a length-N binary sequence consumes energy e_t (for encoding, transmitting, supporting circuits, etc.) and successfully receiving a length-N binary sequence consumes energy e_r (for decoding, supporting circuits, etc.). In our model, all other energy consumption is neglected. Thus, it is clear that the energy consumption on the TWRC of Fig. 1.1(a) for two messages to be delivered to their destinations is $4(e_t+e_r)$, $3e_t+4e_r$, and $3(e_t+e_r)$ for traditional routing, NC, and CF, respectively. Hence by using CF, only 3/4 of the energy is consumed compared to the traditional routing scheme due to the feature that CF can reduce the number of transmissions and receptions in the network.

1.1.3. SECURITY BENEFIT

The third, we still consider the TWRC in Fig. 1.1(a) and assume that only node A has a message m_A to send to node B. In this problem, the relay is assumed to be honest-but-curious, i.e., it eavesdrops the messages transmitted through it but makes no change on the messages. This is another practical scenario since all public Wi-Fi providers could be potential eavesdroppers. Hence, it is desirable to design transmission schemes which send messages via node R while leaking no information to it. The rate of such a reliable and secure transmission is called the *secrecy rate*.

Firstly, a straightforward relaying scheme is considered in which the relay simply receives from A and forwards it to B. Due to the information processing inequality [2], any information retrieved at B can also be retrieved by R as well. Hence, no information can be securely transmitted to node B in this way and the secrecy rate is 0. Then, the cooperative jamming scheme as illustrated in Fig. 1.2 is introduced [14]. In this scheme, node B simultaneously transmits a jamming signal, namely X_B, to confuse R when A is transmitting. As a result, R will not be able to retrieve any information from the reception Y^R. However, when R transmits what it has received to node B, B is able to recover X_A since it knows X_B and is able to subtract it from X_R.

However, the real scenario is not as simple as described above due to the presence of noise. In this scheme, upon the reception of $Y^R = X_A + X_B + Z$ where Z is the noise, since the relay cannot decode X_A or X_B due to the security concern, it is not able to remove the noise from the useful information either. Hence, this noise accumulates to X^R, i.e., its transmission to node B, and causes a severe degradation in the achieved

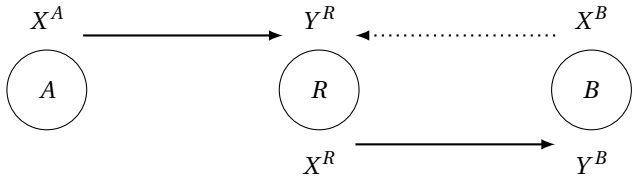


Figure 1.2: The cooperative jamming scheme on a two-hop channel with an untrusted relay

secrecy rate. A CF based scheme can solve this problem by letting the relay decode $X_A + X_B$, which removes the noise with no information leaked during the process. As a result, CF improves the secrecy rate and benefit the network in the security aspect.

1.2. BACKGROUND AND CHALLENGES

1.2.1. THROUGHPUT BENEFIT

BACKGROUND

The fundamental paper [1] introduced the concept of NC and revealed the advantages of NC in the throughput aspect for multicast networks. Numerous studies have been done on the subject of the improvement of NC over traditional routing without the context of wireless network [17, 19, 24, 25]. For wireless networks, the throughput benefit of NC was first introduced in [43], in which the TWRC introduced in the previous section was considered. For broadcast and multicast scenarios, it has been shown in several studies that NC is advantageous over traditional routing [4, 28]. For multiple unicast scenarios, theoretical upper bounds haven been derived for the improvement in general networks [22, 26] and a practical scheme [21] has been proposed which improves the throughput in many real-life wireless networks.

PLNC [20, 48] is a technique which exploits the features of wireless networks and uses the superimposed physical layer signals to decode linear combinations of multiple transmitted messages. It has been shown in [20, 32, 48] that PLNC can improve the throughput on the TWRC. However, these schemes suffer heavily from the noise since no error correcting mechanism is applied. Hence, the improvement of these schemes is quite limited for noisy cases and the improvement of a factor of 2 as indicated in the previous section is not feasible in general. The CF technique (also known as reliable PLNC) [29], on the other hand, is an advanced PLNC scheme which uses nested lattice codes [7] to enable the relay nodes to reliably decode the linear combinations in a noisy environment. As a result, an improvement that is very close to a factor of 2 is achieved on the TWRC in the high SNR regime.

Moreover, since CF allows the relay to remove the noise, for transmissions involving multiple hops and relays, the achievable rate will not be degraded by the noise accumulation along the path. Hence, CF also improves the throughput compared to traditional routing and NC in line networks, multi-way relay networks, and lattice networks [10, 41, 48]. Moreover, in [10] it is shown that the throughput in line and lattice networks can be significantly improved by CF in terms of *transport capacity*. In terms of rate, many studies focus on the fundamental limits of the throughput benefit using PLNC in gen-

eral wireless networks [27, 49]. The results show that PLNC provides improvement of constant factors in 1-D and 2-D networks.

CHALLENGES

As CF been proposed, one of the natural questions in the perspective of throughput is: "how much can it benefit the throughput of wireless networks?" A very important context for this question is multiple unicast networks, which are amongst the most practical and complicated scenarios. For all current results ranging from the TWRC to 2-D random networks, the throughput benefit of PLNC, which is the ratio between the maximum achievable common rate of CF and the corresponding rate of traditional routing, is at most a constant. It raises the following questions: "does there exist a type of networks in which the benefit is more than a constant, e.g., the benefit increases with the number of sessions? If yes, what are the coding schemes? What is the limit for the throughput benefit of CF?" Here, some challenges for this problem are listed as follows.

- What is the fundamental upper bound for the throughput benefit of PLNC over traditional routing and NC in general networks with multiple unicast sessions?
- Can a matching lower bound be found by proposing a scheme which achieves this upper bound? If not, does there exist a network in which such throughput benefit is feasible?
- If the two bounds cannot be matched in general networks, is it possible to match them in some specific networks, e.g., line networks or lattice networks?

1.2.2. ENERGY BENEFIT

BACKGROUND

NC can also benefit energy consumption since it has the potential of reducing the number of transmissions in wireless network. The energy benefit of NC has been studied in several previous studies [8, 12, 22, 23]. The work of [8] considered the broadcast scenario, in which a $\log N$ improvement was achieved, where N is the number of nodes. In [22], both multicast and multiple unicast scenarios have been considered and upper bounds of the energy benefit have been derived for both scenarios. The work of [12] and [23] focused on lower bounds of the energy benefit in specific networks, in particular, the hexagonal (triangular) networks. An energy benefit of 2.4 was achieved in [23] and was later beaten by the benefit of 3 in [12].

Note that all the above-mentioned studies consider the energy consumption as the transmit energy. Other energy consumed for the transmission is neglected, which might not be the best assumption when other energy consumption, e.g., receive energy, is not negligible. For example, the scheme in [12] reduces the number of transmissions at the cost of increasing the number of receptions in the network, which might not be beneficial in the energy consumption if the receive energy is too large.

CHALLENGES

Since it has been shown in the TWRC case that CF has the potential of decreasing the number of not only the transmissions, but also the receptions, it seems that CF can bring

a higher energy benefit than plain NC, especially when the receive power is not negligible. Almost no literature has considered the energy benefit of PLNC except for the very simple cases such as TWRC. Similar to the throughput benefit, some of the challenges for the energy benefit are listed as the following.

- What is the fundamental upper bound for the energy benefit of PLNC over traditional routing and NC in general networks with multiple unicast sessions?
- Can a matching lower bound be found by proposing a scheme which achieves this upper bound? If not, does there exist a network in which such energy benefit is feasible?
- If the two bounds cannot be matched in general networks, is it possible to match them in specific networks?
- How is the energy benefit related to the throughput benefit?

1.2.3. SECURITY BENEFIT

BACKGROUND

Information theoretic security was first introduced by Shannon in one of the fundamental papers in cryptography [36]. Shannon used it to describe the level of secrecy that the eavesdropper cannot retrieve any information about the plain text even if it has access to the cypher text and unbounded computational capability. To achieve this level of secrecy, Shannon proposed the scheme of the "one-time pad", which requires a randomly generated key containing no less entropy than the plain text and should be only used once and kept secret afterward, i.e., the "one-time pad". Obviously, the cost of such encryption is too high to be applied for all secret messages. As a result, the researchers start to seek other encrypting techniques, e.g., the encryption based on computationally hard problems.

The concept of information theoretic security receives a lot of attentions in recent years. One of the reasons is that most of the current encryption schemes are not secure if computers with much higher computational capability, e.g., quantum computers, were born. Another important reason is that, in wireless networks, the "one-time pad" scheme is less costly since it is possible to use the transmissions of other users as the "one-time pad". One of the schemes which uses this idea is the cooperative jamming approach proposed in [14]. This scheme lets a node other than the source, e.g., the destination, generate a "one-time pad" and transmit it to the eavesdropper while the source is transmitting the plain text. The "one-time pad" superimposes with the plain text in the physical layer and prevents the information about the plain text to be obtained by the eavesdropper. Once the cypher text, i.e., the superimposed signal, is received by the destination, it can be decoded if the destination also knows the "one-time pad", i.e., the jamming signal.

The cooperative jamming approach on the TWRC suffers from the noise accumulation, which can be solved by CF (as shown in Section 1.1). Many different CF based approaches have been proposed on this channel which achieve different levels of secrecy (will be specified in Chapter 5) [16, 33, 40]. In [15], it has been proved that the same rate

as [16] can also be achieved for line networks. Some other approaches also applied CF based approaches on the TWRC with asymmetric channel gains [33, 39]. However, the results are suboptimal compared to the upper bound given in [14].

CHALLENGES

In [14], upper bounds of the secrecy rate on the TWRC with both symmetric and asymmetric channel gains are derived. However, no matching lower bound has been given except for some special channel configurations, e.g., symmetric channel gain or infinite relay and jamming power cases. However, in [50], a more advanced CF technique, we call it scaled CF (SCF), is proposed, which seems to be a promising technique for this problem. Hence, here are some challenges.

- Can the upper bound in [14] be achieved on the asymmetric TWRC with SCF?
- If so, can this scheme be used in other secure transmission problems, e.g., the two-hop channel with an external jammer or the two-hop channel with an external eavesdropper?

1.3. MAIN CONTRIBUTIONS AND STRUCTURE OF THE THESIS

1.3.1. THROUGHPUT BENEFIT (CHAPTER 3)

The throughput of wireless networks with multiple unicast sessions is considered under several transmission modes in which the broadcast and superposition features are allowed and/or disallowed. Upper bounds and lower bounds of the throughput benefit of CF over traditional routing and NC are derived by studying the theoretical limits of the throughput in various modes. For general networks, it is proved that the throughput benefit cannot be higher than $3K$ for any network setting, where K is the number of unicast sessions. Also, it is shown that in some networks, the throughput benefit is at least $K/2$. In line networks, the throughput benefit is 2 or smaller than 2 depending on the session placement if all sessions are bidirectional. If the problem is generalized to arbitrary unicast sessions, the throughput benefit is 2 when the sessions are uniformly distributed at random and the number of sessions goes to infinity. Furthermore, the throughput benefit of CF in line networks with random access mechanism is also studied. It is proved that the benefit is $\frac{2}{1-p}$ where p is the probability for each node to transmit.

1.3.2. ENERGY BENEFIT (CHAPTER 4)

Similar to the method used in Chapter 3, the benefit of CF over traditional routing in terms of the energy consumption is studied by deriving the upper and lower bounds of the energy consumption in various transmission modes. The energy benefit of CF is defined as the ratio between the minimum energy consumption with CF and the corresponding consumption of traditional routing. It is proved that in general networks, the energy benefit of CF is upper bounded by $\min(\bar{d}, K, 12\sqrt{K})$, where $\bar{d}$ is the average distance of the sessions. In some specific networks, it is proved that the energy benefit cannot be higher than constant factors. Moreover, in hexagonal lattice networks, it is shown that for a specific session placement, the energy benefit is between 2 and 3 depending on the ratio of the transmit and receive energy.

1.3.3. SECURITY BENEFIT (CHAPTER 5)

The problem of secure transmission on a two-hop channel with an untrusted relay is considered. Two secure transmission schemes based on cooperative jamming and SCF are proposed, which achieve the upper bound on this channel for many different power and channel configurations. More precisely, our schemes outperform all other secure transmission schemes and achieve the upper bound in the following scenarios:

- If the power of the source, the relay, and the destination are linearly related and go to infinity.
- If the relay has a limited power and the power of the source and the destination is large.

In particular, when the source and the destination have symmetric power and channels, a secrecy rate of $\max(0, \frac{1}{2}\log(\frac{1}{2}+\mathrm{SNR})-\frac{1}{2})$ is achieved, which is the best achievable secrecy rate so far on this problem and is proved to be upper bound achieving when the SNR goes to infinity. It is also proved that these schemes can be used on other related channels, i.e., the two-hop channel with an external jammer and the two-hop channel with an external eavesdropper, for secure transmission with relatively high secrecy rate.

1.3.4. STRUCTURE OF THIS THESIS

This thesis is structured as follows: In Chapter II, we briefly introduce CF. In Chapter III, IV, and V, we discuss the benefits of CF in throughput, energy consumption, and security, respectively. At last, we conclude this thesis and give our recommendations in Chapter VI.

2

COMPUTE-AND-FORWARD: A BRIEF INTRODUCTION

Compute-and-forward (CF) [29] is a lattice code [7] based technique which allows a wireless receiver to decode linear functions of multiple messages transmitted by different sources upon receiving the superimposed signal of these messages in the physical layer. For example, considering a 2-user Multiple Access Channel (MAC) with additive white Gaussian noise (AWGN), CF encodes the source messages W^A and W^B into nested lattice codewords X^A and X^B. Then, it allows the destination to decode W^A+W^B after receiving their superimposed signals in the physical layer, i.e., X^A+X^B+Z, where Z is the noise. In this chapter, we introduce nested lattice codes, CF, and the application of CF in multiple channels w.r.t. our problems.

2.1. NESTED LATTICE CODE

In this section, we briefly introduce the nested lattice codes and their properties as described in [7]. Firstly, we define *Lattice* and *Nested Lattice*.

Definition 2.1.1 (Lattice)**.** An N-dimensional lattice Λ is a set of points in $\mathbb{R}^N$ such that $\forall x_1, x_2 \in \Lambda, x_1 + x_2 \in \Lambda$ and $\forall x \in \Lambda, -x \in \Lambda$.

Definition 2.1.2 (Nested lattice)**.** A lattice Λ is said to be nested in Λ_1 if $\Lambda \subseteq \Lambda_1$. In this case, we call Λ_1 the *fine lattice* and Λ the *coarse lattice*.

Then, we introduce some basic properties and functions in lattices.

Definition 2.1.3 (Quantization)**.** A lattice quantizer $Q_\Lambda : \mathbb{R}^N \to \Lambda$ maps a point p to the nearest lattice point, i.e.,

$$Q_\Lambda(p) = \arg\min_{\lambda \in \Lambda} ||p - \lambda||. \tag{2.1}$$

Definition 2.1.4 (Fundamental Voronoi region)**.** The fundamental Voronoi region of a lattice Λ, denoted by $\mathcal{V}$, is a set of point in $\mathbb{R}^N$ that are closest to the zero vector, i.e., $\mathcal{V} = \{p \in \mathbb{R}^N | Q_\Lambda(p) = 0\}$. We use $\mathrm{Vol}(\mathcal{V})$ to denote the volume of $\mathcal{V}$.

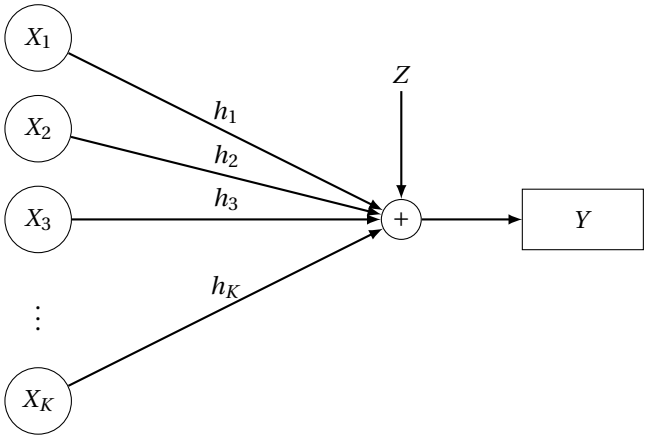


Figure 2.1: K-user MAC with AWGN

Definition 2.1.5 (Modulo)**.** We define the modulo function by

$$x \pmod{\Lambda} = x - Q_\Lambda(x). \tag{2.2}$$

With the definitions given above, we introduce the nested lattice codes.

Definition 2.1.6 (Nested lattice code)**.** A nested lattice code $\mathscr{L}_1$ is the set of all points of a fine lattice Λ_1 that are within the fundamental Voronoi region $\mathscr{V}$ of a coarse lattice Λ, i.e.,

$$\mathscr{L} = \Lambda_1 \cap \mathscr{V} = \{x \in \Lambda_1 | Q_\Lambda(x) = 0\}. \tag{2.3}$$

The rate of this lattice code is

$$R = \frac{1}{N} \log \frac{\mathrm{Vol}(\mathscr{V})}{\mathrm{Vol}(\mathscr{V}_1)}. \tag{2.4}$$

For CF, the nested lattice codes should be good for both mapping and AWGN, which suggests that the coarse lattice should be good at both shaping and quantizing, and the fine lattice should be good for AWGN. More details about the criterion for the goodness of lattices can be found in [7]. Also, it is proved in [7] and [29] that it is able to construct a nested lattice code with lattices $\Lambda \subseteq \Lambda_1$ that are good for both mapping and AWGN.

2.2. ENCODING

Let us consider a MAC with K users, AWGN, and real-value channel gains (Figure 2.1). We assume that the source messages $W_i, i \in \{1,2,\ldots,K\}$ are drawn independently and uniformly from alphabet $\{1,2,\ldots,2^{NR_i}\}, N \in \mathbb{Z}$. We call R_i the message rate of user i.

We construct a nested lattice codebook $\mathscr{L}$ with nested lattices $\Lambda \subseteq \Lambda_1$ as discussed in the previous section. Here, we define the lattice encoder $\mathscr{E}_\mathrm{L} : W_i \to \mathscr{L}$ which encodes the messages W_i to T_i which are real-value N-dimensional vectors in lattice codebook $\mathscr{L}$. Further, we introduce the *dither* denoted by D_i which is uniformly chosen from $\mathscr{V}$. The dithers are introduced to make the distribution of X_i uniform. All dithers are revealed

to the destination. The channel input of source i is then the sum of lattice codeword T_i and dither D_i, denoted by

$$X_i = (T_i + D_i) \pmod{\Lambda}. \tag{2.5}$$

We assume that the power constraint of all users are P, i.e., the channel inputs satisfy

$$||X_i||^2 \leq NP. \tag{2.6}$$

2.3. DECODING OF LINEAR EQUATIONS

The reception at the destination is

$$Y = \sum_{i=1}^{K} h_i X_i + Z, \tag{2.7}$$

where h_i is the channel coefficient and Z is an N-dimensional white Gaussian noise with unit variance in each dimension. Now the destination can decode the linear function

$$V = \sum_{i=1}^{K} a_i T_i \tag{2.8}$$

by first computing

$$\begin{aligned} & \alpha Y - \sum_{i}^{K} a_i D_i \\ = & \sum_{i=1}^{K} (\alpha h_i X_i - a_i D_i) + \alpha Z \\ = & \sum_{i=1}^{K} (a_i (X_i - D_i) + (\alpha h_i - a_i) X_i) + \alpha Z \\ = & \sum_{i=1}^{K} a_i T_i + \sum_{i=1}^{K} (\alpha h_i - a_i) X_i + \alpha Z \\ = & V + Z_0(\alpha). \end{aligned} \tag{2.9}$$

Here, α is a arbitrarily picked real number and we define $Z_0(\alpha) = \sum_{i=1}^{K} (\alpha h_i - a_i) X_i + \alpha Z$ as the effective noise with power $\alpha^2 + P||\alpha h_i - a_i||^2$. Note that since X_i is uniformly distributed over $\mathcal{V}$ and independent of V thanks to the dithers, $Z_0(\alpha)$ is also independent of V.

Then the destination can decode V by mapping the result in (2.9) to the nearest lattice point in the fine lattice Λ_1. Since we have chosen our nested lattice codebook to be good for mapping and AWGN, this decoding is successful [1] if we have

$$R_i < \frac{1}{2} \log \left(\frac{P}{\alpha^2 + P||\alpha h_i - a_i||^2} \right). \tag{2.10}$$

By maximizing (2.10) over all α, we have the CF rate given in the following theorem.

[1] By successful, we mean that the probability of the decoding error goes to 0 when $N \to \infty$.

Theorem 2.3.1 (Computation rates). *For a K-uesr Gaussian MAC, the receiver is able to reliably decode a linear function* $\sum_{i=1}^{K} a_i T_i$ *if for all* i*, the message rates satisfy*

$$R_i \leq R_{\text{CF}} = \max\left(0, \frac{1}{2}\log\left(||\mathbf{a}||^2 - \frac{P(\mathbf{h}^T\mathbf{a})^2}{1+P||\mathbf{h}||^2}\right)^{-1}\right), \tag{2.11}$$

where $\mathbf{a} = (a_1, a_2, \ldots, a_K)$ *and* $\mathbf{h} = (h_1, h_2, \ldots, h_K)$. *[29, Theorem 5]*

Here, we consider some special channel configurations.

2.3.1. EQUAL CHANNEL GAINS

If all channel gains are h and the destination wants to decode $t_1 + t_2 + \ldots + t_K$, it can be easily calculated from (2.15) that the CF rate is simply

$$R_{\text{CF}} = \frac{1}{2}\log(\frac{1}{K} + h^2 P), \tag{2.12}$$

which is very close to the channel capacity for single user Gaussian channel, i.e.,

$$C = \frac{1}{2}\log(1 + h^2 P) \tag{2.13}$$

in the high Signal-to-Noise-Ratio (SNR) scenario.

2.3.2. $\mathbb{F}_q$ SOURCES

We can also consider the sources are drawn from finite field $\mathbb{F}_q$ in which q is a prime power and the destination wants to decode a linear function of the sources message W_i which is also in $\mathbb{F}_q$. This is not straightforwardly feasible for any lattice codebook. However, in [29, Lemma 6] it is shown that there exists such lattice codebooks which keep the linearity while encoding the message. Hence, the destination directly has $\sum_{i=1}^{K} a_i W_i$ when it retrieves $V \pmod{\Lambda}$.

2.3.3. MULTIPLE DESTINATIONS

CF can be extended to multiple destinations with different channel configurations by using a chain of nested lattice codes to construct the codebook. It is proved in [29] that each destination can decode a different linear function if the message rates satisfy the CF rates in (2.15) for this destination. More precisely, if there are M destinations with receptions

$$Y_m = \sum_{i=1}^{K} h_{i,m} X_i + Z_m, m \in \{1, 2, \ldots, M\}, \tag{2.14}$$

we have the following theorem.

Theorem 2.3.2 (Computation rates for multiple destinations). *Each destination* m *is able to reliably decode linear functions* $\sum_{i=1}^{K} a_{i,m} T_i$ *if for all* i*, the message rates satisfy*

$$R_i \leq R_{\text{CF}} = \max\left(0, \frac{1}{2}\log\left(||\mathbf{a}||^2 - \frac{P(\mathbf{h}^T\mathbf{a})^2}{1+P||\mathbf{h}||^2}\right)^{-1}\right), \tag{2.15}$$

where $\mathbf{a} = (a_{1,m}, a_{2,m}, \ldots, a_{K,m})$ *and* $\mathbf{h} = (h_{1,m}, h_{2,m}, \ldots, h_{K,m})$. *[29, Theorem 5]*

2.3.4. SCALED COMPUTE-AND-FORWARD

Scaled CF (SCF) as proposed in [50] is a generalized version of the traditional CF. It allows the senders to scale their lattice codebooks according to their prior knowledge of the channel states to achieve higher computation rates. Here we briefly introduce this technique for a 2-user MAC case.

We consider the two users having power P_A and P_B. Firstly, we construct a lattice Λ. Then we construct two coarse lattices $\Lambda^A, \Lambda^B \subseteq \Lambda$ with second moment

$$\frac{1}{N\text{Vol}(\mathcal{V}^i)} \int_{\mathcal{V}^i} ||X||^2 dX = \beta_i^2 P_i, i \in \{A, B\},$$

where $\mathcal{V}^i$ is the fundamental Voronoi region of Λ^i and $\beta_i \in \mathbb{R}^+$ is called the scaling coefficient. Here we assume that Λ, Λ^A and Λ^B are simultaneously good for quantizing, shaping, and AWGN as discussed in [7].

For user $i \in \{A, B\}$, we construct the codebook $\mathcal{L}^i = \Lambda \cap \mathcal{V}^i$, where $\mathcal{V}^i$ is the fundamental Voronoi region of Λ^i. User i encodes its message into codeword T^i using the codebook $\mathcal{L}^i$, and the channel input is formed as $X^i = [T^i/\beta_i + D^i] \pmod{\Lambda^i/\beta_i}$, where the dither D^i is chosen uniformly at random from $\mathcal{V}_C^i/\beta_i$. Clearly, X^i is also uniform in $\mathcal{V}^i/\beta_i$ and thus it has average power P_i.

The receiver uses the fine lattice Λ for decoding the linear sum $a_1 T^A + a_2 T^B, a_1, a_2 \in \mathbb{Z}$. It is proved in [50] that the destination is able to reliably decode this linear sum as long as the transmit rates are smaller than the computation rates $R_{\text{CF}}^i(\mathbf{a}, \boldsymbol{\beta})$ defined as

$$R_{\text{CF}}^i(\mathbf{a}, \boldsymbol{\beta}) = \frac{1}{2} \log\left(\frac{\beta_i^2 P_i}{\mathcal{N}(\mathbf{a}, \boldsymbol{\beta})}\right), \tag{2.16}$$

where

$$\mathcal{N}(\mathbf{a}, \boldsymbol{\beta}) = \frac{P_A P_B (a_1\beta_A - a_2\beta_B)^2 + (a_1\beta_A)^2 P_A + (a_2\beta_B)^2 P_B}{P_A + P_B + 1}, \tag{2.17}$$

$\mathbf{a} = (a_1, a_2)$, and $\boldsymbol{\beta} = (\beta_A, \beta_B)$.

Remark 2.3.1. For any $\mathbf{a}$ and $\boldsymbol{\beta}$ it can be derived from (2.16) that the computation rates satisfy

$$R_{\text{CF}}^A(\mathbf{a}, \boldsymbol{\beta}) \leq C(P_A), R_{\text{CF}}^B(\mathbf{a}, \boldsymbol{\beta}) \leq C(P_B). \tag{2.18}$$

3

THROUGHPUT BENEFIT

Compute-and-forward (CF) improves the throughput in wireless network by better exploiting the two basic features in wireless communication: broadcast and superposition. In this chapter, we focus on the throughput benefit of CF over other transmission schemes, e.g., traditional routing and network coding (NC), for multiple unicasts. This is a tough problem since it is in general hard to find the theoretical limits of the throughput for multiple unicasts. Hence, a novel network model with four transmission modes inspired by [10] is proposed, in which the network structure is highly abstracted and the features of broadcast and superposition are emphasized. With this model, the theoretical limit for the throughput of each scheme and the throughput benefit of CF over other schemes in various types of networks are found. For general networks, an upper bound and an example in which the improvement is at the same order of the upper bound are given. For line networks, upper and lower bounds considering both the centralized and decentralized scheduling schemes are derived.

3.1. INTRODUCTION

Broadcast and superposition are two characteristic physical layer features of wireless networks. In traditional physical and multiple-access-control layer schemes, broadcast

The material in the following parts of this chapter has appeared in

- Section 3.3:
  Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Maximum throughput gain of compute-and-forward for multiple unicast," *IEEE Comm. Letters*, vol. 18, pp. 1111-14, July, 2014.
- Section 3.4:
  Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Compute-and-forward: multiple bi-directional sessions on the line network," *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Istanbul, Turkey, July, 2013.
- Section 3.6:
  Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Compute-and-forward on a line network with random access," *Proc. of the Thirty-fourth WIC Symp. on Inf. Theory in Benelux*, Leuven, Belgium, May, 2013.

is not well exploited and superposition is seen as an impediment: interfering signals cause an unrecoverable collision. Several techniques have recently been proposed to alleviate these issues. It is shown in [43] that NC is able to exploit the broadcast feature and improves the throughput of the network. In many literature, e.g., [22, 26, 27], several upper bounds of the throughput benefit of NC for multiple unicasts are derived.

CF, also known as reliable physical layer network coding (PLNC), provides a way to exploit both broadcast and superposition[29]. Some work considered the throughput for uncoded versions of PLNC, e.g. [21, 48]. However, their approaches suffer from the noise accumulation along the stages of the network. On the contrary, CF allows nodes to efficiently and reliably recover a function of the messages from multiple senders. Its potential of improving the throughput compared to traditional approaches has already been shown in [10, 29, 46, 48]. In these studies, multiple unicast sessions are considered as pairs of sources and destinations, and the information is forwarded from the sources to the destinations with the help of some nodes in the network functioning as relays. With CF, instead of decoding the transmitted messages for each individual session, the relays decode linear combinations of multiple messages from different sessions upon receiving the superposition of their physical layer signals. The throughput of the network benefits from this alternation under several scenarios.

In the example of the two-way relay channel (TWRC), CF already achieves a doubled throughput in comparison to traditional routing schemes under the scenario of two unicast sessions transmitting in opposite directions [21]. On the multi-way relay channel, where again, CF doubles the throughput [41]. Going beyond rate, [10] studies the transport capacity (the maximum of the sum of the product of source-destination distance and rate over all possible placements of unicast sessions and transmission strategies). The throughput benefit of CF over traditional routing is then between 2.5 and 6 for nodes located on a two-dimensional hexagonal lattice. Some other related papers [26, 27, 45] show that the throughput benefit of PLNC depends on the distribution of the nodes and the allocation of the sessions in 2-D networks. Some of the important challenges in this area are:

- give a fundamental upper bound on the throughput benefit of CF in general networks;
- search for examples with the proof of CF giving high throughput benefit over traditional routing approaches;
- for some specific networks, derive upper bounds for the throughput benefit of CF and propose transmission schemes which achieve these bounds.

To study these problems, inspired by [10], the underlying physical layer and multiple-access-control layer schemes are abstracted into 4 transmission modes, in which the usage of broadcast and/or superposition are allowed or disallowed. Then, upper bounds and lower bounds for the throughput benefit of CF over traditional routing and NC are derived by comparing the theoretical throughput limits in various transmission modes. It is shown that in many different types of networks, CF is beneficial in throughput over the other transmission schemes. A special type of networks is given in which the throughput benefit of CF over traditional routing can be as high as $K/2$. Also, it is proved that the

benefit of CF over traditional routing is upper bounded by $3K$ for any network with multiple unicast sessions.

For some specific networks, e.g., line networks, tight bounds are achieved. In particular, in large line networks with a large number of sessions distributed uniformly at random, it is proved that the throughput benefit of CF over traditional routing and NC are 2 and 1.5. Further, it is shown that the improvement can be even higher if random access is used as the multiple-access-control scheme for the nodes in line networks.

This chapter is organized as follows. In Section 3.2, we set up our network model, give the definitions of the four transmission modes, the rate, and the improvement factors. In Section 3.3, we consider the throughput benefit of CF in general networks. In the following sections, we consider the throughput benefit of CF in line networks. In Section 3.4, we consider the throughput benefit of CF in line networks, in which the unicast sessions are all bidirectional. In Section 3.5, we drop the bidirectional constraint and consider arbitrary session placements. In Section 3.6 we consider line networks in a different context: the random access mechanism is used. In Section 3.7, we conclude our results in this chapter.

3.2. MODEL SET-UP AND NOTATIONS

In this section, a network model represented by a connected graph is proposed. The vertices represent wireless nodes and the edges represent the wireless connectivity between two nodes. We focus on two features of wireless networks, the broadcast nature of wireless signal at the transmitters and the superposition nature of the wireless signal at the receivers. Based on NC which can be used to exploit broadcast and CF which can be used to exploit superposition, four transmission modes are proposed. In these modes, either of these two features are allowed and/or disallowed. The modes are introduced as in Table 3.1.

	Broadcast	Superposition	Representing transmission schemes
PP (Point-to-Point)	No	No	Traditional transmission schemes
B(roadcast)P	Yes	No	NC based transmission schemes
PM(ulti-access)	No	Yes	None
BM	Yes	Yes	CF based transmission schemes

Table 3.1: Four transmission modes and their representing transmission schemes.

The formal definitions of these transmission modes will be given later in this section. Firstly, we introduce our network model.

3.2.1. NETWORK MODEL

The network is denoted by $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$. Here, $\mathcal{V}$ is a vertex set, $\mathcal{E}$ is an edge set, and $(\mathcal{V},\mathcal{E})$ represents a connected, directed, and unweighted graph. Here, the elements in $\mathcal{V}$ are called *nodes*, and node $v \in \mathcal{V}$ is a neighbor of node $u \in \mathcal{V}$ if $(u,v) \in \mathcal{E}$. The wireless connectivity between two nodes is mutual. Hence, if $(u,v) \in \mathcal{E}$, $(v,u) \in \mathcal{E}$. $\mathcal{S} = \{S_1, S_2, \ldots, S_K\}$ is the session set and a session S_i is represented by its source a_i and destination b_i, i.e.,

$S_i = (a_i, b_i), a_i, b_i \in \mathcal{V}$. Here, we assume $a_i \neq a_j, b_i \neq b_j \forall i \neq j$. Further, the notation $\mathcal{A} = \{a_i\}$ is used for the set of the sources and $\mathcal{B} = \{b_i\}$ is used for the set of the destinations.

For this network, assume that time is slotted and half-duplex is used. In each time slot, each node can be in one of the three states of *transmit state*, *receive state*, and *null state*. For a time slot t, the notations $\mathcal{T}_t$, $\mathcal{R}_t$, and $\mathcal{N}_t$ are used for the set of nodes in transmit state, receive state, and null state, respectively. Moreover, the messages are represented by symbols from finite field $\mathbb{F}_q$, in which q is a prime power. The capacity of all edges is 1 message per time slot. It also turns out to be useful in introducing the "silent symbol" notation σ. That is, when u is in transmit state or null state, the received message is written as $Y_t(u) = \sigma$, which is the silent symbol, representing that nothing is received. Similarly, when u is in receive state or null state, its transmitted signal is written as $X_t(u) = \sigma$, representing the fact that u is not transmitting, or namely u is silent. Then, when u is transmitting in time slot t, the transmitted message is denoted by $X_t(u) \in \mathbb{F}_q \cup \{\sigma\}$. When u is receiving in time slot t, the received signal is denoted by $Y_t(u) \in \mathbb{F}_q \cup \sigma$. Note that a node is allowed to transmit or receive σ in the transmit or receive state, respectively. These cases are identical to the case that this node is in null state. Here, the three states are clarified as the following. For any node m

- if $m \in \mathcal{T}_t$, we have $X_t(u) \in \mathbb{F}_q \cup \{\sigma\}, Y_t(u) = \sigma$,
- if $m \in \mathcal{R}_t$, we have $X_t(u) = \sigma, Y_t(u) \in \mathbb{F}_q \cup \{\sigma\}$,
- if $m \in \mathcal{N}_t$, we have $X_t(u) = \sigma, Y_t(u) = \sigma$.

Further, in our model, the features of wireless networks are characterized as the following: The broadcast feature means that a transmitting node sends its signal to all its neighbors. When a node is receiving, it gets the superposition of all the signals transmitted by its neighbors.

3.2.2. TRANSMISSION MODES

In order to study the improvement of CF in such a network, the underlying physical and multiple-access-control layer behaviors are transformed into four transmission modes.

PP MODE

PP mode, which is based on point-to-point communication, is modeled as follows, reflecting that broadcast and superposition are not exploited and traditional routing is used. In each time slot, a node u in the transmit state can communicate a message to at most one neighbor v. For any other neighbor $v' \neq v$ of u, the fact that u is transmitting to v implies that v' cannot receive any useful information in that time slot even if it is in receive state. Finally, successful transmission of a message from u to target node v in time slot t is possible if and only if u is in transmit state, v is in receive state, and all other neighbors of v are silent (in order to avoid collisions at v), i.e.,

$$\begin{aligned} & Y_t(v) = X_t(u) \neq \sigma \\ \Rightarrow \quad & u \in \mathcal{T}_t \wedge v \in \mathcal{R}_t \wedge (\forall u', v' : (u, u'), (v, v') \in \mathcal{E}, u' \notin \mathcal{R}_t, v' \notin \mathcal{T}_t). \end{aligned} \tag{3.1}$$

Note that in PP mode, if node u is transmitting to node v, one of its neighbor u' can also receive the same transmitted message. However, since network coding is not exploited, one transmission cannot be useful for multiple sessions, which suggests that this reception is meaningless. Thus, in this mode, we simply assume that u' is not in receive state as stated in (3.1).

Now, if the notation $M_t(u,v) \in \mathbb{F}_q$ is used for the message transmitted by u through edge (u,v) in time slot t, the rules for message passing in PP mode are

$$\begin{aligned} & Y_t(v) = M_t(u,v) \neq \sigma \\ \Rightarrow \quad & M_t(v,u) = \sigma, \\ & M_t(u,u'), M_t(u',u), M_t(v,v'), M_t(v',v) = \sigma, \forall (u',u), (v',v) \in \mathscr{E} : u' \neq v, v' \neq u, \\ & M_t(u'',u'), M_t(v',v'') = \sigma, \forall (u'',u'), (v'',v') \in \mathscr{E} : (u',u), (v',v) \in \mathscr{E}, u'' \neq u, v'' \neq v. \end{aligned} \tag{3.2}$$

BP MODE

In BP mode, broadcast is exploited by using NC. Instead of transmitting the messages for individual session, a node can broadcast a linear combination of multiple messages which can be useful for multiple sessions. Then, when a node u is transmitting, all of the neighbors in receive state can receive the transmitted message, i.e.,

$$\begin{aligned} & Y_t(v) = X_t(u) \neq \sigma \\ \Rightarrow \quad & u \in \mathscr{T}_t \wedge v \in \mathscr{R}_t \wedge (\forall v' : (v,v') \in \mathscr{E}, v' \notin \mathscr{T}_t). \end{aligned} \tag{3.3}$$

By this constraint, it holds that

$$\begin{aligned} & Y_t(v) = M_t(u,v) \neq \sigma \\ \Rightarrow \quad & M_t(v,u) = \sigma \\ & M_t(u',u), M_t(v,v'), M_t(v',v) = \sigma, \forall (u',u), (v',v) \in \mathscr{E} : u' \neq v, v' \neq u \\ & M_t(u'',u'), M_t(v',v'') = \sigma, \forall (u'',u'), (v'',v') \in \mathscr{E} : (u',u), (v',v) \in \mathscr{E}, u'' \neq u, v'' \neq v \end{aligned} \tag{3.4}$$

PM MODE

This is an artificial conceptual mode which is proposed for comparison. Assume that superposition is exploited by CF and broadcast is not exploited. By the CF technique, by receiving the superposition of multiple transmitted messages, the receiver can compute a linear sum of these messages.

Note that as shown in Subsection 2.3.1, the rate for decoding a linear sum of n messages is not the same as the rate of transmitting a message via the same edge in PP mode. By (2.12), the rate for decoding a linear sum of n messages is $1/2\log(1/n + \mathrm{SNR})$, which is smaller than the channel capacity $1/2\log(1+\mathrm{SNR})$. However, in high SNR scenarios, this difference is negligible. In this model, we neglect this rate difference and assume that the receiver is able to decode that linear sum of all the messages transmitted by its neighbors.

Then, in this mode, we have

$$\begin{aligned} & Y_t(v) = \sum_{u:u\in\mathscr{T}_t\wedge(u,v)\in\mathscr{E}\wedge X_t(u)\neq\sigma} X_t(u) \\ \Rightarrow \quad & v\in\mathscr{R}_t\wedge(\forall u':(u,u')\in\mathscr{E},u'\notin\mathscr{R}_t) \end{aligned} \tag{3.5}$$

and

$$\begin{aligned} & Y_t(v) = \sum_{(u,v)\in\mathscr{E}} M_t(u,v)\neq\sigma, \\ \Rightarrow \quad & M_t(v,u)=\sigma, \\ & M_t(u',u),M_t(u',u),M_t(v,v')=\sigma,\forall(u',u),(v',v)\in\mathscr{E}:u'\neq v,v'\neq u, \\ & M_t(u'',u'),M_t(v',v'')=\sigma,\forall(u'',u'),(v'',v')\in\mathscr{E}:(u',u),(v',v)\in\mathscr{E},u''\neq u,v''\neq v. \end{aligned} \tag{3.6}$$

BM MODE

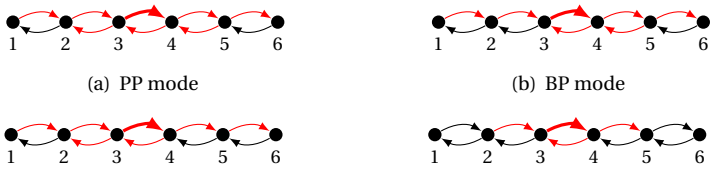
In BM mode, both broadcast and superposition are exploited. Hence we have

$$\begin{aligned} & Y_t(v) = \sum_{u:u\in\mathscr{T}_t\wedge(u,v)\in\mathscr{E}\wedge X_t(u)\neq\sigma} X_t(u) \\ \Rightarrow \quad & v\in\mathscr{R}_t \end{aligned} \tag{3.7}$$

and

$$\begin{aligned} & Y_t(v) = \sum_{(u,v)\in\mathscr{E}} M_t(u,v)\neq\sigma, \\ \Rightarrow \quad & M_t(v,u)=\sigma, \\ & M_t(u',u),M_t(v,v')=\sigma,\forall(u',u),(v',v)\in\mathscr{E}:u'\neq v,v'\neq u. \end{aligned} \tag{3.8}$$

In Fig. 3.1 we show the transmission rules for the four modes in a line network, in which $\mathscr{V}=\{1,2,\ldots,6\}$ and $(u,v)\in\mathscr{E}$ if $u,v\in\mathscr{V}$ and $|u-v|=1$.



(a) PP mode (b) BP mode

(c) PM mode (d) BM mode

Figure 3.1: Illustration of a network $\mathbf{N}(\mathscr{V},\mathscr{E},\mathscr{S})$ with $\mathscr{V}=\{1,2,\ldots,6\}$ and $\mathscr{E}=\{(u,v)|u,v\in\mathscr{V},|u-v|=1\}$ as well as the constraints for the four modes: useful communication on the thick red edges implies that no useful communication is possible on the thin red edges.

3.2.3. COMMON RATES AND IMPROVEMENT FACTOR

The *rate* of a session is the long-term ratio of the number of successfully retrieved messages transmitted from the source at the destination for that session and the number of time slots used. If all sessions communicate at the same rate R, R is called the *common rate*. In this chapter, we focus on the *maximum achievable common rate* in various modes, denoted as R^X in which $X \in \{\text{PP}, \text{BP}, \text{PM}, \text{BM}\}$ for modes PP, BP, PM, and BM, respectively. In particular, the *improvement factor* I_Y^X is investigated, where I_Y^X is defined as

$$I_Y^X = R^X / R^Y, \ X, Y \in \{\text{PP}, \text{BP}, \text{PM}, \text{BM}\}. \tag{3.9}$$

It seems that we compare the common rates achieved in different channel configurations. However, the transmission modes are essentially describing the multiple access control, scheduling, and coding schemes for various transmission schemes. Hence, the improvement factor reflects the throughput improvement between two schemes, rather than two network models.

3.3. GENERAL NETWORKS

In this section, we focus on the maximum throughput benefit of CF over traditional routing. A fundamental bound of $3K$ on the throughput improvement factor $I_{\text{PP}}^{\text{BM}}$ and an example network in which the improvement factor $I_{\text{PP}}^{\text{BM}}$ is at least $K/2$ are given.

3.3.1. UPPER BOUND ON THE IMPROVEMENT FACTOR

In this subsection, we will show that $I_{\text{PP}}^{\text{BM}}$ is upper bounded by $3K$ in any network. In order to do so, we first present a lemma providing a lower bound on the achievable rate in PP mode for any network with a single unidirectional session.

Lemma 3.3.1. *For any network* $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S}), K = 1$, *a common rate of* $1/3$ *is achievable in PP mode, which implies*

$$R^{\text{PP}} \geq 1/3. \tag{3.10}$$

Proof: Let $\mathbf{l} = (r_1, r_2, \ldots, r_L)$ be the sequence of nodes on a shortest path for S_1, i.e., $r_1 = a_1$, $(r_i, r_{i+1}) \in \mathcal{E}$ for all i, $r_L = b_1$, and there does not exist another path $\mathbf{l}'$ from a_1 to b_1 with length $L' < L$. Since $\mathbf{l}$ is the shortest path from a_1 to b_1, it holds that $r_i \neq r_j$ if $i \neq j$.

We use the following simple scheduling scheme in PP mode. In time slot t, all nodes in the network are in the null state, except r_i with $i \equiv t \pmod 3$ and $i \in [1, L-1]$, which transmit to r_{i+1}, and r_i with $i \equiv t \pmod 3 + 1$ and $i \in [2, L]$, which receive the transmission. The transmitted message by r_i is the message received by that node in the previous time slot in case $i \in [2, L]$, while it is a new source message in case $i = 1$.

Suppose that besides r_i also another neighbor r_j of r_{i+1} is transmitting in a time slot $t \equiv i \pmod 3$. Then

$$(r_1, r_2, \ldots, r_j, r_{i+1}, r_{i+2} \ldots, r_L),$$

if $j < i$, or

$$(r_1, r_2, \ldots, r_{i+1}, r_j, r_{j+1} \ldots, r_L),$$

if $j > i$, would be a path from a_1 to b_1 which is shorter than $\mathbf{l}$, since $|i-j| \geq 3$. This contradicts the fact that $\mathbf{l}$ is a shortest path, and thus it can be concluded that all neighbors of r_{i+1} other than r_i are silent. Hence, this scheme shows no conflict with (3.2), and thus it is valid. Clearly, starting at time $t = L-1$, one source symbol is delivered to the destination every three time slots, and thus, a rate of $1/3$ is achieved by the proposed scheme. Then, it follows that $R^{\mathrm{PP}} \geq 1/3$. ■

Theorem 3.3.1 (Upper bound of the throughput benefit in general networks)**.** *For any network* $\mathbf{N}(\mathscr{V}, \mathscr{E}, \mathscr{S})$*,*

$$I_{\mathrm{PP}}^{\mathrm{BM}} \leq 3K. \tag{3.11}$$

Proof: By applying a simple time sharing argument among the K sessions, it follows from Lemma 3.3.1 that $R^{\mathrm{PP}} \geq 1/(3K)$. Further, since every destination receives at most one symbol per time slot, it holds that $R^{\mathrm{BM}} \leq 1$. ■

3.3.2. EXAMPLE NETWORKS

In the previous subsection, we have shown that for any network, the throughput improvement factor of CF over traditional routing can be at most $3K$. In this subsection, we will show that for any $K \geq 3$, there exists a network for which the improvement factor is at least an order of K. More precisely, we propose a class of networks, denoted as $\mathrm{RN}(K)$, for which CF brings such an improvement. The network $\mathrm{RN}(K)$ is constructed as follows.

1. We construct a bipartite graph with the vertex set $\mathscr{P} \cup \mathscr{Q}$, where $\mathscr{P} \cap \mathscr{Q} = \emptyset$ and $|\mathscr{P}| = |\mathscr{Q}| = K \geq 3$. Denote $\mathscr{P} = \{p_1, p_2, \ldots, p_K\}$, $\mathscr{Q} = \{q_1, q_2, \ldots, q_K\}$. Any $p_i \in \mathscr{P}$ connects to all the vertices in $\mathscr{Q}$ except q_i. Hence, all vertices of this graph have degree $K-1$.

2. We add a vertex z, called relay, to this graph, which is connected to all other vertices. Thus it has degree $2K$. As a result, we have vertex set $\mathscr{P} \cup \{z\} \cup \mathscr{Q}$ and edge set $\{(p_i, q_j), (q_j, p_i) | i, j \in \{1, 2, \ldots, K\}, i \neq j\} \cup \{(p_i, z), (z, p_i), (q_i, z), (z, q_i) | i, j \in \{1, 2, \ldots, K\}\}$.

3. Sessions $S_1, S_2, \ldots, S_K$ are placed on this graph in such a way that the source and destination of session S_i are $a_i = p_i$ and $b_i = q_i$, respectively.

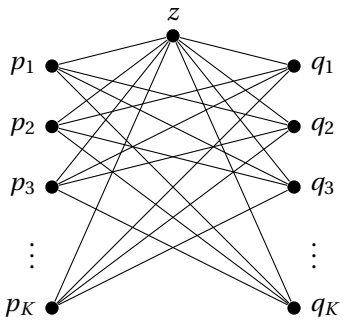
4. As a result, we have the network $\mathrm{RN}(K)$.

$\mathrm{RN}(K)$ is illustrated in Fig. 3.2(a). Note that RN(3) and RN(4) can be geometrically represented as a hexagon and a cube, respectively, with the relay z in their centers (Fig. 3.2(b) and Fig. 3.2(c)).

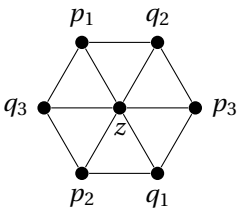
In order to show that $\mathrm{RN}(K)$ has an improvement factor of at least an order of K, we first present a lemma providing an upper bound on the common rate for $\mathrm{RN}(K)$ in PP mode, and then another lemma giving a lower bound on the maximum achievable common rate for $\mathrm{RN}(K)$ in BM mode.

Lemma 3.3.2. *For network* $\mathrm{RN}(K)$*,*

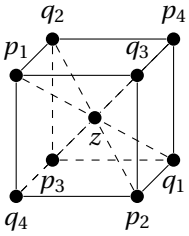
$$R^{\mathrm{PP}} \leq 1/K. \tag{3.12}$$



(a) RN(K)



(b) RN(3)



(c) RN(4)

Figure 3.2: (a) The network RN(K) and geometric representations of (b) RN(3) and (c) RN(4).

Proof: We will show that for any scheme on RN(K) in PP mode, the common rate is at most $1/K$. First, for any time slot t, define

$$E_t = \sum_{i=1}^{K} \left(\Gamma_t(p_i, z) + \Gamma_t(z, q_i) + \sum_{j=1, j\neq i}^{K} \Gamma_t(p_i, q_j) \right) \tag{3.13}$$

with the $\Gamma_t(u,v)$ representing a successful transmission, i.e., $\Gamma_t(u,v) = 1$ if $M_t(u,v) \neq \sigma$ and $\Gamma_t(u,v) = 0$ if $M_t(u,v) = \sigma$. Note that the expression in (3.13) counts the number of successful transmissions in time slot t leaving from a vertex in $\mathscr{P}$ and/or arriving in a vertex in $\mathscr{Q}$.

Since there is no direct link between source and destination of any session S_i in RN(K), at least two successful transmissions are required per retrievable source symbol: one transmission from the source vertex p_i to a vertex in $\{z\} \cup \mathscr{Q} \backslash \{q_i\}$, and another from a vertex in $\{z\} \cup \mathscr{P} \backslash \{p_i\}$ to the destination q_i. Hence, when running any scheme in PP mode during T time slots, the total number of successfully obtained source symbols at the destinations, denoted as N_T, satisfies

$$2N_T \leq \sum_{t=1}^{T} E_t. \tag{3.14}$$

It follows from (3.2) that any term in the summation in (3.13) being equal to one implies that all other terms equal zero, with the possible exception of $\Gamma_t(p_j, q_i)$ in case

$\Gamma_t(p_i, q_j) = 1$. Hence, we have

$$E_t \le 2 \tag{3.15}$$

for all t, and thus it follows from (3.14) that the total number of obtained source symbols at the destinations is at most T. Since rate has been defined as the long-term ratio of the number of retrieved source symbols and the number of time slots used, we thus conclude from (3.14) and (3.15) that the common rate satisfies

$$\begin{aligned} R &\le \frac{1}{K}\sum_{i=1}^{K} R_i = \frac{1}{K}\lim_{T\to\infty}\frac{N_T}{T} \\ &\le \frac{1}{K}\lim_{T\to\infty}\frac{\frac{1}{2}\sum_{t=1}^{T} E_t}{T} \le \frac{1}{K}\lim_{T\to\infty}\frac{\frac{1}{2}\cdot 2T}{T} = \frac{1}{K}. \end{aligned}$$

Since this holds for any scheme and R^{PP} is defined as the maximum achievable common rate over all possible schemes in PP mode, we have $R^{\mathrm{PP}} \le 1/K$. ■

Lemma 3.3.3. *For network* RN(K),

$$R^{\mathrm{BM}} \ge 1/2. \tag{3.16}$$

Proof: We prove this result by presenting a scheduling scheme in BM mode, which allows all the destinations of all sessions to retrieve one source symbol in every two time slots:

1. If $t \equiv 1 \pmod 2$, then all sources p_i simultaneously transmit a new source message, while all other vertices are in the receive state. From (3.7), we have $Y_t(q_j) = \sum_{i=1, i\neq j}^{K} X_t(p_i)$ for all j, $Y_t(z) = \sum_{i=1}^{K} X_t(p_i)$.
2. If $t \equiv 0 \pmod 2$, then relay z broadcasts its reception of the previous time slot to all destinations. Each destination can retrieve its desired source symbol by subtracting its reception in the previous time slot from the reception in this time slot: $Y_t(q_j) - Y_{t-1}(q_j) = \sum_{i=1}^{K} X_{t-1}(p_i) - \sum_{i=1, i\neq j}^{K} X_{t-1}(p_i) = X_{t-1}(p_j)$ for all j.

Since this scheme achieves a common rate of $1/2$ and R^{BM} is defined as the maximum achievable common rate over all possible schemes in BM mode, it follows that $R^{\mathrm{BM}} \ge 1/2$. ■

Combining the bounds from Lemmas 3.3.2 and 3.3.3, we obtain the main result of this subsection, as stated in the next theorem.

Theorem 3.3.2 (Lower bound of the throughput benefit in RN(K))**.** *For network* RN(K),

$$I_{\mathrm{PP}}^{\mathrm{BM}} \ge K/2. \tag{3.17}$$

As a contrasting example, we briefly consider a line network $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$ where $\mathcal{V} = \{1, 2, \ldots, 2K-1\}$, $\mathcal{E} = \{(u, v) | u, v \in \mathcal{V}, |u - v| = 1\}$, $S_i = (2i-1, 2i)$ if $i \equiv 1 \pmod 2$, and $S_i = (2i, 2i-1)$ if $i \equiv 0 \pmod 2$. The simple traditional routing scheme in which all sources send a new symbol to their destinations in every time slot achieves a common rate of 1, which cannot be beaten by any scheme in BM mode since every destination can receive at most 1 symbol per time slot. Hence, $R^{\mathrm{BM}} = R^{\mathrm{PP}} = 1$ and thus we have $I_{\mathrm{PP}}^{\mathrm{BM}} = 1$ for this network. Note that this network and RN(K) both have K sessions, but that their improvement factors are very different. We conclude that the benefit of CF depends very much on the network topology and session placement.

3.4. LINE NETWORKS WITH BIDIRECTIONAL SESSIONS

In the previous section, it is shown that the throughput benefit of CF depends very much on the types of networks. Although networks in which the improvement of CF over traditional routing is at least $K/2$ was found, however, in many other networks, it is very hard to tell how much benefit at least can CF bring. This is because that finding a lower bound for the improvement of CF over other transmission schemes is as difficult as many other multiple unicasts problems.

In this section, the focus is put on a relatively simple case: line networks with bidirectional sessions. Firstly, upper bounds for the common rates in various transmission modes are derived. Then, transmission and coding schemes with common rates achieving these bounds are given. The combinations of these bounds indicate how much CF benefits the throughput over other schemes in line networks with bidirectional sessions, which is the main result of this section.

3.4.1. DEFINITIONS AND NOTATIONS

Firstly, we give the definition of the line network.

Definition 3.4.1 (Line networks)**.** A network $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$ is a line network if $\mathcal{V}=\{1,2,\dots,N\}$, $N\geq 3$, and $\mathcal{E}=\{(u,v):u,v\in\mathcal{V},|u-v|=1\}$, denoted by $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$.

In this section, line networks with bidirectional sessions, i.e., $\forall(u,v)\in\mathcal{S},(v,u)\in\mathcal{S}$, are considered. Here, define $\mathcal{S}^B=\{(u,v)\in\mathcal{S}|u<v\}$. Denote the elements in this set by $\mathcal{S}^B=\{S_1^B,S_2^B,\dots,S_{\frac{K}{2}}^B\}$ and define $S_i^B=(p_i^L,p_i^R)$, where p_i^L and p_i^R are called the left and the right terminal for bidirectional session S_i^B, respectively. Define $\mathcal{P}^L=\{p_1^L,p_2^L,\dots,p_{\frac{K}{2}}^L\}$ and $\mathcal{P}^R=\{p_1^R,p_2^R,\dots,p_{\frac{K}{2}}^R\}$. Clearly, $\mathcal{P}^R\cup\mathcal{P}^L=\mathcal{A}$.

3.4.2. UPPER BOUNDS

In this subsection, general upper bounds on the common rates are derived by using the constraints listed in (3.1), (3.3), (3.5), and (3.7).

Lemma 3.4.1 (Upper bounds for common rates in line networks with bidirectional sessions)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *that* $\forall(u,v)\in\mathcal{S},(v,u)\in\mathcal{S}$*, the common rate in mode* $X\in\{\mathrm{PP},\mathrm{BP},\mathrm{PM},\mathrm{BM}\}$ *is upper bounded by the rate* C^X *specified by*

$$C^{\mathrm{PP}} = \min\left\{\min_{m\notin\mathcal{P}:\alpha_m^B\neq 0}\frac{1}{4\alpha_m^B},\min_{m\in\mathcal{P}}\frac{1}{4\alpha_m^B-2}\right\}, \tag{3.18}$$

$$C^{\mathrm{BP}}=C^{\mathrm{PM}} = \min\left\{\min_{m\notin\mathcal{P}:\alpha_m^B\neq 0}\frac{1}{3\alpha_m^B},\min_{m\in\mathcal{P}}\frac{1}{3\alpha_m^B-1}\right\}, \tag{3.19}$$

$$C^{\mathrm{BM}} = \min_{\alpha_m^B\neq 0}\frac{1}{2\alpha_m^B}. \tag{3.20}$$

Here, α_m^B *is the bidirectional sessions that node* m *involves (either functions as terminal or relay), i.e.,* $\alpha_m^B=|\{(u,v)\in\mathcal{S}^B|m\in[u,v]\}|$.

Proof: Firstly, for line networks, the rules for message passing in (3.2), (3.4), (3.6), and (3.8) can be specified as the following.

PP mode:

$$\begin{aligned} & Y_t(u+1) = M_t(u,u+1) \neq \sigma \\ \Rightarrow \quad & M_t(u-1\pm 1,u-1), M_t(u-1,u), M_t(u+1,u+1\pm 1), M_t(u+2,u+2\pm 1) = \sigma. \end{aligned} \tag{3.21}$$

BP mode:

$$\begin{aligned} & Y_t(u+1) = M_t(u,u+1) \neq \sigma \\ \Rightarrow \quad & M_t(u-2,u-1), M_t(u-1,u), M_t(u+1,u+1\pm 1), M_t(u+2,u+2\pm 1) = \sigma. \end{aligned} \tag{3.22}$$

PM mode:

$$\begin{aligned} & Y_t(u+1) = M_t(u,u+1) + M_t(u+2,u+1) \neq \sigma \\ \Rightarrow \quad & M_t(u-1\pm 1,u-1), M_t(u-1,u), M_t(u+1,u+1\pm 1), M_t(u+2,u+3) = \sigma. \end{aligned} \tag{3.23}$$

BM mode:

$$\begin{aligned} & Y_t(u+1) = M_t(u,u+1) + M_t(u+2,u+1) \neq \sigma \\ \Rightarrow \quad & M_t(u-1,u), M_t(u+1,u), M_t(u,u+1) = \sigma. \end{aligned} \tag{3.24}$$

The transmission rules are illustrated in Fig. 3.1.

For any scheduling scheme, define

$$R(u,v) = \frac{|\{t \in \{1,2,\ldots,T\} : M_t(u,v) \neq \sigma\}|}{T}, \tag{3.25}$$

where T is the total number of time slots. Furthermore, we use the notation $\mathscr{E}_m$ for the set of all edges starting or ending in node m, i.e., $\mathscr{E}_m = \{(m-1,m),(m,m-1),(m,m+1),(m+1,m)\} \cap \mathscr{E}$.

Assume a line network $\mathbf{L}(\mathscr{V},\mathscr{E},\mathscr{S})$ with bidirectional sessions has a common rate of R, then by the max-flow min-cut theorem [6], it holds that

$$\alpha_m^B R \leq R(u,v), \forall (u,v) \in \mathscr{E}_m. \tag{3.26}$$

Then, for $m \in \mathscr{A}$, a tighter bound can be derived taking into account the argument that the terminal nodes do not need to receive its own messages and relay its desired messages. Hence we have

$$\begin{aligned} & (\alpha_m^B - 1)R \leq R(u,v), \\ \forall \quad & ((m-1,m),(m,m-1) : m \in \mathscr{P}^L) \\ & \wedge ((m,m+1),(m+1,m) : m \in \mathscr{P}^R), m' \in \mathscr{E}. \end{aligned} \tag{3.27}$$

Since the following reasoning is similar for all four modes, we only consider PP mode and BP mode.

In PP mode, for any node m, we consider the edges in $\mathscr{E}_m$. If $m \notin \{1, N\}$, there are four edges in $\mathscr{E}_m$ and by (3.26) and (3.27), we have four inequalities for these four edges. We can then obtain a new inequality by summing up the four inequalities. In case of $m \notin \mathscr{A}$, the new inequality is

$$\begin{aligned} 4\alpha_m^B R &\leq \sum_{(u,v)\in\mathscr{E}_m} R(u,v) \\ &= \frac{|\{t \in \{1,2,\dots,T\} : M_t(u,v) \neq \sigma, (u,v) \in \mathscr{E}_m\}|}{T} \\ &\leq 1. \end{aligned} \tag{3.28}$$

The last inequality follows from the constraint (3.21). Similarly, for the nodes $m \in \mathscr{A}$, we have $(4\alpha_m^B - 2)R \leq 1$. Then, considering all nodes that $m \notin \{1, N\}$, we have

$$R \leq \min\left\{ \min_{m\notin\mathscr{A}\cup\{1,N\}:\alpha_m^B\neq 0} \frac{1}{4\alpha_m^B}, \min_{m\in\mathscr{A}\setminus\{1,N\}} \frac{1}{4\alpha_m^B - 2} \right\}, \tag{3.29}$$

which is equivalent to (3.18).

Then, BP mode is considered using the similar argument. For any node m, we obtain new inequalities by summing up the inequalities for one edge starting from node m and all edges ending in node m. Due to the constraint of BP mode indicated in (3.22), the RHS of the new inequality cannot be larger than 1. Hence, for any node $m \notin \mathscr{A} \cap \{1, N\}$ and $\alpha_m^B \neq 0$, we have an upper bound on the common rate $R \leq 1/(3\alpha_m^B)$. For any node $m \in \mathscr{A}\setminus\{1, N\}$, in which case two inequalities are obtained depending on which edge starting from m is chosen for summation. We choose the tighter upper bound $R \leq 1/(3\alpha_m^B - 1)$. Then, the upper bound for common rate can be obtained by considering all nodes that $m \notin \{1, N\}$. Then, this upper bound is equivalent to the one in (3.19).

■

Note that it follows from Lemma 3.4.1 that the maximum common rate is determined by so-called "bottleneck" nodes, i.e., nodes m for which α_m^B is maximum, and that for PP, BP, and PM modes, its value does not only depend on this maximum α_m^B, but also whether or not it is achieved for a non-terminal node.

3.4.3. LOWER BOUNDS

In this subsection, we prove that the upper bound from Lemma 3.4.1 can be achieved.

Lemma 3.4.2 (Lower bounds for common rates in line networks with bidirectional sessions)**.** *For a line network* $\mathbf{L}(\mathscr{V}, \mathscr{E}, \mathscr{S})$ *that* $\forall (u,v) \in \mathscr{S}, (v,u) \in \mathscr{S}$*, the common rate* $R \leq C^X$ *specified by (3.18)–(3.20) is achievable in mode* $X \in \{\mathrm{PP}, \mathrm{BP}, \mathrm{PM}, \mathrm{BM}\}$.

Here, the proof of this lemma is given by giving feasible scheduling and coding schemes. Before that, we introduce the *load factor*, which reflects the number of time slots needed for a node to handle all of its transmissions and receptions.

LOAD FACTOR

We define the load factor of node m for various modes as

$$F_m^{\mathrm{PP}} = \begin{cases} 4\alpha_m^B & m \notin \mathscr{A} \\ 4\alpha_m^B - 2 & m \in \mathscr{A} \end{cases}, \tag{3.30}$$

$$F_m^{\mathrm{BP}} = F_m^{\mathrm{PM}} = \begin{cases} 3\alpha_m^B & m \notin \mathscr{A} \\ 3\alpha_m^B - 1 & m \in \mathscr{A} \end{cases}, \tag{3.31}$$

$$F_m^{\mathrm{BM}} = 2\alpha_m^B. \tag{3.32}$$

Also, define the maximum load factor for $X \in \{\mathrm{PP}, \mathrm{BP}, \mathrm{PM}, \mathrm{BM}\}$ as

$$F_{\max}^X = \max_{m=1}^{N} F_m^X. \tag{3.33}$$

Furthermore, we use

$$\mathscr{K}_i^B = \{m \in \mathscr{V} \mid u \le m \le v, (u,v) = S_i^B\},$$

and

$$\mathscr{J}_m^B = \{(u,v) \in \mathscr{S}^B \mid m \in [u,v]\},$$

for the set of all nodes that are involved in bidirectional session S_i^B and the set of all bidirectional sessions that involve node m, respectively. Note that $\alpha_m^B = |\mathscr{J}_m^B|$.

The following lemma shows important properties of the load factor for the three modes PP, BP, and PM, in which cases the maximum load factor does not only depend on the largest α_m^B value, but also on whether or not it is achieved for a non-terminal node.

Lemma 3.4.3. *For any $X \in \{\mathrm{PP}, \mathrm{BP}, \mathrm{PM}\}$, the following conditions hold.*
(a) If node $m \in \mathscr{P}^L$ and $F_m^X = F_{\max}^X$, then node $m+1 \in \mathscr{P}^R$ and $F_{m+1}^X = F_{\max}^X$.
(b) Under Condition (a), if $F_{m-1}^X = F_{\max}^X$, then node $m-1 \in \mathscr{P}^R$.
(c) If node $m \in \mathscr{P}^R$ and $F_m^X = F_{\max}^X$, then node $m-1 \in \mathscr{P}^L$ and $F_{m-1}^X = F_{\max}^X$.
(d) Under Condition (c), if $F_{m+1}^X = F_{\max}^X$, then node $m+1 \in \mathscr{P}^L$.

Proof: Since cases (a), (b) are symmetric to (c), (d), we only discuss cases (a) and (b):

Firstly, if node $m \in \mathscr{P}^L$ has a load factor that $F_m^X = F_{\max}^X$, the node $m+1$ cannot be in set $\mathscr{V} \setminus \mathscr{A}$, since then node $m+1$ would have exactly the same number of bidirectional sessions as m and a larger load factor due to (3.30). Similarly, it cannot be in $\mathscr{P}^L$, for that will cause $\alpha_{m+1} = \alpha_m^B + 1$ and $F_{m+1}^X > F_m^X$. Hence we have node $m+1 \in \mathscr{P}^R$, and obviously $F_{m+1}^X = F_m^X = F_{\max}^X$.

Then, under Condition (a), if $F_{m-1}^X = F_{\max}^X$, node $m-1$ cannot be in sets $\mathscr{P}^L$ or $\mathscr{V} \setminus \mathscr{A}$. Otherwise, we have $F_{m-1}^X > F_m^X$ which contradicts with our assumption $F_m^X = F_{\max}^X$. Hence, node $m-1$ can only be in set $\mathscr{P}^R$. ∎

By Lemma 3.4.3, we find that in P/P, B/P and P/M modes, any terminal nodes which have $F_m^X = F_{\max}^X$ will always appear in pairs of node $m \in \mathscr{P}^L$ and node $m+1 \in \mathscr{P}^R$ (not necessarily be two terminals of the same bidirectional session).

SCHEDULING SCHEMES

The scheduling processes are described by rounds of a certain time slots. Because of the similarities of the scheduling scheme for PP, BP, and PM modes (due to the same properties claimed by Lemma 3.4.3), we only show the scheduling schemes for BP mode and BM mode for the sake of simplicity. Since the messages from different bidirectional sessions are not coded, the notation $L_t(u,v) = S_i^B$ is used to represent that in time slot t the transmission on the edge (u,v) is assigned for bidirectional session S_i^B. By applying the schemes, schedules with the following properties are obtained.

Property 3.4.1. Each round includes $F_{\max}^X$ time slots, where $X \in \{\text{PP}, \text{BP}, \text{PM}, \text{BM}\}$.

Property 3.4.2. The transmissions in each time slot do not violate the constraints in (3.21)–(3.24).

Property 3.4.3. The transmissions are assigned in such a way that for all bidirectional sessions, all involved relay nodes have 2 transmissions to relay the messages for both directions, and the terminal nodes have 1 transmission for transmitting the original messages.

BP Mode We distinguish two cases.

Case I: $F_{\max}^{\text{BP}}$ is achieved for node $m \notin \mathscr{A}$.

Assume S_i^B is the k-th element of $\mathscr{J}_m^B$. We do the following assignment: $L_{3k-2+t'}(m, m-1), L_{3k-2+t'}(m, m+1) = S_i^B$, where $t' \equiv (m-1) \pmod 3$. Clearly, the maximum value of t for any $L_t(u,v), (u,v) \in \{(m,m'),(m',m)\}$ assigned this way will be $F_{\max}^{\text{BP}}$.

Case II: $F_{\max}^{\text{BP}}$ is achieved for node $m \in \mathscr{A}$.

We first schedule the transmissions for those terminal nodes which achieve $F_{\max}^{\text{BP}}$. For the nodes $m \in \mathscr{P}^L$, if $m \equiv 0$ or $1(4)$, let $L_{F_{\max}^{\text{BP}}-1}(m, m+1) = S_i^B : p_i^L = m$, else let $L_{F_{\max}^{\text{BP}}}(m, m+1) = S_i^B : p_i^L = m$. Then, for the nodes $m \in \mathscr{P}^R$, if $m \equiv 0$ or $3(4)$, let $L_{F_{\max}^{\text{BP}}-1}(m, m-1) = S_i^B : p_i^R = m$, else let $L_{F_{\max}^{\text{BP}}}(m, m-1) = S_i^B : p_i^R = m$. These assignments will not violate (3.22), due to the features listed out in Lemma 3.4.3.

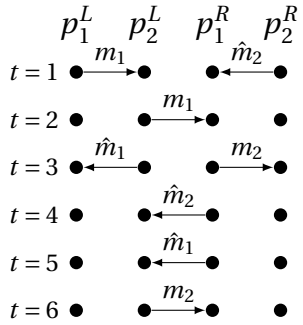
Next, for all nodes, we do the same assignment as in Case I, with the exception of those transmissions which have already been scheduled. Since all nodes with $F_m^{\text{BP}} < F_{\max}^{\text{BP}}$ will have $\alpha_m^B \le \max_{m=1}^N \alpha_m^B - 1$, and we have already scheduled two time slots for the terminal nodes with $\alpha_m^B \le \max_{m=1}^N \alpha_m^B$, the maximum value of t for any $L_t(u,v)$ assigned by the same method as Case I will be $\max_{m=1}^N 3(\alpha_m^B - 1) = F_{\max}^{\text{BP}}$, which make the number of total time slots $F_{\max}^{\text{BP}}$.

BM Mode Firstly we introduce two types of scheduling approaches:

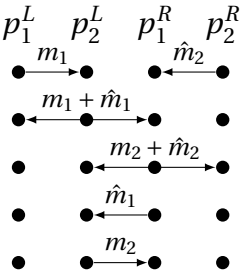
Type A: Let $L_{t+t'}(m, m-1), L_{t+t'}(m, m+1) = S_i^B$, where $t' \equiv (m-1) \pmod 2$;

Type B: Let $L_{t+t'}(m, m-1), L_{t+t'}(m, m+1) = S_i^B$, where $t' \equiv \pmod 2$.

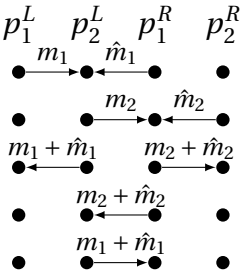
We start the scheduling in BM mode with assigning time slots for any bidirectional session S_i^B. We find the smallest t for which $X_t(m) = \sigma, \forall m \in \mathscr{K}_i^B$, and schedule these nodes according to Type A. Then, find all neighboring bidirectional sessions S_j^B which have $v+1 = u'$ or $u-1 = v'$. Here, $(u,v) = S_i^B$ and $(u',v') = S_j^B$. For each S_j^B, we schedule



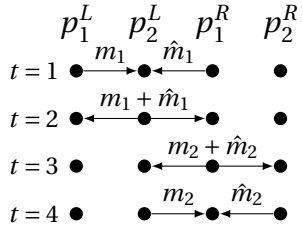
(a) PP mode



(b) BP mode



(c) PM mode



(d) BM mode

Figure 3.3: Scheduling and coding schemes within one round for the line network $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ with $N=4$ and $\mathcal{S}^B=\{(1,3),(2,4)\}$. Here, m_i and $\hat{m}_i$ represent the messages from left and right terminals of bidirectional session S_i^B, respectively. All nodes transmit the messages that are obtained from the previous round.

the nodes in $\mathcal{K}_j^B$ according to Type B. Then, we iteratively find the neighboring unscheduled bidirectional sessions of all the scheduled ones, and switch scheduling type (Type A and Type B) so that there will not be any pair of neighboring bidirectional sessions scheduled with the same type. Hence, there will be no collision at the terminal nodes.

Then we repeat this process until all sessions have been scheduled. It is a simple coloring problem and the maximum value of t for any $L_t(u,v),(u,v)\in\mathcal{E}$ is $2\max_{m=1}^{N}\alpha_m^B$.

CODING SCHEMES

Since we have the schedule with Property 3.4.3, the piggy-backing based NC and CF based schemes can be applied in the same fashion as those for a single bidirectional session. The details can be found in, e.g., [10].

Here, we use an example to give the main idea of the scheduling and the coding scheme.

Example 3.4.1. *Consider a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *with* $N=4$ *and* $\mathcal{S}^B=\{(1,3),(2,4)\}$. *We illustrate the schedules and the network codes of our schemes in Fig. 3.3.*

3.4.4. THROUGHPUT BENEFIT

Now, bringing back the definition of improvement factor in (3.9), we can upper bound the throughput benefit of mode X over mode Y by comparing the upper bound of R^X with the lower bound of R^Y, and lower bound the throughput benefit of mode X over mode Y by comparing the lower bound of R^X with the upper bound of R^Y. Since the bounds are tight for the common rates in all four mode, the bounds for the improvement factors are also tight. We have the following theorem.

Theorem 3.4.1 (Throughput benefit in line networks with bidirectional sessions)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *that* $\forall (u,v)\in\mathcal{S},(v,u)\in\mathcal{S}$*, the improvement factors are given by*

$$I_{\mathrm{PP}}^{\mathrm{BM}} = \frac{\max_{m=1}^{N}(F_m^{\mathrm{PP}})}{\max_{m=1}^{N}(F_m^{\mathrm{BM}})}, \tag{3.34}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PP}}^{\mathrm{PM}} = \frac{\max_{m=1}^{N}(F_m^{\mathrm{PP}})}{\max_{m=1}^{N}(F_m^{\mathrm{BP}})}, \tag{3.35}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}} = I_{\mathrm{PM}}^{\mathrm{BM}} = \frac{\max_{m=1}^{N}(F_m^{\mathrm{BP}})}{\max_{m=1}^{N}(F_m^{\mathrm{BM}})}, \tag{3.36}$$

where F_m^X *is given by (3.30)-(3.32).*

In particular, if $\max_{m=1}^{N}(F_m^{\mathrm{PP}})$ *is reached by* $m\notin\mathcal{A}$*, we have*

$$I_{\mathrm{PP}}^{\mathrm{BM}} = 2, \tag{3.37}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PP}}^{\mathrm{PM}} = 4/3, \tag{3.38}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}} = I_{\mathrm{PM}}^{\mathrm{BM}} = 3/2. \tag{3.39}$$

Next, examples providing some numerical results and illustrations are given. Firstly we consider Example 3.4.1. It can be easily calculated by counting or Theorem 3.4.1 that $I_{\mathrm{PP}}^{\mathrm{BM}} = 1.5$, while exploiting either of these features only gives a factor $I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PP}}^{\mathrm{PM}} = 1.2$. Then we consider another example with a larger network.

Example 3.4.2. *We consider, for fixed* K *and* $N\geq K$*, the average improvement factors over all possible configurations of* $K/2$ *bidirectional sessions in a line network with* N *nodes. We focus on* $I_{\mathrm{PP}}^{\mathrm{BM}}$*, but results for other cases could be obtained in a similar way. It follows from Theorem 3.4.1 that* $I_{\mathrm{PP}}^{\mathrm{BM}}$ *equals 2 except in the case that the "bottleneck" nodes are terminals. By combinatorial arguments, we find that the average improvement factor is*

$$\bar{I}_{\mathrm{PP}}^{\mathrm{BM}} = \begin{cases} 2-\frac{2}{N}, & \text{if } K=2, \\ 2-\frac{4}{3N}-\frac{4}{N(N-1)}, & \text{if } K=4. \end{cases} \tag{3.40}$$

For larger values of K*, the calculations become cumbersome. The simulations are run for four bidirectional sessions uniformly placed at random in the line network with* $8\leq N\leq 100$*, the results of which are depicted in Figure 3.4, together with the results of (3.40). Note that* $\bar{I}_{\mathrm{PP}}^{\mathrm{BM}}$ *is smallest if* $N=K$*, i.e., in case all nodes are terminals. For large values of* N*, the average improvement factor approaches* 2*, which can be observed from both (3.40) and Figure 3.4. Other simulations, with* $N=100$ *and* $1\leq K\leq 100$*, also show average improvement factors very close to 2.*

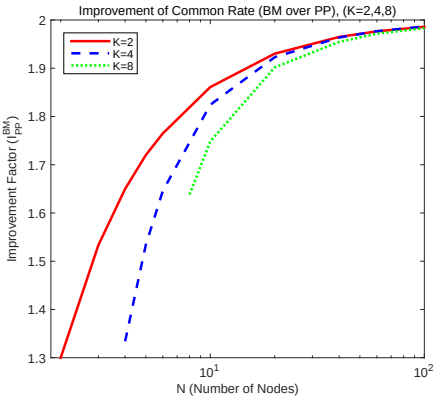


Figure 3.4: Average improvement factor $I_{\text{PP}}^{\text{BM}}$, in case of $K = 2,4,8$ bidirectional , $K \leq N \leq 100$ nodes, and uniformly distributed terminal nodes.

In this section, the problem of the throughput benefit of CF over other transmission schemes for multiple bidirectional sessions is solved in line networks by giving matching upper and lower bounds. It is shown that the improvement factors of CF over traditional routing and NC are 2 and 1.5 if the so-called bottleneck nodes are not terminals. If they are terminals, the improvement factors are smaller than 2 or 1.5.

3.5. LINE NETWORKS WITH ARBITRARY SESSIONS

The study in the previous section can also be seen as line networks with sessions placed in pairs. The result shows that the improvement factor depends on: 1, how many sessions that the "bottleneck nodes" involve; 2, whether the "bottleneck nodes" are terminals. In this section, the throughput benefit of CF in line networks with arbitrarily placed sessions is studied. It turns out that the throughput benefit does not only depend on the "bottleneck nodes", but their neighbors and two-hop neighbors as well. As a result, deriving match bounds for this scenario is much harder than the bidirectional session case. In this section, the upper and lower bounds derived are asymptotically tight when the numbers of the involving sessions of the "bottleneck nodes" are large.

3.5.1. NOTATIONS

Here, some new notations that will be used in this section are introduced. We use $\mathscr{S}^R$ and $\mathscr{S}^L$ for the sessions to the right and the left, respectively, i.e., $\mathscr{S}^R = \{(u,v) \in \mathscr{S} | u < v\}$ and $\mathscr{S}^L = \{(u,v) \in \mathscr{S} | u > v\}$. Obviously, we have $\mathscr{S}^R \cup \mathscr{S}^L = \mathscr{S}$. We then define $\mathscr{A}^R = \{u | (u,v) \in \mathscr{S}^R\}$, $\mathscr{A}^L = \{u | (u,v) \in \mathscr{S}^L\}$, $\mathscr{B}^R = \{v | (u,v) \in \mathscr{S}^R\}$, $\mathscr{B}^L = \{v | (u,v) \in \mathscr{S}^L\}$, $\mathscr{J}_m^R = \{(u,v) \in \mathscr{S}^R | m \in [u,v]\}$, $\mathscr{J}_m^L = \{(u,v) \in \mathscr{S}^L | m \in [v,u]\}$, $\alpha_m^R = |\mathscr{J}_m^R|$, and $\alpha_m^L = |\mathscr{J}_m^L|$. We then define $\alpha_m^{\max} = \max(\alpha_m^R, \alpha_m^L)$, $\alpha_m^{\min} = \min(\alpha_m^R, \alpha_m^L)$. Further, we let $\alpha_m = \alpha_m^R + \alpha_m^L$.

3.5.2. UPPER BOUNDS

In this subsection, the common rates of line networks with arbitrary sessions in various transmission modes are upper bounded.

Lemma 3.5.1 (Upper bounds for common rates in line networks)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *in mode* $X \in \{\text{PP},\text{BP},\text{PM},\text{BM}\}$*, the common rate is upper bounded by* C_U^X *specified by*

$$C_U^{\text{PP}} = \frac{1}{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}-4)}, \tag{3.41}$$

$$C_U^{\text{BP}} = C_U^{\text{PM}} = \frac{1}{\max_{m=1}^{N}(3\alpha_m^{\max}-4)}, \tag{3.42}$$

$$C_U^{\text{BM}} = \frac{1}{\max_{m=1}^{N}(2\alpha_m^{\max}-2)}. \tag{3.43}$$

Proof: Since the proof is similar for the four modes, for simplicity, we only show the proof for PP mode.

Firstly, if a common rate R is achieved, by the max-flow min-cut theorem, we have

$$\begin{aligned}
|\{t\in\{1,2,\ldots,T\}: M_t(m-1,m)\neq\sigma\}| &\geq (\alpha_m^R-\delta_m^{RL})RT, &(3.44)\\
|\{t\in\{1,2,\ldots,T\}: M_t(m,m+1)\neq\sigma\}| &\geq (\alpha_m^R-\delta_m^{RR})RT, &(3.45)\\
|\{t\in\{1,2,\ldots,T\}: M_t(m+1,m)\neq\sigma\}| &\geq (\alpha_m^L-\delta_m^{LR})RT, &(3.46)\\
|\{t\in\{1,2,\ldots,T\}: M_t(m,m-1)\neq\sigma\}| &\geq (\alpha_m^R-\delta_m^{LL})RT, &(3.47)
\end{aligned}$$

where T is an arbitrarily large integer representing the total time slots used, $Y\in\{RR,RL,LR,LL\}$, $\sum_{Y\in\{RR,RL,LR,LL\}}\delta_m^Y\leq 2$, and

$$\begin{aligned}
&\delta_m^Y = 0, \quad \text{if} \quad m\notin\mathscr{A}\cup\mathscr{B},\\
&\delta_m^{RL} = 1 \quad \text{if} \quad m\in\mathscr{A}^R,\\
&\delta_m^{RR} = 1 \quad \text{if} \quad m\in\mathscr{B}^R,\\
&\delta_m^{LR} = 1 \quad \text{if} \quad m\in\mathscr{A}^L,\\
&\delta_m^{LL} = 1 \quad \text{if} \quad m\in\mathscr{B}^L.
\end{aligned}$$

Now w.l.o.g. we consider two cases: $\alpha_m^R=\alpha_m^L$ and $\alpha_m^R>\alpha_m^L$.

If $\alpha_m^R=\alpha_m^L$, by summing up the inequalities (3.44)-(3.47) we straightforwardly have

$$|\{t\in\{1,2,\ldots,T\}: M_t(m\pm1,m),M_t(m,m\pm1)\neq\sigma\}|\geq(4\alpha_m^R-2)RT \tag{3.48}$$

which suggests that $R\leq\frac{1}{4\alpha_m^R-2}$ and (3.41) holds.

If $\alpha_m^R>\alpha_m^L$, then we consider node $m+1$ and the following inequality

$$|\{t\in\{1,2,\ldots,T\}: M_t(m+1,m+2)\neq\sigma\}|\geq(\alpha_{m+1}^R-\delta_{m+1}^{RR})RT, \tag{3.49}$$

which directly follows from (3.45). By our model, since a node can be at most one source and one destination, we have $\alpha_{m+1}^R\geq\alpha_m^R-1$. Hence, $\alpha_{m+1}^R-\delta_{m+1}^{RR}\geq\alpha_m^R-2$. Noticing

that for any t, $M_t(m+1,m+2) \neq \sigma$ and $M_t(m,m-1) \neq \sigma$ is possible, we combine (3.49) and (3.47) and have

$$|\{t \in \{1,2,\ldots,T\} : M_t(m+1,m+2), M_t(m,m-1) \neq \sigma\}| \geq (\alpha_m^R - 2)RT \tag{3.50}$$

Combining (3.50) with (3.44)-(3.46) we have

$$|\{t \in \{1,2,\ldots,T\} : M_t(m \pm 1,m), M_t(m,m \pm 1), M(m+1,m+2) \neq \sigma\}| \geq (3\alpha_m^R + \alpha_m^L - 4)RT \tag{3.51}$$

and (3.41) directly follows.

In all other three modes, similar arguments can be used to obtain the result in (3.42) and (3.43). We thus finish the proof. ■

3.5.3. LOWER BOUNDS

Firstly, we give the lower bounds on common rates in the following lemma.

Lemma 3.5.2 (Lower bounds for common rates in line networks)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *in mode* $X \in \{\text{PP},\text{BP},\text{PM},\text{BM}\}$*, the common rate is lower bounded by* C_L^X *specified by*

$$C_L^{\text{PP}} = \frac{1}{\max_{m=1}^{N}(3\alpha_m^{\max} + \alpha_m^{\min} + 3)}, \tag{3.52}$$

$$C_L^{\text{BP}} = \frac{1}{\max_{m=1}^{N}(3\alpha_m^{\max})}, \tag{3.53}$$

$$C_L^{\text{PM}} = \frac{1}{\max_{m=1}^{N}(3\alpha_m^{\max} + 8)}, \tag{3.54}$$

$$C_L^{\text{BM}} = \frac{1}{\max_{m=1}^{N}(2\alpha_m^{\max} + 8)}. \tag{3.55}$$

We then prove this lemma by giving scheduling schemes and coding schemes with common rates achieving these lower bounds. In particular, we first give the scheduling scheme in each mode with the following properties.

Property 3.5.1. Each round includes F_L^X time slots, where $X \in \{\text{PP},\text{BP},\text{PM},\text{BM}\}$ and $F_L^X = 1/C_L^X$.

Property 3.5.2. The transmissions in each time slot do not violate the constraints in (3.21)–(3.24).

Property 3.5.3. The transmissions are assigned in such a way that for any session, the source and all involved relay nodes have 1 transmission to send the message.

The schedule is described by specifying the edge, the time slot, and the content for each transmission. For PP mode, similar to the bidirectional session scenario, we will use the notation $L_t(u,v)$ to specify the session, i.e., the equation $L_t(u,v) = S_i$ stands for "the transmission on edge (u,v) in time slot t is assigned to session S_i".

Then, for BP, PM, and BM modes, coding schemes are given such that a new message can be reliably decoded at the destination for each session in each round.

PP MODE

In PP mode, we introduce an algorithm which iteratively generates a transmission schedule for a round.

Here, we assume the time slots in a round are numbered as $1,2,\ldots$. During the iterative process, we define $\tilde{\mathscr{J}}_m^R$ as the set of sessions directed to the right involved by node m which have already been assigned by some time slots for transmission, i.e., at a certain stage of the iteration, $\tilde{\mathscr{J}}_m^R = \{S_i \in \mathscr{J}_m^R | \forall t, S_i \neq L_t(m,m+1)\}$. We further define $\bar{\mathscr{J}}_m^R = \mathscr{J}_m^R \backslash \tilde{\mathscr{J}}_m^R$ and define $\tilde{\mathscr{J}}_m^L$ and $\bar{\mathscr{J}}_m^L$ similarly. Moreover, the notation $\mathscr{T}(u,v)$ is used for $\{t|L_t(u,v) \neq 0\}$ and $\bar{\mathscr{T}}(u,v)$ for $\{t|L_t(u,v) = 0\}$.

1: **Initialization** For all t and $(u,v), |u-v| = 1, u, v \in \{-4,-3,\ldots,N\}$, set $L_t(u,v) = 0$
2: **for** $m = 1$ to N **do**
3: **while** $\tilde{\mathscr{J}}_m^R \neq \emptyset \vee \tilde{\mathscr{J}}_m^L \neq \emptyset$ **do**
4: **while** $\mathscr{T}(m-1,m-2) \cap \bar{\mathscr{T}}(m,m+1) \notin \emptyset$ **do**
5: $\tau \leftarrow \min_{t \in \mathscr{T}(m-1,m-2) \cap \bar{\mathscr{T}}(m,m+1)} t$, $j \leftarrow \min_{S_i \in \tilde{\mathscr{J}}_m^R} i$, $L_\tau(m,m+1) \leftarrow S_j$
6: **end while**
7: **while** $\mathscr{T}(m-3,m-2) \cap \bar{\mathscr{T}}(m,m-1) \notin \emptyset$ **do**
8: $\tau \leftarrow \min_{t \in \mathscr{T}(m-3,m-2) \cap \bar{\mathscr{T}}(m,m-1)} t$, $j \leftarrow \min_{S_i \in \tilde{\mathscr{J}}_m^L} i$, $L_\tau(m,m-1) \leftarrow S_j$
9: **end while**
10: **if** $\tilde{\mathscr{J}}_m^R \neq \emptyset$ **then**
11: $\tau \leftarrow \min_{t \in \bar{\mathscr{T}}(m-1,m-2) \cap \bar{\mathscr{T}}(m-1,m) \cap \bar{\mathscr{T}}(m-2,m-1) \cap \bar{\mathscr{T}}(m,m+1)} t$, $j \leftarrow \min_{S_i \in \tilde{\mathscr{J}}_m^R} i$, $L_\tau(m,m+1) \leftarrow S_j$
12: **end if**
13: **if** $\tilde{\mathscr{J}}_m^L \neq \emptyset$ **then**
14: $\tau \leftarrow \min_{t \in \bar{\mathscr{T}}(m-1,m-2) \cap \bar{\mathscr{T}}(m-1,m) \cap \bar{\mathscr{T}}(m-2,m-1) \cap \bar{\mathscr{T}}(m-2,m-3) \cap \bar{\mathscr{T}}(m,m+1) \cap \bar{\mathscr{T}}(m,m-1)} t$, $j \leftarrow \min_{S_i \in \tilde{\mathscr{J}}_m^L} i$, $L_\tau(m,m-1) \leftarrow S_j$
15: **end if**
16: **end while**
17: **end for**

This algorithm is basically a greedy algorithm, in which from the first node to the last, the first appropriate time slot is assigned to the first unassigned session until each session involved by this node has been assigned with a time slot to transmit. By appropriate time slots, we mean that the time slots in which node $m-1$ transmits to the left are prioritized for node m to transmit to the right, and the time slots in which node $m-3$ transmits to the right are prioritized for node m to transmit to the left (line 4-9). After this, the algorithm considers the unassigned time slots which are not violating all previous assigned transmissions according to (3.21) as appropriate time slots (line 10-15). Now, we prove that the schedule generated by this algorithm has no more than F_L^{PP} time slots, i.e.

Statement 3.5.1.

$$\max_{L_t(u,v) \neq 0} t \leq F_L^{\mathrm{PP}} \tag{3.56}$$

holds for the schedule generated by this algorithm.

Proof:

This statement can be proved by deduction. We firstly introduce a local version of the constraint of (3.56) as

$$\max_{L_t(m,m\pm1)\neq 0} t \leq F_L^{\mathrm{PP}}. \tag{3.57}$$

Firstly, for node 1, if it is not a source node, then it does not involve in any sessions and (3.57) holds obviously. If it is a source node, then by our algorithm the transmission is scheduled in the first time slot during the first iteration and (3.57) holds.

Then, for a chosen node m, we assume that for all nodes $m' \leq m-1$ the equation (3.57) holds. We then prove that (3.57) also holds for node m.

We define $\tau_1^R, \tau_1^L, \tau_2^R, \tau_2^L$ as the assigned time slot with the largest index after the assignments in line 4-6, 7-9, 10-12, and 12-15, respectively. Clearly, the first two assignments only assign the time slots which has already been used for other assigned transmissions, which will not violate (3.57) if (3.57) holds for all nodes $m' \leq m-1$. Hence, we only consider the case that $\tau_2^L \neq \tau_1^L$, which suggests that there are time slots assigned by line (10-15), in the following two cases

- Firstly we assume $\tau_2^L = \tau_2^R$, which suggests that no time slots are assigned in line (12-15). In this case, we have

  $$\tau_1^R = \alpha_{m-1}^L \tag{3.58}$$

  and

  $$\tau_1^L - \tau_1^R = \alpha_m^L. \tag{3.59}$$

  By our algorithm, we have

  $$\begin{aligned} \tau_2^R &= \tau_1^L + \alpha_{m-1}^R + \alpha_{m-2}^R + \alpha_m^R - \tau_1^R \\ &= \alpha_m^L + \alpha_{m-1}^R + \alpha_{m-2}^R + \alpha_m^R \\ &\leq 3\alpha_m^R + \alpha_m^L + 3 \\ &\leq F_L^{\mathrm{PP}}. \end{aligned} \tag{3.60}$$

  The second equality follows from (3.59). The first inequality follows from our model assumption that a node can only be the source or destination for at most one session, which suggests

  $$\alpha_{m-1}^R \geq \alpha_m^R - 1, \tag{3.61}$$

  $$\alpha_{m-1}^L \geq \alpha_m^L - 1, \tag{3.62}$$

  $$\alpha_{m-1}^R + \alpha_{m-1}^L \geq \alpha_m^R + \alpha_m^L - 1. \tag{3.63}$$

- Then, we consider the case $\tau_2^L \neq \tau_2^R$ which suggests that there are time slots assigned in line (12-15). In this case, by our algorithm we have

  $$\tau_2^L = \max(\alpha_m^R, \alpha_{m-1}^L) + \max(\alpha_{m-1}^R, \alpha_{m-2}^L) - \alpha_{m-2}^R + \alpha_m^L. \tag{3.64}$$

  This equality simply follows from the way that the transmissions are assigned in our algorithm. Then, by (3.62), (3.63), and the definition of F_L^{PP}, we can discuss the RHS of (3.64) in different cases and prove that it is no larger than F_L^{PP}.

■

BP MODE

In BP mode, a fix schedule is used for the transmissions of all nodes. For node m, the time slots $\{t \in \{1,2,\ldots,F_L^{\mathrm{BP}}\} | t \pmod 3 \equiv m \pmod 3\}$ are given for its transmission. This schedule guarantees that each node will have enough time slots to handle the transmissions for each of its involved sessions. This is because the number of time slots given to the nodes for transmission is $F_L^{\mathrm{BP}}/3 = \max_{m=1}^{N} \alpha_m^{\max}$, which is no less than $\alpha_m^{\max}$ for any m.

Note that for a chance given for transmission, the node can either use it to transmit the message for one session or broadcast a linear sum of two messages for two sessions of opposite directions. The neighboring nodes that receive this linear sum decode the individual messages with their prior knowledge. Hence, any transmitted linear sum is directly decoded at the receivers and will not propagate to other nodes. This network coding scheme guarantees that all the messages are decodable at their destinations.

PM MODE

For PM mode, a similar schedule scheme as BP mode cannot be used due to the differences in NC schemes. For BP mode, the nodes locally decode the messages and re-encode them for the transmission in the next round. The linear sum of two messages will not propagate to more than one hop. However, it is not the case for PM mode and BM mode, in which some of the intermediate relay nodes cannot decode the individual messages but only the linear sum. Hence, we propose a bundling scheme which combines two groups of sessions directed to the left and right, respectively, into a group of unidirectional sessions and bidirectional sessions.

Bundling Scheme Firstly, we define a set of sessions called the *right cluster*, denoted as $\mathscr{C}_k^R, k \in \mathbb{Z}^+$. A right cluster is found with the following steps.

- 1, Find the right session with the smallest index which is not in any right cluster $S_i = (a_i, b_i)$.
- 2, Find the right session which is not in any right cluster and its destination is the closest to a_i at the left side, i.e., $S_j : a_i - b_j = \min_{S_j \notin \mathscr{C}_k^R}(a_i - b_j)$. We call session S_j the *closest left neighboring session of* S_i.
- 3, Iteratively find the closest left neighboring session of S_j and all the sessions found this way.
- 4, Similarly, find the closest right neighboring sessions of S_i denoted by S_l, i.e., $S_l : a_l - b_i = \min_{S_l \notin \mathscr{C}_k^R \forall k}(a_l - b_i)$.
- 5, Iteratively find the closest right neighboring session of S_l and all the sessions found this way.
- 6, The set of all the sessions found in step 1-5 is a right cluster.

We can find all right clusters with the above steps. It can be easily proved that there are precisely $\max_{m=1}^{N} \alpha_m^R$ right clusters. Similarly, we denote the left clusters as $\mathscr{C}_k^L$ and find all left clusters in the same fashion. Clearly, $k \le \max_{m=1}^{N} \alpha_m^L \forall \mathscr{C}_k^L$.

We then construct bundles by combining a right cluster and a left cluster, more precisely, we construct the bundle $\mathscr{D}_k = (\mathscr{C}_k^R, \mathscr{C}_k^L), k \leq \min(\max_{m=1}^N \alpha_m^R, \max_{m=1}^N \alpha_m^L)$. We call the right or left clusters which are not combined into any bundle as *leftover clusters*.

As a result, the sessions are combined into a set of bundles and leftover clusters.

Scheduling Now we propose a scheduling scheme for these bundles and leftover clusters. Before that, we first give the definition of *edge transmissions*.

Definition 3.5.1 (Edge transmissions)**.** Inside a bundle $\mathscr{D}_k = (\mathscr{C}_k^R, \mathscr{C}_k^L)$, if a transmission $L_t(u,v), |u-v| = 1$ falls into one of the following four categories, we call it an edge transmission.

Category 1: $L_t(u,v) = S_i, S_i \in \mathscr{C}_k^R, \exists S_j = (a_j, b_j) \in \mathscr{C}_k^L, a_j = u.$

Category 2: $L_t(u,v) = S_i, S_i \in \mathscr{C}_k^R, \exists S_j = (a_j, b_j) \in \mathscr{C}_k^L, b_j = v.$

Category 3: $L_t(u,v) = S_i, S_i \in \mathscr{C}_k^L, \exists S_j = (a_j, b_j) \in \mathscr{C}_k^R, a_j = u.$

Category 4: $L_t(u,v) = S_i, S_i \in \mathscr{C}_k^L, \exists S_j = (a_j, b_j) \in \mathscr{C}_k^R, b_j = v.$

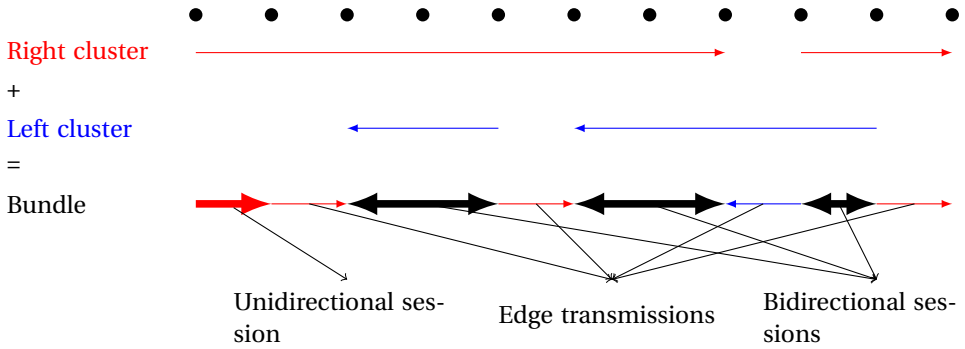


Figure 3.5: The bundling of a right cluster and a left cluster into a bundle containing unidirectional sessions, edge transmissions, and bidirectional sessions

For any bundle, it can be decomposed into a group of bidirectional sessions, unidirectional sessions, and edge transmissions as shown in Fig 3.5. These unidirectional sessions and bidirectional sessions are not overlapping. Moreover, the sessions inside any leftover cluster are also not overlapping. Hence, we can use the scheduling scheme for PM mode in Subsection 3.4.3 and schedule the bidirectional sessions and unidirectional sessions in any bundle or leftover cluster as if it is one bidirectional session with some transmissions skipped. Since the total number of bundles plus the leftover clusters is $\max_{m=1}^N \alpha_m^{\max}$, by (3.31), we can schedule all these transmissions in no more than $3\alpha_m^{\max}$ time slots.

Then we schedule the edge transmissions of all bundles. It can be proved that for each edge (u,v), there are at most two overlapping edge transmissions, i.e., for each edge

(u,v), if there exist an edge transmission $L_t(u,v)$ in any bundle, then there exists at most one other edge transmission $L_{t'}(u,v)$, $t' \neq t$ in all bundles.

This statement can be proved by contradiction: W.l.o.g. we consider an edge $(u,u+1)$. By the definition of edge transmissions, if $L_t(u,u+1)$ is an edge transmission, it must fall into either Category 1 or 2. Assuming there are more than two of such edge transmissions, we can conclude that at least two of them fall into the same category. We denote two of them by $L_\tau(u,u+1) = S_i$ and $L_{\tau'}(u,u+1) = S_j$. Then by the definition of edge transmission, u is the source or $u+1$ is the destination for both S_i and S_j, which contradicts our model.

By the scheduling scheme for PP mode in Subsection 3.4.3, all the edges transmissions can be arranged in 8 time slots with no violation to (3.21), thus they do not violate (3.23) as well.

As a result, the total number of time slots for this scheduling scheme is $3\alpha_m^{\max}+8$.

Coding Here, we only needs to code the decomposed bidirectional sessions for each bundle. The coding scheme is identical to the one used for PM mode in Subsection 3.4.3.

BM MODE

In this mode, with the same bundling and decomposing approaches as PM mode, as well as the scheduling and coding schemes of Subsection 3.4.3 for BM mode, the common rate in (3.55) is achieved.

3.5.4. THROUGHPUT BENEFIT

By the definition of the improvement factor, we have the following theorem.

Theorem 3.5.1 (Throughput benefit in line networks)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$*, the improvement factors are upper bounded by*

$$I_{\mathrm{PP}}^{\mathrm{BM}} \leq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}+3)}{\max_{m=1}^{N}(2\alpha_m^{\max}-2)}, \tag{3.65}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}}, I_{\mathrm{PP}}^{\mathrm{PM}} \leq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}+3)}{\max_{m=1}^{N}(3\alpha_m^{\max}-4)}, \tag{3.66}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}} \leq \frac{\max_{m=1}^{N}(3\alpha_m^{\max})}{\max_{m=1}^{N}(2\alpha_m^{\max}-2)}, \tag{3.67}$$

$$I_{\mathrm{PM}}^{\mathrm{BM}} \leq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+8)}{\max_{m=1}^{N}(2\alpha_m^{\max}-2)}, \tag{3.68}$$

and lower bounded by

$$I_{\mathrm{PP}}^{\mathrm{BM}} \geq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}-4)}{\max_{m=1}^{N}(2\alpha_m^{\max}+8)}, \tag{3.69}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}} \geq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}-4)}{\max_{m=1}^{N}(3\alpha_m^{\max})}, \tag{3.70}$$

$$I_{\mathrm{PP}}^{\mathrm{PM}} \geq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}+\alpha_m^{\min}-4)}{\max_{m=1}^{N}(3\alpha_m^{\max}+8)}, \tag{3.71}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}}, I_{\mathrm{PM}}^{\mathrm{BM}} \geq \frac{\max_{m=1}^{N}(3\alpha_m^{\max}-4)}{\max_{m=1}^{N}(2\alpha_m^{\max}+8)}. \tag{3.72}$$

These bounds are asymptotically tight if $\max_{i=1}^{N}\alpha_m^{\max}\to\infty$. In particular, if the sessions are uniformly distributed as random, we have the following corollary.

Corollary 3.5.1. *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *with* $N\to\infty$*, if the right and left sessions are distributed uniformly at random with probabilities* p_1 *and* p_2*, respectively, i.e., a node can be the source or destination of a right or left transmission with the probabilities of* $p_1/2$ *and* $p_2/2$*, respectively, the improvement factors are*

$$I_{\mathrm{PP}}^{\mathrm{BM}} = 1.5+\frac{\min(p_1,p_2)}{2\max(p_1,p_2)}, \tag{3.73}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PP}}^{\mathrm{PM}} = 1+\frac{\min(p_1,p_2)}{3\max(p_1,p_2)}, \tag{3.74}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}} = I_{\mathrm{PM}}^{\mathrm{BM}} = 1.5. \tag{3.75}$$

From this corollary, it is also clear that the improvement factors are identical to the bidirectional session case if $p_1=p_2$. Moreover, if all sessions have the same direction, i.e., $p_1=0$ or $p_2=0$, BP and PM mode do not have any improvement, but BM mode has a 1.5 improvement factor over all three other modes. In Fig. 3.6(a)-3.6(c) we show the upper bounds and the lower bounds of the improvement factors for $p_1=p_2=0.2$ as a function of the number of nodes N.

Then, if $p_1=p_2$, we have the following corollary, in which the improvement factor is identical to the improvement factor for the bidirectional session case when $N\to\infty$ and sessions are uniformly distributed.

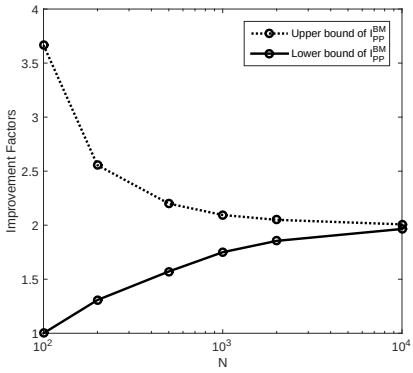
Corollary 3.5.2. *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$ *with* $N\to\infty$*, if the right and left sessions are distributed uniformly at random with the same probability, the improvement factors are*

$$I_{\mathrm{PP}}^{\mathrm{BM}} = 2, \tag{3.76}$$

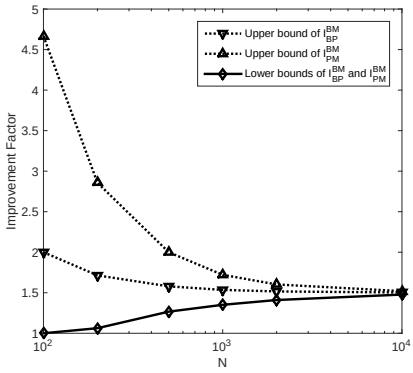
$$I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PP}}^{\mathrm{PM}} = 4/3, \tag{3.77}$$

$$I_{\mathrm{BP}}^{\mathrm{BM}} = I_{\mathrm{PM}}^{\mathrm{BM}} = 3/2. \tag{3.78}$$

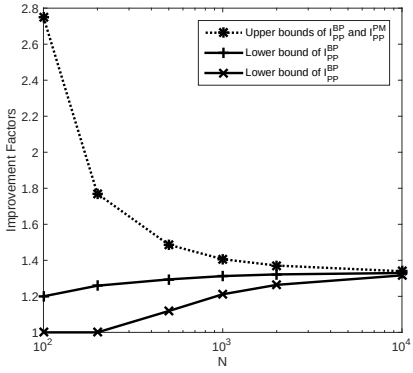
By the results of this section and the previous section, we conclude that for large line networks with heavy and balanced traffic (the numbers of the left and right sessions



(a) $I_{\mathrm{PP}}^{\mathrm{BM}}$



(b) $I_{\mathrm{BP}}^{\mathrm{BM}}$ and $I_{\mathrm{PM}}^{\mathrm{BM}}$



(c) $I_{\mathrm{PP}}^{\mathrm{BP}}$ and $I_{\mathrm{PP}}^{\mathrm{PM}}$

Figure 3.6: The upper bounds and lower bounds of the improvement factors in line networks with sessions uniformly distributed at random with $p_1 = p_2 = 0.2$, simulated over 10000 randomly generated networks.

involved by the bottleneck nodes are large and equal), the improvement of CF over traditional routing and NC are 2 and 1.5, respectively. For different transmission modes and different type of session placements (bidirectional or arbitrary), upper bounds have been derived and lower bounds are given by proposing scheduling and coding schemes. One interesting remark is that, if the traffic for the line network is unbalanced, the improvement of NC over traditional routing can be very limited or even no improvement at all. However, in this case, CF still has an improvement factor of around 1.5 over traditional routing.

3.6. LINE NETWORKS WITH RANDOM ACCESS

In Section 3.4 and 3.5, the throughput benefit of CF in line networks with centralized scheduling has been considered, which is not applicable in many practical scenarios. In this section, line networks in which the nodes do not have fixed schedules, in particular, the case that all nodes apply plain random access mechanism, is considered. It is shown that in this case, CF can bring even higher benefit on the throughput over traditional routing and NC than the cases that fixed scheduling is used.

3.6.1. MODEL

In this section, line networks with only one bidirectional session with terminals placed on both ends of the line, i.e., $\mathscr{S} = \{(1,N),(N,1)\}$, are considered. The messages transmitted by the left and right terminals are denoted by $x^R(i), x^L(i) \in \mathbb{F}_q, i \in \{1,2,\ldots,M\}$.

The key feature of this problem is the random access scheduling mechanism. Assume that all nodes apply the plain random access approach, i.e., in each time slot each node chooses its state to be transmit state or receive state with probability p and $1-p$ ($p \in [0,1]$ is a fixed constant), respectively. This choice is independent of the state in other time slots and other nodes. For PP mode and PM mode, we assume that each node has equal probability of transmitting to either direction.

3.6.2. CODING SCHEME

In this subsection, a coding scheme based on random linear network coding is proposed. This coding scheme can be used in all three of BP, PM, and BM modes. The essence of the scheme is that we guarantee that only innovative messages are transmitted. The scheme consists of the following elements:

- Assume that each node keeps three buffers of sufficiently large size, denoted by B, B^R and B^L, respectively. The use of the buffers will be explained below.
- Define the messages in the buffers of node m as $y_m(i) : i = 1,2,\ldots,M_m$, $y_m^R(i) : i = 1,2,\ldots,M_m^R$, and $y_m^L(i) : i = 1,2,\ldots,M_m^L$, where M_m, M_m^R, and M_m^L are the number of messages in B, B^R, and B^L, respectively. These messages can be expressed as

$$y_m(i) = \sum_{j=1}^{M} g_m(i,j)x^R(j) + \sum_{j=1}^{M} h_m(i,j)x^L(j), \tag{3.79}$$

$$y_m^R(i) = \sum_{j=1}^{M} g_m^R(i,j)x^R(j) + \sum_{j=1}^{M} h_m^R(i,j)x^L(j), \tag{3.80}$$

$$y_m^L(i) = \sum_{j=1}^{M} g_m^L(i,j)x^R(j) + \sum_{j=1}^{M} h_m^L(i,j)x^L(j), \tag{3.81}$$

  where $g_m(i,j), g_m^R(i,j), g_m^L(i,j), h_m(i,j), h_m^R(i,j)$, and $h_m^L(i,j)$ are coefficients from $\mathbb{F}_{q'}$ which is a subspace of $\mathbb{F}_q$.
- Next, $M_m \times M$ matrices G_m and H_m are constructed by setting $g_m(i,j)$ and $h_m(i,j)$, respectively, as the element in its ith row and jth column. Similarly, we construct G_m^R, H_m^R, G_m^L, and H_m^L.

- Assume that node m knows all elements in these matrices, i.e. a node knows which linear combination of messages is being received. This can be guaranteed if we allow the coding coefficients to be communicated without CF. The overhead is negligible since the coefficients are chosen from a subspace of $\mathbb{F}_q$. The size of the subspace should be chosen sufficiently large w.r.t. N. However, $\mathbb{F}_q$ can be chosen to be arbitrarily large.

Now, the scheme operates as follows. Initially, assume that all buffers in all nodes are empty. In each time slot all nodes perform the following steps:

Step 1 For each node, all receptions directly enter B (for the sources nodes on both ends of the network, the original messages directly enter B).

Step 2 At the beginning of each time slot, each node updates the matrices G_m^R, H_m^R, G_m^L, and H_m^L. Initialize the transmission by setting $y_m^* = \sigma$ (σ is the silent symbol defined in Section 3.2).

Step 3 Node m chooses coefficients $c(i)$ uniformly at random from $\mathbb{F}_{q'}, i \in \{1,2,\ldots,M_m\}$ and let y_m^* to be equal to a random linear combination of all $y_m(i)$, i.e., $y_m^* = \sum_{i=1}^{M_m} c(i) y_m(i) = \sum_{j=1}^{M} g_m^*(j) x^R(j) + \sum_{j=1}^{M} h_m^*(j) x^L(j), g_m^*(j), h_m^*(j) \in \mathbb{F}_{q'}$.

Step 4 Each node does the innovative check. Firstly, if $\text{rank}(G_m) > \text{rank}(G_m^R)$ and the vector $[g_m^*(j)], j \in \{1,2,\ldots,M\}$ is not linearly independent of all the rows in G_m^R, it discards y_m^* and goes back to Step 3. It then does the same check for the vector $[h_m^*(j)]$. These two steps are repeated until an innovative message y is generated, which is feasible in limited numbers of iterations if $\mathbb{F}_{q'}$ is chosen properly.

Step 5 If node m is in transmit state in this time slot, it transmits y_m^*. The transmission can be a broadcast (in BP and BM mode) or a transmission to one of its neighbors (in PM mode). If this transmission is successful to the right (the transmitted message is received by its right neighbor, i.e., the right neighbor is at receive state in this time slot), then it adds y_m^* to buffer B^R. Symmetrically, y_m^* is added to B^L if this transmission is successful to the left.

3.6.3. PERFORMANCE

In this subsection, the key result of this section is presented, which is the maximum achievable throughput of CF in line networks with random access.

Theorem 3.6.1 (Capacities of line networks with random access)**.** *For a line network with random access, the capacity for both directions is C_R^X in mode $X \in \{PP, BP, PM, BM\}$, where*

$$C_R^{\text{PP}} = p(1-p)^2/2, \tag{3.82}$$
$$C_R^{\text{BP}} = p(1-p)^2, \tag{3.83}$$
$$C_R^{\text{PM}} = p(1-p)/2, \tag{3.84}$$
$$C_R^{\text{BM}} = p(1-p). \tag{3.85}$$

These capacities can be achieved by using the schemes introduced in the previous subsection.

In PP mode no coding is applied and the capacity has already been given in [35]. Here, we show the proof of the capacity for mode $X \in \{\text{BP}, \text{PM}, \text{BM}\}$.

Proof. **Achievability:** We first consider only the session from left to right, assuming that the right source is not transmitting anything. In this case we can interpret the operation of the scheme as follows. Innovative packets are carried through the network over a series of links from left to right. These links are unreliable in the sense that due to random access and half duplex constraints they are not always available. Observe that the scheme that we described above is exactly the scheme used by Lun et al. in [28]. Therefore, for mode $X \in \{\text{BP}, \text{PM}, \text{BM}\}$ it follows directly from [28, Theorem 2] that we can achieve a rate C_R^X for the left-to-right session. Note, our PM and BM mode does not require any generalizations of the models from [28] in which broadcast, but not CF, is allowed. Even though our underlying model has CF, the abstraction described above is that of innovative packets being transmitted over a directed graph.

Next, we include the other session. Observe that the two sessions can be analyzed independently. More precisely, if both sources are transmitting packets, the flow of innovative packets for each of the sessions can be analyzed by ignoring the other session. Once enough innovative packets are collected at the receiver it can subtract the (linear combinations of) packets from the session for which it is the source and decode the packets from the other source.

Optimality: Since the network is symmetric, we focus on the capacity along one direction only. Following the max-flow min-cut theorem, the capacity of this network is bounded by the capacity of each edge.

We consider an individual edge. In BP mode, with probability p a messages is transmitted. However, the transmit is successful if and only if its neighbor is at receive state and its two-hop neighbor is not at transmit state. Hence the probability of a successful transmission is $p(1-p)^2$. In PM mode, a transmission to one direction is made with the probability of $p/2$. The neighbor can successfully receive it as long as it is in receive state. Its two-hop neighbor can be in transmit state and will not violate this transmission due our model set-up. The probability of a successful transmission is thus $p(1-p)/2$. With the similar argument, we have the probability for a successful transmission in BM mode equals to $p(1-p)$.

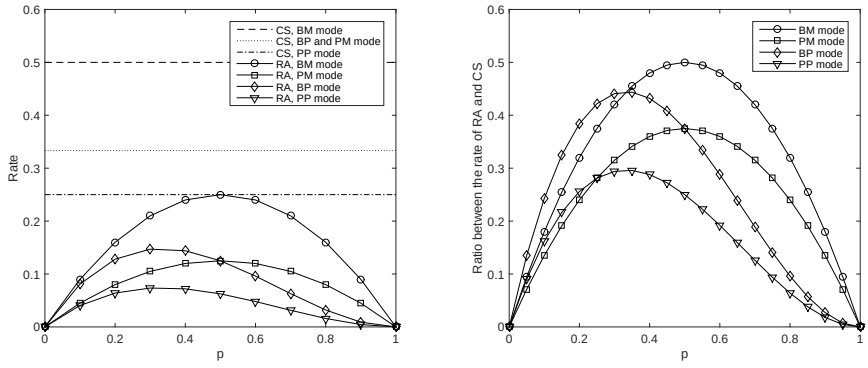
Hence, each edge can be considered as an erasure channel with erasure probability $1-C_R^X$, $X \in \{\text{BP}, \text{PM}, \text{BM}\}$ and the capacity of each edge as well as the network are C_R^X. As a result, the throughput of our scheme is optimal. □

Remark 3.6.1. The results of Theorem 3.6.3 in PP and BP mode are identical to the results shown in [35, Theorem 6], in which a different scheme is used in BP mode.

Here, our results are compared between various transmission modes. Figure 3.7(a) shows the comparison of the rate of either centralized scheduling (CS) and random access (RA) schemes in the four modes, in which the CS case is just the result obtained in Section 3.4. As observed, in RA case, the performance of BM mode is significantly higher than PP and BP mode. If we allow the probability of transmission p to be adjusted to the modes, then the rates will be maximized in BP and PP modes when $p = 1/3$. The maximum achievable rates are 0.074 and 0.148, respectively. In PM and BM mode, the

maximum rate 0.125 and 0.25 are achieved when $p = 1/2$. Hence, the maximum achievable rates in PP, BP, and PM modes are improved by factors of 3.378, 1.689, and 2, respectively. These improvement factors are significantly higher than for the case of centralized scheduling shown in Theorem 3.4.1, which has factors of 2, 1.5, and 1.5, respectively.

Figure 3.7(b) shows the ratio between the rates of random access and the rates of centralized scheduling for various transmission modes. In other words, it shows the compatibility of these transmission modes with random access. As the figure shows, in BM mode, the random access scheduling mechanism utilizes the network in a more efficient way.



(a) The rates for various modes

(b) The ratio between the rates of random access and centralized scheduling

Figure 3.7: The throughput performance of various modes in the line network using random access.

Then, straightforwardly we have the improvement factors in line networks with the random access setting.

Theorem 3.6.2 (Throughput benefit in line networks with random access)**.** *For a line network* $\mathbf{L}(\mathcal{V},\mathcal{E},\mathcal{S})$, $\mathcal{S} = \{(1,N),(N,1)\}$, *if the random access scheduling mechanism is applied, the improvement factors are given by*

$$I_{\mathrm{PP}}^{\mathrm{BM}} = \frac{2}{1-p}, \tag{3.86}$$

$$I_{\mathrm{PP}}^{\mathrm{BP}} = I_{\mathrm{PM}}^{\mathrm{BM}} = 2, \tag{3.87}$$

$$I_{\mathrm{PP}}^{\mathrm{PM}} = I_{\mathrm{BP}}^{\mathrm{BM}} = \frac{1}{1-p}, \tag{3.88}$$

$$I_{\mathrm{BP}}^{\mathrm{PM}} = \frac{1}{2(1-p)}. \tag{3.89}$$

By this theorem, it is clear that CF also brings significant improvement on the throughput in line networks for the random access case. Comparing the result of Theorem 3.6.2 to Theorem 3.4.1, it can be observed that the improvement of BM and PM modes over

PP and BP modes is unbounded if p is close to 1, which are much higher than that for the centralized scheduling case. It indicates that CF has great potential to be applied with random access, since it turns the collisions in traditional routing or NC into useful transmissions.

3.7. CONCLUSION

In this chapter, upper bounds for the throughput benefit of CF over traditional routing for networks with multiple unicast sessions are derived. For general networks, we upper bounded the improvement by $3K$ and found a special type of networks in which CF brings an improvement of at least $K/2$. For $K = 3$ or 4, this special network can be represented by a hexagon or a cube with relays in their centers. However, if K is large, no geometric representation for these networks has yet been found. Hence, it remains as an interesting problem to find practical networks in which the throughput benefit of CF is higher than 2.

In line networks, if centralized scheduling is used and the traffic load of both directions is balanced, it is proved that the improvement factor of CF over traditional routing is upper bounded by a constant which is 2 or very close to 2, depending on the session placement. Also, a CF based scheme is proposed which gives an asymptotically tight lower bound when the number of the sessions is large. For unbalanced traffic cases, despite that NC is sometimes not beneficial, CF can still improve the throughput by a factor of around 1.5. It is an important observation that CF also benefits the throughput of unidirectional transmissions in line networks, which is essentially different from NC.

If the random access scheme is used instead of centralized scheduling schemes in line networks, the upper bounds on the throughput improvement factors of CF over traditional routing and NC are $\frac{2}{1-p}$ and $\frac{1}{1-p}$, respectively. A scheme that achieves this upper bound has been proposed for a bidirectional session with terminals at both ends of the line network. Note that this improvement is much higher than the improvement for the centralized scheduling cases when p is large, which shows a good compatibility of CF with random access. Clearly, random access is a mechanism which suffers a lot from collisions. However, CF can turn the collisions in traditional routing and NC into linear functions which are useful for communication. This feature has already been addressed in [11] for multi-user MAC. Here, it is shown that CF can also be applied with random access in line networks. Note that our scheme cannot be straightforwardly extended to arbitrary session cases, which leaves as an interesting problem for following studies.

4

ENERGY BENEFIT

In the previous chapter, the benefit of compute-and-forward (CF) in the perspective of throughput was considered. In this chapter, the attention is put on the benefit of CF on the energy saving aspect, which is another important problem in wireless networks since many wireless devices are battery-driven equipments with limited energy to transmit and receive signals. We follow the same path as the previous chapter: firstly, the upper bound of the energy benefit in general networks is derived, then the upper and lower bounds of the energy benefit in some specific networks are derived.

4.1. INTRODUCTION

Since network coding (NC) [1] was introduced, many studies considered the energy benefit of NC because it reduces the number of transmissions in wireless networks by letting the relay nodes transmit linear combinations of messages. A broadcast scenario has been considered in [8], in which both centralized and decentralized schedules are considered and matching upper and lower bounds are given on the energy benefit. The problem of the energy benefit of NC in the multiple unicasts case, on the other hand, is more complicated. Upper bounds have been given for the energy benefit of NC for some multiple unicast networks in [22, 26]. In some specific networks, namely hexagonal lattice networks, a lower bound on the energy benefit for multiple unicasts of 2.4 has been derived in [23], which has been further improved to 3 in [12].

The material in this chapter has appeared in

- Section 4.3

  Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "On the Energy Benefit of Compute-and-forward for Multiple Unicasts," Submitted to *IEEE Int. Symp. on Inf. Theory (ISIT)*, Barcelona, Spain, May, 2016.

- Section 4.5

  Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "On the energy benefit of compute-and-forward on the hexagonal lattice," *Proc. of the Thirty-Fifth WIC Symp. on Inf. Theory in Benelux*, Eindhoven, the Netherlands, May, 2014.

All of the above-mentioned studies considered the transmit energy only, which are not very practical in the scenarios that the energy consumed for receiving signals (for decoding, demodulation) is not negligible. Furthermore, it has also been shown in some studies, e.g., [13], that some NC based schemes decrease the number of transmissions at the cost of increasing the number of receptions. If the energy consumption for receiving is not negligible, some of the NC based schemes will have less improvement, or even no benefit at all. Hence, it is more general and practical to study the energy benefit in networks taking into account both the transmit and receive energy.

In this chapter, the energy benefit of CF, defined as the ratio of the minimum energy consumption by traditional routing techniques and the corresponding CF consumption, is studied for the multiple unicasts case with both transmit and receive energy considered. An upper bound on the energy benefit is given, which is $\min(\bar{d}, K, 12\sqrt{K})$. It shows that the upper bound depends on not only the number of the sessions, but also the average distance of the sessions. Also, if the number of the sessions K is large and the average distance scales faster than $\sqrt{K}$, the energy benefit is upper bounded by a factor of $\sqrt{K}$. This is a new scaling law for the energy benefit of CF and also NC in general networks with multiple unicast sessions. Furthermore, it is very different from the throughput benefit given in Section 3.3, which is proved to be upper bounded by $3K$ and there exists a network with the benefit of $K/2$.

Also, the upper bound of the energy benefit in some special networks, e.g., line and rectangular/hexagonal lattice networks, are considered. It is shown that the energy benefit is upper bounded by 2, 4, 6, and 3 for line networks, 2-D and 3-D rectangular lattice networks, and hexagonal lattice networks, respectively. Furthermore, if the network has a node which divides all sources from all destinations, CF will not benefit in energy consumption.

Further, lower bounds on the energy benefit are also studied in some specific networks. Achievable CF based schemes on hexagonal lattice networks with a specific session placement studied in [12] are given. By our schemes, the energy consumption is decreased by a factor between 2 and 3 comparing to the traditional routing and a factor between 1 and 3 comparing to the NC based scheme proposed in [12]. With some special transmit/receive power configurations, our schemes achieve the upper bound on the energy benefit of CF.

This chapter is organized as follows. In Section 4.2, we extend the model used in the previous chapter in energy aspect and introduce some important notations including the *energy improvement factor*. In Section 4.3, we give an upper bound of the energy improvement factor. In Section 4.4, we tighten the upper bound for some specific networks, namely star networks, line networks, and lattice networks. In Section 4.5 a new lower bound on the energy benefit in hexagonal lattice networks is given by proposing two CF based schemes which outperform all existing schemes on energy consumption for a specific session placement. At last, we conclude our results of this chapter in Section 4.6.

4.2. MODEL SET-UP AND NOTATIONS

In this section, we use the same network model $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$ and the transmission modes PP, BP, PM, and BM as introduced in Section 3.2.

Further, we introduce some new notations which describe the properties of the network. We use the notation d_i for the (hop-count) distance of session S_i and $d(u,v)$ for the distance between node u and v. Hence, $d_i = d(a_i, b_i)$. We further define $d(\mathcal{V}', m), \mathcal{V}' \subseteq \mathcal{V}, m \in \mathcal{V}$ as $d(\mathcal{V}', m) = \min_{u\in\mathcal{V}'} d(u,m)$ and define $d(m,\mathcal{V}')$ in the same fashion. We let $\bar{d} = \frac{\sum_{i=1}^{K} d_i}{K}$.

In this chapter, the energy consumption of any transmission scheme is always discussed in the context of a *round*. In each round, a transmission scheme should guarantee a new message from the corresponding source to be successfully decoded by each destination after the initial state of a long-term transmission. We then define E^X as the *minimum energy consumption* of any scheme for each round in mode $X \in \{\text{PP}, \text{BP}, \text{PM}, \text{BP}\}$. We use the notations e_t for the energy consumed (for broadcast, encoding, modulation, etc.) by a node to transmit (broadcast) a symbol from $\mathbb{F}_q$ to its neighbors and e_r for the energy consumed (for decoding, demodulation, etc.) by a node to receive a symbol (either one message or the sum of multiple messages) from $\mathbb{F}_q$.[1] The energy consumed for computing when CF is applied and all other energy consumption (supporting circuits, routing, signaling, etc.) are neglected. The *energy improvement factor* of mode X over mode Y is defined as

$$J_Y^X = E^Y / E^X. \tag{4.1}$$

4.3. UPPER BOUND OF GENERAL NETWORKS

In this section, the upper bound of the energy improvement factor of CF in general networks is studied. Here, only PP and BM modes are considered. The upper bound for the energy improvement factor $J_{\text{PP}}^{\text{BM}}$ are derived by studying lower bounds for E^{BM} and establishing an explicit expression for E^{PP}. Firstly, we give the main result of this section.

Theorem 4.3.1 (Upper bound of the energy benefit in general networks)**.** *For any network* $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$*, the energy benefit satisfies*

$$J_{\text{PP}}^{\text{BM}} \le \min(\bar{d}, K, 12\sqrt{K}). \tag{4.2}$$

In the following three subsections, three upper bound of $J_{\text{PP}}^{\text{BM}}$ which are $\bar{d}$, K, and $12\sqrt{K}$, respectively, will be derived.

4.3.1. THE $\bar{d}$ UPPER BOUND OF $J_{\text{PP}}^{\text{BM}}$

Firstly, the expression for the minimum energy consumption E^{PP} is given.

Lemma 4.3.1 (Minimum energy consumption in PP mode)**.** *For any network* $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$*, the minimum energy consumption in PP mode is*

$$E^{\text{PP}} = K\bar{d}(e_t + e_r). \tag{4.3}$$

[1] As introduced in [29] CF is based on lattice codes, which can be any linear code, e.g., low-density parity-check (LDPC) code, satisfying certain properties introduced in [7]. It is then clear that decoding a linear combination consumes no more energy than decoding a message encoded with the same linear channel codes in traditional routing. Hence, we assume that the decoding of both the individual message and the sum of multiple messages consumes energy e_r.

Proof:
An upper bound on the minimum energy consumption can be given by any valid transmission scheme. Here, we use the same transmission scheme described in the proof of Lemma 3.3.1 for all sessions, which consumes

$$E = \sum_{i=1}^{K} d_i(e_t + e_r) = K\bar{d}(e_t + e_r) \tag{4.4}$$

energy in each round. Hence we have the upper bound for E^{PP}. Then, it is clear that it is also the lower bound for E^{PP} since we assume that no network coding is allowed in PP mode. Hence, the shortest-path routing strategy is optimal. ■

In the following lemma, a distance based upper bound of $J_{\mathrm{PP}}^{\mathrm{BM}}$ is given.

Lemma 4.3.2. *For any network* $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$*, the energy benefit satisfies*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq \bar{d}. \tag{4.5}$$

Proof: The proof of this lemma is straightforward since in BM mode, each source needs to transmit once and each destination needs to receive once in each round. Thus we have

$$E^{\mathrm{BM}} \geq K(e_t + e_r). \tag{4.6}$$

Combining this with (4.1) and (4.3) we finish our proof. ■

4.3.2. THE K UPPER BOUND OF $J_{\mathrm{PP}}^{\mathrm{BM}}$

In the next lemma, we show that the energy improvement factor is upper bounded by the number of sessions.

Lemma 4.3.3. *For any network* $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$*, the energy benefit satisfies*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq K. \tag{4.7}$$

Proof:
Firstly, we introduce a notation N_r for the minimum number of non-source non-destination nodes needed to connect all sessions. More specifically, defining $\mathcal{V}^* \subseteq \mathcal{V}\setminus(\mathcal{A}\cup\mathcal{B})$ and $\mathcal{E}^* = \{(u,v) \in \mathcal{E} | u,v \in \mathcal{V}^* \cup \mathcal{A} \cup \mathcal{B}\}$, for a network $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$, if the network $\mathbf{N}(\mathcal{V}^* \cup \mathcal{A} \cup \mathcal{B}, \mathcal{E}^*, \mathcal{S})$ is also a valid network model (all the sessions are connected), then $|\mathcal{V}^*| \geq N_r$. In other words, there does not exist a non-source non-destination node set $\mathcal{V}^*$ with $|\mathcal{V}^*| < N_r$ such that $\mathbf{N}(\mathcal{V}^* \cup \mathcal{A} \cup \mathcal{B}, \mathcal{E}^*, \mathcal{S})$ is a valid network.

Then we can prove

$$E^{\mathrm{BM}} \geq (N_r + K)(e_t + e_r) \tag{4.8}$$

by contradiction: If there exist a transmission scheme which consumes energy

$$E' < (N_r + K)(e_t + e_r), \tag{4.9}$$

since the sources have to transmit at least K times and the destinations have to receive at least K times, it is clear that in this scheme the energy consumption of all the other nodes is less than $N_r(e_t+e_r)$. Since a node must transmit and receive at least once to function in

the network if it is not a source or destination, we conclude that in this scheme there are less than N_r non-source non-terminal nodes involved, which contradicts the definition of N_r.

Combining (4.1), (4.3), and (4.8) we have

$$J_{\text{PP}}^{\text{BM}} \leq \frac{\sum_{i=1}^{K} d_i}{N_r + K}. \tag{4.10}$$

Now we prove $\sum_{i=1}^{K} d_i \leq K(N_r - 1) + K(K+1)$ by considering the networks with the sum distance achieving this upper bound. More precisely, for given K and N_r, if a network $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$ has the maximum value of the sum distance $\sum_{i=1}^{K} d_i$ among all networks with the same K and N_r, it should have the following properties:

1. None of the sources is collocated with any destination. This can be proved by contradiction: Assume node u is both a_i and b_j, then we can find another network with node $u = a_i$, an additional node $v = b_j$, and edges $(u, v), (v, u)$ that has a larger sum distance.

2. It is a line network. Firstly, it is straightforward that the network is acyclic since the sum distance of any network with cycles can be increased by removing edges to break the cycles. Then, we prove that any node can have at most two neighbors by contradiction. Assume node u has neighbors v_1, v_2, and v_3. Since the network is acyclic, w.l.o.g. we assume v_3 is closer to $\mathcal{V}^*$, i.e., $d(v_3, \mathcal{V}^*) \leq d(v_1, \mathcal{V}^*) = d(v_2, \mathcal{V}^*)$. We consider the network with edges $(u, v_1), (v_1, u)$ removed and $(v_1, v_2), (v_2, v_1)$ added. This network has a larger sum distance since the paths of all sessions involving v_1 are now 1 hop longer.

3. The paths of all sessions go through all the nodes in $\mathcal{V}^*$. This property holds since any line network without this property can be easily modified to a network with this property and an increased sum distance.

With all the properties above, it can then be concluded that the maximum sum distance is achieved by a line network consisting of $N_r + 2K$ nodes. In this network, the sources and destinations are non-collocated and the paths of all sessions go through $\mathcal{V}^*$. It can be easily calculated the sum distance of this network is $K(N_r - 1) + K(K+1)$. Then we have

$$J_{\text{PP}}^{\text{BM}} \leq \frac{\sum_{i=1}^{K} d_i}{N_r + K} \leq \frac{K(N_r - 1) + K(K+1)}{N_r + K} = K. \tag{4.11}$$

■

4.3.3. THE $12\sqrt{K}$ UPPER BOUND OF $J_{\text{PP}}^{\text{BM}}$

In the following lemma, we give an upper bound of $J_{\text{PP}}^{\text{BM}}$ which is in the order of $\sqrt{K}$.

Lemma 4.3.4. *For any network $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$, the energy benefit satisfies*

$$J_{\text{PP}}^{\text{BM}} < 12\sqrt{K}. \tag{4.12}$$

Before proving this lemma, we give the following lemmas and their proofs.

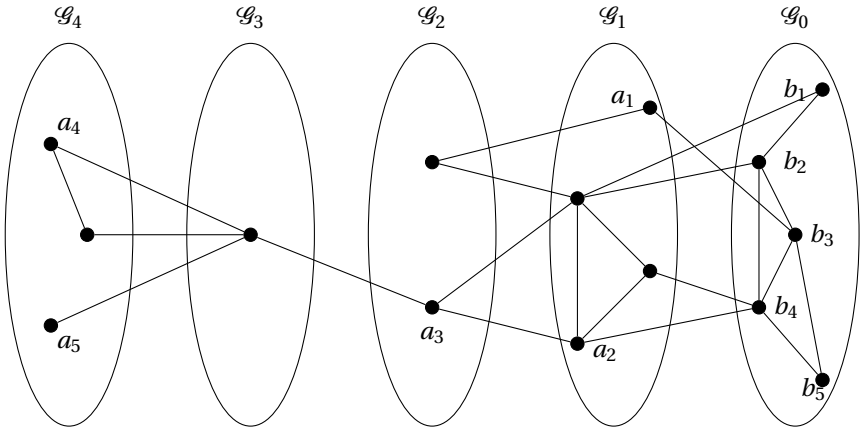


Figure 4.1: An example of grouping by $\mathscr{B}$, in which $K_0 = K_1 = 5$, $K_2 = 3$, and $K_3 = K_4 = 2$.

Lemma 4.3.5. *For any network* $\mathbf{N}(\mathscr{V},\mathscr{E},\mathscr{S})$*, the energy benefit satisfies*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq \frac{\bar{d}K}{\max_{\mathscr{S}^*\subseteq\mathscr{S}} \max(\sum_{a_i\in\mathscr{A}^*} d(a_i,\mathscr{B}^*), \sum_{b_i\in\mathscr{B}^*} d(\mathscr{A}^*,b_i))}, \tag{4.13}$$

where $\mathscr{S}^*$ *is a subset of* $\mathscr{S}$ *and* $\mathscr{A}^*,\mathscr{B}^*$ *are its source and destination sets, respectively.*

Proof. This lemma is similar to [22, Theorem 5.1], which gives a lower bound on the energy consumption of a network with only NC but no CF. Here, we use the same proving technique to give a lower bound of E^{BM}.

Firstly, we divide the node set $\mathscr{V}$ by the distance to $\mathscr{B}$. We define the node set $\mathscr{G}_0 = \mathscr{B}$ and $\mathscr{G}_l = \{u \in \mathscr{V} | d(u,\mathscr{B}) = l\}$. It is easy to prove that the node in $\mathscr{G}_l$ only connects to the nodes in $\mathscr{G}_{l-1}$ and $\mathscr{G}_{l+1}$. An example of such division is given in Fig. 4.1.

We then divide the sessions by $\mathscr{S}_l = \{S_i^U \in \mathscr{S}^U | a_i \in \mathscr{G}_l\}$ and define $K_l = \sum_{l'=l}^{\infty} |\mathscr{S}_{l'}|$. Obviously we have $K = K_0$. Also, note that the sessions in $\mathscr{S}_l$ are the sessions that satisfy $d(a_i,\mathscr{B}) = l$. By the max-flow min-cut theorem, the number of transmissions and receptions required for the communication between $\mathscr{G}_l$ and $\mathscr{G}_{l-1}$ is K_l. Hence, the energy consumption satisfies

$$\begin{aligned} E^{\mathrm{BM}} &\geq \sum_{l=1}^{\infty} K_l(e_t+e_r) \\ &= \sum_{i=1}^{K} d(a_i,\mathscr{B})(e_t+e_r), \end{aligned} \tag{4.14}$$

where the equality follows straightforwardly by counting.

Similarly, we have

$$E^{\mathrm{BM}} \geq \sum_{i=1}^{K} d(\mathscr{A},b_i)(e_t+e_r). \tag{4.15}$$

Combining (4.14) and (4.15) we have

$$E^{\mathrm{BM}} \geq \max\left(\sum_{i=1}^{K} d(a_i, \mathscr{B}), \sum_{i=1}^{K} d(\mathscr{A}, b_i)\right)(e_t + e_r). \tag{4.16}$$

Since adding sessions will not decrease the energy consumption, a lower bound in (4.16) for a subset of the session set $\mathscr{S}$ is also a lower bound for the whole network. Hence, we have

$$E^{\mathrm{BM}} \geq \max_{\mathscr{S}^* \subseteq \mathscr{S}} \max\left(\sum_{a_i \in \mathscr{A}^*} d(a_i, \mathscr{B}^*), \sum_{b_i \in \mathscr{B}^*} d(\mathscr{A}^*, b_i)\right)(e_t + e_r). \tag{4.17}$$

Combining this with (4.1) and (4.3) we finish our proof. ■

Now we analyze the bound given in (4.13) by introducing the distance matrix.

Definition 4.3.1 (Distance matrix)**.** For a network $\mathbf{N}(\mathscr{V}, \mathscr{E}, \mathscr{S})$, a distance matrix denoted by D is a $K \times K$ matrix with $d(a_i, b_j)$ as the entry in the i-th row and the j-th column, i.e.,

$$D = \begin{bmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \dots & d_{1,K} \\ d_{2,1} & d_{2,2} & d_{2,3} & \dots & d_{2,K} \\ d_{3,1} & d_{3,2} & d_{3,3} & \dots & d_{3,K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{K,1} & d_{K,2} & d_{K,3} & \dots & d_{K,K} \end{bmatrix}, \tag{4.18}$$

in which $d_{i,i} = d_i$ and $d_{i,j} = d(a_i, b_j)$.

A distance matrix has the following properties.

Property 4.3.1. The entries on the diagonal are non-zero.

Property 4.3.2. If $d_{i,j} = 0$, then $d_{i',j}, d_{i,j'} \neq 0$ for all $i' \neq i$, $j' \neq j$.

Property 4.3.3. $\forall i, j, k, l \in \{1, 2, \dots, K\}, k \neq i, l \neq j$, $d_{i,j} \leq d_{i,l} + d_{k,j} + d_{k,l}$.

The first property is trivial. The second property follows from our assumption in the model that a node cannot be the sources or destinations for multiple sessions. The third property follows from the fact that the route $a_i \to b_l \to a_k \to b_j$ is a valid path in the network and the length should not be smaller than $d(a_i, b_j)$.

For a subset $\mathscr{S}^*$ of $\mathscr{S}$, we denote the submatrix which contains only sessions in $\mathscr{S}^*$ by D^*, i.e., D^* is a submatrix with entries $d_{i,j}$ that $S_i, S_j \in \mathscr{S}^*$. We further use the notation $d^*_{i,j}$ to represent the (i,j)-th entry of D which is also an entry for D^*. Note that $d^*_{i,j}$ is not necessarily the (i,j)-th entry of D^*. Then, we can rewrite (4.13) as

$$J^{\mathrm{BM}}_{\mathrm{PP}} \leq \frac{\sum_{i=1}^{K} d_{i,i}}{\max_{\mathscr{S}^* \subseteq \mathscr{S}} \max(\sum_i \min_j d^*_{i,j}, \sum_j \min_i d^*_{i,j})}. \tag{4.19}$$

For some simple cases, the relationship between the dividend and the divisor in the RHS of (4.19) can be easily found. For example, if all sessions have the same distance d and for all $i \neq j$, $d_{i,j} = d'$, then by Property 4.3.3 we have $d' \geq d/3$. As a result, the dividend in the RHS of (4.19) is simply Kd and the divisor is no less that $Kd/3$, which leads to the following lemma.

Lemma 4.3.6. *For a network* $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$*, if* $d_i = d$ *for all* i *and* $d(a_i,b_j) = d'$ *for all* $i \neq j$*, we have*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq 3. \tag{4.20}$$

If we drop the constraint that for all $i \neq j$, $d_{i,j} = d'$, we have the following lemma.

Lemma 4.3.7. *For a network* $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$*, if* $d_i = d$ *for all* i*, we have*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq 6\sqrt{K}, \tag{4.21}$$

Proof: Firstly, for $K < 36$, (4.21) holds since (4.7) holds.
Then, for $K \geq 36$, we discuss two cases.

- **Case 1**: There exists a row or column which contains at least $\sqrt{K}/2$ entries which are smaller than or equal to $d/3$, i.e., $\exists i$, $|\{j|d_{i,j} \leq d/3\}| \geq \sqrt{K}/2$ or $|\{j|d_{j,i} \leq d/3\}| \geq \sqrt{K}/2$.

  Firstly we consider the case that $\exists i$, $|\{j|d_{i,j} \leq d/3\}| \geq \sqrt{K}/2$. Since the sessions can be arbitrarily indexed, w.l.o.g., we assume that the first $f \in \mathbb{Z} \cap [\frac{1}{2}\sqrt{K}+1, K]$ entries of the first row are smaller or equal than $d/3$ except the first one, i.e., $d_{1,j} \leq d/3$, $j \in \{2,3,\ldots,f\}$. By Property 4.3.3, we have $d_{k,l} \geq d/3$ for all $k \in \{2,3,\ldots,f\}, l \in \{2,3,\ldots,f\}$. Then we consider the submatrix D^* with the 2-fth rows and columns of D and have $\sum_i \min_j d^*_{i,j} \geq (f-1)d/3 \geq \sqrt{K}d/6$.

  For the case that $\exists i, |\{j|d_{j,i} \leq d/3\}| \geq \sqrt{K}/2$, with the same argument we have $\sum_i \min_j d^*_{i,j} \geq (f-1)d/3 \geq \sqrt{K}d/6$.

- **Case 2**: For any row or column, it contains fewer than $\sqrt{K}/2$ entries which are smaller or equal than $d/3$, i.e., $\forall i$, $|\{j|d_{i,j} \leq d/3\}| < \sqrt{K}/2$ and $|\{j|d_{j,i} \leq d/3\}| < \sqrt{K}/2$.

  In this case, w.l.o.g. we assume that the first $f \in \mathbb{Z} \cap [0, \frac{1}{2}\sqrt{K}+1)$ entries of the first row are smaller or equal than $d/3$ except the first one, i.e., $d_{1,j} \leq d/3, j \in \{2,3,\ldots,f\}$. Moreover, we assume that the entries in the rows $\mathbb{Z} \cap [g',g]$ of the first column are smaller or equal than $d/3$, i.e., $d_{i,1} \leq d/3, i \in \{g', g'+1, \ldots, g\}$. Here, $g', g \in \mathbb{Z}, g' \in (1, \frac{1}{2}\sqrt{K}+2], g \in [g', \sqrt{K}+1)$, and $g - g' < \sqrt{K}/2$. Here, the structure of D is shown:

$$D = \begin{bmatrix} d_{1,1} & d_{1,2}\ldots d_{1,f} & d_{1,f+1}\ldots d_{1,g} & d_{1,g+1}\ldots d_{1,K} \\ d_{2,1} & & & \\ \vdots & \ddots & \ddots & \ddots \\ d_{g'-1,1} & & & \\ d_{g',1} & & & \\ \vdots & \ddots & \ddots & \ddots \\ d_{g,1} & & & \\ d_{g+1,1} & & & d_{g+1,g+1} \quad \ldots \quad d_{g+1,K} \\ \vdots & \ddots & \ddots & \vdots \quad \ddots \quad \vdots \\ d_{K,1} & & & d_{K,g+1} \quad \ldots \quad d_{K,K} \end{bmatrix}, \tag{4.22}$$

in which the green parts are the entries with $d_{i,j} \le d/3$ and the blue and brown parts are the entries with $d_{i,j} \ge d/3$.

Then we consider the submatrix D_1 which is the matrix D with the 2nd to g-th rows and columns removed, i.e.,

$$D_1 = \begin{bmatrix} d_{1,1} & d_{1,g+1} & \dots & d_{1,K} \\ d_{g+1,1} & d_{g+1,g+1} & \dots & d_{g+1,K} \\ \vdots & \vdots & \ddots & \vdots \\ d_{K,1} & d_{K,g+1} & \dots & d_{K,K} \end{bmatrix}. \tag{4.23}$$

Apparently, all entries in the first row and column of D_1 are larger than $d/3$. Moreover, the property that any column or row contains less than $\sqrt{K}/2$ entries which are smaller or equal than $d/3$ still holds for this submatrix D_1. As a result, this puncturing process can be iteratively repeated for other rows and columns which still contain entries that are smaller or equal than $d/3$. During each iteration, less than $\sqrt{K}$ rows and columns are removed. After $h \in \mathbb{Z} \cap [\sqrt{K}/2, \sqrt{K}-1]$ iterations, we obtain a submatrix D_h in which all entries in at least h rows and columns are larger than $d/3$. Then, if we consider $D^* = D_h$, we have $\sum_i \min_j d^*_{i,j} \ge hd/3 \ge \sqrt{K}d/6$.

Combining the results of these two cases with (4.19) and the fact that $d_{i,i} = d$ for all i we finish our proof. ■

Lemma 4.3.7 can be easily extended to the following lemma.

Lemma 4.3.8. *For a network* $\mathbf{N}(\mathcal{V}, \mathcal{E}, \mathcal{S})$*, if* $d_i \ge d$ *for all* i*, we have*

$$E^{\mathrm{BM}} \ge \frac{1}{6}\sqrt{K}d(e_t + e_r). \tag{4.24}$$

In other words, it holds that

$$E^{\mathrm{BM}} \ge \frac{1}{6}\sqrt{K}(\min_{i=1}^{K} d_i)(e_t + e_r). \tag{4.25}$$

This lemma can be proved using similar arguments as the proof of Lemma 4.3.7 with all $d/3$ changed to $\min_{i=1}^{K} d_i/3$.

With all the lemmas established above, we prove Lemma 4.3.4.

Proof: Since the indexing of the sessions is arbitrary, w.l.o.g. we assume $d_1 \le d_2 \le \cdots \le d_K$.

Now, by Lemma 4.3.5 it is clear that for any session set $\mathcal{S}^* \subseteq \mathcal{S}$ we can derive a lower bound for E^{BM} as shown in Lemma 4.3.8, which is

$$E^{\mathrm{BM}} \ge \frac{1}{6}\sqrt{|\mathcal{S}^*|}\min_i d^*_{i,i}(e_t + e_r). \tag{4.26}$$

Hence, we have

$$E^{\mathrm{BM}} \ge \frac{1}{6}\max_{\mathcal{S}^* \subseteq \mathcal{S}} \sqrt{|\mathcal{S}^*|}\min_i d^*_{i,i}(e_t + e_r). \tag{4.27}$$

Then, since $d_1 \le d_2 \le \ldots \le d_K$, we do not need to consider all subsets of $\mathcal{S}$. More precisely, let us consider a subset $\mathcal{S}^* \subset \{S_k, S_{k+1}, \ldots, S_K\}$. It is clear that the lower bound of

(4.26) for this subset is strictly smaller than the lower bound for the subset $\{S_k, S_{k+1}, \ldots, S_K\}$. Hence, we only consider the subsets $\mathscr{S}^* = \{S_k, \ldots, S_K\}, k \in \{1, 2, \ldots, K\}$ and (4.27) is simplified to

$$E^{\mathrm{BM}} \geq \frac{1}{6} \max_{k=1}^{K} \sqrt{K-k+1}\, d_k (e_t + e_r). \tag{4.28}$$

Then we consider the energy improvement factor $J_{\mathrm{PP}}^{\mathrm{BM}}$. By (4.1), (4.3), and (4.28) we have

$$\begin{aligned}
J_{\mathrm{PP}}^{\mathrm{BM}} &= \frac{\sum_{k=1}^{K} d_k (e_t + e_r)}{E^{\mathrm{BM}}} \\
&\leq \frac{\sum_{k=1}^{K} d_k}{\frac{1}{6} \max_{k=1}^{K} \sqrt{K-k+1}\, d_k} \\
&= 6\left(\frac{d_1}{\max_{k=1}^{K} \sqrt{K-k+1}\, d_k} + \frac{d_2}{\max_{k=1}^{K} \sqrt{K-k+1}\, d_k} + \cdots + \frac{d_k}{\max_{k=1}^{K} \sqrt{K-k+1}\, d_k} \right) \\
&\leq 6\left(\frac{d_1}{\sqrt{K} d_1} + \frac{d_2}{\sqrt{K-1} d_2} + \cdots + \frac{d_K}{\sqrt{1} d_K} \right) \\
&= 6\left(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{K}} \right) \\
&< 12\sqrt{K}.
\end{aligned} \tag{4.29}$$

The last inequality can be proved by simple algebra, the details of the proof are omitted here.

■

Combining Lemmas 4.3.2-4.3.4, we prove Theorem 4.3.1.

4.3.4. CONCLUSION AND DISCUSSION

Unlike the throughput benefit for general networks given in Theorem 3.3.1, it is shown in Theorem 4.3.1 that the upper bound of the energy benefit of CF in (4.2) does not only depend on K but also the average distance of the sessions. Moreover, it is shown that if K is large and $\bar{d}$ scales faster than $\sqrt{K}$, the energy benefit is upper bounded by a factor of $\sqrt{K}$. This is a different phenomenon in comparison to the throughput benefit which can be as high as a factor of $K/2$ as shown in Section 3.3.

Also, note that the applicable schemes in BP mode can also be applied in BM mode. Hence, we have the following corollary.

Corollary 4.3.1 (Upper bound of the energy benefit of NC in general networks)**.** *For any network* $\mathbf{N}(\mathscr{V}, \mathscr{E}, \mathscr{S})$*, the energy benefit of BP mode over PP mode satisfies*

$$J_{\mathrm{PP}}^{\mathrm{BP}} \leq \min(\bar{d}, K, 12\sqrt{K}). \tag{4.30}$$

This corollary reveals the energy benefit of NC over traditional routing in general networks. So far as we know, this is the best upper bound for the energy benefit of NC in general networks with multiple unicast sessions when K is large.

4.4. UPPER BOUNDS OF SPECIFIC NETWORKS

In the previous section, an upper bound for the energy benefit of CF in general networks is given. In this section, some specific networks in which tighter upper bounds can be derived are considered. Firstly, a type of networks, namely the star networks, is considered, in which a node can be removed to separate all sources from all destinations. It is shown that CF can bring no energy benefit in this kind of networks. The line networks and the networks with rectangular or hexagonal lattice structures are also studied. It is shown that the energy improvement factors in such networks are upper bounded by some constants. Similar to the previous section, only PP and BM modes are considered.

4.4.1. STAR NETWORKS

Here, a kind of networks, namely star networks, in which the CF is not beneficial in energy consumption aspect is studied.

Definition 4.4.1 (Star networks)**.** In a network $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$, if there exists a node c such that in the graph $(\mathcal{V}\backslash\{c\},\mathcal{E}\backslash\{(u,v)|u,v\in\mathcal{V}\backslash\{c\}\})$, none of the sources a_i is connected to any of the destinations b_i, we call this network a star network.

For such networks, we have the following theorem.

Theorem 4.4.1 (Energy benefit in star networks)**.** *For any star network, the energy improvement factor* $J_{\text{PP}}^{\text{BM}}=1$.

Proof: Firstly we consider the energy required for the transmissions and receptions from the sources to node c. Since node c separates the sources from all destinations, all messages must be transmitted through node c. With the same max-flow min-cut arguments that we used in the proof of Lemma 4.3.5, the total energy consumption for this part of the network satisfies

$$E_1 \geq \sum_{i=1}^{K} d(a_i,c)(e_t+e_r). \tag{4.31}$$

Similarly, the total energy consumption for the part including node c and the destinations satisfies

$$E_2 \geq \sum_{i=1}^{K} d(c,b_i)(e_t+e_r). \tag{4.32}$$

Note that these are the energy consumption required for two separated parts of the network. Hence we have $E^{\text{BM}} \geq E_1+E_2$.

Apparently, since node c is on the shortest paths of all sessions, we have $d_i = d(a_i,c)+d(c,b_i)$. Combining with (4.1) and (4.3) we finish the proof.

■

4.4.2. LINE NETWORKS

In this subsection, the upper bound of the energy improvement factor in line networks is given.

Theorem 4.4.2 (Energy benefit in line networks)**.** *For any line network* $\mathbf{L}(\mathscr{V},\mathscr{E},\mathscr{S})$*, the energy benefit satisfies* $J_{\mathrm{PP}}^{\mathrm{BM}} \leq 2$.

Proof: Firstly we consider only the right sessions. By the max-flow min-cut theorem, for any node m, it needs to transmit at least $|\{S_i|a_i \leq m, b_i > m\}|$ times and receive at least $|\{S_i|a_i < m, b_i \geq m\}|$ times in each round. We can then lower bound E^{BM} by summing up the energy consumption of all nodes, which is

$$\begin{aligned} E^{\mathrm{BM}} &\geq \sum_{i}^{K}(|\{S_i|a_i \leq m, b_i > m\}|e_t + |\{S_i|a_i < m, b_i \geq m\}|e_r) \\ &= \sum_{i:S_i \in \mathscr{S}^R} d_i K(e_t + e_t). \end{aligned} \tag{4.33}$$

The equality can be straightforwardly established by counting. Similarly, we have

$$E^{\mathrm{BM}} \geq \sum_{i:S_i \in \mathscr{S}^L} d_i K. \tag{4.34}$$

Combining (4.33) and (4.34), we have

$$\begin{aligned} E^{\mathrm{BM}} &\geq \max(\sum_{i:S_i \in \mathscr{S}^R} d_i K, \sum_{i:S_i \in \mathscr{S}^L} d_i K)(e_t + e_t) \\ &\geq (\sum_{i:S_i \in \mathscr{S}^R} d_i K + \sum_{i:S_i \in \mathscr{S}^L} d_i K)(e_t + e_t)/2 \\ &= (\sum_{i=1}^{K} d_i K)(e_t + e_t)/2. \end{aligned} \tag{4.35}$$

Combining (4.35) with (4.1) and (4.3) we finish the proof.

■

Remark 4.4.1. This upper bound can be achieved by using the scheme proposed in Section 3.4 in a line network $\mathbf{L}(\mathscr{V},\mathscr{E},\mathscr{S})$ with $N \to \infty$ and $\mathscr{S} = \{(1,N),(N,1)\}$.

4.4.3. LATTICE NETWORKS

In this section we consider the networks with lattice structures. More precisely, the 2 dimensional (2-D) and 3 dimensional (3-D) rectangular lattices and hexagonal lattices are studied.

Firstly, we give the definition of such lattice networks.

Definition 4.4.2 (2-D rectangular lattice networks)**.** If a network $\mathbf{N}(\mathscr{V},\mathscr{E},\mathscr{S})$ has the following property, we call this network a 2-D rectangular lattice network.

If $N = N_0^2, N_0 \in \mathbb{Z}^+$ *and we represent the node* m *by* $[x_m, y_m], x_m, y_m \in \{1,2,\ldots,N_0\}$ *where* $x_m \equiv (m-1) \pmod{N_0} + 1$ *and* $y_m = \lceil m/N_0 \rceil$*, then* $\mathscr{E} = \{(u,v)|(x_u = x_v \pm 1, y_u = y_v) \wedge (x_u = x_v, y_u = y_v \pm 1)\}$.

Definition 4.4.3 (3-D rectangular lattice networks)**.** If a network $\mathbf{N}(\mathscr{V},\mathscr{E},\mathscr{S})$ has the following property, we call this network a 3-D rectangular lattice network.

If $N = N_0^3, N_0 \in \mathbb{Z}^+$ *and we represent the node* m *by* $[x_m, y_m, z_m], x_m, y_m, z_m \in \{1, 2, \ldots, N_0\}$ *where* $x_m \equiv (m-1) \pmod{N_0}+1$, $y_m = \lceil \frac{m-\lfloor \frac{m-1}{N_0^2} \rfloor N_0^2}{N_0} \rceil$, *and* $z_m = \lceil \frac{m}{N_0^2} \rceil$, *then* $\mathscr{E} = \{(u,v) | (x_u = x_v \pm 1, y_u = y_v, z_u = z_v) \wedge (x_u = x_v, y_u = y_v \pm 1, z_u = z_v) \wedge (x_u = x_v, y_u = y_v, z_u = z_v \pm 1)\}$.

Definition 4.4.4 (Hexagonal lattice networks)**.** If a network $\mathbf{N}(\mathscr{V}, \mathscr{E}, \mathscr{S})$ have the following property, we call this network a hexagonal lattice network.

If $N = N_0(N_0-1)/2, N_0 \in \mathbb{Z}^+$ *and we represent the node* m *by* $[x_m, y_m], x_m, y_m \in \{1, 2, \ldots, N_0\}$ *where* $x_1 = y_1 = 1$, $y_m = y_{m-1} + 1, x_m = x_{m-1}$ *if* $y_{m-1} < x_{m-1}$, *and* $x_m = x_{m-1} + 1, y_m = 1$ *if* $y_{m-1} = x_{m-1}$, *then* $\mathscr{E} = \{(u,v) | (x_u = x_v \pm 1, y_u = y_v) \wedge (x_u = x_v, y_u = y_v \pm 1) \wedge (x_u = x_v - 1, y_u = y_v + 1) \wedge (x_u = x_v + 1, y_u = y_v - 1)\}$.

For the lattice networks, we have the following theorem.

Theorem 4.4.3 (Energy benefit in lattice networks)**.** *For any 2-D, 3-D rectangular lattice network or hexagonal lattice network, the energy improvement factors satisfy*

$$J_{\mathrm{PP}}^{\mathrm{BM}} \leq \begin{cases} 4 & \text{for 2-D rectangular lattice networks,} \\ 3 & \text{for hexagonal lattice networks,} \\ 6 & \text{for 3-D rectangular lattice networks,} \end{cases} \tag{4.36}$$

Proof:

- **2-D Rectangular Lattice Networks.** We use the similar idea as the one we used in the proof of Theorem 4.4.2. Firstly, we consider 2-D lattice networks placed as shown in Fig. 4.2(a). We take a cut on the nodes on column x and consider the traffic to the right. By the max-flow min-cut theorem, for all the nodes in column x, they have to transmit at least $|\{S_i | x_{a_i} \leq x, x_{b_i} > x\}|$ times to the right and receives $\{S_i | x_{a_i} < x, x_{b_i} \geq x\}|$ times from the left in each round. Then we can derive an lower bound on E^{BM} by consider the sum of this lower bounds of all columns, which gives

$$E^{\mathrm{BM}} \geq \sum_{x=1}^{N_0} (|\{S_i | x_{a_i} \leq x, x_{b_i} > x\}| e_t + |\{S_i | x_{a_i} < x, x_{b_i} \geq x\}| e_r). \tag{4.37}$$

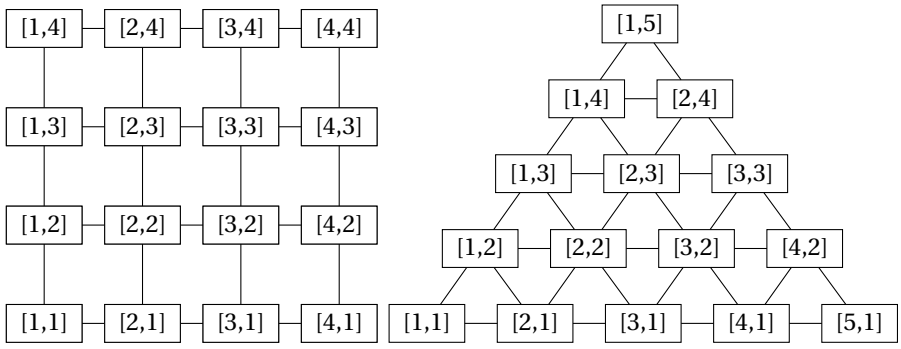
Similarly, it holds that

$$E^{\mathrm{BM}} \geq \sum_{x=1}^{N_0} (|\{S_i | x_{a_i} \geq x, x_{b_i} < x\}| e_t + |\{S_i | x_{a_i} > x, x_{b_i} \leq x\}| e_r), \tag{4.38}$$

$$E^{\mathrm{BM}} \geq \sum_{y=1}^{N_0} (|\{S_i | y_{a_i} \leq y, y_{b_i} > y\}| e_t + |\{S_i | y_{a_i} < y, y_{b_i} \geq y\}| e_r), \tag{4.39}$$

$$E^{\mathrm{BM}} \geq \sum_{y=1}^{N_0} (|\{S_i | y_{a_i} \geq y, y_{b_i} < y\}| e_t + |\{S_i | y_{a_i} > y, y_{b_i} \leq y\}| e_r). \tag{4.40}$$

A new lower bound of E^{BM} can be derived by considering the maximum value of the RHS of (4.37)-(4.40), which is no less than the sum of the RHS of (4.37)-(4.40) divided by 4. Then, it can be observed that the sum of the RHS of (4.37)-(4.40) is simply $\sum_{i=1}^{K} d_i K(e_t + e_r)$. Combining this with (4.1) and (4.3) we finish the proof for the 2-D rectangular lattice network.



(a) A rectangular lattice network with $N_0 = 4$.

(b) A hexagonal lattice network with $N_0 = 5$.

Figure 4.2: Examples for the rectangular lattice and hexagonal lattice networks.

- **Hexagonal Lattice Networks.** The proof in this network is similar to the one for 2-D rectangular lattice networks. Here, the networks are structured as shown in Fig. 4.2(b). It can be observed that in this case we can take 3 cuts which are the edges sets $\{m|x_m = x\}$, $\{m|y_m = y\}$, and $\{m|x_m + y_m = c\}$. Here, x, y are positive integers smaller or equal to N_0 and c is a positive integer smaller or equal to N_0+1.

  Here, we take the horizontal cut for example. We consider the traffics going up, which can either be up-left or up-right. Then, by the max-flow min-cut theorem, all the nodes in row y should make at least $|\{S_i|y_{a_i} \le y, y_{b_i} > y\}|$ times transmissions and $|\{S_i|y_{a_i} < y, y_{b_i} \ge y\}|$ times receptions in each round. Hence, E^{BM} is lower bounded by

$$E^{\mathrm{BM}} \ge \sum_{y=1}^{N_0} (|\{S_i|y_{a_i} \le y, y_{b_i} > y\}|e_t + |\{S_i|y_{a_i} < y, y_{b_i} \ge y\}|e_r). \tag{4.41}$$

  Similarly, we have

$$E^{\mathrm{BM}} \ge \sum_{y=1}^{N_0} (|\{S_i|y_{a_i} \ge y, y_{b_i} < y\}|e_t + |\{S_i|y_{a_i} > y, y_{b_i} \le y\}|e_r) \tag{4.42}$$

  and four other lower bounds derived by the other two cuts.

  It is clear that E^{BM} is lower bounded by the sum of the RHS of these six inequality divided by 6, which is exactly $\sum_{i=1}^{K} 2d_i K(e_t + e_r)/6$. Combining this with (4.1) and (4.3) we finish the proof for the hexagonal lattice network.

- **3-D Rectangular Lattice Networks.** The proof for the 3-D rectangular lattice network is similar to the 2-D case, hence the proof is omitted here.

■

4.4.4. CONCLUSION AND DISCUSSION

In this section, upper bounds in many networks with special properties are given. These networks all have their own practical representations. Many centralized wireless network structures can be seen as the star networks, for example, a Wi-Fi network can be seen as a star network with the router as node c since it separates the sources from any destination. It is proved that CF is not beneficial to this kind of networks.

Also, the networks with line or lattice structures are studied, which are good models for some wireless sensor networks. It is shown that the energy benefit of CF in these networks is upper bounded by some constants. Moreover, it is shown that the upper bound of the energy benefit in line networks can be achieved by the scheme proposed for BM mode in Subsection 3.4.3. In the next section, we give CF based schemes which achieve the energy benefit upper bound of hexagonal lattice networks for some e_t/e_r configurations.

4.5. LOWER BOUND IN HEXAGONAL LATTICE NETWORKS

In Section 4.3 and Section 4.4, we mainly focused on the upper bounds of the energy benefit in networks. The other part of the problem of the energy benefit, establishing lower bounds, has only been addressed in Remark 4.4.1, in which a matching lower bound in line networks was given.

In this section, a lower bound of the energy benefit in hexagonal lattice networks with a specific session placement is derived. It is shown that we can achieve an energy improvement factor between 2 and 3 in BM mode, depending on the ratio between the transmit and receive energy. This result is compared to the lower bound of the energy improvement factor in BP mode.

4.5.1. MODEL AND NOTATIONS

In this section, we consider the hexagonal lattice network $\mathbf{N}(\mathcal{V},\mathcal{E},\mathcal{S})$ defined in Subsection 4.4.3 with each node m in $\mathcal{V}$ represented by an integer pair $[x_m, y_m]$. The session set is specified as the following:

- $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$.
- $\mathcal{S}_1 = \{S_i = (a_i, b_i) | x_{a_i} = 1, y_{a_i} = i+1, x_{b_i} = N_0 - i, y_{b_i} = i+1, i \in [1, N_0 - 2]\}$.
- $\mathcal{S}_2 = \{S_i = (a_i, b_i) | x_{a_i} = j+1, y_{a_i} = N_0 - j, x_{b_i} = j+1, y_{b_i} = 1, j = i - N_0 + 2 \in [1, N_0 - 2]\}$.
- $\mathcal{S}_3 = \{S_i = (a_i, b_i) | x_{a_i} = N_0 - j, y_{a_i} = 1, x_{b_i} = 1, y_{b_i} = N_o - j, j = i - 2N_0 + 4 \in [1, N_0 - 2]\}$.
- $K = 3N_0 - 6$.

In this section, we alternatively denote $S_i = (a_i, b_i)$ by $S_{n,j} = (a_{n,j}, b_{n,j}), n \in \{1,2,3\}, j \in \{1,2,\ldots,N_0-2\}, i = (N_0-2)(n-1)+j$, e.g., if $N_0 = 10$, the session $S_{12} = (a_{12}, b_{12})$ can be alternatively denoted by $S_{2,4} = (a_{2,4}, b_{2,4}) = ([5,6],[5,1])$. Further, we define $\mathcal{A}_n = \{a_{i,j} | i = n\}, \mathcal{B}_n = \{b_{i,j} | i = n\}$. A hexagonal lattice network with the sessions is illustrated in Fig 4.3. We further denote the messages for session $S_{n,j}$ by $M_{n,j}(1), M_{n,j}(2), \ldots$. The notation

$\mathcal{V}^{(t)} = \{m \in \mathcal{V} | x_m \equiv y_m + t \mod 3\}$ is used to divide all nodes into 3 sets. In Fig. 4.4(a) we show this division.

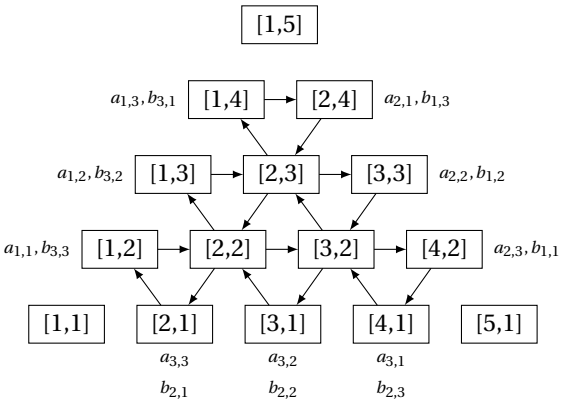


Figure 4.3: The nodes and session placement of our model if $N_0 = 5$.

4.5.2. SCHEMES

In this subsection, two CF based coding and scheduling schemes inspired by [12] are proposed. The schemes work in rounds, in which at each destination, a new source symbol for its corresponding session is decoded after the initial startup phase. We define the notation $X_r^{(t)}(m)$ and $Y_r^{(t)}(m)$, respectively, as the transmission and reception of node m in time slot t of round $r \in \mathbb{Z}^+$.

4.5.3. SCHEME 1

We consider a round of 6 time slots $t \in \{0,1,2,3,4,5\}$, and describe the scheme by defining the transmissions of node $[x_m, y_m]$ at round r. Here, we define function $i \oplus j$ as the summation in $\mathbb{Z}_3$. This notation will be used throughout this paper for simplicity.

If node $m \in \mathcal{V}_t \backslash \mathscr{A}$, it receives at time slot $t \oplus 1$ and $t \oplus 2$ and transmits

$$X_r^{(t)}(m) = Y_{r-1}^{(t\oplus 2)}(m) - Y_{r-2}^{(t\oplus 1)}(m) + X_{r-3}^{(t)}(m). \tag{4.43}$$

at time slot t.

If node $m \in \mathscr{A} \cap \mathcal{V}_t$, it receives 3 times at time slot $t \oplus 1$, $t \oplus 2$ and $(t \oplus 2) + 3$, and transmits twice. At time slot t it transmits

$$X_r^{(t)}(m) = \begin{cases} M_{1,y_m-1}(r), & \text{if } m \in \mathscr{A}_1, \\ M_{2,x_m-1}(r), & \text{if } m \in \mathscr{A}_2, \\ M_{3,N_0-x_m-1}(r), & \text{if } m \in \mathscr{A}_3, \end{cases} \tag{4.44}$$

and at time slot $t+3$ it transmits

$$X_r^{(t+3)}(m) = \begin{cases} M_{3,N_0-y_m-1}(r-y_m+1) - M_{1,y_m-1}(r), & \text{if } m \in \mathscr{A}_1, \\ M_{1,y_m-1}(r-x_m+1) - M_{2,x_m-1}(r), & \text{if } m \in \mathscr{A}_2, \\ M_{2,x_m-1}(r-N_0+x_m-1) - M_{3,N_0-x_m-1}(r), & \text{if } m \in \mathscr{A}_3. \end{cases} \tag{4.45}$$

Scheme 1 is illustrated in Fig. 4.4(b).

4.5.4. SCHEME 2

Scheme 2 is a dual scheme of Scheme 1, in which each interior node needs to transmit twice but only receive once in each round. Similarly, we consider the transmissions of node $[x_m, y_m]$ in round r.

If node $m \in \mathcal{V}_t \backslash \mathscr{A}$, it receives at time slot t, transmits

$$X_r^{(t\oplus 1)}(m) = Y_{r-1}^{(t)}(m) + X_{r-3}^{(t\oplus 1)}(m) \tag{4.46}$$

at time slot $t \oplus 1$ and transmits

$$X_r^{(t\oplus 2)}(m) = -Y_{r-2}^{(t)}(m) + X_{r-3}^{(t\oplus 2)}(m) \tag{4.47}$$

at time slot $t \oplus 2$.

If node $m \in \mathscr{A} \cap \mathcal{V}_t$, it receives at time slot t and $(t \oplus 2) + 3$, transmits

$$X_r^{(t\oplus 1)}(m) = \begin{cases} M_{1,y_m-1}(r-1), & \text{if } m \in \mathscr{A}_1, \\ M_{2,x_m-1}(r-1), & \text{if } m \in \mathscr{A}_2, \\ M_{3,N_0-x_m-1}(r-1), & \text{if } m \in \mathscr{A}_3, \end{cases} \tag{4.48}$$

at time slot $t \oplus 1$, transmits

$$X_r^{t\oplus 2}(m) = \begin{cases} -M_{1,y_m-1}(r-2), & \text{if } m \in \mathscr{A}_1, \\ -M_{2,x_m-1}(r-2), & \text{if } m \in \mathscr{A}_2, \\ -M_{3,N_0-x_m-1}(r-2), & \text{if } m \in \mathscr{A}_3, \end{cases} \tag{4.49}$$

at time slot $t \oplus 2$, and transmits (4.45) at time slot $t+3$.

Scheme 2 is illustrated in Fig. 4.4(c).

4.5.5. VALIDITY OF THE SCHEMES

Firstly, we denote the extra transmission and reception in the last 3 time slots of node $m \in \mathscr{A}$ in round r as $\tilde{X}_r(m)$ and $\tilde{Y}_r(m)$. Then, we consider Scheme 1. Observe that each interior node, as well as each of the boundary nodes during the first 3 time slots, only transmit once. Hence, we use the notation $X_r(x_m, y_m)$ for the transmitted symbol of node $[x_m, y_m]$ in round r during the first 3 time slots. Then by (4.43) we have

$$\begin{aligned} &X_r(x_m, y_m) = X_{r-1}(x_m - 1, y_m) + X_{r-1}(x_m, y_m + 1) + X_{r-1}(x_m + 1, y_m - 1) \\ &- X_{r-2}(x_m - 1, y_m + 1) - X_{r-2}(x_m + 1, y_m) - X_{r-2}(x_m, y_m - 1) + X_{r-3}(x_m, y_m). \end{aligned} \tag{4.50}$$

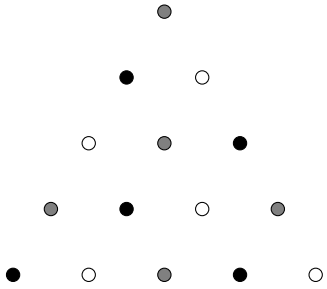
Now we establish the following lemma.

Lemma 4.5.1. *If* $x_m \neq 1, y_m \neq 1, x_m + y_m \neq N_0 + 1$,

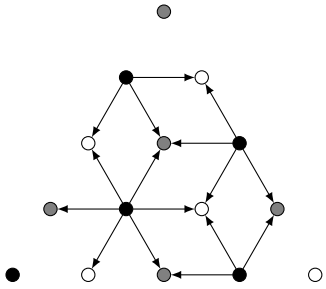
$$X_r(x_m, y_m) = M_{1,y_m-1}(r - x_m + 1) + M_{2,x_m-1}(r - N_0 + x_m + y_m - 2) + M_{3,N_0-x_m-y_m+2}(r - y_m + 1). \tag{4.51}$$

The proof of this lemma is similar to the proof for Lemma 2 in [12], since the coding scheme in (4.50) is similar to the one used in [12], which considers symbols in $\mathbb{F}_2$ instead of $\mathbb{F}_q$. Thus, we omit the proof of this lemma here to save space.

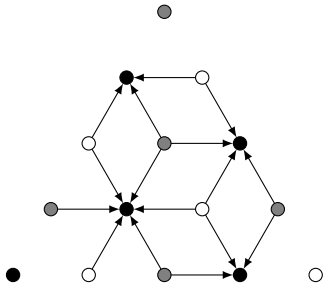
Now we prove that in each round, a source symbol is decoded at each destination, which validate the scheme. Since the network and our coding schemes are symmetric, w.l.o.g. we consider only the sessions $S_{1,j}$ from left to right.



(a) Three node sets.



(b) Scheme 1.



(c) Scheme 2.

Figure 4.4: (a) The node sets $\mathcal{V}^{(0)},\mathcal{V}^{(1)},\mathcal{V}^{(2)}$, represented by black, white, and gray circles, respectively, (b) Scheme 1 at time slot 1, and (c) Scheme 2 at time slot 1.

Lemma 4.5.2. *For the session $S_{1,j}$ and its destination $b_{1,j}, x_{b_{1,j}} = N_0 - j, y_{b_{1,j}} = j+1$, the symbol $M_{1,j}(r - N_0 + j + 1)$ can be decoded at the end of round $r-1$ by*

$$Y_{r-1}^{(t\oplus 2)}(b_{1,j}) - Y_{r-2}^{(t\oplus 1)}(b_{1,j}) + X_{r-3}^{(t)}(b_{1,j}) + \tilde{Y}_{r-1}(b_{1,j}), \tag{4.52}$$

for Scheme 1.

Proof: W.l.o.g. we assume $m \in \mathcal{V}^{(0)}$. By the definition of the categories, for the four neighbors of node m, we have nodes $(x_m-1, y_m+1), (x_m, y_m-1) \in \mathcal{V}^{(1)}$ and nodes $(x_m-1, y_m), (x_m+1, y_m-1) \in \mathcal{V}^{(2)}$. Thus we have $Y_{r-1}^{(2)}(x_m, y_m) = X_{r-1}(x_m-1, y_m) + X_{r-1}(x_m+1, y_m-1)$, $Y_{r-2}^{(1)}(x_m, y_m) = X_{r-2}(x_m-1, y_m+1) + X_{r-2}(x_m, y_m-1)$ and $\tilde{Y}_{r-1}(x_m, y_m) = \tilde{X}_{r-1}(x_m+1, y_m-1)$. Thus, by (4.44), (4.45) and Lemma 4.5.1 we have (4.52) equal to

$$\begin{aligned}
&X_{r-1}(x_m-1, y_m) + X_{r-1}(x_m+1, y_m-1) + X_{r-2}(x_m-1, y_m+1) + X_{r-2}(x_m, y_m-1) \\
&+X_{r-3}(x_m, y_m) + \tilde{X}_{r-1}(x_m+1, y_m-1) \qquad (4.53)\\
&= M_{1,j}(r - N_0 + j + 1) + M_{2,N_0-j-2}(r-2) + M_{3,2}(r-j-1) + M_{2,N_0-j}(r-1) \\
&\quad -M_{2,N_0-j-2}(r-2) - M_{1,j-1}(r - N_0 + j - 1) - M_{2,N_0-j-1}(r-3) - M_{3,2}(r-j-1) \\
&\quad +M_{2,N_0-j-1}(r-3) + M_{1,j-1}(r - N_0 + j - 1) - M_{2,N_0-j}(r-1) \qquad (4.54)\\
&= M_{1,j}(r - N_0 + j + 1). \qquad (4.55)
\end{aligned}$$

■

The proof for the validity of Scheme 2 is similar to Scheme 1 since the two schemes are dual. For Scheme 2, observe that for $m \in \mathcal{V}^{(t)}$, $X_{r+1}^{(t\oplus 1)}(m) = -X_{r+2}^{(t\oplus 2)}(m) = Y_r^{(t)}(m) + X_{r-2}^{(t\oplus 1)}(m) = -Y_r^{(t)}(m) - X_{r-1}^{(t\oplus 2)}(m)$. The symbol $M_{1,j}(r - N_0 + j + 1)$ can be decoded by $Y_r^{(0)}(b_{1,j}) + X_{r-2}^{(1)}(b_{i,j}) + \tilde{Y}_{r-1}(b_{i,j})$ follows the same steps as the (4.53)-(4.55). The validity of Scheme 2 is thus proved.

4.5.6. ENERGY BENEFIT

In this section, we compare our schemes to some existing schemes, in particular, the traditional routing based scheme, and the network coding based scheme proposed in [12].

Firstly, by Lemma 4.3.1 we have the minimum energy consumption in PP mode for this network

$$E^{\mathrm{PP}} = K\bar{d}(e_t + e_r) = \frac{3}{2}(N_0 - 1)(N_0 - 2) \tag{4.56}$$

In [12], a network coding scheme is proposed, in which the interior nodes broadcast the linear sums of the symbols heading different directions, instead of transmit them separately. In each round, which is defined similarly to the round in our schemes, each interior node needs to transmit only once but receive 6 times, and each boundary node needs to transmit twice and receive 4 times. We thus have the lower bound on E^{BP}

$$E^{\mathrm{BP}} \leq 3(N_0 - 2)(2e_t + 4e_r) + \frac{1}{2}(N_0 - 3)(N_0 - 4)(e_t + 6e_r). \tag{4.57}$$

Then, our scheme 1 gives a lower bound of E^{BM}

$$E^{\mathrm{BM}} \leq 3(N_0 - 2)(2e_t + 3e_r) + \frac{1}{2}(N_0 - 3)(N_0 - 4)(e_t + 2e_r) \tag{4.58}$$

and our scheme 2 gives a lower bound of

$$E^{\mathrm{BM}} \leq 3(N_0 - 2)(3e_t + 2e_r) + \frac{1}{2}(N_0 - 3)(N_0 - 4)(2e_t + e_r). \tag{4.59}$$

Then, bringing in the definition of energy benefit in (4.1), we have the following theorem.

Theorem 4.5.1 (Lower bound for the energy improvement factors in hexagonal lattice networks)**.** *In our network model with $N_0 \to \infty$, the energy improvement factors are lower bounded by*

$$J_{\mathrm{PP}}^{\mathrm{BP}} \geq \max(1, \frac{3e_t + 3e_r}{e_t + 6e_r}), \tag{4.60}$$

$$J_{\mathrm{BP}}^{\mathrm{BM}} \geq \max(\frac{e_t + 6e_r}{e_t + 2e_r}, \frac{e_t + 6e_r}{e_t + 6e_r}), \tag{4.61}$$

$$J_{\mathrm{PP}}^{\mathrm{BM}} \geq \max(\frac{3e_t + 3e_r}{e_t + 2e_r}, \frac{3e_t + 3e_r}{2e_t + e_r}). \tag{4.62}$$

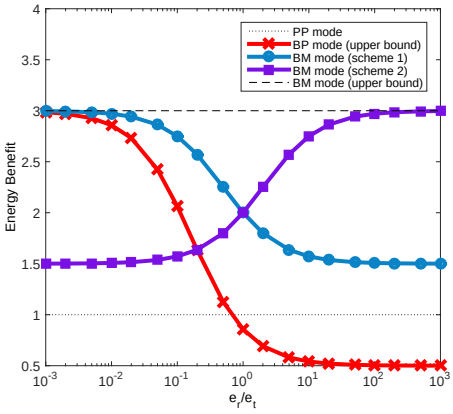


Figure 4.5: The energy benefit comparison between schemes as a function of e_r/e_t.

It shows that the energy improvement factor of BP mode is 3 if $e_r = 0$. However, the scheme of [12] in BP mode is not beneficial at all when $e_t > 1.5e_r$. Our schemes guarantee that the CF technique is always beneficial in energy consumption in this network. The energy improvement factor is in between 2 to 3, depending on the ratio between e_t and e_r. Also, note that by Theorem 4.4.3 the energy improvement factor of BM mode in hexagonal lattice network is upper bounded by 3. Hence, the energy benefit of our schemes is upper bound achieving when $e_t = 0$ or $e_r = 0$. We show $I_{\text{PP}}^{\text{BM}}$ as a function of e_r/e_t in Fig. 4.5.

4.6. CONCLUSION

In this chapter, an upper bound of $\min(\bar{d}, K, 12\sqrt{K})$ for the energy benefit of CF over traditional routing in general networks with multiple unicast sessions has been derived. It has been shown that the energy benefit is not only upper bounded by a function of K, but also bounded by the average distance of sessions. Hence, for the type of networks in which the distances of the sessions are short, e.g., the network RN(K) proposed in Section 3.3 in which the throughput benefit is proportional to K, the energy benefit is very limited. Also, this upper bound shows that if K is large, the energy benefit of CF and also NC are at most at the order of $\sqrt{K}$. To the best of our knowledge, this is the best upper bound on this problem when $K \to \infty$. It gives new insights on the problem of the energy benefit of NC and CF for multiple unicasts.

Also, upper bounds of the energy benefit in some specific networks have been derived. Similar to the throughput case, the results show that in many practical scenarios, the energy benefit of CF does not grow with the number of sessions. In particular, if there is a node which separates all sources from all destinations, CF is not beneficial in the energy consumption. Also, it has been proved that for line networks, 2-D and 3-D rectangular lattice networks, and hexagonal lattice networks, the energy improvement factors are upper bounded by 2, 4, 6, and 3, respectively. Notice that in all of our con-

sidered networks, the upper bounds are constants. Hence, an important challenge for the following studies is to fill in the gap between the constant upper bounds in specific networks and the $12\sqrt{K}$ upper bound in general networks either by finding a network with the energy benefit at the order of $\sqrt{K}$ or by deriving an upper bound of a constant.

Further, the achievability of the derived bounds has also been considered. For line networks with a long bidirectional session, it is clear that the schemes proposed in the previous chapter also achieve the factor 2 improvement on the energy consumption. For hexagonal lattice networks with a specific session placement, schemes which achieve improvements of 2 to 3 depending on the ratio between the transmit energy and the receive energy have been proposed. If either the transmit or receive energy is 0, the upper bound on the energy improvement factor can be achieved. However, in other lattice networks, e.g., 2-D rectangular networks, to the best of our knowledge, there is no upper bound achieving scheme. This remains as an interesting problem for follow-up studies.

5

SECURITY BENEFIT

In this chapter, we study the benefit of compute-and-forward (CF) in the secrecy aspect. The two-hop channel using cooperative jamming against the untrusted relay is studied. Two secure transmission schemes based on a novel version of CF technique, we called scaled CF (SCF), are proposed, which significantly boost the secrecy rate on this problem. We also introduce another problem in which we can also use these schemes to achieve secure transmission.

5.1. INTRODUCTION

Information theoretic security is a problem considered by Shannon whereby no message can be retrieved even if an eavesdropper knows the coding scheme and has infinite computational capabilities [36]. This concept has been well studied for many channels, e.g., the wire-tap channel [44]. The concept "secrecy rate" is proposed in [44] for the rate of the communication under the constraint that the information leaked to the eavesdropper per channel use tends to zero when the number of channel uses tends to infinity (a constraint also known as weak secrecy). As many other classic channels, the secure transmission problem on a two-hop channel with an untrusted relay has been well studied. This channel consists of a pair of source and destination using an untrusted relay to forward the message. The relay is considered to be malicious but cooperative (sometimes referred as "curious-but-honest"), it overhears the message but makes no change on it. This channel was first studied in [31], in which a rather pessimistic conclusion is drawn that no positive secrecy rate can be achieved by the straightforward transmission

The material in this chapter has appeared in

- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission using an untrusted relay with SCF," *IEEE Inf. Theory Workshop (ITW)*, Jerusalem, Israel, Apr. 2015.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission on two-hop relay channel with SCF," *Submitted to IEEE Trans. on Inf. Theory.*

scheme. However, a later study in [14] proposed a cooperative jamming [38] based approach to achieve a positive secrecy rate, in which a cooperative node (sometimes the destination) is introduced to simultaneously transmit a jamming signal to confuse the relay while the source is transmitting. The relay then encodes its reception and transmits it to the destination. With prior knowledge of the jamming signal, the destination is able to decode the source message.

Several secure transmission schemes have been proposed based on cooperative jamming in [14–16, 33, 37, 40, 48]. In [14], the source is encoded with a Gaussian code, the cooperative jammer transmits a random Gaussian signal, and the relay forwards the description of its received signal using the compress-and-forward scheme [5]. A similar scheme based on amplify-and-forward [9] is used in [37]. The amplify-and-forward based scheme is improved in [48] by using a lattice code instead of Gaussian code at the source. This scheme is called modulo-and-forward, since the relay can take a modulo operation w.r.t. lattice structure of the code to achieve a higher secrecy rate. A CF [29] based scheme was introduced in [15] for a symmetric two-hop channel, in which both of the transmitting and the jamming messages are encoded with lattice codes. The relay decodes a linear combination of these messages and then sends it to the destination. Albeit the achievable secrecy rate of [15] is lower than [14], this CF based scheme can be used in a line network since it does not suffer from noise accumulation. In [16], a similar CF based scheme was introduced which achieves strong secrecy with the same secrecy rate as [15]. In [34], another CF based scheme was proposed for the multi-way relay channel which achieves weak secrecy rate. Bi-directional transmission on this channel is studied in [40], in which a higher level of secrecy, namely perfect secrecy, is achieved by another CF based scheme.

In this chapter, we propose two novel secure and reliable transmission schemes based on a modified version of CF [50] which is introduced in Subsection 2.3.4, namely SCF. The main contributions of this chapter are the following:

- Two novel SCF based secure transmission schemes are proposed for the two-hop channel with an untrusted relay, which use a random binning code and a lattice chain to create randomness at the source, respectively. These are the first secure transmission schemes for this problem that are based on the SCF technique.
- In the symmetric case where the power and channel gains for the source, the relay, and the destination are identical, both of our schemes achieve a secrecy rate of $1/2\log(1/2+\mathrm{SNR})-1/2$, in which SNR stands for Signal-to-Noise-Ratio. This is merely 1/2 bit per channel use away from the transmit rate using CF on this channel. This rate is upper bound achieving when the SNR is high and is the best secrecy rate achieved so far on this channel.
- Our schemes significantly improve the achievable secrecy rate and achieve the upper bound in many asymmetric scenarios. In general, our schemes have better performance than other existing schemes in the high SNR scenario for almost all channel configurations.
- We consider a novel secure transmission problem on the two-hop channel, in which the relay is trusted and there exist an external eavesdropper. We prove that

one of our schemes can also be applied on this channel and achieves a positive secrecy rate.

This chapter is organized as follows. In Section 5.2, we build up the model and give the state-of-the-art on the problem. In Section 5.3, we introduce a reliable SCF based code for transmission, which will be used as the transmission code throughout this chapter. In Section 5.4, we introduce two secure coding schemes which are built upon our reliable transmission scheme and provide secrecy. In Section 5.5, we compare the rates of our schemes with the state-of-the-art. In Section 5.6, we consider another two-hop channel model in which the relay is trusted and there exist an external eavesdropper. We show that one of our schemes can also achieve a positive secrecy rate in this case. In Section 5.7, we conclude this chapter.

5.2. PRELIMINARIES

5.2.1. MODEL

In this chapter, we consider the model used in [14]. The model consists of a two-hop channel, in which node A wants to transmit information to node C using an untrusted relay node R to forward the information. To guarantee secure communication, another node B, a *cooperative Jammer*, is added to the network, which transmits a jamming signal to confuse the relay. We assume that the communication takes places over two phases, each including N channel uses. We use $X^A, X^B, X^R \in \mathbb{R}^N$ for the transmitted sequences of node A, the cooperative jammer B, and the relay R, respectively. We use $Y^R, Y_1^C, Y_2^C \in \mathbb{R}^N$ for the receptions of the relay and node C in Phase 1 and 2, respectively. In the first phase, node A transmits to the relay and the cooperative jammer B simultaneously transmits a jamming signal to confuse the relay. The jamming signal transmitted by the cooperative jammer B is also received by node C. We have

$$Y^R = X^A + X^B + Z_1^R, \tag{5.1}$$
$$Y_1^C = X^B + Z_1^C, \tag{5.2}$$

where Z_1^R and Z_1^C are N-dimensional independent Gaussian noise vectors with variance 1 and σ^2 in each dimension, respectively. Note that when $\sigma = 0$, the model is equivalent to the model in which the destination is used as jammer.

In the second phase, the relay transmits to node C. We have

$$Y_2^C = X^R + Z_2^C, \tag{5.3}$$

where Z_2^C is an N-dimensional independent Gaussian noise vector with variance 1 in each dimension. The power constraints for the three nodes are defined as

$$E[||X^i||^2] \leq NP_i,\ i \in \{A, B, R\}. \tag{5.4}$$

It seems that we lose some generality by assuming the channel coefficients and Z_1^R, Z_2^C to be unit. However, this assumption is actually w.l.o.g. and can be easily extended to any configuration of power constraints, channel coefficients, and noise variances with the same SNR for the receptions Y^R, Y_1^C, and Y_2^C.

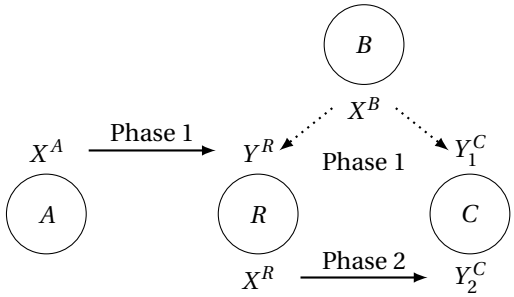


Figure 5.1: Two-hop channel with a cooperative jammer.

We assume that the power constraints as well as σ^2 are revealed to all nodes. The source message of node A is defined as $W^A \sim \mathcal{U}(\{1,2,\ldots,2^{NR_s}\})$, where the notation $X \sim \mathcal{U}(\mathcal{S})$ is used for a random variable X that is uniformly chosen at random from the alphabet $\mathcal{S}$. A secrecy rate R_s is said to be achievable if for any $\delta > 0$, there exists a sequence of $(2^{NR_s}, N)$ codes such that the reliability constraint

$$\lim_{N\to\infty} \Pr(\hat{W}^A \neq W^A) = 0 \tag{5.5}$$

and the (weak) secrecy constraint

$$\lim_{N\to\infty} \frac{1}{N} I(W^A; Y^R) \leq \delta \tag{5.6}$$

hold. Here, $\hat{W}^A$ is the estimate of W^A based on the reception Y_1^C and Y_2^C at node C.

Further, we use the notation $\mathbb{R}^+$ for the set of positive real numbers, $\mathbb{Z}^+$ for the set of positive integers, and $C(x)$ for the capacity of Gaussian channel with SNR equal to x, i.e.,

$$C(x) = \frac{1}{2}\log(1+x). \tag{5.7}$$

5.2.2. STATE-OF-THE-ART

AN UPPER BOUND ON THE SECRECY RATE

An upper bound on the secrecy rate is derived in [14] by transforming this model to an equivalent multiple access wire-tap channel. The secrecy rate is upper bounded by

$$R_b = \frac{1}{2}\log\frac{(P_A+1)(P_A+P_B+1)-(P_A+\rho)^2}{(P_A+P_B+1)(1-\rho^2)}, \tag{5.8}$$

where

$$\rho = \frac{2P_A + P_AP_B + P_B - \sqrt{4P_BP_A^2 + 4P_BP_A + P_B^2P_A^2 + 2P_B^2P_A + P_B^2}}{2P_A}. \tag{5.9}$$

AMPLIFY-AND-FORWARD BASED SCHEME

A straightforward amplify-and-forward based scheme is proposed in [37] for the case that the destination is used as the jammer, i.e., $\sigma = 0$. In this scheme the destination transmits a Gaussian jamming signal and the relay simply amplifies the received signal and transmits it to the destination. This scheme achieves any secrecy rate satisfying

$$R_s < \frac{1}{2}\log\left(1+\frac{P_A P_R}{P_A+P_B+P_R+1}\right)-\frac{1}{2}\log\left(1+\frac{P_A}{P_B+1}\right). \tag{5.10}$$

MODULO-AND-FORWARD BASED SCHEME

In [48] another scheme is proposed which uses a lattice code based coding scheme to transmit the message with an extra random vector. The destination, which is also the cooperative jammer ($\sigma = 0$), transmits a Gaussian signal to confuse the relay. Due to the lattice chain structure, the relay can take a modulo operation to remove the random part of the transmission which is useless in the decoding at the destination. This results in a higher SNR for the actual message vector. In other words, it is an advanced amplify-and-forward scheme which makes uses of the properties of lattice code and lattice chain. Any secrecy rate satisfying

$$R_s < \frac{1}{2}\log\frac{P_A+P_R+P_A P_R+1}{P_A+P_R+2}-\frac{1}{2}\log\left(1+\frac{P_A}{P_B+1}\right) \tag{5.11}$$

is achievable.

COMPRESS-AND-FORWARD BASED SCHEME

A compress-and-forward based scheme is given in [14], where the relay forwards a description of its noisy reception to the destination. Any secrecy rate

$$R_s < \max_{p_A\le P_A, p_B\le P_B}\left(C\left(\frac{p_A}{(1+\sigma^2+\sigma_c^2)-\sigma^4/(p_B+\sigma^2)}\right)-C\left(\frac{p_A}{1+p_B}\right)\right) \tag{5.12}$$

is achievable, where

$$\sigma_c^2 = \frac{p_A+1+p_B\sigma^2/(p_B+\sigma^2)}{P_R}. \tag{5.13}$$

COMPUTE-AND-FORWARD BASED SCHEME

A CF based scheme is proposed in [15] for a symmetric two-hop channel with jammer and destination collocated, in which node A transmits the source message encoded with a lattice codebook and node B (node C) transmits a random codeword choosing uniformly at random from the same lattice codebook. An algebraic proof is given that the sum of two N-dimensional lattice codewords will leak no more than N bits of information to the relay. Then, a random binning based scheme is used to eliminate the information leakage. For $P_A = P_B = P_R$ and $\sigma = 0$, any secrecy rate satisfying

$$R_s' < \frac{1}{2}\log\left(\frac{1}{2}+P_A\right)-1 \tag{5.14}$$

is achievable. It is proved in [16] that this rate is also achievable if we change the weak secrecy constraint (5.6) to a *strong secrecy* constraint

$$\lim_{N\to\infty} I(W^A; Y^R) \le \delta \tag{5.15}$$

by replacing the random binning based scheme to a universal hashing function based scheme.

Another CF based scheme is proposed in [40], which also considers the case of $P_A = P_B = P_R$ and $\sigma = 0$. The focus of [40] is on *"perfect secrecy"*, which is defined through

$$\lim_{N\to\infty} I(W^A; Y^R) = 0. \tag{5.16}$$

A binning approach within the lattice codebook used for both A and B is used. The bins are selected such that for each source message, A randomly selects from a certain bin of codewords with a certain probability mass function. It is proved that if the bins and the probability mass functions are chosen appropriately, perfect secrecy is achievable with any secrecy rate satisfying

$$R_s'' < \frac{1}{2}\log\left(\frac{1}{2} + P_A\right) - 1 - \log e. \tag{5.17}$$

This scheme is extended in [39], in which the asymmetric channel/power case is considered. It is proved that perfect secrecy is achievable for some asymmetric configurations.

5.3. A SCF BASED CODE FOR RELIABLE TRANSMISSION

As introduced in Subsection 2.3.4, if the source messages W^i, $i \in \{A, B\}$ are encoded with the SCF code and the channel input

$$X^i = [T^i/\beta_i + D^i] \pmod{\Lambda^i/\beta_i} \tag{5.18}$$

satisfy (5.4), the relay node is able to compute the linear combination $a_1 T^A + a_2 T^B$ if the transmit rates are smaller than the computation rates in (2.16). In this section, we propose a reliable code for our channel, namely an $(\mathbf{a}, \boldsymbol{\beta})$ SCF code. For given power constraints $P_i, i \in A, B, R$, this code guarantees reliable transmission from A to C for a source symbol chosen uniformly at random from $\{1, 2, \ldots, 2^{NR_t^A(\mathbf{a},\boldsymbol{\beta})}\}$ if

$$R_t^A(\mathbf{a}, \boldsymbol{\beta}) < \min(C(P_R), R_{\mathrm{CF}}^A(\mathbf{a}, \boldsymbol{\beta})) \tag{5.19}$$

and

$$R_{\mathrm{CF}}^B(\mathbf{a}, \boldsymbol{\beta}) \le C(P_B/\sigma^2). \tag{5.20}$$

We firstly introduce the lattice codebook construction in detail, then describe the transmission process. In the end, the rate of information leaked to the relay with this scheme during the transmission is calculated.

5.3.1. CODEBOOK CONSTRUCTION

Here we describe our codebook constructed with the SCF technique. For an $(\mathbf{a}, \boldsymbol{\beta})$ SCF code and an arbitrarily chosen positive real number δ', we select a fine lattice Λ and a pair of shaping lattices $\Lambda_C^i(\mathbf{a}, \boldsymbol{\beta}) \subseteq \Lambda, i \in \{A, B\}$ which have the following properties:

- **Power:** We have

$$\frac{1}{N\mathrm{Vol}(\mathcal{V}_C^i(\mathbf{a},\boldsymbol{\beta}))} \int_{\mathcal{V}_C^i(\mathbf{a},\boldsymbol{\beta})} ||X||^2 dX = \beta_i^2 P_i, i \in \{A, B\}, \tag{5.21}$$

  where $\mathcal{V}_C^i$ is the fundamental Voronoi region of $\Lambda_C^i(\mathbf{a}, \boldsymbol{\beta})$.

- **Nesting:** The coarser one of $\Lambda_C^i(\mathbf{a}, \boldsymbol{\beta})$ is nested in the finer one.

- **Rate:** Denote $\hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta}) = \frac{1}{N} \log|\Lambda \cap \mathcal{V}_C^i(\mathbf{a}, \boldsymbol{\beta})|$. Then, for the chosen δ', we have

$$R_{\mathrm{CF}}^i(\mathbf{a}, \boldsymbol{\beta}) - \delta' < \hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta}) < R_{\mathrm{CF}}^i(\mathbf{a}, \boldsymbol{\beta}). \tag{5.22}$$

- **Goodness:** These lattices are all good for both mapping and additive white Gaussian noise (AWGN) in the sense of [7].

By [7], the lattices satisfying the above-mentioned properties can be found. Then, we construct the lattice codebooks $\Lambda \cap \mathcal{V}_C^i(\mathbf{a}, \boldsymbol{\beta})$ for transmission.

5.3.2. RELIABLE TRANSMISSION PROCESS

- **Phase 1, node** A**.**

  Firstly, the message W^A is uniquely mapped to a lattice vector in $\Lambda \cap \mathcal{V}_C^A(\mathbf{a}, \boldsymbol{\beta})$ by the encoder, Then, a dither D^A is uniformly chosen from the scaled Voronoi region $\mathcal{V}_C^A(\mathbf{a}, \boldsymbol{\beta})/\beta_A$. Note that dithers are chosen to fulfill the power constraints of lattice codes and are revealed to all nodes. The transmitted lattice vector of node A is

$$X^A = [T^A/\beta_A + D^A] \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})/\beta_A). \tag{5.23}$$

- **Phase 1, node** B**.**

  Node B transmits a jamming signal, namely V^B, which is uniformly chosen at random from $\Lambda \cap \mathcal{V}_C^B(\mathbf{a}, \boldsymbol{\beta})$. The transmitted vector is thus

$$X^B = [V^B/\beta_B + D^B] \ (\mathrm{mod}\ \Lambda_C^B(\mathbf{a}, \boldsymbol{\beta})/\beta_B), \tag{5.24}$$

  in which $D^B \sim \mathcal{U}(\mathcal{V}_C^B(\mathbf{a}, \boldsymbol{\beta})/\beta_B)$. It it clear from the definition that the average power of both X^A and X^B does not exceed the power constraint of (5.4).

- **Phase 1, node** C

  By our codebook construction, node C can reliably decode V^B if (5.20) holds.

- **Phase 1, the relay.**

  Upon receiving Y^R in (5.1), by [50], the relay is able to decode

  $$U^R = a_1 T^A + a_2 V^B$$

  with the lattice Λ with high probability if

  $$\hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta}) < R_{\mathrm{CF}}^i(\mathbf{a}, \boldsymbol{\beta}), i \in \{A, B\}, \tag{5.25}$$

  which has already be guaranteed by the codebook construction in (5.22).

- **Phase 2, the relay**

  The relay firstly scales the decoded vector down by computing $U^R/a_1 = T^A + (a_2/a_1)V^B$. Then, similar to the CF scheme proposed for the two-way relay channel [30], a modulo operation is taken on the decoded vector. The lattice for the modulo operation Λ^* should be chosen such that $\Lambda^* \subseteq \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})$ to guarantee that the vector T^A can be retrieved by node C. For the sake of power, we let the relay take a modulo operation on the decoded vector w.r.t. $\Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})$. The resulting vector is denoted by $\tilde{U}^R$ and

  $$\tilde{U}^R = U^R/a_1 \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) = (T^A + (a_2/a_1)V^B) \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})). \tag{5.26}$$

  Then, the relay transmits this vector using any capacity achieving channel code on the AWGN channel. By definition, the entropy of this vector has the property of

  $$\frac{1}{N} H(\tilde{U}^R) \le \hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta}) \le R_{\mathrm{CF}}^A(\mathbf{a}, \boldsymbol{\beta}) \le C(P_A). \tag{5.27}$$

  When $P_R \ge P_A$, this vector can be reliably transmitted by the relay straightforwardly. When $P_R < P_A$, we consider a long term of transmission during which the model is used for $K \in \mathbb{Z}^+$ times. We only use $\lceil K \frac{C(P_R)}{\hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta})} \rceil$ times Phase 1 and fully use all K times Phase 2 of these model uses. By choosing K sufficiently large, the transmit rate can be made arbitrarily close to

  $$R_t^A(\mathbf{a}, \boldsymbol{\beta}) \frac{C(P_R)}{\hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta})}. \tag{5.28}$$

  Combining these two cases, in a long term transmission, any rate satisfying (5.19) is achievable.

- **Phase 2, node C.**

  Since node C can reliably decode $\tilde{U}^R$, it can then decode T^A by computing

  $$\begin{aligned}
  & [\tilde{U}^R - (a_2/a_1)V^B] \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) \\
  = \ & [(T^A + (a_2/a_1)V^B) \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) - (a_2/a_1)V^B] \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) \\
  = \ & [T^A + (a_2/a_1)V^B - (a_2/a_1)V^B] \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) \\
  = \ & [T^A] \ (\mathrm{mod}\ \Lambda_C^A(\mathbf{a}, \boldsymbol{\beta})) \\
  = \ & T^A.
  \end{aligned} \tag{5.29}$$

  Since T^A is reliably decoded, W^A can then be retrieved.

As we have already discussed the reliability of the decoding in each step of the process, by choosing δ' arbitrarily small we have the following lemma.

Lemma 5.3.1 (Transmit rate for the $(\mathbf{a},\boldsymbol{\beta})$ SCF code)**.** *For any $\mathbf{a},\boldsymbol{\beta}$, an $(\mathbf{a},\boldsymbol{\beta})$ SCF code guarantees power constraint (5.4) and reliability constraint (5.5) with any rate satisfying (5.19) if (5.20) holds.*

5.3.3. INFORMATION LEAKAGE RATE

By Lemma 5.3.1, it is guaranteed that the information can be reliably transmitted from the source to the destination with the given power constraint. However, during the process, part of the information is leaked to the relay. Here we define the information leakage rate $R_o(\mathbf{a},\boldsymbol{\beta})$ (sometimes referred as equivocation rate) as

$$R_o(\mathbf{a},\boldsymbol{\beta}) = \frac{1}{N} I(W^A; Y^R) \tag{5.30}$$

and bound it by

$$\begin{aligned} R_o(\mathbf{a},\boldsymbol{\beta}) &= \frac{1}{N}(H(W^A) - H(X^A,X^B|Y^R) - H(W^A|Y^R,X^A,X^B) + H(X^A,X^B|Y^R,W^A)) \\ &= \frac{1}{N}(H(W^A) - H(X^A,X^B) + I(X^A,X^B;Y^R)) \\ &< \frac{1}{N}(H(W^A) - H(X^A) - H(X^B)) + C(P_A+P_B) \\ &= R_t^A(\mathbf{a},\boldsymbol{\beta}) - R_t^A(\mathbf{a},\boldsymbol{\beta}) - R_t^B(\mathbf{a},\boldsymbol{\beta}) + C(P_A+P_B) \\ &= -R_t^B(\mathbf{a},\boldsymbol{\beta}) + C(P_A+P_B). \end{aligned} \tag{5.31}$$

The second equality holds since the third term on the RHS of the first equality is 0 since W^A is one-to-one mapped to X^A. Further, the fourth term is also 0 for that the relay knows X^A by knowing W^A, and it can reliably decode X^B when X^A is known. Then, the inequality follows from the capacity for Gaussian MAC and the third equality follows from the definition of the $(\mathbf{a},\boldsymbol{\beta})$ SCF code. In the next section, we will propose two schemes to eliminate the information leakage.

5.4. SECURE CODING SCHEMES

In the previous section, a reliable code for transmission, namely an $(\mathbf{a},\boldsymbol{\beta})$ SCF code, has been proposed. For any $\mathbf{a},\boldsymbol{\beta}$, a reliable transmission of a source symbol chosen uniformly at random from $\{1,2,\ldots,2^{NR_t^A(\mathbf{a},\boldsymbol{\beta})}\}$ is guaranteed if conditions (5.19) and (5.20) hold. Then, we bounded the information leakage rate during the process $R_o(\mathbf{a},\boldsymbol{\beta})$ in (5.31).

In this section, we introduce two schemes of adding extra randomness at the source, which can eliminate the information leakage. Both schemes are built upon the $(\mathbf{a},\boldsymbol{\beta})$ SCF code. The first one uses the classical random binning idea and is constructed in a two-layer structure. We use the $(\mathbf{a},\boldsymbol{\beta})$ SCF code as inner code and a random binning code as outer code. The second scheme is a lattice chain based scheme using an $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain code, in which a mid-layer lattice is added to the lattice codebook of the $(\mathbf{a},\boldsymbol{\beta})$ SCF

code to create randomness. Since this code is a modified version of $(\mathbf{a}, \boldsymbol{\beta})$ SCF code, the differences between this code and the $(\mathbf{a}, \boldsymbol{\beta})$ SCF code are extensively clarified.

5.4.1. RANDOM BINNING BASED SCHEME

The classical random binning idea is introduced in [44] and widely used in many secure transmission scenarios. Here, we borrow the idea of the random binning codes from [3] and the two-layer structure from [15]. We propose a random binning based scheme (RB scheme), which is constructed by an $(\mathbf{a}, \boldsymbol{\beta})$ SCF code as inner code and a random binning code as outer code. The random binning code is designed to encode the messages into a long sequence of lattice codewords of a chosen $(\mathbf{a}, \boldsymbol{\beta})$ SCF code. Here we introduce our random binning code in detail.

RANDOM BINNING CODE

- **Codebook Construction** Generate $2^{\lfloor lH(W^A)\rfloor}$ bins, where l should be chosen sufficiently large. Label each bin by a different length-l typical sequence of W^A. The size of each bin (the upper bound for the number of the codewords in each bin) is $2^{\lfloor l' NR_o(\mathbf{a},\boldsymbol{\beta})\rfloor}$, where $l' = l\frac{H(W^A)}{N(R_t^A(\mathbf{a},\boldsymbol{\beta})-R_o(\mathbf{a},\boldsymbol{\beta}))}$.

  Generate $2^{NR_t^A(\mathbf{a},\boldsymbol{\beta})\lceil l'\rceil}$ codewords. The codewords are length $\lceil l'\rceil$ sequences of N-dimensional lattice codewords generated with the codebook described in Section 5.3.1. Put the codewords into the bins uniformly at random until all bins are filled.

- **Encoding** For each length-l sequence of source messages, the encoder chooses the bin with the same label, then chooses a codeword from the bin uniformly at random and transmits it. If the message sequence does not match any label of bins, or there is no codeword in the matching bin, it transmits a random length-$\lceil l'\rceil$ sequence of lattice codewords as its codeword. The code structure of the RB scheme is illustrated in Fig. 5.2.

- **Transmission** Here, we consider that our model is used for $\lceil l'\rceil$ times. Each time a lattice codeword is reliably transmitted from node A to B. Thus, after $\lceil l'\rceil$ times, a random binning codeword is reliably transmitted. For each phase, the channel is used for $N\lceil l'\rceil$ times.

- **Decoding** By receiving the codeword, it looks that up into the codebook and uses the label of the bin as the estimation.

RELIABILITY

Since the reliability of the $(\mathbf{a}, \boldsymbol{\beta})$ SCF code is already shown in Section 5.3, we now show the reliability of the random binning code.

A length-l sequence of source messages can be reliably retrieved if the length-$\lceil l'\rceil$ sequence of lattice codewords is reliably decoded and is the codeword for the correct messages. The former is guaranteed by Lemma 5.3.1. An error in the latter can be caused either by an unlabeled message or an empty bin. There are two situations for the unlabeled messages. 1, the message is typical but there is no matching label. 2, the message is not typical. By the property of typicality, the probability for both situations to occur

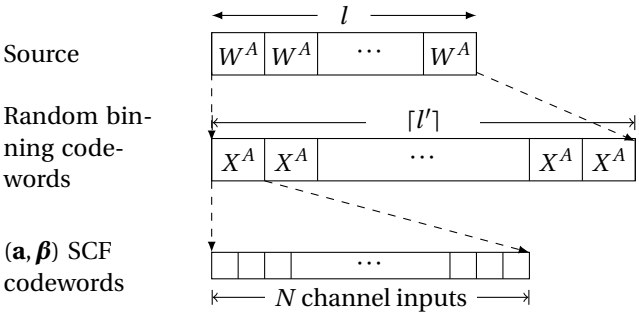


Figure 5.2: Structure of the random binning based scheme.

are negligible when $N, l \to \infty$. Moreover, since the expected number of codewords in one bin is almost $2^{lNR_o(\mathbf{a},\boldsymbol{\beta})}$, by the law of large number, the probability of the existence of empty bins is also negligible when $N, l \to \infty$. Hence, the estimation error is vanishing when $N, l \to \infty$.

5

INFORMATION LEAKAGE RATE

Here, we show that the RB scheme achieves the information theoretic security.

Lemma 5.4.1. *For any $\delta > 0$, there exist a sequence of codes constructed with an $(\mathbf{a}, \boldsymbol{\beta})$ SCF code as inner code and a random binning code as outer code which achieves*

$$\frac{1}{N} I(W^A; Y^R) < \delta \tag{5.32}$$

Proof: By analyzing the information leakage rate, we have

$$\begin{aligned}
&\frac{1}{lN} I(\mathscr{W}^A; \mathscr{Y}^R) \\
&= \frac{1}{lN}\left(H(\mathscr{W}^A) - H(\mathscr{X}^A, \mathscr{X}^B|\mathscr{Y}^R) - H(\mathscr{W}^A|\mathscr{Y}^R, \mathscr{X}^A, \mathscr{X}^B) + H(\mathscr{X}^A, \mathscr{X}^B|\mathscr{Y}^R, \mathscr{W}^A)\right) \qquad (5.33)\\
&= \frac{1}{lN}\left(H(\mathscr{W}^A) - H(\mathscr{X}^A, \mathscr{X}^B) + I(\mathscr{X}^A, \mathscr{X}^B; \mathscr{Y}^R) + H(\mathscr{X}^A, \mathscr{X}^B|\mathscr{Y}^R, \mathscr{W}^A)\right), \qquad (5.34)
\end{aligned}$$

where $\mathscr{W}^A$ is length-l sequence of source messages and $\mathscr{X}^A$, $\mathscr{X}^B$, and $\mathscr{Y}^R$ are length-$\lceil l' \rceil$ sequences of the transmissions of the source, the transmissions of the jammer, and the receptions at the relay, respectively. The third term in (5.33) is 0 since the mapping error from the codewords to the source messages is almost zero as we stated in Subsection 5.4.1. Then we focus on the last term $H(\mathscr{X}^A, \mathscr{X}^B|\mathscr{Y}^R, \mathscr{W}^A)$. This term can be upper bounded by Fano's inequality since the relay can determine the transmitted codeword almost surely. The reason is that the size of the bin is chosen accordingly to the information leakage rate.

More precisely, for any transmitted message, by the leaked information, the relay is able to list almost $2^{\lfloor lH(W^A) \rfloor}$ possible $\mathscr{X}^A$ as candidates from a total of $2^{\lfloor lH(W^A) \rfloor + \lfloor l' NR_o(\mathbf{a},\boldsymbol{\beta}) \rfloor}$

codewords. Then, since the random binning process is independent and uniform, the relay can determine the transmitted codeword almost surely if it also knows the label of the bin when $N, l \to \infty$.

Then, by Fano's inequality, we have

$$\begin{aligned} & H(\mathscr{X}^A, \mathscr{X}^B | \mathscr{Y}^R, \mathscr{W}^A) \\ \leq & \frac{1}{lN} + \frac{1}{lN} P_e \log 2^{\lfloor lH(W^A) \rfloor + \lfloor l' N R_o(\mathbf{a}, \boldsymbol{\beta}) \rfloor} \\ \leq & \epsilon', \end{aligned} \tag{5.35}$$

where $P_e, \epsilon' \to 0$ when $N \to \infty$.

Hence, we have

$$\begin{aligned} & \frac{1}{lN} I(\mathscr{W}^A; \mathscr{Y}^R) \\ = & \frac{1}{lN} (H(\mathscr{W}^A) - H(\mathscr{X}^A) - H(\mathscr{X}^B) + I(\mathscr{X}^A, \mathscr{X}^B; \mathscr{Y}^R) + H(\mathscr{X}^A, \mathscr{X}^B | \mathscr{Y}^R, \mathscr{W}^A)) \\ = & \frac{1}{lN} (lH(W^A) - \lfloor lH(W^A) \rfloor - \lfloor l' N R_o(\mathbf{a}, \boldsymbol{\beta}) \rfloor - \lceil l' \rceil N R_t^B(\mathbf{a}, \boldsymbol{\beta}) + \lceil l' \rceil I(X^A, X^B; Y^R) + \epsilon' \\ < & \frac{1}{lN} (lH(W^A) - \lfloor lH(W^A) \rfloor - \lfloor l' N R_o(\mathbf{a}, \boldsymbol{\beta}) \rfloor - \lceil l' \rceil N R_t^B(\mathbf{a}, \boldsymbol{\beta}) + \lceil l' \rceil NC(P_A + P_B)) + \epsilon' \\ \leq & \frac{1}{lN} (1 - \lfloor l' NC(P_A + P_B) - l' N R_t^B(\mathbf{a}, \boldsymbol{\beta}) \rfloor - \lceil l' \rceil N R_t^B(\mathbf{a}, \boldsymbol{\beta}) + \lceil l' \rceil NC(P_A + P_B)) + \epsilon' \\ \leq & \frac{1}{lN} (2 - l' N(C(P_A + P_B) - R_t^B(\mathbf{a}, \boldsymbol{\beta})) + \lceil l' \rceil N(C(P_A + P_B) - R_t^B(\mathbf{a}, \boldsymbol{\beta}))) + \epsilon' \\ \leq & \frac{2}{lN} + \frac{-R_t^B(\mathbf{a}, \boldsymbol{\beta}) + C(P_A + P_B)}{l} + \epsilon', \end{aligned} \tag{5.36}$$

which can be made arbitrarily small by choosing sufficiently large l, N. Here, the second equality follows from our codebook construction, where $H(\mathscr{X}^A) = \lfloor lH(W^A) \rfloor + \lfloor l' N R_o(\mathbf{a}, \boldsymbol{\beta}) \rfloor$ and $H(\mathscr{X}^B) = \lceil l' \rceil N R_t^B(\mathbf{a}, \boldsymbol{\beta})$. The first inequality follows from the capacity of the Gaussian MAC. The second inequality follows from (5.31).

■

ACHIEVABLE SECRECY RATE

Here, we discuss three cases of whether the relay has limited power and whether σ is larger than a threshold $\underline{\sigma}$ where

$$\underline{\sigma} = \sqrt{1 + \frac{1 + P_A + P_B}{P_A P_B - P_A - 1}}. \tag{5.37}$$

Note that a chosen $(\mathbf{a}, \boldsymbol{\beta})$ SCF code is associated with a threshold for transmit rate $\hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta})$. The actual transmit rate $R_t^A(\mathbf{a}, \boldsymbol{\beta})$ can be chosen arbitrarily in $[0, \hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta})]$. Hence, for each case, we specify the code and transmit rate, i.e., $\mathbf{a}$, $\boldsymbol{\beta}$, and $R_t^i(\mathbf{a}, \boldsymbol{\beta})$.

- $P_R \geq P_A$ and $\sigma \leq \underline{\sigma}$.

Firstly, for any $(\mathbf{a}, \boldsymbol{\beta})$, we can bound the achievable secrecy rate of a RB scheme by

$$\begin{aligned} R_s &= \frac{lH(W^A)}{N\lceil l' \rceil} \\ &\geq R_t^A(\mathbf{a}, \boldsymbol{\beta}) - R_o(\mathbf{a}, \boldsymbol{\beta}) - \epsilon \\ &> R_t^A(\mathbf{a}, \boldsymbol{\beta}) + R_t^B(\mathbf{a}, \boldsymbol{\beta}) - C(P_A + P_B) - \epsilon \end{aligned} \tag{5.38}$$

where ϵ can be made arbitrarily small by choosing sufficiently large l and small δ'. The first and the second inequality simply follow from the definition of l' and $R_o(\mathbf{a}, \boldsymbol{\beta})$, respectively.

Then, when $P_R \geq P_A$ and $\sigma \leq \underline{\sigma}$, (5.38) is maximized when $R_t^i(\mathbf{a}, \boldsymbol{\beta}) = \hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta})$. Note that by (5.22), $\hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta})$ is arbitrarily close to $R_{\mathrm{CF}}^i(\mathbf{a}, \boldsymbol{\beta})$ when δ' is chosen arbitrarily small. Hence, any secrecy rate satisfying

$$R_s < \max_{\mathbf{a}, \boldsymbol{\beta}} R_s(\mathbf{a}, \boldsymbol{\beta}) \tag{5.39}$$

is achievable, where

$$R_s(\mathbf{a}, \boldsymbol{\beta}) = R_{\mathrm{CF}}^A(\mathbf{a}, \boldsymbol{\beta}) + R_{\mathrm{CF}}^B(\mathbf{a}, \boldsymbol{\beta}) - C(P_A + P_B). \tag{5.40}$$

It can be easily calculated that the maximum is reached when $\mathbf{a} = (1, 1)$ and $\frac{\beta_A}{\beta_B} = \sqrt{\frac{P_B(1+P_A)}{P_A(1+P_B)}}$. In this case we have

$$\max_{\mathbf{a}, \boldsymbol{\beta}} R_s(\mathbf{a}, \boldsymbol{\beta}) = \frac{1}{2} \log \frac{1 + P_A + P_B}{(\sqrt{(1+P_A)(1+P_B)} - \sqrt{P_A P_B})^2} - 1. \tag{5.41}$$

- $P_R \geq P_A$ and $\sigma > \underline{\sigma}$.

  In this case, first of all, if we simply apply the code of the previous case, $R_t^B(\mathbf{a}, \boldsymbol{\beta})$ will be larger than $C(P_B/\sigma^2)$ and the transmitted vector V^B will not be decodable at node C. Also, it can be calculated that the achievable secrecy rate is not optimal by adjusting $\mathbf{a}, \boldsymbol{\beta}$ such that $\hat{R}_t^i(\mathbf{a}, \boldsymbol{\beta}) < C(P_B/\sigma^2)$.

  Actually, the maximum secrecy rate will be given by choosing $\mathbf{a}$, $\boldsymbol{\beta}$, and $R_t^i(\mathbf{a}, \boldsymbol{\beta})$ such that $R_{\mathrm{CF}}^A(\mathbf{a}, \boldsymbol{\beta}) = C(P_A)$, $R_t^A(\mathbf{a}, \boldsymbol{\beta})$ very close to $C(P_A)$, and $R_t^B(\mathbf{a}, \boldsymbol{\beta})$ very close to $C(P_B/\sigma^2)$. The choice of $R_t^B(\mathbf{a}, \boldsymbol{\beta})$ is feasible because $\hat{R}_t^B(\mathbf{a}, \boldsymbol{\beta})$ can be chosen arbitrarily close to $R_{\mathrm{CF}}^B(\mathbf{a}, \boldsymbol{\beta})$ and when $\sigma > \underline{\sigma}$, $R_{\mathrm{CF}}^B(\mathbf{a}, \boldsymbol{\beta}) > C(P_B/\sigma^2)$. Thus, by (5.38), any secrecy rate satisfying

  $$R_s < C(P_A) + C(P_B/\sigma^2) - C(P_A + P_B) \tag{5.42}$$

  is achievable.

- $P_R < P_A$.

  In this case, for $\sigma \leq \underline{\sigma}$ and $\sigma > \underline{\sigma}$, the setting for $\mathbf{a}$, $\boldsymbol{\beta}$, and $R_t^i(\mathbf{a}, \boldsymbol{\beta})$ are identical to the previous two cases, respectively. The difference is that the relay should apply the transmission scheme for $P_R < P_A$, which has already been stated in Subsection 5.3.2. As a result, the achievable secrecy rate is simply the achievable secrecy rate of the previous two cases times $\frac{C(P_R)}{\hat{R}_t^A(\mathbf{a}, \boldsymbol{\beta})}$.

Combining the three cases, we have the following theorem.

Theorem 5.4.1 (Achievable secrecy rate with the RB scheme)**.** *For a two-hop channel with an untrusted relay, with the RB scheme, any secrecy rate R_s satisfying*

$$R_s < \max_{\mathbf{a},\boldsymbol{\beta}} [\min(\frac{C(P_R)}{R^A_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta})}, 1) R_s(\mathbf{a},\boldsymbol{\beta})] \tag{5.43}$$

is achievable if $\sigma \leq \underline{\sigma}$ and

$$R_s < \min(\frac{C(P_R)}{C(P_A)}, 1)(C(P_A) + C(P_B/\sigma^2) - C(P_A + P_B)) \tag{5.44}$$

is achievable if $\sigma > \underline{\sigma}$.

5.4.2. LATTICE CHAIN BASED SCHEME

The lattice chain based scheme (LC scheme) is inspired by the lattice chain code used in [33]. Here, we propose an $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain code, which is an $(\mathbf{a},\boldsymbol{\beta})$ SCF code with the transmitted lattice vector splitting into two parts, a message vector and a random vector. Since it is modified over an $(\mathbf{a},\boldsymbol{\beta})$ SCF code, we only focus on the parts that are modified. All the notations and terms have the same meanings as in Section 5.3 without further explanation.

CODING SCHEME

The codebook of an $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain code is also constructed with the lattices Λ and $\Lambda^i_C(\mathbf{a},\boldsymbol{\beta})$ of an $(\mathbf{a},\boldsymbol{\beta})$ SCF code. Besides, a mid-layer lattice $\Lambda^A_E(\mathbf{a},\boldsymbol{\beta})$ for which $\Lambda^A_C(\mathbf{a},\boldsymbol{\beta}) \subseteq \Lambda^A_E(\mathbf{a},\boldsymbol{\beta}) \subseteq \Lambda$ is introduced for the codebook construction. For arbitrarily chosen $\delta' > 0$ and $\delta'' \in (0, (\sum_{i\in\{A,B\}} R^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta}) - C(P_A+P_B))/2]$, these lattices should satisfy all properties listed in Subsection 5.3.1, and three additional properties as follows.

- **Rate of the Randomness:** For the given δ'', we have

$$R_o(\mathbf{a},\boldsymbol{\beta}) - \delta'' < R^A_e(\mathbf{a},\boldsymbol{\beta}) < R_o(\mathbf{a},\boldsymbol{\beta}), \tag{5.45}$$

  where $R^A_e(\mathbf{a},\boldsymbol{\beta}) = \frac{1}{N}\log|\Lambda^A_E(\mathbf{a},\boldsymbol{\beta}) \cap \mathcal{V}^A_C(\mathbf{a},\boldsymbol{\beta})|$.

- **Nesting of $\Lambda^A_E(\mathbf{a},\boldsymbol{\beta})$:** The coarser one of $\Lambda^A_E(\mathbf{a},\boldsymbol{\beta})$ and $\Lambda^B_C(\mathbf{a},\boldsymbol{\beta})$ is nested in the finer one.

- **Goodness of $\Lambda^A_E(\mathbf{a},\boldsymbol{\beta})$:** The lattice $\Lambda^A_E(\mathbf{a},\boldsymbol{\beta})$ is good at both quantizing and shaping.

By [7], lattices satisfying these properties can be found. We then define $\hat{R}^A_s(\mathbf{a},\boldsymbol{\beta}) = \frac{1}{N}\log|\Lambda \cap \mathcal{V}^A_E(\mathbf{a},\boldsymbol{\beta})|$ as the rate of the lattice codebook for the messages and $\hat{R}^A_t(\mathbf{a},\boldsymbol{\beta}) = \frac{1}{N}\log|\Lambda \cap \mathcal{V}^A_C(\mathbf{a},\boldsymbol{\beta})|$ as rate of the codebook for transmission.

In Fig. 5.3 we show the structure of a codebook of node A.

Clearly, we have

$$\hat{R}^A_t(\mathbf{a},\boldsymbol{\beta}) = \hat{R}^A_s(\mathbf{a},\boldsymbol{\beta}) + R^A_e(\mathbf{a},\boldsymbol{\beta}). \tag{5.46}$$

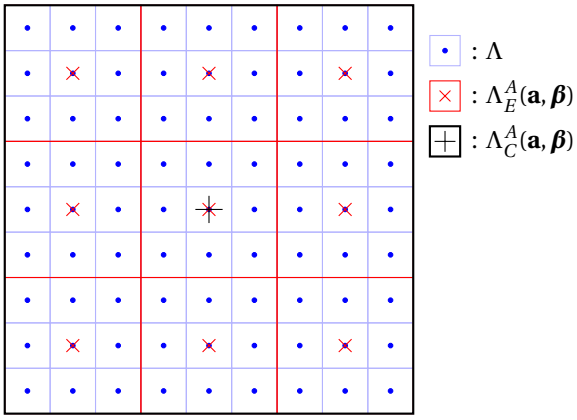


Figure 5.3: A codebook of node A for an $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain code.

The source symbol chosen uniformly at random from $\{1,2,\ldots,2^{NR_s^A(\mathbf{a},\boldsymbol{\beta})}\}$, $R_s^A(\mathbf{a},\boldsymbol{\beta}) \in [0, \hat{R}_s^A(\mathbf{a},\boldsymbol{\beta})]$ is mapped to a codeword in the lattice codebook $\Lambda \cap \mathcal{V}_E^A(\mathbf{a},\boldsymbol{\beta})$. Further, we denote

$$R_t^A(\mathbf{a},\boldsymbol{\beta}) = R_s^A(\mathbf{a},\boldsymbol{\beta}) + R_e^A(\mathbf{a},\boldsymbol{\beta}). \tag{5.47}$$

We assume all the lattices and codebooks are revealed to all four nodes.

TRANSMISSION PROCESS

The transmission process is similar to the transmission process described in Subsection 5.3.2. Here, we only focus on the steps which are different, which are **(Phase 1, node** A**)**, **(Phase 1, the relay)**, **(Phase 2, the relay)**, and **(Phase 2, node** C**)**.

- **Phase 1, node** A**.** Firstly, the message W^A is uniquely mapped to a lattice vector in $\Lambda \cap \mathcal{V}_E^A(\mathbf{a},\boldsymbol{\beta})$ by the encoder, Then the encoder adds a vector V^A which is chosen uniformly at random from $\Lambda_E^A(\mathbf{a},\boldsymbol{\beta}) \cap \mathcal{V}_C^A(\mathbf{a},\boldsymbol{\beta})$. Then, a dither $D^A \sim \mathcal{U}(\mathcal{V}_C^A(\mathbf{a},\boldsymbol{\beta})/\beta_A)$ is chosen. The transmitted lattice vector of node A is

$$X^A = [(T^A + V^A)/\beta_A + D^A] \pmod{\Lambda_C^A(\mathbf{a},\boldsymbol{\beta})/\beta_A}. \tag{5.48}$$

- **Phase 1, the relay.** Upon receiving Y^R in (5.1), by [50], the relay can reliably decode

$$U^R = a_1(T^A + V^A) + a_2 V^B$$

with the lattice Λ.

- **Phase 2, the relay** The relay firstly scales the decoded vector down by computing $U^R/a_1 = (T^A + V^A) + (a_2/a_1)V^B$. Then, instead of $\Lambda_C^A(\mathbf{a},\boldsymbol{\beta})$, the relay takes a modulo operation on the decoded vector w.r.t. $\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})$. We denote the resulting vector as $\tilde{U}_*^R$ and

$$\tilde{U}_*^R = U^R/a_1 \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} = (T^A + (a_2/a_1)V^B) \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})}. \tag{5.49}$$

The relay then transmits this vector using any capacity achieving channel code on the AWGN channel. Since by definition we have $\frac{1}{N}H(\tilde{U}_*^R) \le \hat{R}_s^A(\mathbf{a},\boldsymbol{\beta})$, the transmission is reliable when $C(P_R) \ge \hat{R}_s^A(\mathbf{a},\boldsymbol{\beta})$. Thus we have the power constraint

$$P_R > 2^{2\hat{R}_s^A(\mathbf{a},\boldsymbol{\beta})} - 1. \tag{5.50}$$

Note that if P_R is smaller than the requirement in the constraint, a similar approach as the one stated in Section 5.3 can be used. However, it can be calculated that the optimal solution is that we adjust $\mathbf{a},\boldsymbol{\beta}$ as well as the codebook to P_R. The details and the achievable rate of this solution will be given later in this subsection.

- **Phase 2, Node C.** Since the vector $\tilde{U}_*^R$ is reliably decoded, node C can then decode T^A by computing

$$\begin{aligned}
&[\tilde{U}_*^R - (a_2/a_1)V^B] \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} \\
&= [(T^A + (a_2/a_1)V^B) \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} - (a_2/a_1)V^B] \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} \\
&= [T^A + (a_2/a_1)V^B - (a_2/a_1)V^B] \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} \\
&= [T^A] \pmod{\Lambda_E^A(\mathbf{a},\boldsymbol{\beta})} \\
&= T^A.
\end{aligned} \tag{5.51}$$

Since T^A is reliably decoded, W^A can then be retrieved.

INFORMATION LEAKAGE RATE

Here, we prove that the LC scheme is information theoretically secure.

Lemma 5.4.2. *For any $\delta > 0$, if*

$$R_t^B(\mathbf{a},\boldsymbol{\beta}) = \hat{R}_t^B(\mathbf{a},\boldsymbol{\beta}), \tag{5.52}$$

there exist a sequence of $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain codes which achieves

$$\frac{1}{N}I(W^A;Y^R) < \delta. \tag{5.53}$$

Proof: Firstly, since X^B is independent of X^A and the dithers are known, by (5.47) we have

$$\begin{aligned}
&\frac{1}{N}(H(W^A) - H(X^A) - H(X^B)) \\
&= R_s^A(\mathbf{a},\boldsymbol{\beta}) - R_t^A(\mathbf{a},\boldsymbol{\beta}) - R_t^B(\mathbf{a},\boldsymbol{\beta}) \\
&= -R_e^A(\mathbf{a},\boldsymbol{\beta}) - R_t^B(\mathbf{a},\boldsymbol{\beta}).
\end{aligned} \tag{5.54}$$

Then, the information leakage rate at the relay is upper bounded by

$$\begin{aligned}
&\frac{1}{N}I(W^A;Y^R) \\
&= \frac{1}{N}(H(W^A) - H(X^A,X^B|Y^R) - H(W^A|Y^R,X^A,X^B) + H(X^A,X^B|Y^R,W^A)) \\
&= \frac{1}{N}(H(W^A) - H(X^A) - H(X^B) + I(X^A,X^B;Y^R)) + \frac{1}{N}H(X^A,X^B|Y^R,W^A). \\
&< -R_e^A(\mathbf{a},\boldsymbol{\beta}) - R_t^B(\mathbf{a},\boldsymbol{\beta}) + C(P_A+P_B) + \frac{1}{N}H(X^A,X^B|Y^R,W^A).
\end{aligned} \tag{5.55}$$

Here, the second equality follows a similar argument as (5.36). The inequality follows from (5.54) and the Gaussian multiple access channel (MAC) capacity.

By [51, Theorem 2, 3], the decoder can reliably decode X^A and X^B from Y^R and W^A with all the dithers, lattices and coefficients by a regular lattice decoding scheme if (5.52) holds. Here, we briefly explain the decoding process.

Firstly, we let the relay decode $a_1(V^A+T^A)+a_2V^B$. By [50], the decoding is successful if (5.25) holds, which is guaranteed by (5.22). Then, since the relay already knows W^A and the codebook, it knows T^A as well. We let it subtract a_1T^A and decode V^A by treating $a_1(V^A+T^A)+a_2V^B$ as noise. It is proved that the decoding is reliable if

$$R_e^A(\mathbf{a},\boldsymbol{\beta}) < C(P_A+P_B) - \hat{R}_t^B(\mathbf{a},\boldsymbol{\beta}), \tag{5.56}$$

which is guaranteed by (5.31), (5.45), and (5.52). Then, it can also decode V^B by subtracting $a_1(V^A+T^A)$ from $a_1(V^A+T^A)+a_2V^B$. Hence, both V^A and V^B are decoded and then X^A and X^B are reliably decoded as well.

As a result, by Fano's inequality we have

$$\begin{aligned}
&\frac{1}{N}H(X^A,X^B|Y^R,W^A)\\
\leq\ & \frac{1}{N}+\frac{1}{N}P_e\log 2^{N(R_e^A(\mathbf{a},\boldsymbol{\beta})+R_t^B(\mathbf{a},\boldsymbol{\beta}))}\\
=\ & \frac{1}{N}+P_e(R_e^A(\mathbf{a},\boldsymbol{\beta})+R_t^B(\mathbf{a},\boldsymbol{\beta})),
\end{aligned} \tag{5.57}$$

where P_e is the probability of decoding errors which tends to 0 when $N\to\infty$. Then, bringing back the expression of information leakage rate in (5.55), combining (5.31), (5.45), and (5.57), the information leakage rate can be made arbitrarily small by choosing sufficiently large N and sufficiently small δ''. Hence, we finish the proof. ■

ACHIEVABLE SECRECY RATE

Similar as the previous section, we also distinct three cases w.r.t. P_R and σ. For each case, we specify the settings of $\mathbf{a}$, $\boldsymbol{\beta}$, and $R_t^i(\mathbf{a},\boldsymbol{\beta})$.

- $P_R \geq P_A$ and $\sigma \leq \underline{\sigma}$.

  In this case, similar to the RB scheme, we can set $R_t^i(\mathbf{a},\boldsymbol{\beta})$ equals to $\hat{R}_t^i(\mathbf{a},\boldsymbol{\beta})$ and set $\hat{R}_t^i(\mathbf{a},\boldsymbol{\beta})$ accordingly to (5.22). Combining with (5.31), (5.45), and (5.47), we achieve any secrecy rate satisfying (5.39) by choosing sufficiently large N and sufficiently small δ'.

- $P_R \geq P_A$ and $\sigma > \underline{\sigma}$.

  In this case, if the same settings as the previous case is used, (5.20) is violated. Moreover, unlike the RB scheme, due to the constraint of the $(\mathbf{a},\boldsymbol{\beta})$ SCF lattice chain code, using the same lattice codebook with a simple decreasing of the transmit rate violates (5.52). Hence a new lattice codebook with different $\mathbf{a}$, $\boldsymbol{\beta}$ should be generated w.r.t. the constraint

  $$R_{\mathrm{CF}}^B(\mathbf{a},\boldsymbol{\beta}) \leq C(P_B/\sigma^2) \tag{5.58}$$

and $\hat{R}_t^i(\mathbf{a},\boldsymbol{\beta})$ should be set accordingly to (5.22). Then, we set $R_t^i(\mathbf{a},\boldsymbol{\beta})$ equal to $\hat{R}_t^i(\mathbf{a},\boldsymbol{\beta})$. Thus, any secrecy rate satisfying

$$R_s < \max_{\mathbf{a},\boldsymbol{\beta}:R_{\mathrm{CF}}^B(\mathbf{a},\boldsymbol{\beta})\le C(P_B/\sigma^2)} R_s(\mathbf{a},\boldsymbol{\beta}) \tag{5.59}$$

is achievable.

- $P_R < P_A$.

  In this case, unlike the RB scheme, the LC scheme guarantees a reliable transmission of T^A as long as (5.50) holds. Note that our scheme holds for any pair of $\mathbf{a},\boldsymbol{\beta}$. Moreover, as long as $P_R < P_A$, by [50], for any secrecy rate $\hat{R}_s^A(\mathbf{a},\boldsymbol{\beta})$ satisfying (5.50), there exists a pair of $\mathbf{a},\boldsymbol{\beta}$ which achieves that rate. Hence, by choosing $\mathbf{a},\boldsymbol{\beta}$, and the codebook accordingly to (5.50), we can straightforwardly achieve any secrecy rate smaller than $C(P_R)$.

Combining the three cases we have the following lemma.

Theorem 5.4.2 (Achievable secrecy rate with the LC scheme)**.** *For a two-hop channel with an untrusted relay, with the LC scheme, any secrecy rate R_s satisfying*

$$R_s < \min(\max_{\mathbf{a},\boldsymbol{\beta}} R_s(\mathbf{a},\boldsymbol{\beta}), C(P_R)) \tag{5.60}$$

is achievable if $\sigma \le \underline{\sigma}$ and

$$R_s < \min(\max_{\mathbf{a},\boldsymbol{\beta}:R_{\mathrm{CF}}^B(\mathbf{a},\boldsymbol{\beta})\le C(P_B/\sigma^2)} R_s(\mathbf{a},\boldsymbol{\beta}), C(P_R)) \tag{5.61}$$

is achievable if $\sigma > \underline{\sigma}$.

5.4.3. ACHIEVABLE SECRECY RATES FOR SPECIAL CHANNEL CONFIGURATIONS

Here, we consider two special channel configurations. Firstly, if $P_R \ge P_A$ and the jammer is collocated with the destination, i.e., $\sigma = 0$,the first term in (5.64) can be maximized by choosing $\mathbf{a} = (1,1)$ and $\boldsymbol{\beta} = (\sqrt{\frac{P_B(1+P_A)}{P_A(1+P_B)}}, 1)$, which gives us the following corollary.

Corollary 5.4.1 (Achievable secrecy rate on a two-hop channel with an untrusted relay and the destination used as the jammer)**.** *On a two-hop channel with an untrusted relay, if $P_R \ge P_A$ and $\sigma = 0$, any secrecy rate R_s satisfying*

$$R_s < \frac{1}{2}\log\frac{1+P_A+P_B}{(\sqrt{(1+P_A)(1+P_B)}-\sqrt{P_AP_B})^2} - 1 \tag{5.62}$$

is achievable.

Then, if $P_A = P_B = P_R$ and $\sigma = 0$, by Corollary 5.4.1 we straightforwardly have the following corollary.

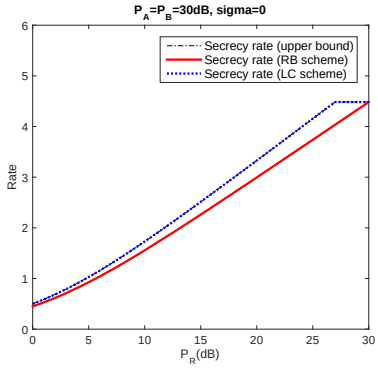
Corollary 5.4.2 (Achievable secrecy rate on a symmetric two-hop channel with an untrusted relay and the destination used as the jammer)**.** *On a two-hop channel with an untrusted relay, if* $\sigma = 0$ *and* $P_A = P_B = P_R$*, any secrecy rate* R_s *satisfying*

$$R_s < \frac{1}{2}\log(\frac{1}{2} + P_A) - \frac{1}{2} \tag{5.63}$$

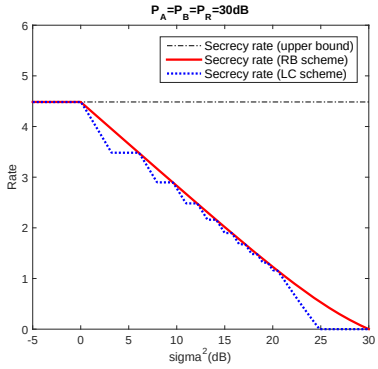
is achievable.

5.4.4. COMPARISON BETWEEN TWO SCHEMES

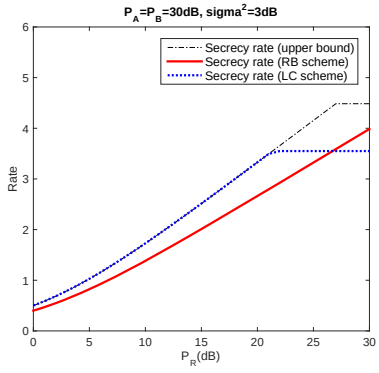
Firstly, we compare the two schemes in terms of simplicity in deployment, the LC scheme surely enjoys the benefit of a simpler structure and decoding. Also, the RB scheme requires a very long sequence of lattice codewords to achieve secrecy, i.e. N and length l should be sufficiently large, which is not the case for the LC scheme in which only N needs to be chosen sufficiently large.



(a) The comparison under the limited relay power condition (destination functions as the jammer).



(b) The comparison under the non-collocated jammer and destination condition.



(c) The comparison under both conditions

Figure 5.4: Comparison between the achievable secrecy rate of the RB scheme and the LC Scheme

Then, we compare the achievable secrecy rates of the two schemes. In the case of $P_R \geq P_A$ and $\sigma \leq \underline{\sigma}$, both of the two schemes achieve the same secrecy rate of (5.39). Then, when $P_R < P_A$, thanks to the chain structure, the LC scheme allows the relay to save the part of the energy of transmitting the random vector V^A. This feature allows the LC scheme to achieve a secrecy rate that equals the capacity when the relay has limited power, while the RB scheme underperforms. In other word, when $\sigma \leq \underline{\sigma}$, the rate of the LC scheme (5.60) is always no lower than the rate of the RB scheme (5.43). In Fig. 5.4(a) where $P_A = P_B = 30$dB and the destination is used as the jammer, it is clear that the curve of the LC scheme is higher than the RB scheme and coincides with the upper bound. Note that in this chapter all the powers are shown in dB, since they are actually the SNR with unit noise.

In the case of $P_R \geq P_A$ and $\sigma > \underline{\sigma}$, for the sake of reliable decoding of V^B at node C, the transmit rate should be reduced. For the LC scheme, due to the constraint of (5.52), node B cannot simply use the same lattice codebook and reduce its transmit rate. Hence, in this case, the RB scheme could achieve a higher rate than the LC scheme. In Fig. 5.4(b), the rate of the RB scheme is always higher than the LC scheme. However, they are both far away from the upper bound when σ is large. The shape of the curve of the LC scheme is due to the fact that sometimes the achievable secrecy rate is maximized by choosing a different a_1 for the different σ, which is a positive integer.

In the case of $P_R < P_A$ and $\sigma > \underline{\sigma}$, it will be a trade-off between these two issues. As observed in Fig. 5.4(c), when $\sigma^2 = 3$dB, the LC scheme performs better when P_R is low, but is overtaken by the RB scheme when P_R is larger than some threshold.

Summarizing the three cases discussed above, a new lower bound on the achievable secrecy rate on this channel is derived.

Corollary 5.4.3 (Lower bound of the achievable secrecy rate on the two-hop channel with an untrusted relay)**.** *On a two-hop channel with an untrusted relay, any secrecy rate R_s satisfying*

$$R_s < \min\left(\max_{\mathbf{a},\boldsymbol{\beta}} R_s(\mathbf{a},\boldsymbol{\beta}), C(P_R)\right) \tag{5.64}$$

is achievable if $\sigma \leq \underline{\sigma}$, and

$$\begin{aligned} R_s \quad < \quad \max\Bigg[\min\Bigg(&\max_{\mathbf{a},\boldsymbol{\beta}:R^B_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta})\leq C(P_B/\sigma^2)} R_s(\mathbf{a},\boldsymbol{\beta}), C(P_R)\Bigg), \\ &\left(C(P_A)+C(P_B/\sigma^2)-C(P_A+P_B)\right)\frac{C(P_R)}{C(P_A)}\Bigg] \end{aligned} \tag{5.65}$$

is achievable if $\sigma > \underline{\sigma}$.

5.5. PERFORMANCE ANALYSIS AND COMPARISON

In this section, the achievable secrecy rate of our schemes and other schemes are compared under various scenarios.

5.5.1. SYMMETRIC TWO-HOP CHANNEL WITH DESTINATION AS JAMMER

We first discuss the very well studied symmetric two-hop channel with the destination functioning as a cooperative jammer, which is a special case of our model when $P_A =$

$P_R = P_B$ and $\sigma^2 = 0$. Here, both our schemes achieve the sames secrecy rate of (5.63). We compare it to the achievable secrecy rate with an amplify-and-forward based scheme proposed by Sun *et al.* in [37] and a modulo-and-forward based scheme propose by Zhang *et al.* in [48]. Their achievable secrecy rates are in (5.10) and (5.11), respectively. In particular, (5.11) can be simplified to

$$R_s < C(P_A) - \frac{1}{2} - \frac{1}{2}\log\left(1 + \frac{P_A}{1+P_A}\right). \tag{5.66}$$

We also compare our schemes with the compress-and-forward based scheme proposed by He *et al.* in [14].The achievable secrecy rate is in (5.12) and can be simplified to

$$R_s < \frac{1}{2}\log\left(2 + \frac{1}{P_A} + P_A\right) - 1. \tag{5.67}$$

In Fig. 5.5, we set $P_A = P_B = P_R = 20$dB and compare these schemes with the upper bound (5.8). Moreover, the rate of He *et al.* in [16] and Vatedka *et al.* in [40] are illustrated in the same figure, although these are the rates for strong secrecy and perfect secrecy, respectively. We also show the capacity without the consideration of secrecy as a reference. It is clear that our scheme outperforms all other existing secure transmission scheme in the high SNR region and is upper bound achieving when $P_A \to \infty$. Also, it is interesting to observe that, in the high SNR region, to achieve strong secrecy and perfect secrecy, a rate of 0.5 and $0.5 + \log e$ bits/channel use is lost, respectively.

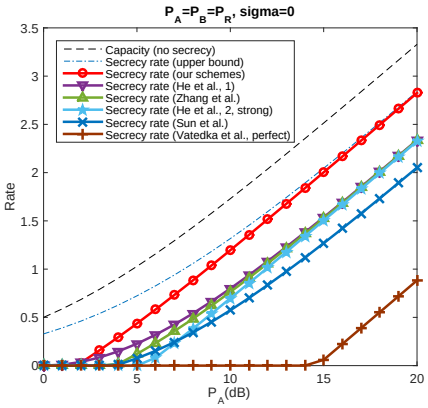
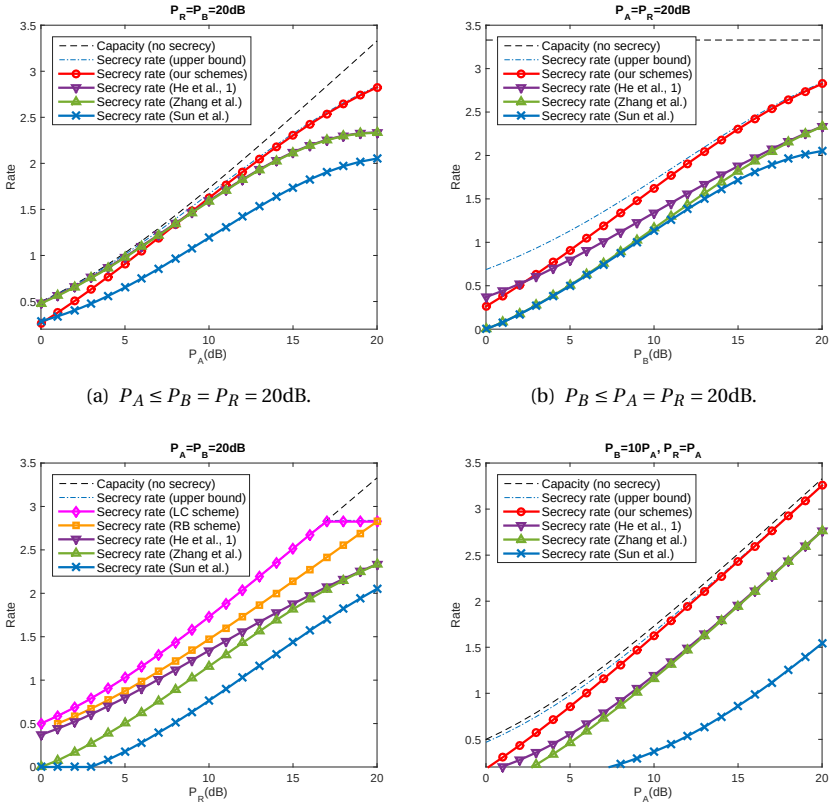


Figure 5.5: Comparison between the achievable secrecy rates of variant schemes in a symmetric two-hop channel using the destination as jammer.

5.5.2. ASYMMETRIC TWO-HOP CHANNEL WITH DESTINATION AS JAMMER

In case of $\sigma = 0$, we compare our schemes to the capacity without secrecy constraint, the upper bound (5.8), as well as the schemes by Sun *et al.* in [37], Zhang *et al.* in [48], and He *et al.* in [14], the rates of which are in (5.10), (5.11), and (5.12), respectively. It can be observed from Fig 5.6(a)-5.6(c) that if we fix two of $P_i, i \in \{A, B, R\}$ and change one of them, our schemes outperform all other schemes except for the low source and/or jammer



(a) $P_A \le P_B = P_R = 20$dB. (b) $P_B \le P_A = P_R = 20$dB.

(c) $P_R \le P_A = P_B = 20$dB. (d) $P_B = 10P_A, P_R = P_A$.

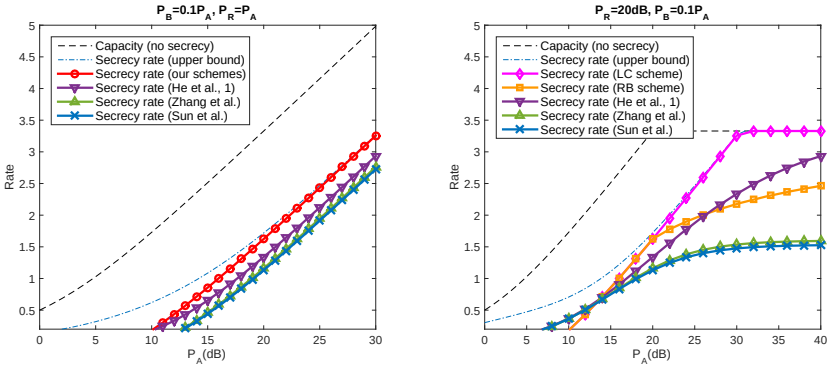
Figure 5.6: Comparison between the achievable secrecy rates of various schemes in asymmetric two-hop channels using the destination as jammer.

power case. Moreover, the LC scheme achieves the upper bound for the low relay power cases (the curve coincides with the upper bound). To the best of our knowledge, this is the first upper bound achieving scheme for the limited relay power and non-infinity source power case.

Furthermore, we compare the achievable secrecy rate of various schemes with the upper bound in the case of $P_B = \alpha P_A, \alpha > 0$, and $P_A \to \infty$. In this case, we define the gap between the upper bound of the secrecy rate derived in [14] and the channel capacity without secrecy consideration as

$$G_0 = \lim_{P_A \to \infty} [\min(C(P_A), C(P_R)) - \min(R_b, C(P_R))], \tag{5.68}$$

where R_b is the upper bound given in (5.8). Note that this upper bound is only for the secrecy rate in Phase 1. In Phase 2, the secrecy rate is upper bounded by $C(P_R)$. Similarly, for each secure transmission scheme, we define the gap between the achievable secrecy



(a) $P_B = 0.1P_A, P_R = P_A$. (b) $P_B = 0.1P_A, P_R = 20$dB.

Figure 5.7: Comparison between the achievable secrecy rates of various schemes in asymmetric two-hop channels using destination as jammer (Continued).

rate and the capacity without secrecy consideration as

$$G = \lim_{P_A \to \infty} [\min(C(P_A), C(P_R)) - \limsup_{N \to \infty} R_s], \tag{5.69}$$

where R_s is the achievable secrecy rate of the scheme.

When $P_R \geq P_A$, both our schemes achieve any rate satisfying (5.39), in which the RHS equals the RHS of (5.41). It can be calculated that we have $G = G_0 = C(1/\alpha)$, which reflects that our schemes are upper bound achieving in this case. Then, when $P_R < P_A$, the LC scheme still achieves the upper bound, which in this case is the channel capacity without secrecy consideration, i.e., $G = G_0 = 0$.

The G_0 value as well as the G values of various secure transmission schemes are shown in Table 5.1 for some channel configurations. Here, γ is defined as a positive real number. Is is shown that the LC scheme is the only upper bound achieving scheme in all the three cases considered in the table. For all other existing schemes, there are always gaps of at least a constant between the achievable secrecy rate and the upper bound in one or more cases.

In Fig. 5.6(d) and 5.7(a), the cases of $\gamma = 1, \alpha = 10$ and $\gamma = 1, \alpha = 0.1$ are illustrated, respectively. In Fig. 5.7(b), P_i is fixed to $P_R = 20$dB, $P_B = 0.1P_A$ and the performance of various schemes when P_R is limited is shown.

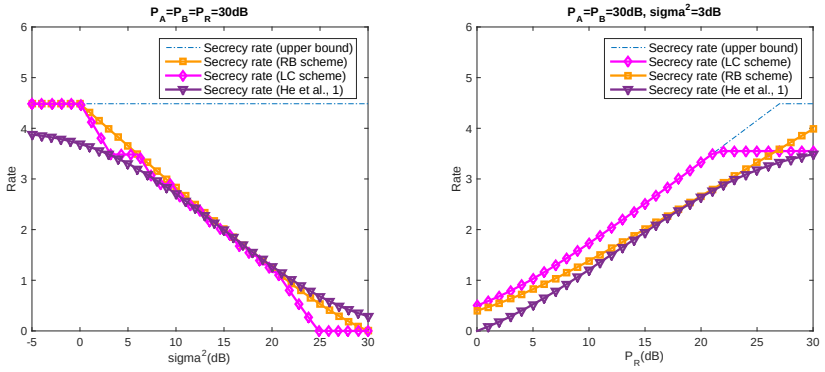
5.5.3. EXTERNAL JAMMER

Since the external jammer case is only considered by He *et al.* in [14], we compare our schemes to their scheme in Fig. 5.8(a) and Fig. 5.8(b) for different σ^2 and P_R. In Fig. 5.8(a) it can be observed that our schemes perform better when σ is small. When the channel between B and C is too noisy, the scheme of He *et al.* achieves a better rate. In Fig. 5.8(b), it is shown that our schemes have better performance in the limited relay power case. In particular, if the relay power is very low, the LC scheme is upper bound achieving even for large σ.

	$P_R = \gamma P_A$		P_R fixed
	$\gamma < 1$	$\gamma \geq 1$	
G_0 (Upper bound [14])	0	$C(\frac{1}{\alpha})$	0
G (RB scheme)	$\frac{C(P_R)}{C(P_A)} C(\frac{1}{\alpha})$	$C(\frac{1}{\alpha})$	0
G (LC scheme)	0	$C(\frac{1}{\alpha})$	0
G (He's scheme [14])	$C(\frac{1}{\alpha}) + C(\gamma)$	$[C(\frac{1}{\alpha}), C(\frac{1}{\alpha}) + C(\frac{1}{\gamma})]$ [a]	0
G (Zhang's scheme [48])	$C(\frac{1}{\alpha}) + C(\gamma)$	$C(\frac{1}{\alpha}) + C(\frac{1}{\gamma})$	$C(\frac{1}{\alpha})$
G (Sun's scheme [37])	$C(\frac{1}{\alpha}) + C(\gamma + \alpha)$	$C(\frac{1}{\alpha}) + C(\frac{\alpha+1}{\gamma})$	$C(\frac{1}{\alpha}) + C(\frac{\alpha P_R}{P_R+\alpha+1})$

[a] If $\alpha \geq 1$, the G value is $C(\frac{1}{\alpha}) + C(\frac{1}{\gamma})$. However, if $\alpha < 1$, the G value can be smaller than $C(\frac{1}{\alpha}) + C(\frac{1}{\gamma})$ depending on α. Hence, we only show the interval for the rate here.

Table 5.1: The G_0 and G values for various schemes when $P_B = \alpha P_A$ and $P_A \to \infty$.



(a) $\sigma \geq -5$dB, $P_A = P_B = P_R = 30$dB. (b) $\sigma^2 = 3$dB and $P_R \leq P_A = P_B = 20$dB.

Figure 5.8: Comparison between the achievable secrecy rates of various schemes in two-hop channels with an external jammer.

5.6. TWO-HOP CHANNEL WITH AN EAVESDROPPER

In this section, we propose another channel model, in which we consider the case that the relay is honest and cooperative, but there is an external eavesdropper.

5.6.1. MODEL

We firstly consider a two-hop channel in which node A wants to transmit information to node B using a relay node R to forward the information. During the process an eavesdropper is trying to obtain the information transmitted by node A. In this model we assume that the destination B also functions as a cooperative jammer. We also assume that the communication takes places over two phases, each including N channel uses. We use $X^A, X^B, X^R \in \mathbb{R}^N$ for the transmissions of node A, the destination B, and the relay

R, respectively. We use $Y^R, Y_1^E, Y_2^E, Y^B \in \mathbb{R}^N$ for the receptions of the relay, the eavesdropper in the two phases, and node B, respectively. In the first phase, node A transmits to the relay R and this transmission is eavesdropped by the eavesdropper E. The destination B simultaneously transmits a jamming signal to confuse the eavesdropper, which is also superimposed with the transmission of node A at the relay R. Hence, we have

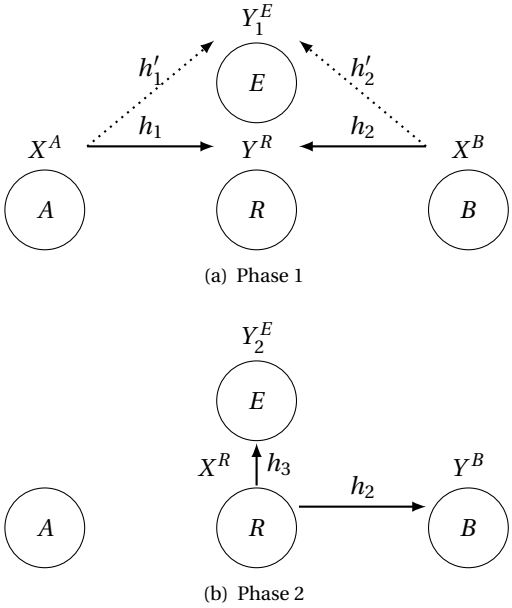
$$Y^R = h_1 X^A + h_2 X^B + Z^R, \tag{5.70}$$
$$Y_1^E = h_1' X^A + h_2' X^B + Z_1^E, \tag{5.71}$$

where Z^R and Z_1^E are N-dimensional independent Gaussian noise vectors and $h_1, h_2, h_1', h_2' \in \mathbb{R}^+$ are the channel coefficients. We further denote $\mathbf{h} = (h_1, h_2)$ and $\mathbf{h}' = (h_1', h_2')$.

In the second phase, the relay transmits to node B, which is also overheard by the eavesdropper.

$$Y^B = h_2 X^R + Z^B, \tag{5.72}$$
$$Y_2^E = h_3 X^R + Z_2^E, \tag{5.73}$$

where channel coefficient $h_3 \in \mathbb{R}^+$ and Z^B, Z_2^E are also N-dimensional independent Gaussian noise vectors. The model is illustrated in Fig. 5.9.



(a) Phase 1

(b) Phase 2

Figure 5.9: Two-hop channel with an eavesdropper.

The power constraints for the transmission of node A, B, and R are given in (5.4). W.l.o.g., we let all noise vectors have unit variance in each dimension. We assume the power constraints as well as all channel coefficients are revealed to all nodes. In this

model, the reliability constraint is still (5.5). However, the secrecy constraint becomes

$$\lim_{N\to\infty}\frac{1}{N}I(W^A;Y_1^E,Y_2^E)\le\delta \tag{5.74}$$

for any chosen $\delta>0$.

Remark 5.6.1. This problem is essentially different from the normal wire-tap type of problems or the problem we introduced in Subsection 5.2.1. The main difference is that the information is leaked to the eavesdropper twice from the source and the relay, respectively. Most of the existing secure transmission problems only focus on preventing the eavesdropper from getting information from one source.

5.6.2. CODING SCHEME

Here, we show that the RB scheme can be straightforwardly applied to achieve a positive secrecy rate if the transmit rate of the $(\mathbf{a},\boldsymbol{\beta})$ SCF code is set appropriately. The key for the deployment of the RB scheme is that the transmit rate should be chosen such that the eavesdropper can decode the same linear combination that the relay decodes. Then, the reception of the eavesdropper in the second phase will be a degraded version of the first phase, i.e., $H(Y_2^E|Y_1^E)=0$.

Before setting the transmit rate, we first give the definition of the computation rate in this model. Note that the expression of the computation rate is different from (2.16), which is due to the non-unit channel coefficients. The code and the transmit process are essentially the same. We define the computation rate in this model for $i\in\{A,B\}$ as

$$\tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}^*)=\frac{1}{2}\log\Big(\frac{\beta_i^2h_i^2P_i}{\mathcal{N}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}^*)}\Big), \tag{5.75}$$

where

$$\mathcal{N}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}^*)=\frac{h_A^2h_B^2P_AP_B(a_1\beta_A-a_2\beta_B)^2+(a_1h_A\beta_A)^2P_A+(a_2h_B\beta_B)^2P_B}{h_A^2P_A+h_B^2P_B+1}. \tag{5.76}$$

Here, $\mathbf{h}^*=(h_A,h_B)\in\mathbb{R}^+$. Note that $\mathcal{N}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}^*)$ is simply $\mathcal{N}(\mathbf{a},\boldsymbol{\beta})$ in (2.17) with all P_i substituted by $h_i^2P_i$.

Now we set the value for the transmit rate $R_t^i(\mathbf{a},\boldsymbol{\beta}), i\in\{A,B\}$. Firstly, to guarantee $H(Y_2^E|Y_1^E)=0$, we let the relay decode a linear combination $a_1X^A+a_2X^B$ which the eavesdropper can also decode. In this case, the transmission of the relay at Phase 2 will not leak more information since we have a Markov chain $Y_E^1\to a_1X^A+a_2X^B\to X^R\to Y_2^E$. By the data processing inequality we have $H(Y_2^E|Y_1^E)=0$ and

$$I(W^A;Y_1^E,Y_2^E)=I(W^A;Y_1^E). \tag{5.77}$$

By [50], there exists a sequence of lattice codes with which the relay and the eavesdropper are both able to decode $a_1X^A+a_2X^B$ if the transmit rate of node $i\in\{A,B\}$ satisfies

$$R_t^i(\mathbf{a},\boldsymbol{\beta})<\min(\tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}),\tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}')). \tag{5.78}$$

Similarly to (5.31), the information leakage rate of this code can be bounded by

$$R_o(\mathbf{a},\boldsymbol{\beta}) < C({h'_1}^2 P_A + {h'_2}^2 P_B) - R_t^B(\mathbf{a},\boldsymbol{\beta}). \tag{5.79}$$

Now, using the RB scheme with the transmit rate of the $(\mathbf{a},\boldsymbol{\beta})$ SCF code set accordingly to (5.78) and the random binning code generated w.r.t. (5.79), the reliable and secure transmission is guaranteed. The proof for the reliability and security are identical to the proof we given in Subsection 5.4.1. We thus have the following theorem for the achievable secrecy rate.

Theorem 5.6.1 (Achievable secrecy rate on two-hop channels with an eavesdropper)**.** *In a two-hop channel with an eavesdropper, any secrecy rate satisfying*

$$R_s < \max_{\mathbf{a},\boldsymbol{\beta}} \sum_{i\in\{A,B\}} \left(\min(\tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}), \tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}'))\right) - C({h'_1}^2 P_A + {h'_2}^2 P_B) \tag{5.80}$$

is achievable if $P_R \geq \frac{h_1^2}{h_2^2} P_A$ *and any secrecy rate satisfying*

$$R_s < \max_{\mathbf{a},\boldsymbol{\beta}} \left\{ \left[\sum_{i\in\{A,B\}} \left(\min(\tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}), \tilde{R}^i_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}'))\right) - C({h'_1}^2 P_A + {h'_2}^2 P_B) \right] \right.$$
$$\left. \frac{C(h_2^2 P_R)}{\min(\tilde{R}^A_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}), \tilde{R}^A_{\mathrm{CF}}(\mathbf{a},\boldsymbol{\beta},\mathbf{h}'))} \right\} \tag{5.81}$$

is achievable if $P_R < \frac{h_1^2}{h_2^2} P_A$.

Remark 5.6.2. When $h'_1 = h_1$, $h'_2 = h_2$, and $P_R \geq \frac{h_1^2}{h_2^2} P_A$, Theorem 5.6.1 mimics our result in Corollary 5.4.1. However, when the eavesdropper has a bad channel, e.g., $h'_1 \to 0$ and $h'_2 \to 0$, the achievable rate in Theorem 5.6.1 tends to zero, which reflect the suboptimality of this scheme.

Remark 5.6.3. As long as the sum computation rate w.r.t. the relay is larger than the MAC capacity of the eavesdropper $C({h'_1}^2 P_A + {h'_2}^2 P_B)$, our scheme achieves a positive secrecy rate. This is an interesting observation since the decode-and-forward based scheme [18] requires the MAC capacity of the relay to be higher than the eavesdropper to achieve a positive secrecy rate. In other words, SCF based schemes can sometimes achieve a positive secrecy rate even when the eavesdropper has a better channel than the relay, which is not feasible for decode-and-forward based schemes.

In Fig. 5.10 we show an example in which the RB scheme achieves a positive rate on a two-hop channel with an eavesdropper. The achievable secrecy rate is identical to the untrusted relay case when $h_1 = h_2 = h'_1 = h'_2 = 1$ and decreases if the h'_2 increases. With our scheme, a large h'_1 or a large h_2 will both result in small or even no secrecy rate at all.

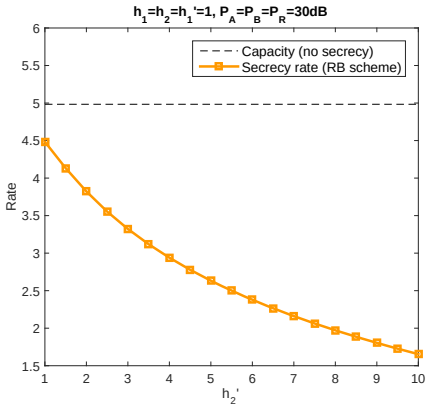


Figure 5.10: Achievable secrecy rate in a two-hop channel with an eavesdropper when $h_1 = h_2 = h_1' = 1$ as a function of h_2'.

5.7. CONCLUSION

In this chapter, we proposed two novel reliable and secure transmission schemes for the two-hop channel with an untrusted relay. These are the first secure transmission schemes that use the SCF technique. It has been shown that when the cooperative jammer and the destination are collocated, both of our schemes achieve relatively good secrecy rates in the high SNR region. Especially, for $P_B = \alpha P_A, P_R = \gamma P_A, \alpha, \gamma \in \mathbb{R}^+$, and $P_A \to \infty$, our schemes are the first upper bound achieving schemes for any α and γ. Moreover, the LC scheme is the first upper bound achieving scheme if P_R is limited and P_A is not unbounded. In summary, our schemes significantly improve the achievable secrecy rate lower bound and achieve the upper bound in two cases: 1, P_R is limited and P_A does not go to infinity. 2, P_A, P_B, P_R are linearly related and go to infinity.

Also, we proposed another two-hop channel model in which the relay is trusted but there exists an external eavesdropper. It has been shown that our RB scheme can also be exploited in this model and achieves a positive secrecy rate.

6

CONCLUSION

In this thesis, the benefit of compute-and-forward (CF) has been studied in three aspects: throughput, energy, and security. For the throughput and energy benefit, the focus is put on the multiple unicasts scenario in which CF is compared with other transmission schemes like traditional routing and network coding (NC). For security, the focus is on the problem of secure transmission on a two-hop channel with an untrusted relay.

6.1. THROUGHPUT BENEFIT

The throughput for multiple unicasts is recognized by many researches as one of the most difficult problems to solve amongst all communication problems. In this thesis, this problem has been studied with multiple transmission schemes to show the fundamental limit of the throughput benefit of CF. A generalized version of the model in [10] has been used, which abstracts two basic features of wireless networks: broadcast and superposition. The improvement factor of CF over traditional routing has been upper bounded by $3K$, where K is the number of sessions. Then, it has been shown that this upper bound gives a good insight of this problem since networks in which the improvement factor is at least $K/2$ are given. On the other hand, some networks in which CF is not beneficial have also been shown. These results revealed the fact that the throughput benefit of CF over traditional routing can be ranged from 1 to the order of K, depending on the types of networks.

Since it seemed that deriving tight bounds of the throughput benefit for general networks is not feasible, we studied a less complicated case: line networks with multiple bidirectional sessions, where the improvement factors of CF over traditional routing and NC are upper bounded by 2 and 1.5, respectively (or constants which are smaller than 2 or 1.5 depending on the session placements, respectively). Moreover, coding schemes have been proposed to achieve this improvement, which provide matching lower bounds. Our line network model can be seen as an extension to the two-way relay channel (TWRC) model in which the throughput benefit of CF is firstly put forward [42], and the multiple bidirectional sessions case can be seen as an extension of the line

networks with one bidirectional session case considered in [48]. Hence, the problem of the throughput of multiple bidirectional sessions on line networks has been extensively studied and a complete answer for the question of "how much can CF benefit in line networks over other schemes" is given with matching upper and lower bounds. The results turned to be very similar to that in the TWRC.

One step further, this problem has been studied with the "bidirectional" constraint dropped. For arbitrarily placed sessions, upper and lower bounds on the benefit have been derived which are asymptotically tight when the number of the sessions involved by each of the "bottleneck" nodes is large. For the large session number case, if the sessions are distributed uniformly at random and the traffic is balanced, the improvement factors of CF over traditional routing and NC are 2 or 1.5, respectively, which are exactly the same as the bidirectional session case as expected. Also, if the traffic is very imbalanced, CF can still provide an improvement factor of around 1.5 over traditional routing, while the improvement of NC over traditional routing is very limited.

Also, besides fixed centralized scheduling, the scenario that only decentralized scheduling is applied on line networks has also been considered. Line networks with all nodes applying the plain random access mechanism have been studied. It turned out that the throughput benefit of CF can be even higher since the improvement factors of CF over traditional routing and NC are upper bounded by $\frac{2}{1-p}$ and $\frac{1}{1-p}$, where p is the probability for each node to transmit. Also, a coding scheme which achieves these bounds has been proposed for the single bidirectional session scenario. This result did not come as a surprise since it has already been shown in many studies that CF can significantly improve the throughput while random access is used, e.g., [11]. Note that coding schemes have not yet been considered for multiple session scenarios, which remains as one of the last pieces of the puzzle for the throughput benefit study on line networks.

6.2. ENERGY BENEFIT

The same network and transmission model as the throughput benefit study have been used to study the energy benefit of CF in wireless networks with multiple unicast sessions, which has not been studied extensively in the existing literature. Firstly, the energy benefit on general networks has been considered. It turned out that the upper bound of the energy improvement factor is $\min(\bar{d}, K, 12\sqrt{K})$, where $\bar{d}$ is the average distance. This is very different from the throughput improvement factor. Firstly, the energy improvement is upper bounded by not only a function of K, but also the average distance. Secondly, it has been shown that there exists networks with the throughput improvement factors of at least $K/2$. However, this improvement is not feasible for the energy improvement factor when K is large since the energy improvement factor is upper bounded by $12\sqrt{K}$. Note that this upper bound also applies to the energy benefit of NC, which is the first result indicating that the energy benefit of NC is upper bounded by a factor of $\sqrt{K}$.

The energy benefit of CF over traditional routing has also been studied in some specific networks, namely star networks, line networks, and lattice networks. It has been derived that the energy improvement factors are upper bounded by some constants in all of these networks. In particular, for the star networks in which a node separates all sources from all destinations, CF is not beneficial at all. Furthermore, for line networks, 2-D and 3-D rectangular lattice networks, and hexagonal lattice networks, the energy

improvement factors are upper bounded by 2, 4, 6, and 3, respectively.

The lower bounds on the energy benefit of CF over traditional routing has also been studied by giving coding schemes which achieve these upper bounds. For line networks, the schemes proposed in Section 3.4 can achieve the factor of 2 improvement in energy for one long bidirectional session. For hexagonal lattice networks with a specific session placement, two novel coding schemes have been proposed which give energy improvement factors of between 2 and 3 depending on the ratio between the transmit and the receive power. For the cases that the transmit or receive power is negligible, our schemes achieve the upper bound of the energy benefit in hexagonal lattice networks.

6.3. SECURITY BENEFIT

The secure transmission on a two-hop channel with an untrusted (curious-but-honest) relay and the destination used as the cooperative jammer has been studied in many literature, in which various transmission schemes have been proposed [14, 15, 33, 37, 39, 40, 47] to achieve different levels of secrecy. For weak secrecy, an upper bound on secrecy rate has been derived in [14], which has not yet been achieved by any existing schemes in general. We proposed two secure transmission schemes based on a novel relaying technique, namely scaled CF (SCF). In terms of the secrecy rate w.r.t. weak secrecy, our schemes outperform all other existing schemes and achieve the upper bound in the high signal-to-noise-ratio (SNR) region. Our schemes can also be used in some other related channels, e.g., the two-hop channel with an untrusted relay and an external jammer (the destination is not used as the jammer) or the two-hop channel with an external eavesdropper (the relay is trusted in this case). It has been shown that our schemes outperform all existing schemes in some channel configurations. In particular, if the power of the relay is limited, one of our schemes achieves a secrecy rate as high as the channel capacity, while the achievable secrecy rates of all other schemes are strictly smaller than the channel capacity. Furthermore, for the external eavesdropper case, one of our schemes can sometimes achieve a positive secrecy rate even if the eavesdropper has a better channel than the relay, which is not feasible by the traditional decode-and-forward based secure transmission scheme [18].

6.4. SUGGESTIONS

Of course, this thesis leaves several unsolved problems and questions that are yet to be answered. Here, we list a few of them which we think are the most interesting ones.

- **Matching lower bounds.**

  It has already been shown that both the throughput benefit and the energy benefit are highly situational, which means that they differ from networks to networks. Hence, we believe that it is more promising and practical to find the matching lower bounds of the throughput and energy benefit in some specific networks, e.g., lattice networks, rather than to seek universal matching upper and lower bounds in general networks.

- **The gap between $\sqrt{K}$ and constant for the energy benefit**

As shown in Chapter 4, the energy improvement factor is upper bounded by $12\sqrt{K}$. However, for all the cases that have been considered so far, the energy improvement factors are no larger than constants. This leads to two possible explanations: either the upper bound can be proved to be a constant, or there exists a network in which the energy benefit is a factor at the order of $\sqrt{K}$. In our opinion, either of them could be true.

- **Other secure transmission problems with SCF based schemes**

  In this thesis, we proposed SCF based schemes which significantly improve the secrecy rate on the two-hop channel with an untrusted relay or an external eavesdropper. It has already been shown that it is beneficial to use CF in wireless networks in the sense of hiding individual messages from the untrusted parties, since it allows nodes to directly decode linear combinations of messages. Therefore, because SCF improves the rate for computing linear combinations in many asymmetric channel configurations, we believe that SCF has the potential of improving the achievable secrecy rate for many other secure transmission problems.

BIBLIOGRAPHY

[1] Rudolf Ahlswede, Ning Cai, Shuo-Yen R. Li, and Raymond W. Yeung. Network information flow. *Information Theory, IEEE Transactions on*, 46(4):1204–1216, 2000.

[2] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[3] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, 1978.

[4] Supratim Deb, Michelle Effros, Tracey Ho, David R. Karger, Ralf Koetter, Desmond S. Lun, Muriel Médard, and Niranjan Ratnakar. Network coding for wireless applications: A brief tutorial. In *In IWWAN*, 2005.

[5] Abbas El Gamal and Young-Han Kim. *Network information theory*. Cambridge university press, 2011.

[6] Peter Elias, Amiel Feinstein, and Claude E. Shannon. A note on the maximum flow through a network. *Information Theory, IRE Transactions on*, 2(4):117–119, 1956.

[7] Uri Erez and Ram Zamir. Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding. *Information Theory, IEEE Transactions on*, 50(10):2293–2314, 2004.

[8] Christina Fragouli, Jörg Widmer, and Jean-Yves Le Boudec. Efficient broadcasting using network coding. *IEEE/ACM Transactions on Networking (TON)*, 16(2):450–463, 2008.

[9] Michael Gastpar and Martin Vetterli. On the capacity of wireless networks: The relay case. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1577–1586. IEEE, 2002.

[10] Jasper Goseling, Michael Gastpar, and Jos H. Weber. Line and lattice networks under deterministic interference models. *Information Theory, IEEE Transactions on*, 57(5):3080–3099, 2011.

[11] Jasper Goseling, Michael Gastpar, and Jos H. Weber. Physical-layer network coding on the random-access channel. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2339–2343. IEEE, 2013.

[12] Jasper Goseling, Ryutaroh Matsumoto, Tomohiko Uyematsu, and Jos H. Weber. Lower bounds on the maximum energy benefit of network coding for wireless multiple unicast. *Eurasip Journal on Wireless Communications and Networking*, 2010:3, 2010.

[13] Jasper Goseling and Jos H. Weber. On the energy savings of network coding in wireless networks. In *the Thirty-first Symposium on Information Theory in the Benelux*, pages 177–184. WIC, 2010.

[14] Xiang He and Aylin Yener. Two-hop secure communication using an untrusted relay. *EURASIP Journal on Wireless Communications and Networking*, 2009:9, 2009.

[15] Xiang He and Aylin Yener. End-to-end secure multi-hop communication with untrusted relays. *Wireless Communications, IEEE Transactions on*, 12(1):1–11, 2013.

[16] Xiang He and Aylin Yener. Strong secrecy and reliable byzantine detection in the presence of an untrusted relay. *Information Theory, IEEE Transactions on*, 59(1):177–192, 2013.

[17] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong. A random linear network coding approach to multicast. *Information Theory, IEEE Transactions on*, 52(10):4413–4430, 2006.

[18] Jing Huang and A. Lee Swindlehurst. Secure communications via cooperative jamming in two-hop relay systems. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5. IEEE, 2010.

[19] Sidharth Jaggi, Peter Sanders, Philip Chou, Michelle Effros, Sebastian Egner, Kamal Jain, Ludo M.G.M. Tolhuizen, et al. Polynomial time algorithms for multicast network code construction. *Information Theory, IEEE Transactions on*, 51(6):1973–1982, 2005.

[20] Sachin Katti, Shyamnath Gollakota, and Dina Katabi. Embracing wireless interference: Analog network coding. *ACM SIGCOMM Computer Communication Review*, 37(4):397–408, August 2007.

[21] Sachin Katti, Hariharan Rahul, Wenjun Hu, Dina Katabi, Muriel Médard, and Jon Crowcroft. Xors in the air: practical wireless network coding. *ACM SIGCOMM Computer Communication Review*, 36(4):243–254, 2006.

[22] Alireza Keshavarz-Haddad and Rudolf H. Riedi. Bounds on the benefit of network coding for wireless multicast and unicast. *Mobile Computing, IEEE Transactions on*, 13(1):102–115, 2014.

[23] Sukwon Kim, Michelle Effros, and Tracey Ho. On low-power multiple unicast network coding over a wireless triangular grid. In *the 45th Annual Allerton Conference on Communication, Control and Computing*. Citeseer, 2007.

[24] Ralf Koetter and Muriel Médard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking (TON)*, 11(5):782–795, 2003.

[25] Zongpeng Li and Baochun Li. Network coding: The case of multiple unicast sessions. In *Allerton Conference on Communications*, volume 16, 2004.

[26] Junning Liu, Dennis Goeckel, and Don Towsley. Bounds on the gain of network coding and broadcasting in wireless networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 724–732. IEEE, 2007.

[27] Kejie Lu, Shengli Fu, Yi Qian, and Hsiao-Hwa Chen. On capacity of random wireless networks with physical-layer network coding. *Selected Areas in Communications, IEEE Journal on*, 27(5):763–772, 2009.

[28] Desmond S. Lun, Niranjan Ratnakar, Muriel Médard, Ralf Koetter, David R. Karger, Tracey Ho, Ebad Ahmed, and Fang Zhao. Minimum-cost multicast over coded packet networks. *Information Theory, IEEE Transactions on*, 52(6):2608–2623, 2006.

[29] Bobak Nazer and Michael Gastpar. Compute-and-forward: Harnessing interference through structured codes. *Information Theory, IEEE Transactions on*, 57(10):6463–6486, 2011.

[30] Bobak Nazer and Michael Gastpar. Reliable physical layer network coding. *Proceedings of the IEEE*, 99(3):438–460, 2011.

[31] Yasutada Oohama. Relay channels with confidential messages. *arXiv preprint cs/0611125*, 2006.

[32] Petar Popovski and Hiroyuki Yomo. Physical network coding in two-way wireless relay channels. In *Communications, 2007. ICC'07. IEEE International Conference on*, pages 707–712. IEEE, 2007.

[33] Johannes Richter, Christian Scheunert, Sabrina Engelmann, and Eduard Jorswieck. Weak secrecy in the multi-way relay channel with compute-and-forward. In *European School of Information Theory*. IEEE, 2014.

[34] Johannes Richter, Christian Scheunert, Sabrina Engelmann, and Eduard Jorswieck. Weak secrecy in the multi-way untrusted relay channel with compute-and-forward. *Information Forensics and Security, IEEE Transactions on*, 10(6):1262 – 1273, 2014.

[35] Yalin E. Sagduyu and Anthony Ephremides. Cross-layer optimization of mac and network coding in wireless queueing tandem networks. *Information Theory, IEEE Transactions on*, 54(2):554–571, 2008.

[36] Claude E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[37] Li Sun, Taiyi Zhang, Yubo Li, and Hao Niu. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *Vehicular Technology, IEEE Transactions on*, 61(8):3801–3807, 2012.

[38] Ender Tekin and Aylin Yener. The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *arXiv preprint cs/0702112*, 2007.

[39] Shashank Vatedka and Navin Kashyap. Nested lattice codes for secure bidirectional relaying with asymmetric channel gains. In *Information Theory Workshop (ITW), 2015 IEEE*, pages 1–5. IEEE, 2015.

[40] Shashank Vatedka, Navin Kashyap, and Andrew Thangaraj. Secure compute-and-forward in a bidirectional relay. *Information Theory, IEEE Transactions on*, 61(5):2531–2556, 2015.

[41] Gengkun Wang, Wei Xiang, and Jinhong Yuan. Outage performance for compute-and-forward in generalized multi-way relay channels. *Communications Letters, IEEE*, 16(12):2099–2102, 2012.

[42] Makesh P. Wilson, Krishna Narayanan, Henry D. Pfister, and Alex Sprintson. Joint physical layer coding and network coding for bidirectional relaying. *Information Theory, IEEE Transactions on*, 56(11):5641–5654, 2010.

[43] Yunnan Wu, Philip A. Chou, Sun-Yuan Kung, et al. Information exchange in wireless networks with network coding and physical-layer broadcast. Technical report, MSR-TR-2004, 2005.

[44] Aaron D. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8):1355–1387, 1975.

[45] Xican Yang, Jian Li, Changliang Xie, and Li Li. Throughput gain of random wireless networks with physical-layer network coding. *Tsinghua Science and Technology*, 17(2):161–171, 2012.

[46] S.M.S. Tabatabaei Yazdi, Serap A. Savari, Gerhard Kramer, Kelli Carlson, and Farzad Farnoud. On the multimessage capacity region for undirected ring networks. *Information Theory, IEEE Transactions on*, 56(4):1930–1947, 2010.

[47] Shengli Zhang, Lisheng Fan, Mugen Peng, and H. Vincent Poor. Near-optimal modulo-and-forward scheme for the untrusted relay channel. *arXiv preprint arXiv:1503.08928*, 2015.

[48] Shengli Zhang, Soung C. Liew, and Patrick P. Lam. Hot topic: physical-layer network coding. In *Proceedings of the 12th annual international conference on Mobile computing and networking*, pages 358–365. ACM, 2006.

[49] Tao Zhang, Kejie Lu, Ayat Jafari, Shengli Fu, and Yi Qian. On the capacity bounds of large-scale wireless network with physical-layer network coding under the generalized physical model. In *Communications Workshops (ICC), 2010 IEEE International Conference on*, pages 1–5. IEEE, 2010.

[50] Jingge Zhu and Michael Gastpar. Asymmetric compute-and-forward with CSIT. *arXiv preprint arXiv:1401.3189*, 2014.

[51] Jingge Zhu and Michael Gastpar. Multiple access via compute-and-forward. *arXiv preprint arXiv:1407.8463*, 2014.

ACKNOWLEDGEMENTS

During my years in TU Delft, there are a number of people who have played important roles in various aspects of my study and personal life. Herewith, I would like to express my gratitude to all of you.

Firstly, I would like to thank my promoter, Prof. dr. Michael C. Gastpar. Although we only met for a couple of weeks each year, you were always helpful and reserved as much time as possible for guidances discussions to make every visit of mine fruitful. Your suggestions are always insightful and inspiring, which leads to many interesting results in this thesis. Most of the times, we communicated via Skype, which is not the most efficient way of communication. I am very glad and thankful that I reach this satisfiable end under your supervision.

Next, I would like to express my sincere appreciation to my co-promoter and daily supervisor, Dr. ir. Jos. H. Weber. We first met 7 years ago when you was my teacher in the course of error correcting codes. You then became my teacher and mentor in both academic and personal life and guided me through all these years as a MSc and PhD student. You are critical about my mistakes while being extremely helpful, patience, and encouraging to me. As a person, you are a perfect role model to me for a senior researcher, that I am still trying to learn from. I would not be able to have this thesis without your priceless suggestions and support.

Then, I would also like to thank Dr. ir. Jasper Goseling, who selflessly offered lots of valuable suggestions and comments during the whole period of my PhD study. All of our discussions and exchanged opinions eventually turns into nice publications and parts of this thesis.

Of course, I owe a big thank to my parents, who always stand behind me and are always there for me. Especially to my father, who also helped me a lot in revising this thesis. I am very glad and proud that I followed your path to Delft. I love both of you very much.

Last but not least, I would like to give affectionate appreciation to my lovely girlfriend, Yu Xin. Meeting you is one of the best moments that I have in the Netherlands, and being with you is the luckiest thing that could ever happen to me. I must be blessed to have you during my PhD study. Thank you for all the supports and encourages that you warmly offered.

There are a lot of people who have helped and supported me in different ways during various period of my stay in the Netherlands. Having the privilege to know you and have you by my side is such an unmatchable pleasure and honor. Thank you all very, very much.

Zhijie Ren
July 2016
Delft, the Netherlands

LIST OF FIGURES

LIST OF THEOREMS

CURRICULUM VITÆ

Zhijie REN

26-09-1988 Born in Beijing, China.

EDUCATION

2003 – 2007 BS in Telecommunication
Beihang University, Beijing China

2007 – 2011 MSc in Telecommunication
Delft University of Technology, Delft, the Netherlands
Thesis: The Stopping Set Property and the Iterative Decoding Performance of Binary Block Codes on BSC and AWGN Channel
Supervisor: Dr. ir. Jos H. Weber

2012 – 2016 PhD Candidate in Department of Intelligent Systems
Delft University of Technology, Delft, the Netherlands
Topic: Benefits of Compute-and-forward in Throughput, Energy, and Security
Promotor: Prof. dr. Michael C. Gastpar
Copromotor: Dr. ir. Jos H. Weber

PUBLICATIONS

- Z. Ren, J. H. Weber, A. J. van Zanten"Impact of stopping set properties on iterative decoding of FG-LDPC codes on the binary symmetric channel," *Proc. of the Thirty-third WIC Symp. on Inf. Theory in Benelux*, Boekelo, the Netherlands, May, 2012.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Compute-and-forward on a line network with random access," *Proc. of the Thirty-fourth WIC Symp. on Inf. Theory in Benelux*, Leuven, Belgium, May, 2013.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Compute-and-forward: multiple bi-directional sessions on the line network," *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Istanbul, Turkey, July, 2013.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Maximum throughput gain of compute-and-forward for multiple unicast," *IEEE Comm. Letters*, vol. 18, pp. 1111-14, July, 2014.

- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "On the energy benefit of compute-and-forward on the hexagonal lattice," *Proc. of the Thirty-Fifth WIC Symp. on Inf. Theory in Benelux*, Eindhoven, the Netherlands, May, 2014.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission using an untrusted relay with scaled compute-and-forward," *IEEE Inf. Theory Workshop (ITW)*, Jerusalem, Israel, Apr. 2015.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission on two-hop relay channel with scaled compute-and-forward," *Submitted to IEEE Trans. on Inf. Theory*.
- Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "On the energy benefit of compute-and-forward for multiple unicasts," to appear in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Barcelona, Spain, July, 2016.