國立中山大學通訊工程研究所

碩士論文

Institute of Communications Engineering

National Sun Yat-sen University

Master Thesis

在放大後前送多中繼系統中預防惡意竊聽之預編碼器設計

Precoder Design for Amplify-and-Forward Cooperative Systems with Multiple Wiretapping Relays

研究生：李家豪

Chia-Hao Lee

指導教授：黃婉甄 博士

Dr. Wan -Jen Huang

中華民國一百零二年六月

June 2013

論文審定書

國立中山大學研究生學位論文審定書

本校通訊工程研究所碩士班

研究生李家豪（學號：M003070009）所提論文

在放大後前送多中繼系統中預防惡意竊聽之預編碼器設計
Precoder Design for Amplify-and-Forward Cooperative Systems With Multiple Wiretapping Relays

於中華民國 102年 6月 28日經本委員會審查並舉行口試，符合碩士學位論文標準。

學位考試委員簽章：

召集人 鍾偉和 鍾偉和　　委　員 黃婉甄 黃婉甄

委　員 葉家宏 葉家宏　　委　員 曾凡碩 曾凡碩

委　員 _____　　委　員 _____

指導教授(黃婉甄) 黃婉甄 (簽名)

致謝

首先，我想最應該謝的是我爸爸媽媽，可以讓我在高雄念書並且住得舒服，沒有他們的幫忙，我想現在也不會有這篇文章吧!再來，就是感謝黃婉甄老師和學長姐們，老師的教導方式非常自由和人性，讓我們可以自己分配自己的時間，我們可以在比較沒有壓力的情況下學習，也讓我的研究生生活也可以多采多姿，和老師亦師亦友的相處模式，我到現在其實還不是那麼習慣，不過，也因為這樣跟老師的關係良好，我想有機會一定會再回來實驗室聊聊天!學長姐總是可以有耐心地幫忙解決我的疑惑，並且總是可以一針見血說出我不懂的地方，真的很厲害!最後，謝謝我中山認識的所有人，謝謝實驗室同學們一起討論課業，互相砥礪，讓彼此都有所收穫，也謝謝曾經一起出去遊玩的大家，真的創造了很多很棒的回憶!

摘要

對無線通訊系統而言，由於其向四面八方廣播的特性，如何對其傳送的資訊加以保密，是個很值得研究的問題，除了利用應用層的加密技術之外，在文獻中亦有實體層保密(physical layer secrecy)技術之相關探討，其重點在於如何利用實體層通道的傳輸特性，進一步讓竊聽者無法竊取重要資訊，讓合法的傳輸更加可靠。本文考慮一個放大後前送(amplify-and-forward, AF)的合作式傳輸網路，網路中資料源與目的端皆配備多根天線，且有多個具備單天線的中繼端(relay)，中繼端扮演著資料源與目的端之間溝通的橋梁角色，然而在本文中，我們假設中繼端是不可靠的，可能會在未經許可的狀況下，竊取資料源的訊息。有鑑於此，在尋求不可靠的中繼端幫助傳送的同時，也要避免中繼端成功竊聽，因此在資料傳送訊號的同時，由目的端產生一個人工雜訊(artificial noise, AN)，以期破壞中繼端對來源訊號的解碼，因為人工雜訊由目的端產生，所以其接收到中繼端傳送的訊號時，可自行消除人工雜訊的部分，不至於影響正常通訊。我們在資料源與目的端各佈置一個預編碼器(precoder)，用來設計傳送端訊號與目的端人工雜訊的統計特性，在中繼端乘上預編碼係數後，傳送給目的端，為了要系統的具備保密的效能，欲藉由確保服務品質(quality of service, QoS)為系統考慮依據，將使用最佳化的方式來聯合設計傳送訊號與人工雜訊的統計特性，以及中繼端放大後前送的預編碼係數，達到需求品質下的最佳保密容量(secrecy capacity)，透過模擬方式可以得知，使用人工雜訊干擾竊聽者，以及最佳化傳輸訊號與人工雜訊的統計特性，確實可以提升合作式系統中，對於不可靠中繼端的保密容量。

關鍵字:合作式通訊、實體層保密、保密容量、預編碼器。

Abstract

Due to the broadcast nature of wireless medium, how to ensure the security of wireless transmission is worth investigating. In addition to the encryption techniques commonly adopted in the application-layer, physical-layer secrecy communications drawn significant research concern recently. Physical-layer secrecy communication is achieved by exploiting spatial property of the physical-layer channel, such that the eavesdroppers can't decode source important information successfully, and the legitimate transmission becomes more reliable. This thesis considers an amplify-and-forward cooperative network, where the source and destination are equipped with multiple antennas, while multiple relays have single antenna. The relays act a bridge between the source and destination, but we assume that these relays are not reliable and may wiretap the information without authorization. As a result, while being assisted by those untrusted relays, we must avoid relays eavesdropping source information. In order to prevent relay from wiretapping information, the destination generates artificial noise(AN) simultaneously to interfere signal reception at relays, when the source transmits information. Since AN is generated by the destination, the destination can eliminate AN by itself after receiving signal forwarded from the relays to fully eliminate additional interference at the destination. We employ linear precoder at the source and destination to optimize the statistical properties of the transmission signal and artificial noise. On the other hand, the relays scale the received signal by a precoding coefficient before retransmission. Instead of maximizing the secrecy rate, we adopt quality of service(QoS)-based criterion to ensure secrecy transmission implicitly since the secrecy rate is

non-convex. More specifically, the precoders at the source, relays and destination are jointly optimazed in terms of maximum SNR of the destination subject to the SINRs at all relays are constrained. Through computer simulation, it shows that secrecy rate is improved obviously through introducing artificial noise and joint optimization of precoders compare with the scheme without AN and the scheme using arbitrary precoders.

***Key words*—Cooperative network, physical-layer secrecy, precoder, optimization.**

目錄

圖次

第一章 簡介

近年來，人們對多媒體無線通訊的需求逐漸脫離萌芽期，而進入爆炸性成長的階段，除了對穩定和高速資料傳輸的渴求外，無論何時何地皆能享受無間斷的通訊服務成為這世代的通訊願景與重要的議題。雖然今日無線通訊技術已帶來相當多的便利，但仍然有很多潛在的問題需要克服，在訊號傳遞的過程中，很少的訊號會經由直接路徑(direct link)傳送到目的端，大部分訊號會經過許多障礙物，經歷多次折射、散射與繞射後，才會抵達目的端，然而這些經過折射、散射與繞射的訊號，抵達目的端的時間和相位不盡相同，就會形成所謂的多重路徑衰減(multipath fading)，因此，為了對抗多重路徑對目的端所造成的訊號雜訊比值(signal-to-noise ratio, SNR)衰減，導致訊息在目的端無法被順利解碼，我們運用提升分集(diversity)的方法，來降低訊號雜訊比值的衰減，其中包含了時間分集(temporal diversity)、頻率分集(frequency diversity)與空間分集(spatial diversity)，而多重輸入多重輸出(multi-input multi-output, MIMO)系統[1]，就是利用空間分集的方法，使用多根傳送天線與接收天線，讓訊號傳送的路徑有更多的選擇性，降低多重路徑衰減對接收訊號所造成的影響。

在很多無線傳輸的系統中，傳送端與接收端可能因為外觀限制輕薄短小方便攜帶，電池體積也變小，功率受到限制，或著因為成本關係，複雜度不能做得太高等原因，無法提供多根天線傳送與接收訊號，所以，多重輸入與多重輸出系統衍伸出了合作式通訊(cooperative communication)系統[2]-[5]，合作式通訊系統的架構是由一組傳送端與目的端，和一個或多個中繼端(relay)所組成，當傳送端傳送至目的端的訊號遭受多重路徑衰減時，我們可以透過中繼端幫忙傳送訊號，此

時，傳送端靠著多個中繼端所提供的多條通道，與自身到達目的端的直視訊號，可以獲得和多重輸入與多重輸出系統一樣的空間分集優勢，並且可以在目的端使用多重輸入與多重輸出系統中的最大比例合併(maximum ratio combining, MRC)、相等增益合併(equal gain combining, EGC)、選擇合併(selection combining, SC)等技術，結合接收至不同通道的訊號，來達到分集增益(diversity gain)的效果。中繼端對於接收訊號有幾種常見的傳輸技術，例如：放大後前送(amplify and forward, AF)和解碼後前送(decode and forward, DF)[6]等；在放大後前送的技術中，中繼端對接收到的訊號單純進行放大後，傳送給目的端；而解碼後前送技術中，傳送端訊號經編碼後傳送，中繼端接收訊號後進行解碼，再將解碼後的訊號傳送給目的端，若未解碼成功則不傳送給目的端，目的端會將直視訊號與中繼端傳來的訊號合併，可以增加訊號的品質，再經解調求得原本的訊號。

本文考慮一個放大後前送(amplify-and-forward, AF)的多中繼合作式傳輸網路，並考慮資料源與目的端相距遙遠的特殊情況，因此資料源傳至目的端的直視訊號，因為會隨著路徑衰減的關係，目的端可以忽略之。在一般放大後前送的合作式系統中，各中繼端會幫忙資料源傳送訊號給目的端，且過程中並不會進行解碼的動作，而目的端可因此得到分集增益的效果，但本文各中繼端被假設為潛在竊聽者，具有潛在的威脅性，亦即他可能會擅自解開資料源送出的訊息，因為不知道會進行竊聽的中繼端數量，所以必須防範全部的中繼端，因此，我們在使用這些不可靠的中繼端幫助傳送的同時，也要避免中繼端獲得足夠的資訊來破壞傳輸者的隱私。為了預防這些中繼端從接收訊號獲得重要的隱私資訊，資料源傳送訊號的同時，從目的端產生人工雜訊(artificial noise, AN)[7][8]，即目的端兼具干擾器(jammer)[9]的功能；因為通道完美已知，因此目的端可以自行消除其產生的人工雜訊，不會對目的端的接收造成不良影響，並且可以降低中這些中繼端順利

解開資料源訊息的機率。雖然保密通訊亦可藉由網路應用層的加密(encryption)來達成，但加密之前須傳遞金鑰，而金鑰的保密則只能靠實體層來協助，可以透過傳輸方向的特性，干擾竊聽者的接收，因此，探討實體層的保密是有其重要性，並且可以強化應用層保密。實體層的保密效能是藉由保密容量[10]-[13]來評估，其涵義為在保證對不可靠的中繼端完全保密的前提下，能順利傳送給目的端的最大資訊量，計算方法為資料源到目的端的通道容量，減去資料源到不可靠的中繼端的通道容量，在系統存在多個竊聽者時，通常考慮被竊聽程度最糟糕的案例，也就是將系統目的端的通道容量，以及所有竊聽者中最大的通道容量相減，若此差值為負值，那保密容量則為零，表示系統傳輸沒有保密的效能，為了使系統具備保密的效能，我們基於參考文獻，在資料源與目的端皆配備多天線，且具備多個不可靠的單天線中繼端的合作式網路中，提出在資料源與目的端各佈置一個預編碼器，並由設計傳送訊號計特性，與多個中繼端的最佳的預編碼係數，以及目的端產生人工雜訊的主動保密策略，在各節點的功率限制下，達到系統保密容量的最佳化；本篇文章中，我們以保密容量為問題出發點，想使其值達到最大，但因為保密容量並非為一個凸函數(convex)形式，因此，以確保服務品質(quality of service, QoS)為系統考慮依據，化簡一開始的最佳化問題，讓目的端的 SNR 值可以達到最大，並限制各個不可靠中繼端的訊號與干擾雜訊比值(signal & interference-to-noise ratio, SINR)，又因為想一次設計傳送訊號及人工雜訊統計特性，與中繼端預編碼係數最佳值，相當困難，又將問題拆解成兩個子問題，先求得中繼端傳送訊號的最佳預編碼係數後，再依據確保服務品質的最佳化問題，去聯合設計我們最佳的傳送端傳送訊號及人工雜訊統計特性，以這兩子問題交互疊代，至目的端的 SNR 值收斂為止，即求出資料源訊號與人工雜訊最佳的傳送方式，以及此時中繼端最佳的預編碼係數，因為問題中使用確保 QoS 的形式，對各個中繼端的接收訊號品質有所限制，相對於最佳化得到的目的端接收品質，在

通道容量上的造成差距，進一步對系統提供了保密容量。由模擬結果可驗證，我們在多個不可靠的單天線中繼端系統中所提出的策略，使用人工雜訊幫助，以及設計最佳的傳輸訊號與人工雜訊統計特性，確實可以增進系統的保密容量，提供系統保密的效能。

本論文主要結構如下:第二章會先介紹過去所提出的保密主題相關研究文獻；第三章將考慮一個具備多個不可靠中繼端的合作式通訊系統模型；第四章將說明各中繼端的放大系數分配,以及傳送端預編碼器與目的端人工雜訊的設計方法；第五章展示電腦模擬結果，並探討系統保密容量；第七章為論文總結。

第二章 文獻探討

在過去的通訊系統保密的議題中，大部分是直接對傳送訊號進行編碼加密等技術來達成，近年來，越來越多文獻提出對於無線通訊系統的實體層保密技術，可以透過施加人工雜訊的方式，有效的干擾竊聽者端的接收訊號，以導致竊聽者無法順利的解出實際傳送資訊，達到實體層保密的功效。

2.1 使用人工雜訊干擾的保密

在文獻[14]中，討論一個具備三個節點的多重輸入單輸出(multiple-input single- output, MISO)，並且存在一個竊聽者的系統，當傳送端傳送訊息到正統的接收端的同時，也有竊聽者跟著竊聽所傳送的訊息，各端所具備的天線數分別是 M_t 、 M_r 與 $M_e(M_t > M_e = M_r = 1)$，如下圖

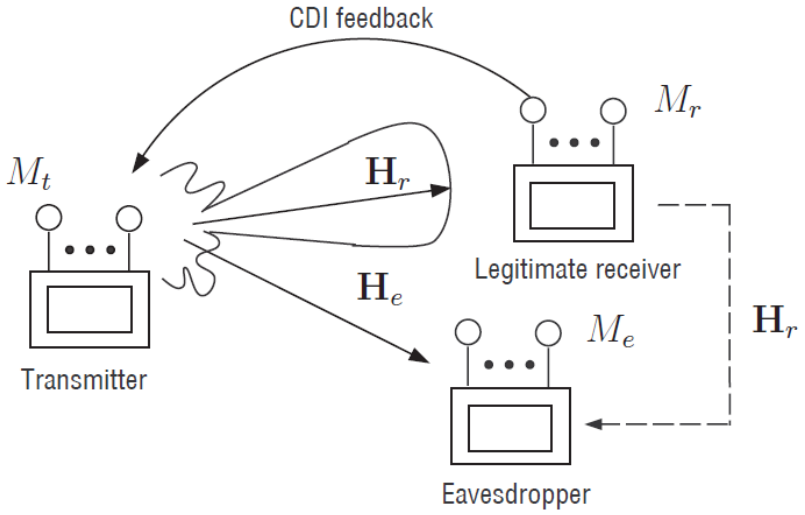

圖 2-1 三節點中有竊聽者存在的系統圖

此系統中，正統接收端和竊聽者的接收訊號為

$$y_r[i] = h_r x[i] + z_r[i] \tag{2.1}$$

$$y_e[i] = h_e x[i] + z_e[i] \tag{2.2}$$

其中 h_r, $h_e \in \mathrm{C}^{1\times M_t}$ 為傳送端到正統接收端與竊聽者端的通道係數，且具有相同的統計特性 $CN\left(\mathbf{0},\mathbf{I}_{M_t}\right)$，$x[i]$ 為在單一時間巢(time slot) i 中的傳送訊號，功率限制以 $\mathrm{E}\left[\left\|x[i]\right\|^2\right] \le P$ 表示，而 $z_r[i]$ 為正統接收端雜訊，其統計特性為 $CN(0,1)$，$z_e[i]$ 為竊聽者端的雜訊，其統計特性為 $CN\left(0,\sigma_e^{\,2}\right)$。

為了確保通訊保密，使用人工雜訊來阻斷竊聽者的接收，同時使用束波成形(beamforming)向量傳送訊息到正統的接收端，傳輸的訊號為

$$x[i] = \mathrm{p}s[i] + \mathrm{Qa}[i] \tag{2.3}$$

其中 $s[i]$ 為單一時間巢(time slot) i 中攜帶訊息的訊號，且能量為 $\mathrm{E}\left[\left|s[i]\right|^2\right] = \sigma_s^{\,2}$，p 為束波成形向量，而 Q 為人工雜訊在正統接收通道子空間的正交基底，$\mathrm{a}[i] \sim CN\left(\mathbf{0},\sigma_a^2\mathbf{I}_{M_t-1}\right)$ 為隨機高斯產生的人工雜訊向量，並假設 $s[i]$ 和 $\mathrm{a}[i]$ 為獨立。討論量化通道方向資訊(channel direction information, CDI)下的保密容量時，本篇先定義 $g_r = h_r / \left\|h_r\right\|$，並假設 g_r 被量化到 2^B 的向量碼字書 $C = \left\{c_1, c_2, ..., c_{2^B}\right\}$ 中， 以及 $v_l = \left\{g \,|\, \left|gc_l^{\,H}\right|^2 \ge \left|gc_j^{\,H}\right|^2 \forall\, j \ne l\right\}$ 為碼字書中在實際通道上投影量最大的向量，藉此判定 c_l 與實際通道是否最吻合的，並且回傳給傳送端，再來將我們上面式子近似為

$$\nu_l \approx \left\{ g \,|\, \left| g c_l^{\,H} \right|^2 \geq 1-\delta \right\} \tag{2.4}$$

其中 $\delta = 2^{-\frac{R}{M_t-1}}$，以及 $\left| g_r \hat{g}_r^{\,H} \right|^2 = \left| g_r c_{l^*}^{H} \right|^2 = \cos^2\theta \geq 1-\delta$。

所以當只知道量化通道方向資訊時，訊號可以寫成下面式子

$$x[i] = \hat{g}_r^{\,H} s[i] + \mathrm{N}_{\hat{g}_r} \mathrm{a}[i] \tag{2.5}$$

其中 $\hat{g}_r$ 為量化的正統通道方向資訊，而 $\mathrm{N}_{\hat{g}_r}$ 為 $\hat{g}_r$ 零和空間中的向量，此時，假設傳送端傳輸功率限制為 $\mathrm{E}\left[\left\| \mathrm{x}[i] \right\|^2 \right] = \sigma_s^2 + (M_t - 1)\sigma_a^2 \leq P$，當中的 $\sigma_s^2 = \alpha P$ 和 $\sigma_a^2 = \dfrac{(1-\alpha)P}{M_t - 1}$，且 $0 \leq \alpha \leq 1$。

考慮最差情況下，$\sigma_e^2 = 0$ 時，接收端和竊聽者的接收訊號為

$$\hat{y}_r[i] = \left\| \mathrm{h}_r \right\| \left(g_r \hat{g}_r^{\,H} \right) s[i] + \left\| \mathrm{h}_r \right\| \left(g_r \mathrm{N}_{\hat{g}_r} \right) \mathrm{a}[i] + z_r[i] \tag{2.6}$$

$$\hat{y}_e[i] = \mathrm{h}_e \hat{g}_r^{\,H} s[i] + \mathrm{h}_e \mathrm{N}_{\hat{g}_r} \mathrm{a}[i] \tag{2.7}$$

由上面兩式，可以得到我們在量化 CDI 情況下的保密容量為

$$\begin{aligned} &\hat{R}(\alpha) \\ &= \left(\mathrm{E}\left[\log\left(1 + \frac{\left\| \mathrm{h}_r \right\|^2 \cos^2\theta \cdot \alpha P}{\left\| \mathrm{h}_r \right\|^2 \sin^2\theta \left(\frac{1-\alpha}{M_t - 1} \right) P + 1} \right) \right] - \mathrm{E}\left[\log\left(1 + \frac{\left| \mathrm{h}_e \hat{g}_r^{\,H} \right|^2 \alpha}{\left\| \mathrm{h}_e \mathrm{N}_{\hat{g}_r} \right\|^2 \left(\frac{1-\alpha}{M_t - 1} \right)} \right) \right] \right) \end{aligned} \tag{2.8}$$

又當 P 到無限大的時候，可以寫成

$$\hat{R}(\alpha)=\left(\mathrm{E}\left[\log\left(1+\frac{\cos^2\theta\cdot\alpha}{\sin^2\theta\left(\frac{1-\alpha}{M_t-1}\right)}\right)\right]-\mathrm{E}\left[\log\left(1+\frac{\left|\mathrm{h}_e\hat{g}_r^{\,H}\right|^2\alpha}{\left\|\mathrm{h}_e\mathrm{N}_{\hat{g}_r}\right\|^2\left(\frac{1-\alpha}{M_t-1}\right)}\right)\right]\right)^+ \tag{2.9}$$

其保密容量可為一常數。相對的，在充分知道 CDI 情況下的保密容量為

$$R(\alpha)=\left(\mathrm{E}\left[\log\left(1+\left\|\mathrm{h}_r\right\|^2\alpha P\right)\right]-\mathrm{E}\left[\log\left(1+\frac{\left|\mathrm{h}_e\hat{g}_r^{\,H}\right|^2\alpha}{\left\|\mathrm{h}_e\mathrm{N}_{\hat{g}_r}\right\|^2\left(\frac{1-\alpha}{M_t-1}\right)}\right)\right]\right)^+ \tag{2.10}$$

由上式可以得知，在充分知道 CDI 的情況下，增加傳輸功率 P ，可以使保密容量任意的加大。

2.2 合作式系統中的保密

在文獻[15]中，討論一個具備三個節點的多重輸入輸出合作式系統，其通道環境皆為慢速衰減(slow fading)通道，三個節點分別是傳送端(S)、目的端(D)和不可靠的中繼端(untrusted relay, UR)，具備的天線數分別是 M_S 、 M_D 與 M_R ，如圖 2-2。

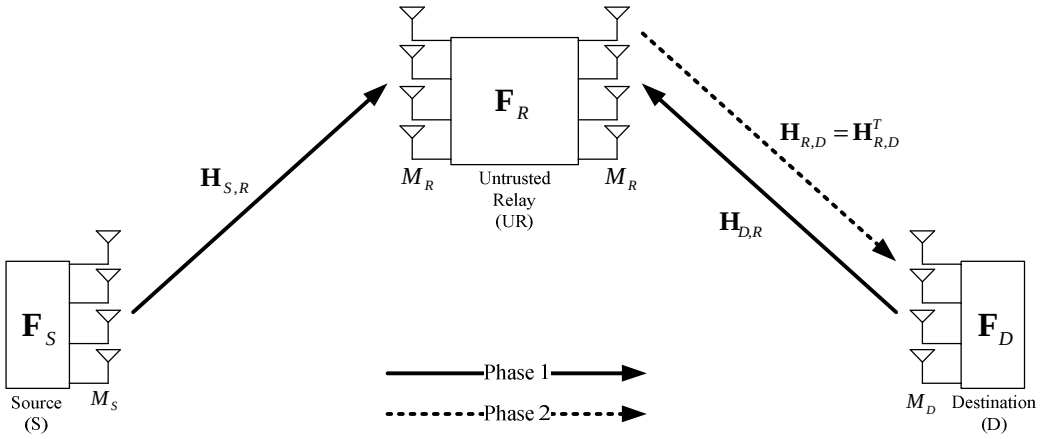

圖 2-2 存在不可靠中繼端的合作式系統圖

因為此中繼端是不可靠的，他可能會在未經許可的狀況下，解碼並竊取資料源訊息，因此必須採取預防措施，使不可靠的中繼端無法得到足夠的訊息。在一般的合作式通訊架構下，訊息傳輸分成兩個階段，本文中，第一階段除了資料源經由預編碼器 $\mathbf{F}_S$ 傳送訊息 $\mathbf{x}_s$ 給中繼端之外，目的端也會同時經由預編碼器 $\mathbf{F}_D$ 傳送人工雜訊(AN) $\mathbf{a}$ 給中繼端，以干擾中繼端接收，在第二階段，中繼端依舊把收到的訊息與人工雜訊放大後經由預編碼器 $\mathbf{F}_R$ 傳給目的端。在第一階段，中繼端收到的資訊如下

$$\mathbf{y}_R=\sqrt{P_s}\mathbf{H}_{S,R}\mathbf{F}_S\mathbf{x}_s+\sqrt{P_d}\mathbf{H}_{D,R}\mathbf{F}_D\mathbf{a}+\mathbf{w}_r \tag{2.11}$$

其中 P_s 為資料源的傳送功率，P_d 為資料源的傳送功率，$\mathbf{w}_r\sim CN\left(\mathbf{0}_{M_R},\sigma_r^2\mathbf{I}_{M_R\times M_R}\right)$ 為在中繼端的可加性高斯白雜訊(AWGN)。

在傳送的第二階段中，中繼端把來自資料源和目的端的訊息，經過預編碼器 $\mathbf{F}_R$ 後傳給目的端，$\mathbf{H}_{R,D}$ 為中繼端到目的端的鏈結之通道矩陣。在慢速衰減(slow fading)的情況下，我們假設互換原則(reciprocity principle)成立，即 $\mathbf{H}_{R,D}=\mathbf{H}_{D,R}^T$，而且中繼端所使用的預編碼器 $\mathbf{F}_R$ 則由資料源或目的端以回授告知。在第二階段傳送，目的端的接收訊息如下

$$\begin{aligned}\mathbf{y}_D &= \sqrt{P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{y}_R + \mathbf{w}_d \\ &= \sqrt{P_r P_s}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{H}_{S,R}\mathbf{F}_S\mathbf{x}_s + \sqrt{P_r P_d}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{H}_{D,R}\mathbf{F}_D\mathbf{a} \\ &\quad + \sqrt{P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{w}_r + \mathbf{w}_d\end{aligned} \tag{2.12}$$

其中 $\mathbf{w}_d \sim CN\left(\mathbf{0}_{M_D}, \sigma_d^2\mathbf{I}_{M_D\times M_D}\right)$ 是第二階段在目的端的可加性高斯白雜訊(AWGN)。因為人工雜訊為目的端所產生，且目的端知道 $\mathbf{H}_{D,R}$ 通道資訊，因此目的端可以自行消去人工雜訊項，目的端收到訊息可改寫如下

$$\begin{aligned}\tilde{\mathbf{y}}_D &= \sqrt{P_s P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{H}_{S,R}\mathbf{F}_S\mathbf{x}_s + \sqrt{P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{w}_r + \mathbf{w}_d \\ &= \sqrt{P_s}\mathbf{H}\mathbf{x}_s + \mathbf{w}\end{aligned} \tag{2.13}$$

其中 $\mathbf{H} = \sqrt{P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{H}_{S,R}\mathbf{F}_S$ 及 $\mathbf{w} = \sqrt{P_r}\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{w}_r + \mathbf{w}_d$ 。

因為人工雜訊項對中繼端來說是干擾雜訊，所以我們把雜訊合成一項，可以推得來源訊號至中繼端的最高可達率(achievable rate)如下

$$C_R = \frac{1}{2}\log_2\left[\det\left(\mathbf{I}_{M_S} + \frac{P_s}{M_S}\mathbf{F}_S^H\mathbf{H}_{S,R}^H\mathbf{R}_{\tilde{w}}^{-1}\mathbf{H}_{S,R}\mathbf{F}_S\right)\right] \tag{2.14}$$

其中 $\mathbf{R}_{\tilde{w}} = \mathrm{E}\left[\tilde{\mathbf{w}}_r\tilde{\mathbf{w}}_r^H\right] = \sqrt{P_d}\left(\mathbf{H}_{D,R}\mathbf{F}_D\right)\mathbf{R}_a\left(\mathbf{F}_D^H\mathbf{H}_{D,R}^H\right) + \sigma_r^2\mathbf{I}_{M_R}$ ，$\mathbf{R}_a$ 為人工雜訊向量之協方差，以及 $\tilde{\mathbf{w}}_r = \sqrt{P_d}\left(\mathbf{H}_{D,R}\mathbf{F}_D\right)\mathbf{a} + \mathbf{w}_r$ 。

前兩式中，雜訊項 $\mathbf{w}$ 有協方差 $\mathbf{R}_w = P_r\sigma_r^2\mathbf{H}_{R,D}\mathbf{F}_R\mathbf{F}_R^H\mathbf{H}_{R,D}^H + \sigma_d^2\mathbf{I}_{M_D}$ ，推得來源訊號在目的端的最高可達率如下

$$C_D = \frac{1}{2}\log_2\left[\det\left(\mathbf{I}_{M_S} + \frac{P_s}{M_S}\mathbf{H}^H\mathbf{R}_w^{-1}\mathbf{H}\right)\right] \tag{2.15}$$

可以列出保密容量如下

$$C_S = \left(C_D - C_R\right)^+ \tag{2.16}$$

其中$(x)^+=\max(0,x)$。

文獻中欲設計一組預編碼器，在滿足各節點功率限制的前提下，提高系統的保密容量，此最佳化問題表示如下

$$\begin{aligned} \max_{\mathbf{F}_S,\mathbf{F}_R,\mathbf{F}_D} \quad & C_S = \left(C_D - C_R\right)^+ \\ \text{s.t.} \quad & \mathrm{tr}\left(\mathbf{F}_R\left(\frac{P_s}{M_S}\left(\mathbf{H}_{S,R}\mathbf{F}_S\right)\left(\mathbf{F}_S^H\mathbf{H}_{S,R}^H\right)+\mathbf{R}_{\tilde{w}}\right)\mathbf{F}_R^H\right)\le 1 \\ & \mathrm{tr}\left(\mathbf{F}_S\mathbf{R}_S\mathbf{F}_S^H\right)\le 1 \\ & \mathrm{tr}\left(\mathbf{F}_D\mathbf{R}_a\mathbf{F}_D^H\right)\le 1 \end{aligned} \tag{2.17}$$

因為無法證明其目標函數是否為只具有一個高點的凹向下(concave)函數，更有可能的是這個函數具有多個高點，因此本篇文獻只能找到函數區域中最佳化的點。本文先假設在資料源的預編碼器 $\mathbf{F}_S$ 與在目的端的預編碼器 $\mathbf{F}_D$ 為已知，求解出最佳的中繼端預編碼器 $\mathbf{F}_R$；第二階段則假設在資料源的預編碼器 $\mathbf{F}_S$ 與在第一階段求得的中繼端預編碼器 $\mathbf{F}_R$ 為已知，求解出最佳的目的端預編碼器 $\mathbf{F}_D$；第三階段則使用在第一階段求得的中繼端預編碼器 $\mathbf{F}_R$ 與在第二階段求得的目的端預編碼器 $\mathbf{F}_D$ 為已知，求解出最佳的資料源預編碼器 $\mathbf{F}_S$，並重複此三階段的迭代計算直到求得一個保密容量收斂解，即為區域最佳解。

2.3 以確保 QoS 為系統考慮依據的保密

在文獻[16]中，討論一個多天線的傳送端與一個單天線的接收端的 MISO 系統，在系統中，傳送端與接收端之間散佈了多個單天線的竊聽者，文獻以確保服務品質(quality of service, QoS)為出發點，藉由設計最佳的波束成型向量以及人工雜訊的幫助，進而達到最佳的保密容量。此系統由傳送端(Alice)、接收端(Bob)

以及多個竊聽者(Eve)所組成，傳送端具備 N_t 個天線，傳送波束成型布置於傳送端上，其波束成型向量 $\mathbf{w}$ 維度是 $N_t \times 1$，訊號經由波束成型向量後傳送給接收端，同時傳送端也分配部分能量產生人工雜訊(AN)，干擾周圍的竊聽者，避免其竊聽訊號，如圖所示

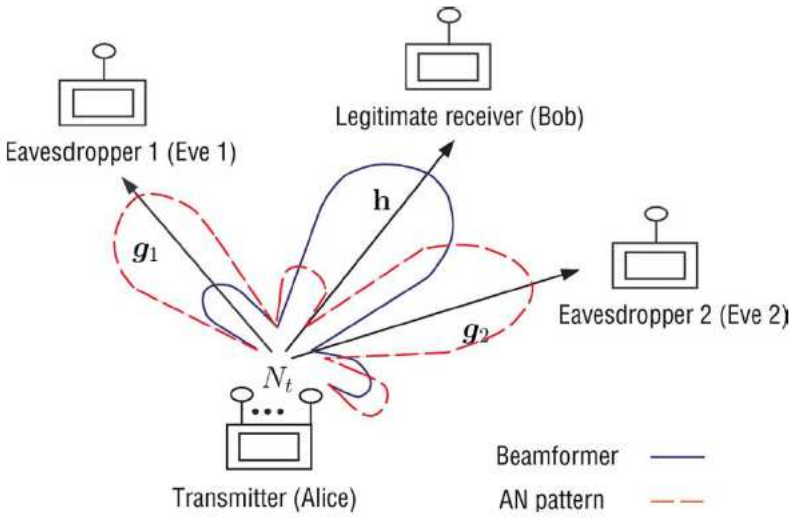

圖 2-3 存在多竊聽者的 MISO 系統圖

上圖為竊聽者數量為 2 的示意圖，圖中 $\mathbf{h}$、$\mathbf{g}_1$ 和 $\mathbf{g}_2$ 分別為傳送端到接收端鏈結、傳送端到竊聽者 1 鏈結，與傳送端到竊聽者 2 鏈結的通道係數向量，藍色實線為我們要傳送訊號的波束成型向量方向，紅色虛線則為人工雜訊(AN)所要傳送的方向。接收端與竊聽者所接收到的訊號分別表示為

$$y_b(t) = \mathbf{h}^H \mathbf{x}(t) + n(t) \tag{2.18}$$

$$y_{e,m}(t) = \mathbf{g}_m^H \mathbf{x}(t) + v_m(t), \quad m = 1, ..., M \tag{2.19}$$

其中 $\mathbf{x}(t) = \mathbf{w}s(t) + \mathbf{z}(t) \in \mathbb{C}^{N_t}$，$\mathbf{w}$ 為訊號波束成型向量。上式 $\mathbf{h} \in \mathbb{C}^{N_t}$ 與 $\mathbf{g}_m \in \mathbb{C}^{N_t}$ 分別為傳送端到接收端與傳送端到竊聽者 m 的通道係數向量，且 $\mathbf{z}(t)$ 的統計特性

為 $CN(0,\boldsymbol{\Sigma})$，而 $n(t)$ 與 $v_m(t)$ 分別為接收端與竊聽者 m 的獨立且同分布的複數圓對稱高斯雜訊，其變異數分別

為 $\sigma_n^2 > 0$ 和 $\sigma_{v,m}^2 > 0$。確保服務品質為系統考慮的理念是基於分析訊號與干擾雜比值(SINR)方法，假設通道係數 $\mathbf{h}$ 平均值為 $\bar{\mathbf{h}}$ 共變異矩陣為 $\mathbf{C}_h$，接收端的 SINR 就可以表示如下

$$\mathrm{SINR}_b(\mathbf{w},\boldsymbol{\Sigma}) = \frac{\mathrm{E}\left\{\left|\mathbf{h}^H\mathbf{w}s(t)\right|^2\right\}}{\mathrm{E}\left\{\left|\mathbf{h}^H\mathbf{z}(t)\right|^2\right\}+\sigma_n^2} = \frac{\mathbf{w}^H\mathbf{R}_h\mathbf{w}}{\mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_h)+\sigma_n^2} \tag{2.20}$$

其中 $\mathbf{R}_h = \mathrm{E}\{\mathbf{h}\mathbf{h}^H\} = \bar{\mathbf{h}}\bar{\mathbf{h}}^H + \mathbf{C}_h$。

同樣的，竊聽者的 SINR 可以表示如下

$$\mathrm{SINR}_{e,m}(\mathbf{w},\boldsymbol{\Sigma}) = \frac{\mathrm{E}\left\{\left|\mathbf{g}_m^H\mathbf{w}s(t)\right|^2\right\}}{\mathrm{E}\left\{\left|\mathbf{g}_m^H\mathbf{z}(t)\right|^2\right\}+\sigma_{v,m}^2} = \frac{\mathbf{w}^H\mathbf{R}_{g,m}\mathbf{w}}{\mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_{g,m})+\sigma_{v,m}^2} \tag{2.21}$$

其中 $\mathbf{R}_{g,m} = \mathrm{E}\{\mathbf{g}_m\mathbf{g}_m^H\} = \bar{\mathbf{g}}_m\bar{\mathbf{g}}_m{}^H + \mathbf{C}_{g,m}$。將接收端與竊聽者的 SINR 定義出來後，文中討論兩個議題，首先，最小化總功率，限制接收端與竊聽者的 SINR，其最佳化問題可寫成

$$\begin{aligned} \min_{\mathbf{w}\in\mathbb{C}^{N_t},\ \boldsymbol{\Sigma}\in\mathrm{H}^{N_t}} \quad & \|\mathbf{w}\|^2 + \mathrm{Tr}(\boldsymbol{\Sigma}) \\ \text{s.t.} \quad & \mathrm{SINR}_b(\mathbf{w},\boldsymbol{\Sigma}) \ge \gamma_b \\ & \mathrm{SINR}_{e,m}(\mathbf{w},\boldsymbol{\Sigma}) \le \gamma_e \quad m = 1,\ldots,M \\ & \boldsymbol{\Sigma} \ge \mathbf{0} \end{aligned} \tag{2.22}$$

其中 $\gamma_b > 0$，$\gamma_e > 0$。再來，最大化接收端的 SINR，限制竊聽者的 SINR 及傳輸功率，其最佳化問題可以寫成

$$\begin{aligned} \min_{\mathbf{w},\,\boldsymbol{\Sigma}} \quad & \|\mathbf{w}\|^2 + \mathrm{Tr}(\boldsymbol{\Sigma}) \\ \text{s.t.} \quad & \frac{1}{\gamma_b}\mathbf{w}^H\mathbf{R}_h\mathbf{w} \geq \mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_h) + \sigma_n^2 \\ & \frac{1}{\gamma_e}\mathbf{w}^H\mathbf{R}_{g,m}\mathbf{w} \leq \mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_{g,m}) + \sigma_{v,m}^2 \quad m = 1,\ldots,M \\ & \boldsymbol{\Sigma} \geq \mathbf{0} \end{aligned} \tag{2.23}$$

這兩種最佳化問題作者利用半正定寬鬆策略(SDR)的方法，分別將第一個最佳化問題化簡為

$$\begin{aligned} \max_{\mathbf{W},\boldsymbol{\Sigma}} \quad & \mathrm{Tr}(\mathbf{W}) + \mathrm{Tr}(\boldsymbol{\Sigma}) \\ \text{s.t.} \quad & \frac{1}{\gamma_b}\mathrm{Tr}(\mathbf{W}\mathbf{R}_h) - \mathrm{Tr}(\mathbf{R}_h\boldsymbol{\Sigma}) \geq \sigma_n^2 \\ & \frac{1}{\gamma_e}\mathrm{Tr}(\mathbf{W}\mathbf{R}_{g,m}) - \mathrm{Tr}(\mathbf{R}_{g,m}\boldsymbol{\Sigma}) \geq \sigma_{v,m}^2 \\ & m = 1,\ldots,M \\ & \boldsymbol{\Sigma} \geq \mathbf{0},\ \ \mathbf{W} \geq \mathbf{0} \end{aligned} \tag{2.24}$$

以及第二個最佳化問題化簡為

$$\begin{aligned} \max_{\bar{\mathbf{W}},\,\bar{\boldsymbol{\Sigma}},\,\eta} \quad & \mathrm{Tr}(\bar{\mathbf{W}}\mathbf{R}_h) \\ \text{s.t.} \quad & \mathrm{Tr}(\bar{\boldsymbol{\Sigma}}\mathbf{R}_h) + \eta\sigma_n^2 = 1 \\ & \frac{1}{\gamma_e}\mathrm{Tr}(\bar{\mathbf{W}}\mathbf{R}_{g,m}) \leq \mathrm{Tr}(\bar{\boldsymbol{\Sigma}}\mathbf{R}_{g,m}) + \eta\sigma_{v,m}^2 \\ & m = 1,\ldots,M \\ & \mathrm{Tr}(\bar{\mathbf{W}}) + \mathrm{Tr}(\bar{\boldsymbol{\Sigma}}) \leq \eta P_{\max} \\ & \bar{\mathbf{W}} \geq \mathbf{0},\ \bar{\boldsymbol{\Sigma}} \geq \mathbf{0},\ \eta \geq 0 \end{aligned} \tag{2.25}$$

並且在 $\mathbf{R}_h, \mathbf{R}_{g,1},\ldots,\mathbf{R}_{g,M} \geq \mathbf{0}$ 為必要條件的同時，順利的在三種情況找出最佳解，

首先為瞬時通道係數在接收端已知的情況，再來是在傳送端到接收端與竊聽者的通道皆具有白通道共變異矩陣，最後是竊聽者數量小於 2 的時候，在上述三種情況皆可以找出最佳的波束成型向量 $\mathbf{w}^*$。

第三章 系統模型

在本章節中，我們將簡介所用到的通道模型，如圖 3-1 所示，我們考慮的模型是一個多個單天線的中繼端(relay, $R_1, R_2, ..., R_K$)，且資料源(Alice)與目的端(Bob)的皆為多天線的合作式系統，假設其通道環境為慢速衰減通道(slow fading)，即在兩個階段傳送中，通道狀況為不變，而資料源(Alice)與目的端(Bob)的天線數量分別為 N_a 與 N_b，中繼端數量為 K 個。假設網路中這些中繼端是不可靠的，也就是說，全部的中繼端都會負責幫忙傳遞訊息，但這些中繼端有可能會竊聽資料源要傳給接收端的訊號，並且假設中繼端採用半雙工的機制，傳送與接收都經由同一支天線，不能同時傳送與接收。中繼端扮演的角色為資料源與目的端溝通的橋樑，使用放大後前送的策略傳遞訊號；也因為各個中繼端皆不可靠，他們可能在未經許可的情況下，解碼與竊取資料源的訊息，並且假裝自己是一個正當的放大後前送中繼端，所以我們必須要採取一些預防措施，讓不可靠的中繼

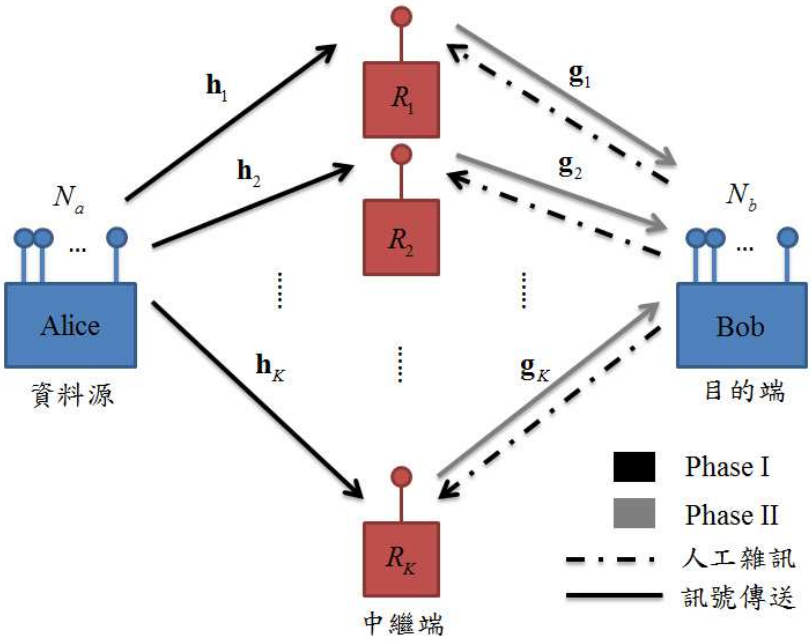

圖 3-1 多個不可靠單天線中繼端的系統模型

端在不利解碼的環境中，無法順利竊取資料；更明確的說，藉由目的端負責傳送人工雜訊，使得不可靠的中繼端在接收訊號的同時，亦會受到人工雜訊的干擾，以降低不可靠的中繼端的訊號雜訊比值，陷入不利解碼的環境中。

在一般合作式通訊的架構下，訊息的傳輸分為兩個階段，第一階段是資料源經由預編碼器設計好的訊息傳送給各中繼端，第二階段是各中繼端將收到訊息的功率正規化之後，再乘上各自的預編碼係數後，傳送給目的端。在本篇論文中，我們假設資料源與目的端的距離遙遠，因此沒有直接連結訊號的存在，為了降低中繼端接收訊號的訊號雜訊比值，目的端同時在第一階段經由預編碼器設計，產生統計特性為$CN\left(\mathbf{0},\ \mathbf{Q}\right)$的人工雜訊(AN)，傳送給各中繼端，第二階段中，各個中繼端將包含訊息與人工雜訊的接收訊號進行功率正規化，再乘上各自的預編碼係數後，傳送給目的端。

如圖 3-2 所示，資料源將第一階段傳送預編碼後的訊號符元向量$\mathbf{x}=\left[x[1],\ x[2],\ \ldots,\ x[N_a]\right]^T$給中繼端，其中$x\left[m\right]$指的是第 m 根天線所傳送的符元，$\mathbf{x}$平均值為$\mathrm{E}\left[\mathbf{x}\right]=0$，且共變異(covariance)矩陣以$\mathbf{R}_x=\mathbf{E}\left[\mathbf{x}\mathbf{x}^H\right]$表示，其資料源所有天線加總的傳輸功率限制為$P_s$，在同一時間，目的端也傳送人工雜訊$\mathbf{q}$給中繼端，人工雜訊平均值為 0，且共變異矩陣為$\mathbf{Q}=\mathrm{E}\left[\mathbf{q}\mathbf{q}^H\right]$，其目的端所有天線加總傳輸的功率限制為$P_b$。從圖 3-2 中，令$\mathbf{y}_R=\left[y_{R1}\ y_{R2}\ \ldots y_{RK}\right]$為所有中繼端在第一階段接收的符元，其數值為

$$\mathbf{y}_R=\mathbf{H}\mathbf{x}+\mathbf{G}\mathbf{q}+\mathbf{w}_r \tag{3.1}$$

在上式中，$\mathbf{w}_r\sim CN\left(\mathbf{0}_K,\sigma_r^2\mathbf{I}_{K\times K}\right)$是在中繼端的可加性高斯白雜訊(AWGN)，矩陣

$\mathbf{H}=[\mathbf{h}_1\ \mathbf{h}_2\ \ldots\ \mathbf{h}_K]^T$ 以及 $\mathbf{G}=[\mathbf{g}_1\ \mathbf{g}_2\ \ldots\ \mathbf{g}_K]^T$ 分別為資料源到中繼端，和目的端到中繼端的鏈結之間的通道係數矩陣，$\mathbf{h}_k$ 為資料源到第 k 個中繼端的通道係數向量，$\mathbf{g}_k$ 為目的端到第 k 個中繼端的通道係數向量，其大小皆為 $K\times 1$，而所構成的矩陣維度分別是 $K\times N_a$ 和 $K\times N_b$，並假設通道互換原則(reciprocity principle)成立，也就是說，中繼端到目的端的通道係數矩陣為 $\mathbf{G}^T$。在此系統中，我們假設資料源、中繼端和目的端皆可以取得完美的瞬時通道資訊，用來設計最佳的資料源及人工雜訊統計特性，即 $\mathbf{R}_x$ 與 $\mathbf{Q}$，以及中繼端預編碼係數。

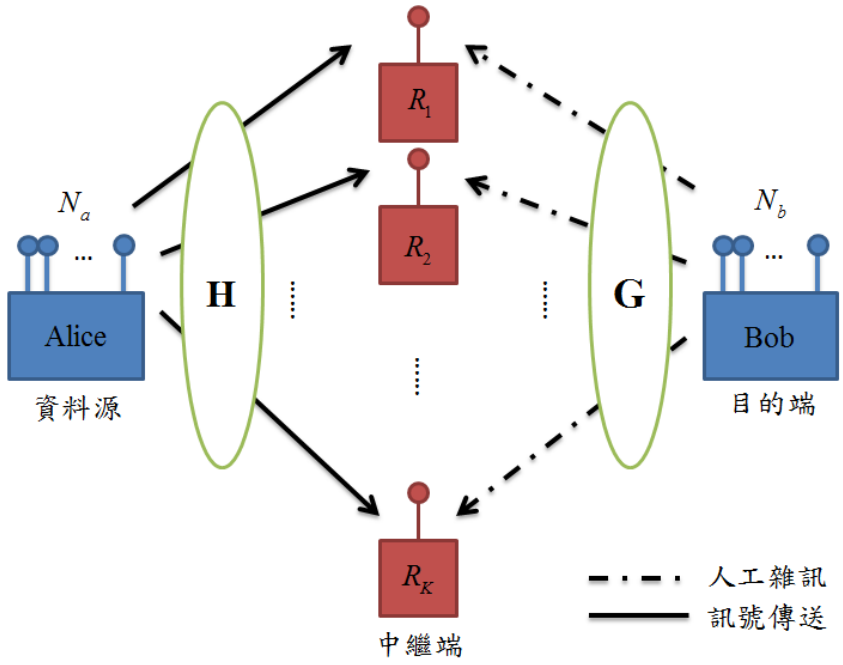

圖 3-2 多個不可靠單天線中繼端系統，第一階段傳送示意圖

由第一階段中繼端所接收到的訊號，我們可以求出第 l 個中繼端的訊號與干擾雜訊比值(signal & interference to noise ratio, SINR)如下

$$\mathrm{SINR}_{Rk}=\frac{\mathrm{E}\left[\left\|\mathbf{h}_k^T\mathbf{x}\right\|^2\right]}{\mathrm{E}\left[\left\|\mathbf{g}_k^T\mathbf{q}\right\|^2\right]+\sigma_r^2}=\frac{\mathrm{tr}\left(\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*\right)}{\mathrm{tr}\left(\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*\right)+\sigma_r^2}\quad,\quad k=1,\ldots,K \tag{3.2}$$

如圖 3-3 所示，在第二階段的傳送過程中，中繼端把來自資料訊號與人工雜訊的總接收功率正規化後，乘上各自的預編碼係數，再傳送給目的端，且假設全部中繼端的傳輸功率總和限制為 P_r 。

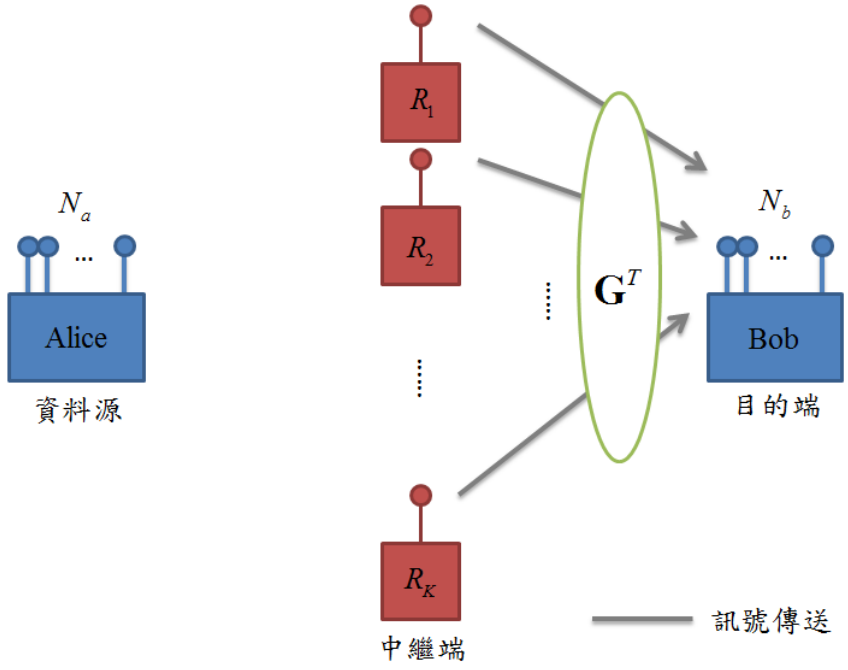

圖 3-3 多個不可靠單天線中繼端系統，第二階段傳送示意圖

在第二階段的傳送中，目的端接收的訊息如下

$$\mathbf{y}_D=\mathbf{G}^T\mathbf{L}\mathbf{y}_R+\mathbf{w}_d \tag{3.3}$$

其中 $\mathbf{L}=diag\left[L_{v1}\ L_{v2}\ ...\ L_{vK}\right]$ 為接收訊號正規化再進行放大的係數矩陣，L_{vk} 是第 k 個中繼端將接收訊號正規化再進行放大的係數，如下

$$L_{vk}=\frac{\beta_k}{\sqrt{\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*+\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*+\sigma_r^2}}\ ,\quad k=1,...,K \tag{3.4}$$

β_l 是第 l 個中繼端將接收訊號進行放大的係數，$\mathbf{w}_d\sim CN\left(\mathbf{0}_{N_b},\ \sigma_d^2\mathbf{I}_{N_b\times N_b}\right)$ 是第二階段在目的端的可加性高斯白雜訊(AWGN)。因為人工雜訊是由目的端所產生，且目的端知道 $\mathbf{G}$ 的通道資訊，所以目的端可以完美的自行消去人工雜訊的部分，移除人工砸雜訊目的端接收的訊息改寫如下

$$\tilde{\mathbf{y}}_D=\mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}\mathbf{x}+\mathbf{G}^T\mathbf{B}\tilde{\mathbf{w}}_r+\mathbf{w}_d \tag{3.5}$$

其中 $\mathbf{B}=diag\left[\beta_1\ \beta_2\ ...\ \beta_K\right]$ 為接收訊號進行放大的係數所構成的對角矩陣，而 $\tilde{\mathbf{w}}_r=\left[\tilde{w}_{r1}\ \tilde{w}_{r2}\ ...\ \tilde{w}_{rK}\right]$ 為 $K\times 1$ 的向量，第 k 個元素為

$$\tilde{w}_{rk}=\frac{w_{rk}}{\sqrt{\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*+\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*+\sigma_r^2}}\ ,\quad k=1,...,K \tag{3.6}$$

$\tilde{\mathbf{H}}$ 為區塊對角(block diagonal)矩陣，其表示如下

$$\tilde{\mathbf{H}}=\begin{bmatrix}\frac{\mathbf{h}_1^T}{\sqrt{\mathbf{h}_1^T\mathbf{R}_x\mathbf{h}_1^*+\mathbf{g}_1^T\mathbf{Q}\mathbf{g}_1^*+\sigma_r^2}} & 0 & \cdots & 0\\ 0 & \frac{\mathbf{h}_2^T}{\sqrt{\mathbf{h}_2^T\mathbf{R}_x\mathbf{h}_2^*+\mathbf{g}_2^T\mathbf{Q}\mathbf{g}_2^*+\sigma_r^2}} & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & \frac{\mathbf{h}_K^T}{\sqrt{\mathbf{h}_K^T\mathbf{R}_x\mathbf{h}_K^*+\mathbf{g}_K^T\mathbf{Q}\mathbf{g}_K^*+\sigma_r^2}}\end{bmatrix} \tag{3.7}$$

由第二階段目的端所接收到的訊號，我們可以使用 MIMO 技術中的最大比例合

併(maximal ratio combining, MRC)方法，目的端接收訊號合併後的訊號雜訊比值如下

$$\mathrm{SNR}_D = \mathrm{tr}\left(\left(\tilde{\mathbf{H}}^H \mathbf{B}^H \mathbf{G}^* \mathbf{C}^{-1} \mathbf{G}^T \mathbf{B} \tilde{\mathbf{H}}\right) \mathbf{R}_x\right) \tag{3.8}$$

其中

$$\mathbf{C} = \sigma_d^2 \mathbf{I} + \sigma_r^2 \mathbf{G}^T \mathbf{B} \begin{bmatrix} \frac{1}{\mathbf{h}_1^T \mathbf{R}_x \mathbf{h}_1^* + \mathbf{g}_1^T \mathbf{Q} \mathbf{g}_1^* + \sigma_r^2} & 0 & \cdots & 0 \\ 0 & \frac{1}{\mathbf{h}_2^T \mathbf{R}_x \mathbf{h}_2^* + \mathbf{g}_2^T \mathbf{Q} \mathbf{g}_2^* + \sigma_r^2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{1}{\mathbf{h}_K^T \mathbf{R}_x \mathbf{h}_K^* + \mathbf{g}_K^T \mathbf{Q} \mathbf{g}_K^* + \sigma_r^2} \end{bmatrix} \mathbf{B}^H \mathbf{G}^* \tag{3.9}$$

第四章　預編碼器之設計

本章節中，我們欲藉由中繼端預編碼設計，以及資料源與目的端編碼後的訊號和人工雜訊，來達成保密的效果，但使此系統保密容量最大所設計的最佳化問題，並不是一個凸函數(convex)，因此，改以確保目的端服務品質為目標，來達成通訊保密，又因三節點無法聯立求得最佳解，所以採用中繼端預編碼係數，與資料源和目的端訊號統計特性，兩部分交互迭代方式求得最佳解。在第一小節中，將介紹多中繼系統中的保密效能的評估依據，接著在第二小節，介紹最佳化問題的設計，最後在第三及第四小節中，介紹最佳解求解及迭代的過程。

4.1 多中繼系統中的保密

本篇論文中，我們以保密容量來討論系統的保密效能，可以利用系統模型章節中，所求出資料源到各節點的訊號與雜訊比值，計算各個的通道容量，將目的端的通道容量減去竊聽者的通道容量，即為保密容量，而在此多中繼系統中，我們討論被竊聽程度最嚴重的情況，也就是系統目的端的通道容量減去各中繼端中最大的通道容量，其保密容量如下

$$R_s = \left[\log_2 \det\left(\mathbf{I} + \mathbf{O}\mathbf{R}_x\right) - \log_2\left(1 + \max_{k=1,\ldots,K}\left(\mathrm{SINR}_{Rk}\right)\right)\right]^+ \tag{4.1}$$

其中$[x]^+=\max(0,x)$以及$\mathbf{O} = \tilde{\mathbf{H}}^H\mathbf{B}^H\mathbf{G}^*\mathbf{C}^{-1}\mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}$。

4.2 設計最佳化問題

根據第三章訊號模型，我們可以首先計算出各中繼端的訊號與干擾雜訊比值，再來，訊號經過各中繼端正規化的過程後，乘上各自的預編碼係數傳送至目的端，目的端接收訊號雜訊比值也可以依序求得，根據上述各中繼端的 SINR 與目的端的 SNR 數值，可以計算來源訊號至各節點的通道容量，為了使保密容量最大，我們可以針對 $\mathbf{B}$ 、$\mathbf{R}_x$ 與 $\mathbf{Q}$ 矩陣，設計一個最佳化問題，如下

$$\begin{aligned} \underset{\mathbf{B},\,\mathbf{R}_x,\mathbf{Q}}{\max} \quad & R_s = \left[\log_2 \det\left(\mathbf{I}+\mathbf{O}\mathbf{R}_x\right) - \log_2\left(1+\max_{k=1,\ldots,K}\left(\mathrm{SINR}_{Rk}\right)\right)\right]^+ \\ \text{s.t.} \quad & \mathrm{tr}\left(\mathbf{R}_x\right) \le P_s,\, \mathrm{tr}\left(\mathbf{Q}\right) \le P_b, \\ & \mathbf{R}_x \ge \mathbf{0},\ \mathbf{Q} \ge \mathbf{0}, \\ & \left\|\boldsymbol{\beta}\right\|^2 \le P_r \end{aligned} \tag{4.2}$$

其中$[x]^+=\max(0,x)$。上式目的為聯合設計中繼端預編碼係數矩陣 $\mathbf{B}$，與資料源及人工雜訊的統計特性，即 $\mathbf{R}_x$ 與 $\mathbf{Q}$，並限制各個節點的傳輸功率，使系統中最差的保密容量，也就是目的端通道容量減去各中繼端中最大容量的差值，使其達到最大，但由上式最佳化問題中，可以看出目標函數並非為一個凸函數(convex)，故無法利用工具 CVX 求解，欲求最佳解相當複雜，且無法保證所求得的最佳解為整體的最佳解，於是我們改以確保系統服務品質為目標，藉由限制各個中繼端的 SINR 數值在 γ_e 之下，也就是我們容忍中繼端竊聽程度上限為 γ_e，利用最佳的中繼端預編碼係數矩陣 $\mathbf{B}$，與資料源及人工雜訊的統計特性，即 $\mathbf{R}_x$ 與 $\mathbf{Q}$，得到最好的目的端接收訊號 SNR，進而使得目的端的通道容量減去各中繼端中最大通道容量產生差值，即為系統中最差保密容量的情況。而限制各個中繼端 SINR

數值，主要是因為我們假設系統中各個中繼端皆為不可靠的，他們可能會在沒有經過允許的情況下，解碼並竊取重要的訊息，其最佳化問題改以下面表示

$$\begin{aligned}
\max_{\mathbf{B},\mathbf{R}_x,\mathbf{Q}} \quad & \mathrm{SNR}_D = \mathrm{tr}\left(\left(\tilde{\mathbf{H}}^H\mathbf{B}^H\mathbf{G}^*\mathbf{C}^{-1}\mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}\right)\mathbf{R}_x\right) \\
\text{s.t.} \quad & \mathrm{SINR}_{Rk} = \frac{\mathrm{tr}\left(\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*\right)}{\mathrm{tr}\left(\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*\right)+\sigma_r^2} \le \gamma_e,\ k=1,...,K \\
& \mathrm{tr}\left(\mathbf{R}_x\right) \le P_s,\ \mathrm{tr}\left(\mathbf{Q}\right) \le P_b, \\
& \mathbf{R}_x \ge \mathbf{0},\ \mathbf{Q} \ge \mathbf{0}, \\
& \left\|\boldsymbol{\beta}\right\|^2 \le P_r
\end{aligned} \tag{4.3}$$

但若同時求$\mathbf{B}$、$\mathbf{R}_x$及$\mathbf{Q}$矩陣最佳解時，其中任兩矩陣數值會影響另外一個矩陣的最佳解，且三者無法聯立求得，因此，我們以迭代的方式，逐步逼近最佳解，在給定$\mathbf{R}_x$及$\mathbf{Q}$矩陣下，求得最佳的$\mathbf{B}$矩陣，再用此最佳解更新數值，交互迭代至三矩陣最佳解收斂為止。首先，求$\mathbf{B}$矩陣的最佳解子問題中，發現此矩陣只與目的端的 SNR 有關，因此，在給定$\mathbf{R}_x$及 $\mathbf{Q}$ 矩陣的情況下，可以最大化目的端 SNR 為設計目標，在中繼端有總傳輸功率限制時，找出最佳的中繼端預編碼係數矩陣，其最佳化問題可寫成

$$\begin{aligned}
\max_{\boldsymbol{\beta}} \quad & \mathrm{SNR}_D\left(\boldsymbol{\beta}\right) \\
\text{s.t.} \quad & \left\|\boldsymbol{\beta}\right\|^2 \le P_r
\end{aligned} \tag{4.4}$$

而求$\mathbf{R}_x$及$\mathbf{Q}$矩陣最佳解的子問題中，則是在給定$\mathbf{B}$矩陣的情況下，以確保服務品質為系統考慮依據，即各節點有傳輸功率限制的情況下，限制各中繼端的接收訊號品質，並最大化目的端的接收訊號品質，來設計最佳的資料源及人工雜訊統計特性，即$\mathbf{R}_x$與$\mathbf{Q}$，其最佳化問題如下

$$\begin{aligned}
\max_{\mathbf{R}_x,\mathbf{Q}} \quad & \mathrm{SNR}_D = \mathrm{tr}\left(\left(\tilde{\mathbf{H}}^H\mathbf{B}^H\mathbf{G}^*\mathbf{C}^{-1}\mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}\right)\mathbf{R}_x\right) \\
\text{s.t.} \quad & \mathrm{SINR}_{Rk} = \frac{\mathrm{tr}\left(\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*\right)}{\mathrm{tr}\left(\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*\right)+\sigma_r^2} \le \gamma_e,\ k=1,...,K \\
& \mathrm{tr}\left(\mathbf{R}_x\right) \le P_s,\ \mathrm{tr}\left(\mathbf{Q}\right) \le P_b, \\
& \mathbf{R}_x \ge \mathbf{0},\ \mathbf{Q} \ge \mathbf{0},
\end{aligned} \tag{4.5}$$

由上式可以知道這是一個半正定(semi-definite programming, SDP)的最佳化問題，我們要最大化目的端的訊號雜訊比值，即SNR_D，接著限制各個中繼端的訊號與干擾雜訊比值，即SINR_{Rk}，其中k為中繼端的個數，總數有K個，最後限制傳送端的傳輸功率P_s，以及目的端人工雜訊的傳輸功率P_b，此最佳化問題的目的為找出傳送訊號最佳的統計特性，亦即共變異矩陣$\mathbf{R}_x$，及人工雜訊最佳的共變異矩陣$\mathbf{Q}$。

接下來，我們將在第二節中詳細說明給定$\mathbf{R}_x$與$\mathbf{Q}$情況下，如何求出最佳的$\mathbf{B}$矩陣，在第三節中，介紹如何利用計算出的最佳$\mathbf{B}$矩陣，找出在確保服務品質為系統考慮依據的情況中，最佳的傳送端與目的端預編碼設計，以及此時最佳的目的端 SNR。

4.3 中繼端預編碼向量的最佳化

我們假設資料源到中繼端通道係數矩陣$\mathbf{H}$，以及目的端到中繼端的通道係數矩陣$\mathbf{G}$皆為完美已知，且中繼端的總傳輸能量須滿足能量限制，也假設訊號經過資料源編碼後的共變異矩陣$\mathbf{R}_x$，以及目的端編碼後的人工雜訊的共變異矩陣$\mathbf{Q}$

已給定，在此情況下，我們欲找出中繼端最佳的放大後前送預編碼係數，使目的端接收訊號的訊號雜訊比值可以達到最大，其問題可寫成

$$\begin{aligned} \max_{\boldsymbol{\beta}} \quad & \mathrm{SNR}_D(\boldsymbol{\beta}) \\ \text{s.t.} \quad & \|\boldsymbol{\beta}\|^2 \le P_r \end{aligned} \tag{4.6}$$

目的端的 SNR 已由上一章節中(3.8)式得知，但此 SNR 數值為 **B** 矩陣表示，不易求得最佳解，因此欲化簡問題，想將各中繼端預編碼係數方便提出，我們改寫 **B** 矩陣為向量形式 $\boldsymbol{\beta}$，並且將 **x** 併入 $\tilde{\mathbf{H}}$ 中為 **D**，目的端的接收訊號改寫為

$$\begin{aligned} \tilde{\mathbf{y}}_D &= \mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}\mathbf{x} + \mathbf{G}^T\mathbf{B}\tilde{\mathbf{w}}_r + \mathbf{w}_d \\ &= \mathbf{G}^T\mathbf{D}\boldsymbol{\beta} + \left(\mathbf{G}^T\tilde{\mathbf{W}}_r\boldsymbol{\beta} + \mathbf{w}_d\right) \end{aligned} \tag{4.7}$$

其中 $\mathbf{D} = diag\left(d_1\ d_2\ ...\ d_K\right)$ 為對角(diagonal)矩陣，其中第 k 項表示如下

$$d_k = \frac{\mathbf{h}_k^T\mathbf{x}}{\sqrt{\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^* + \mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^* + \sigma_r^2}},\ \ k = 1,...,K \tag{4.8}$$

而 $\boldsymbol{\beta} = \left[\beta_1\ \beta_2\ ...\ \beta_K\right]^T$ 為中繼端的預編碼係數向量形式，由上式目的端接收訊號，可以計算其 SNR 為

$$\mathrm{SNR}_D = \frac{\mathrm{E}\left[\left\|\mathbf{G}^T\mathbf{D}\boldsymbol{\beta}\right\|^2\right]}{\mathrm{E}\left[\left\|\mathbf{G}^T\tilde{\mathbf{W}}_r\boldsymbol{\beta}\right\|^2\right] + N_b\sigma_d^2} \tag{4.9}$$

可以再將此 SNR 數值進行改寫

$$\begin{aligned}\mathrm{SNR}_D &= \frac{\mathrm{E}\left[\left\|\mathbf{G}^T\mathbf{D}\boldsymbol{\beta}\right\|^2\right]}{\mathrm{E}\left[\left\|\mathbf{G}^T\tilde{\mathbf{W}}_r\boldsymbol{\beta}\right\|^2\right]+N_b\sigma_d^2} \\ &= \frac{\boldsymbol{\beta}^H\mathrm{E}\left[\mathbf{D}^H\mathbf{G}^*\mathbf{G}^T\mathbf{D}\right]\boldsymbol{\beta}}{\boldsymbol{\beta}^H\mathrm{E}\left[\tilde{\mathbf{W}}_r^H\mathbf{G}^*\mathbf{G}^T\tilde{\mathbf{W}}_r\right]\boldsymbol{\beta}+N_b\sigma_d^2} \\ &= \frac{\boldsymbol{\beta}^H\mathbf{A}_1\boldsymbol{\beta}}{\boldsymbol{\beta}^H\mathbf{A}_2\boldsymbol{\beta}}\end{aligned} \tag{4.10}$$

其中 $\tilde{\mathbf{W}}_r = diag\left(\tilde{w}_{r1}\ \tilde{w}_{r2}\ ...\ \tilde{w}_{rK}\right)$ 為對角(diagonal)矩陣，其中第 k 項表示如下

$$\tilde{w}_{rk} = \frac{w_{r1}}{\sqrt{\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^* + \mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^* + \sigma_r^2}},\ \ k=1,...,K \tag{4.11}$$

且因為 $\mathbf{D}$ 與 $\tilde{\mathbf{W}}_r$ 皆為隨機變數，因此要對其取期望值，而 $\mathbf{A}_1$=$\mathrm{E}\left[\mathbf{D}^H\mathbf{G}^*\mathbf{G}^T\mathbf{D}\right]$ 和 $\mathbf{A}_2 = \mathrm{E}\left[\tilde{\mathbf{W}}_r^H\mathbf{G}^*\mathbf{G}^T\tilde{\mathbf{W}}_r\right] + \frac{\sigma_d^2}{P_r}N_b\mathbf{I}$，利用矩陣 $\mathbf{D}$ 對角項的相關性，可以求得 $\mathbf{A}_1$ 的第 ij 項為

$$\begin{aligned}\left[\mathbf{A}_1\right]_{ij} &= \mathrm{E}\left[d_i d_j^*\right]\mathbf{g}_i^T\mathbf{g}_j^* \\ &= \frac{\mathbf{h}_i^T\mathbf{R}_x\mathbf{h}_j^*}{\sqrt{\mathbf{h}_i^T\mathbf{R}_x\mathbf{h}_i^* + \mathbf{g}_i^T\mathbf{Q}\mathbf{g}_i^* + \sigma_r^2}\sqrt{\mathbf{h}_j^T\mathbf{R}_x\mathbf{h}_j^* + \mathbf{g}_j^T\mathbf{Q}\mathbf{g}_j^* + \sigma_r^2}}\mathbf{g}_i^T\mathbf{g}_j^*,\quad i,\ j=1,...,K\end{aligned} \tag{4.12}$$

同理，利用矩陣 $\tilde{\mathbf{W}}_r$ 對角項的相關性，亦可以求得 $\mathbf{A}_2$ 的第 ij 項為

$$\begin{aligned}\left[\mathbf{A}_2\right]_{ij} &= \mathrm{E}\left[\tilde{w}_{ri}\tilde{w}_{rj}^*\right]\mathbf{g}_i^T\mathbf{g}_j^* + \frac{\sigma_d^2}{P_r}N_b \\ &= \begin{cases}\frac{\sigma_r^2}{\mathbf{h}_i^T\mathbf{R}_x\mathbf{h}_i + \mathbf{g}_i^T\mathbf{Q}\mathbf{g}_i^* + \sigma_r^2}\mathbf{g}_i^T\mathbf{g}_j^* + \frac{\sigma_d^2}{P_r}N_b, & i=j \\ 0, & i\neq j\end{cases},\quad i,\ j=1,...,K\end{aligned} \tag{4.13}$$

可以看出目的端的 SNR 為雷利商(Rayleigh quotient)的形式，在各參數都已給定

的情況下，我們可以利用代數運算找出最佳的中繼端預編碼係數向量$\boldsymbol{\beta}$，使得目的端 SNR 達到最大，最佳的$\boldsymbol{\beta}$向量解為

$$\boldsymbol{\beta}^{*} = c_0 \left(\mathbf{A}_2^{-1/2}\right)^H \mathbf{v} \tag{4.14}$$

其中c_0為中繼端傳輸功率正規化的係數，而$\mathbf{v}$為$\mathbf{A}_2^{-1/2}\mathbf{A}_1\left(\mathbf{A}_2^{-1/2}\right)^H$中最大特徵值所對應的特徵向量，求出最佳的中繼端預編碼係數後，就可以進一步設計最佳的資料源及人工雜訊統計特性，即$\mathbf{R}_x$與$\mathbf{Q}$。

4.4 $\mathbf{R}_x$與 Q 的最佳化

我們可裡利用 4.1 小節求得的中繼端最佳的預編碼係數，進一步在中繼端 SINR 受到限制的情況下，以提升目的端的服務品質為目標，更新更佳的$\mathbf{R}_x$與$\mathbf{Q}$矩陣，其最佳化問題如下

$$\begin{aligned}
\max_{\mathbf{R}_x,\mathbf{Q}} \quad & \mathrm{SNR}_D = \mathrm{tr}\left(\left(\tilde{\mathbf{H}}^H\mathbf{B}^H\mathbf{G}^*\mathbf{C}^{-1}\mathbf{G}^T\mathbf{B}\tilde{\mathbf{H}}\right)\mathbf{R}_x\right) \\
\text{s.t.} \quad & \mathrm{SINR}_{Rk} = \frac{\mathrm{tr}\left(\mathbf{h}_k^T\mathbf{R}_x\mathbf{h}_k^*\right)}{\mathrm{tr}\left(\mathbf{g}_k^T\mathbf{Q}\mathbf{g}_k^*\right)+\sigma_r^2} \le \gamma_e, \;\; k=1,...,K \\
& \mathrm{tr}\left(\mathbf{R}_x\right) \le P_s, \mathrm{tr}\left(\mathbf{Q}\right) \le P_b, \\
& \mathbf{R}_x \ge \mathbf{0}, \; \mathbf{Q} \ge \mathbf{0}
\end{aligned} \tag{4.15}$$

可以看出目標函數為$\mathbf{R}_x$的線性函數，並且可以將各中繼端的限制進行移項，如下

$$\frac{1}{\gamma_e}\mathrm{tr}\left(\mathbf{h}_k^H\mathbf{R}_x\mathbf{h}_k\right)-\mathrm{tr}\left(\mathbf{g}_k^H\mathbf{Q}\mathbf{g}_k\right)\le\sigma_r^2,\ \ k=1,...,K \tag{4.16}$$

此限制亦為一個$\mathbf{R}_x$與 $\mathbf{Q}$ 線性函數，所以得知這個最佳化問題為一個線性規劃(linear programming)的最佳化問題，可利用最佳化的工具 CVX 找出最佳的資料源及人工雜訊統計特性，即$\mathbf{R}_x$與 $\mathbf{Q}$，以及最佳的目的端 SNR，我們採用迭代法，再由已更新的最佳$\mathbf{R}_x$與 $\mathbf{Q}$，計算出最佳的中繼端的預編碼係數矩陣$\mathbf{B}$，反覆更新最佳的目的端 SNR，以及最佳的資料源訊號與目的端人工雜訊的統計特性，直到目的端 SNR 收斂為止。

最後將整個最佳化問題流程由圖 4.1 表示，在第一步驟，我們先初始化資料源與目的端的預編碼器，然後透過 4.1 小節中的運算，在滿足中繼端的總傳輸功率限制的情況下，計算出最佳的中繼端傳輸預編碼係數向量$\boldsymbol{\beta}$，使目的端 SNR 達到最大，第二步驟中，將所計算出的最佳預編碼係數帶入最佳化問題中，利用 CVX 工具將最佳的目的端 SNR，以及最佳的資料源統計特性$\mathbf{R}_x$和人工雜訊統計特性 $\mathbf{Q}$ 計算出來，並且取代原先資料源與目的端的初始統計特性設定，將上兩步驟反覆迭代，直到目的端最佳的 SNR 收斂才停止，即求出資料源訊號與目的端人工雜訊最佳的統計特性，以及此時最佳的目的端 SNR。

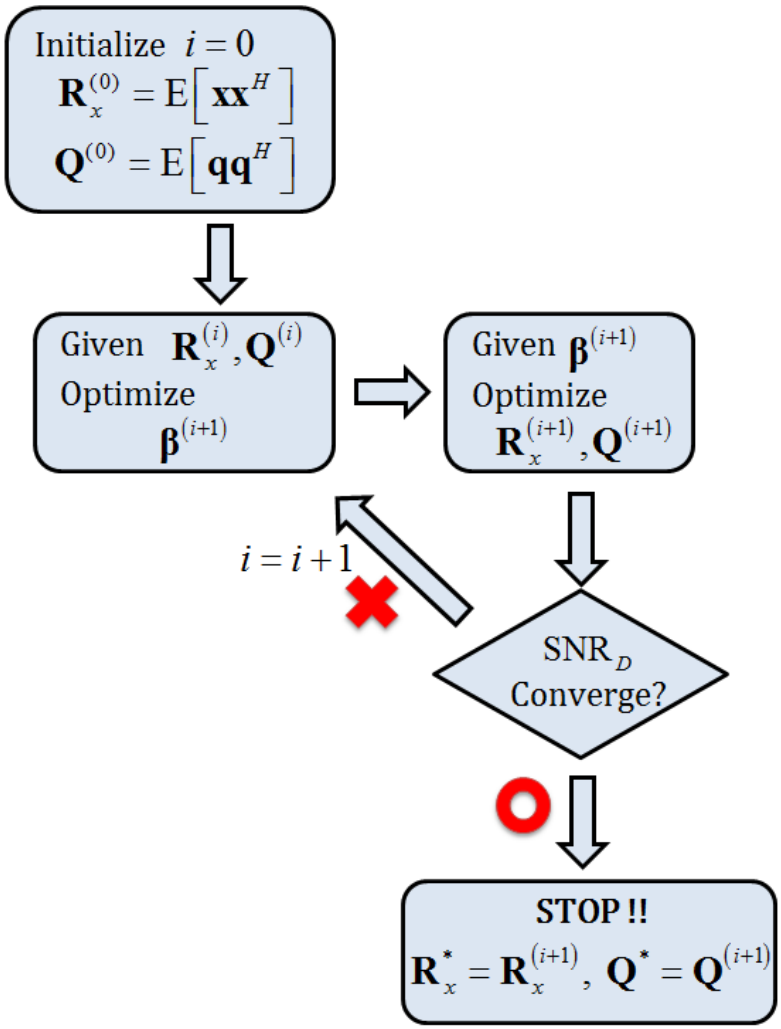

圖 4-1 預編碼器求解流程圖

第五章 模擬結果

在本章我們將模擬第四章所提出的最佳傳送策略，在本章所有模擬圖中，假設資料源與目的端具備三根天線，即 $N_a = N_b = 3$，共有三個中繼端，即 $K = 3$，而資料源與中繼端的傳送功率一致，即 $P_s = P_r$，調整目的端傳送人工雜訊的功率 P_b，觀察其保密效能；在以確保 QoS 為系統最佳設計的問題中，限制各中繼端的 SINR 在 10dB 之下，即 $\gamma_e = 10\text{dB}$；各節點的通道統計特性為 $CN(0,1)$，而各接收端的雜訊統計特性為 $CN(0,1)$，即 $\sigma_r^2 = \sigma_d^2 = 1$；在每一次模擬中，我們隨機產生 1000 次不同的通道狀況統計平均效能。在一開始計算最佳的中繼端傳送預編碼係數時，資料源與目的端預編碼器的初始統計特性為使用單一方向傳輸單一訊號的方式，且兩端皆有傳送功率限制，以 $\mathbf{R}_x = \frac{P_s}{N_a}\mathbf{1}\mathbf{1}^T$ 與 $\mathbf{Q} = \frac{P_b}{N_b}\mathbf{1}\mathbf{1}^T$ 表示。

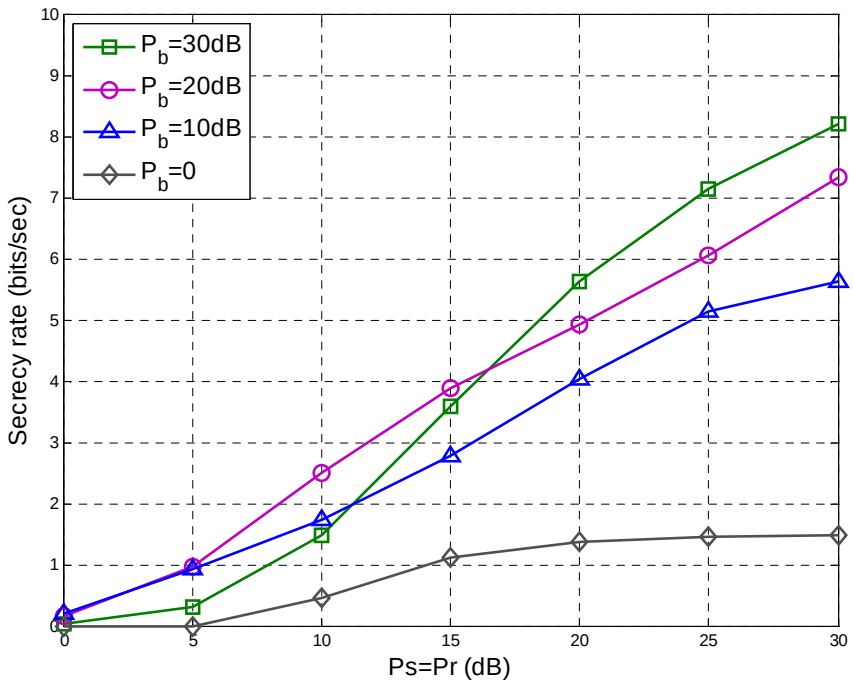

圖 5-1 使用不同人工雜訊強度的保密容量比較圖($N_a = N_b = 3$，$k = 3$)

圖 5-1 為第四章中所提出以 QoS 為系統考慮依據，設計出的最佳資料源與目的端預編碼器，可以發現在資料源與中繼端傳送功率偏低的情況，因為這時候中繼端所收到的訊號成分，相對於目的端欲干擾其接收的人工雜訊少很多，進而影響中繼端預編碼係數的選擇，導致目的端接收品質較差，故較大的人工雜訊功率會導致目的端的接收品質不佳，進而影響到整體系統的保密容量。以 30dB 的人工雜訊為例，在資料源與中繼端的傳送功率低於在 10dB 時，其保密容量比起人工雜訊強度在 20dB 和 10dB 的數值相對較低，而在人工雜訊功率為 0 的情況，最佳的資料源傳送預編碼器，亦可以對竊聽程度最多的中繼端達到些微的保密效果。

接著我們將提出方法和兩個延伸案例進行比較，第一個案例是將第四章節(4.15)式的最佳化問題中，針對各中繼端接收訊號 SINR 的限制條件去除，並且只考慮資料源的傳輸功率限制，所以此最佳化問題為

$$\begin{aligned} \max_{\mathbf{R}_x} \quad & \mathrm{SNR}_D = \mathrm{tr}\left(\left(\tilde{\mathbf{H}}^H \mathbf{B}^H \mathbf{G}^* \mathbf{C}^{-1} \mathbf{G}^T \mathbf{B} \tilde{\mathbf{H}}\right) \mathbf{R}_x\right) \\ \text{s.t.} \quad & \mathrm{tr}\left(\mathbf{R}_x\right) \le P_s \\ & \mathbf{R}_x \ge \mathbf{0} \end{aligned}$$

上述最佳化問題直接將各中繼端假設為可靠節點，也就是不去顧慮被竊聽可能性，利用最佳的中繼端預編碼係數矩陣 $\mathbf{B}$，透過上一章所使用的迭代方法，設計資料源訊號的統計特性，而目的端的人工雜訊的設計，直接採用各天線互相獨立且等功率的傳送方式，其統計特性以 $\mathbf{Q} = \frac{P_b}{N_b}\mathbf{I}$ 表示。

第二案例中，最佳化資料源訊號與目的端人工雜訊的統計特性，直接使用單一方向傳送單一訊號給各中繼端，其統計特性為

$$\mathbf{R}_x = \frac{P_s}{N_a}\mathbf{1}\mathbf{1}^T$$

$$\mathbf{Q} = \frac{P_b}{N_b}\mathbf{1}\mathbf{1}^T$$

其中$\mathbf{1}=[1\,1\,...\,1]^T$，其維度大小決定於傳送天線數量，各中繼端再利用此統計特性產生最佳的預編碼係數矩陣$\mathbf{B}$，幫忙資料源傳送訊號。圖 5-2 及圖 5-3 分別為觀察兩案例系統的保密效能的模擬圖。

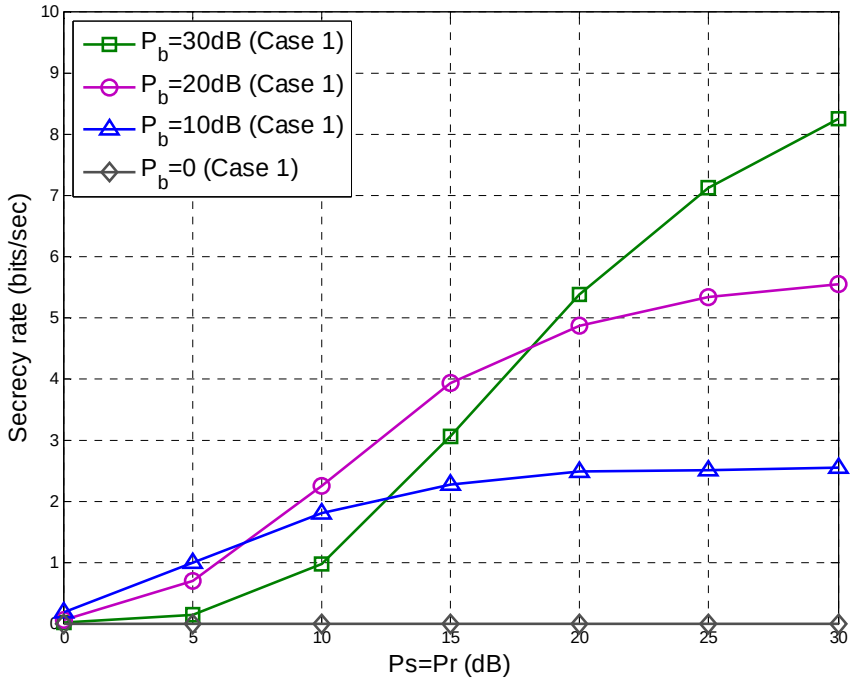

圖 5-2 案例 1 的保密容量比較圖($N_a = N_b = 3$，$k = 3$)

圖 5-2 資料源設計為不考慮竊聽風險的情況，設計最佳資料源預編碼器，目的端的人工雜訊直接設計為平均總傳送功率給各個天線方向，亦可以發現在資料源與中繼端傳送功率偏低的情況，較大的人工雜訊功率會導致目的端的接收品質不佳，進而影響到整體系統的保密容量。與圖 5-1 不同，在此系統中，人工雜訊功率為 0 時，單純依靠資料源預編碼設計的訊號，無法有效提供保密效果。

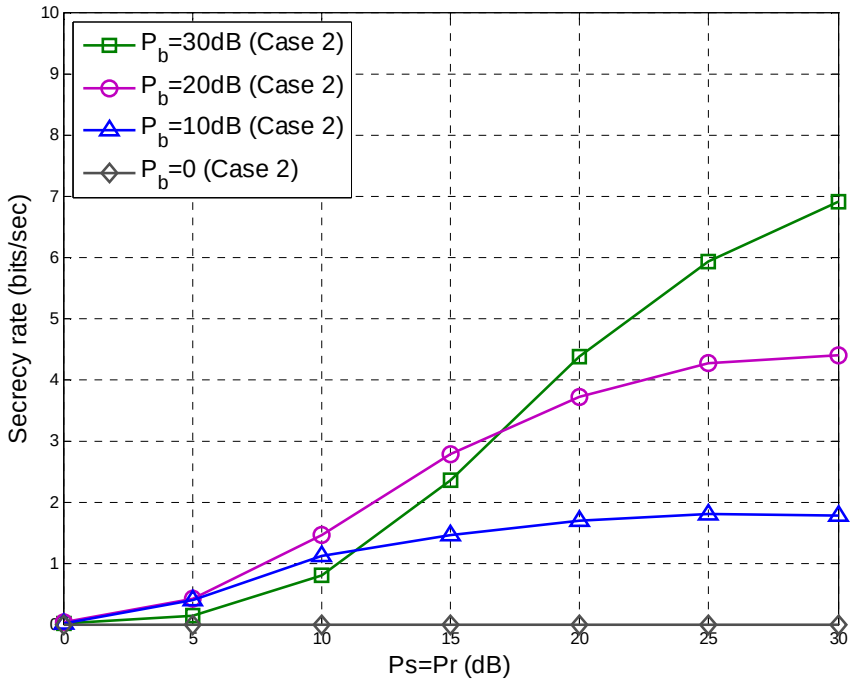

圖 5-3 案例 2 的保密容量比較圖($N_a = N_b = 3$ ， $k = 3$)

圖 5-3 為資料源與目的端天線傳送單一方向的情況，資料源與目的端各天線使用相等的功率傳送單一訊號及人工雜訊，其趨勢和圖 5-1 以及圖 5-2 相同，在資料源與中繼端傳送功率偏低的情況中，過度的人工雜訊會導致目的端的接收訊號品質不佳。與圖 5-2 相同，人工雜訊功率為 0 時，資料源只在單一方向傳送訊號，並無法抵抗不可靠中繼端的竊聽行為。

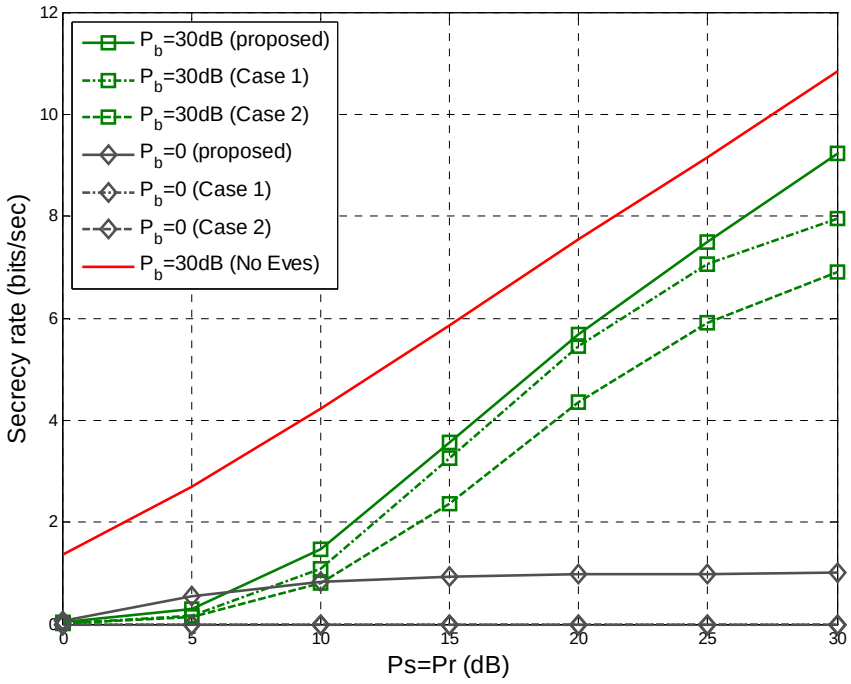

圖 5-4 比較保密效果圖($N_a = N_b = 3$ ， $k = 3$ ， $\gamma_e = 0\text{dB}$)

圖 5-4 為本論文所提出傳輸策略與案例 1 及案例 2 的比較，我們可以看出在三種傳輸策略中，第四章所提出以確保 QoS 為系統最佳傳輸設計目標中，所設計出的最佳資料源與目的端預編碼器，可以使其保密的效果在其他兩案例之上，限制中繼端 SINR 對保密確實有正面的效果，甚至在不使用人工雜訊的時候，利用最佳的傳送端預編碼器，可以使系統達到保密的效果。為了瞭解中繼端存在竊聽行為時，為了抵抗竊聽者所產生的效能流失，無圖案標記的實線為沒有竊聽者情況，在一般多中繼合作式通訊所能傳輸的最大資料量，當竊聽者存在的時候，發現為了要達到通訊保密，在傳輸效能上有 1~2bits/sec/Hz 的流失，並且發現若未經過好的設計，所使用的資料源訊號與目的端人工雜訊統計特性，為了抵抗竊聽行為，系統的效能流失將會更大。

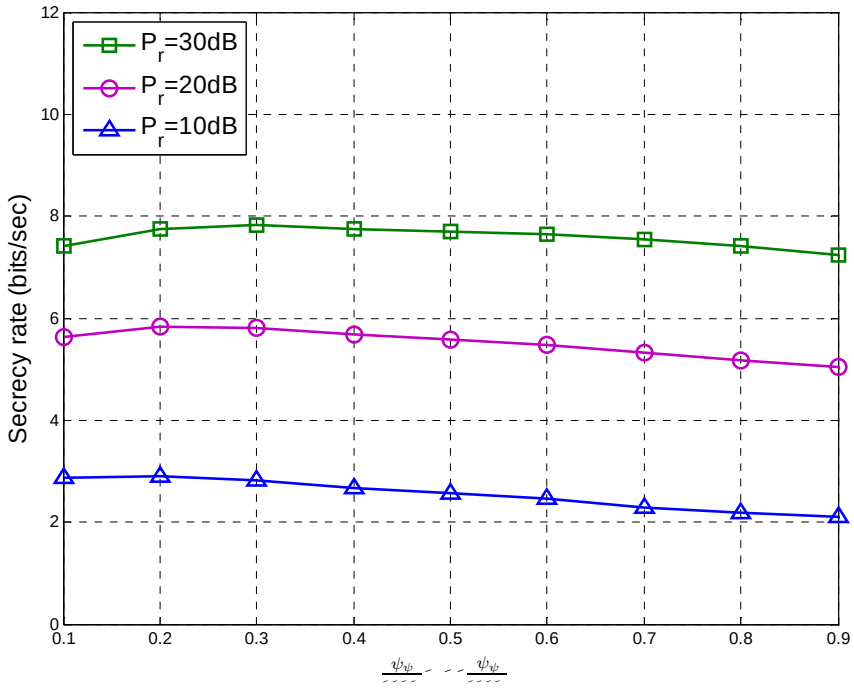

圖 5-5 給定 $P_s + P_b = 30\text{dB}$ 時，資料源與目的端傳送功率比值和保密容量關係圖

圖 5-5，我們觀察資料源與目的端傳送功率分配，與系統保密效能的關係，其中也變動中繼端的傳送功率，而資料源與目的端的傳送功率總和為 30dB，可以直覺的發現當中繼端的傳送功率增加時，對目的端的接收是很有幫助的，相對也提升了系統的保密效果。再來觀察中繼端使用不同傳送功率，對系統保密效能的影響，當 $P_r = 30\text{dB}$ 時，最佳的資料源與目的端傳送功率比值為 0.3，而當 $P_r = 10\text{dB}$ 時，最佳傳送功率的比值明顯往前移動，表示系統傾向於較多的人工雜訊幫助，才能得到較多的保密效果，主要是因為當中繼端傳送功率增加時，目的端處於接收品質較好的情況，較少的人工雜訊干擾，就可以產生較佳的保密效果，而中繼端傳送功率減少時，就需要較多的人工雜訊比例，來降低中繼端的接收品質，使目的端的接收品質相對較佳，進而得到較佳的保密效果。

另外我們也在確保 QoS 為系統考慮依據的最佳傳輸策略中，對傳送端與目的端的預編碼器傳送方向做了討論，如圖 5-6a、圖 5-6b、圖 5-6c 以及圖 5-6d。

其中圖 5-6a 和圖 5-6c，分別在人工雜訊功率為 10dB 和 30dB 下，對 P 的秩數所做的統計，我們發現有趣的現象，在此策略中，$\mathbf{R}_x$ 的秩數幾乎百分之百為 1，換句話說，最佳的資料源傳送方式為單一方向傳送一筆訊號。而圖 5-6b 和圖 5-6d，別在人工雜訊功率為 10dB 和 30dB 下，對 **Q** 的秩數所做的統計，可以發現在人工雜訊為 30dB 時，其秩數皆為 3，表示經過目的端預編碼器所產生的人工雜訊有三個方向，而在人工雜訊為 10dB 時，當資料源與中繼端的傳輸功率變大，人工雜訊的方向就逐漸變少，主要原因是當人工雜訊擁有較多功率時，可以將功率分配給各個中繼端的方向，達到干擾竊聽者的功用，而在資料源與中繼端的傳輸功率較大的情況，表示竊聽者擁有比較好的竊聽環境，而這時目的端傳輸功率不足以影響所有中繼端，而去選擇接收品質較佳的中繼端，進行人工雜訊的干擾，因此並不會各個方向皆傳送人工雜訊。

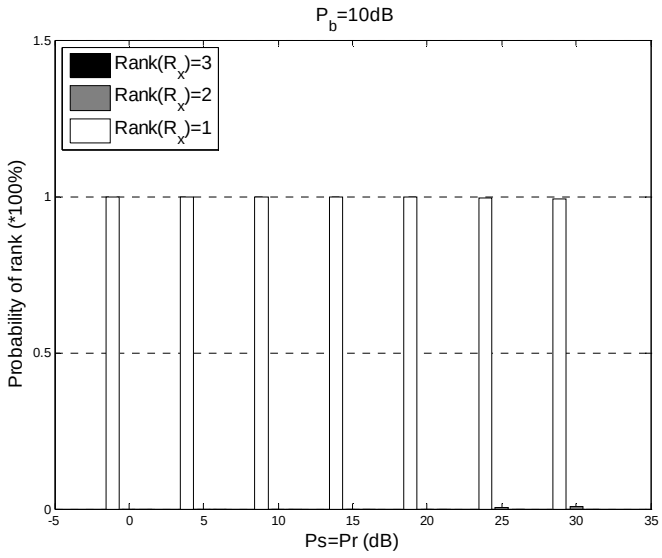

圖 5-6a P_b=10dB 時，$\mathbf{R}_x$ 的秩數統計圖($N_a = N_b = 3$，$k = 3$)

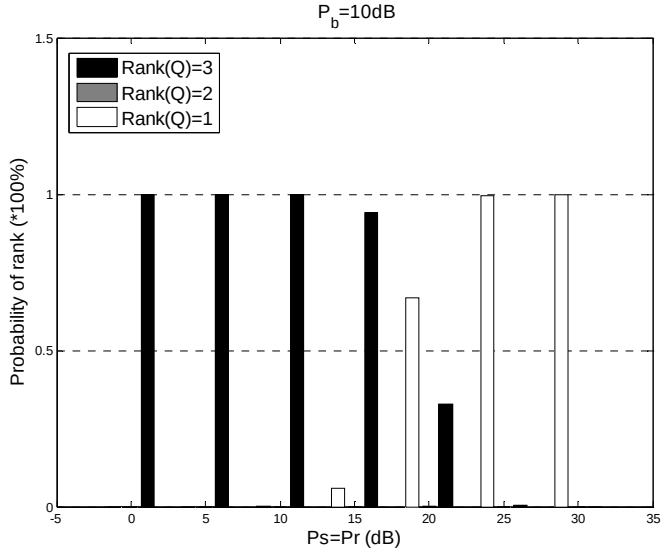

圖 5-6b P_b=10dB 時，**Q** 的秩數統計圖($N_a = N_b = 3$ ， $k = 3$)

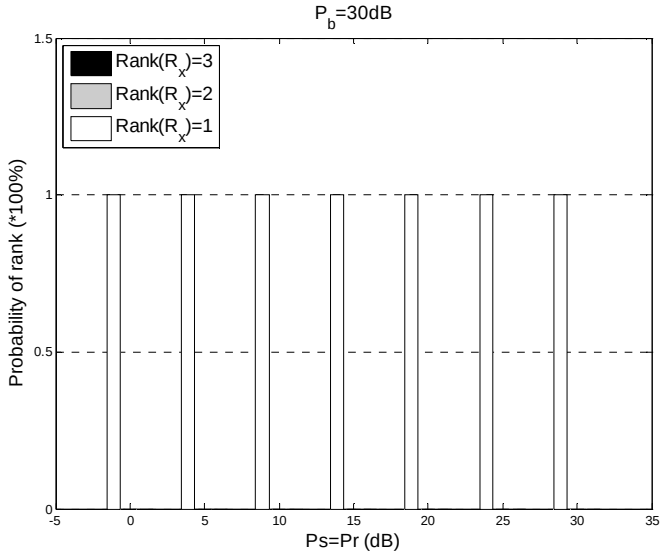

圖 5-6c P_b=30dB 時， $\mathbf{R}_x$ 的秩數統計圖($N_a = N_b = 3$ ， $k = 3$)

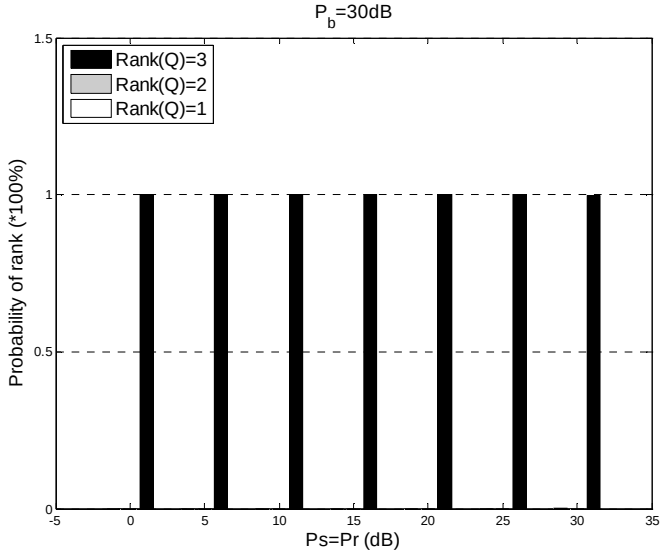

圖 5-6d P_b=30dB 時，**Q** 的秩數統計圖($N_a = N_b = 3$，$k = 3$)

我們還對資料源與目的端天線數量，以及中繼端的數量進行了討論。圖 5-7 和圖 5-8 為在確保 QoS 為系統考慮依據的最佳傳輸策略中，固定資料源與目的端的天線數量為三根，討論中繼端的數量對整體系統保密效能的影響；圖 5-6 中，人工雜訊功率為 30dB，可以觀察當中繼端的數量變多時，系統的保密效能也相對提升；而圖 5-7 中，人工雜訊功率為 10dB，我們刻意觀察資料源與中繼端的功率至 40dB，在資料源與中繼端高傳輸功率情況下，9 個中繼端的系統保密效能比 6 個中繼端的系統保密效能差，可以得知當中繼端數量增加，且各中繼端處在接收品質較佳的情況時，若人工雜訊的功率較低，將無法有效干擾中繼端群中的竊聽者，所以當中繼端數量增加的同時，應該要有足夠的人工雜訊功率，才能保證系統的保密效能。

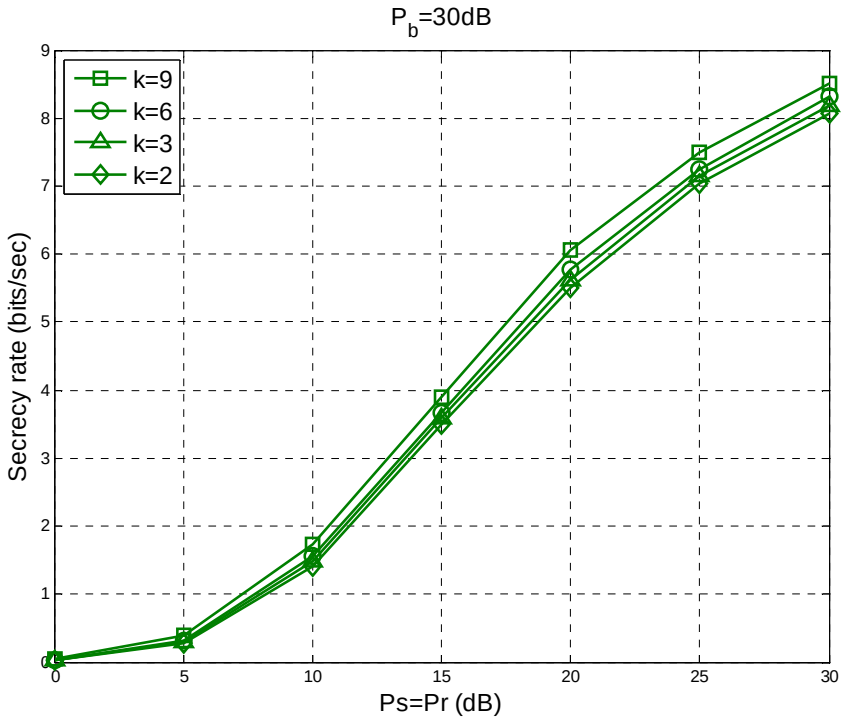

圖 5-7 P_b=30dB 時，中繼端的數量與保密效能關係圖($N_a = N_b = 3$)

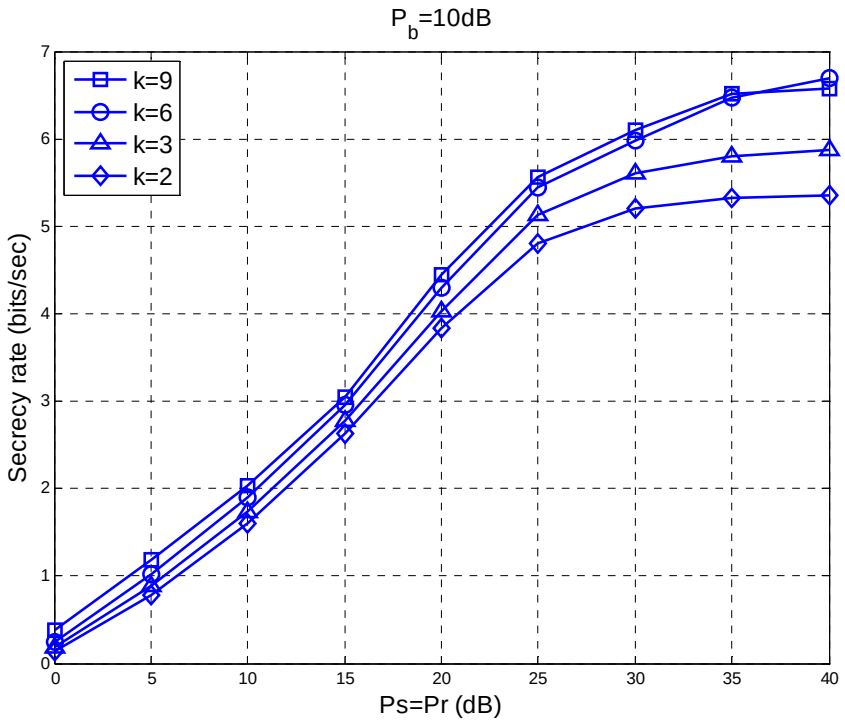

圖 5-8 P_b=10dB 時，中繼端的數量與保密效能關係圖($N_a = N_b = 3$)

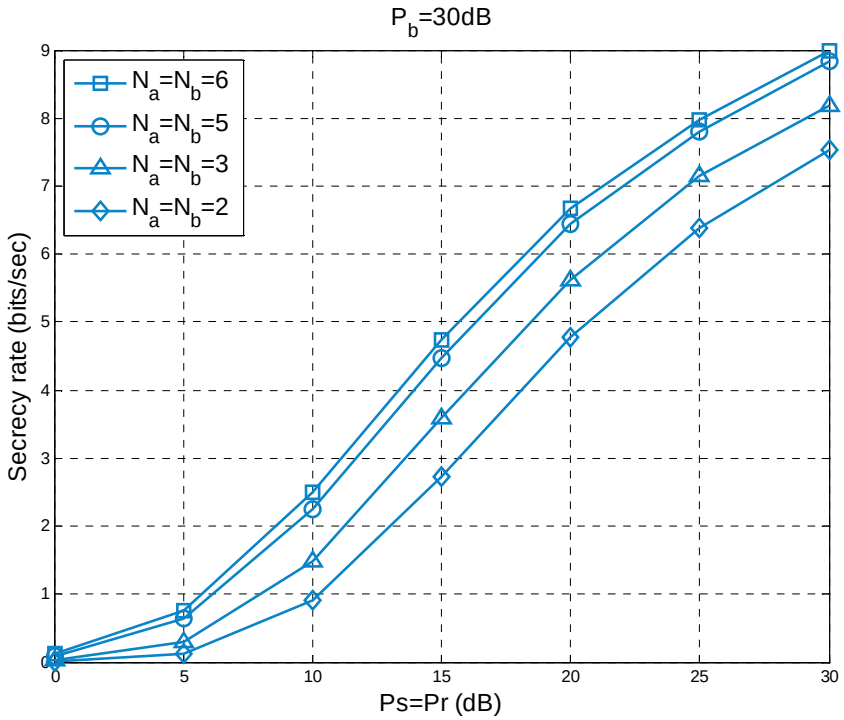

圖 5-9 P_b=30dB 時，資料源與目的端天線數量與保密效能關係圖($N_a = N_b$，$k = 3$)

圖 5-9 則是表示當中繼端的數量固定為三個時，改變資料源與目的端的天線數量，觀察其對系統保密效能的影響，可以發現當資料源與目的端的天線增加時，系統的保密效能也會隨之增加，其實這也是很直覺性的，因為當天線數量增加時，可以增加訊號傳送的多樣性(diversity)，對系統中的目的端而言是一個正向的影響。

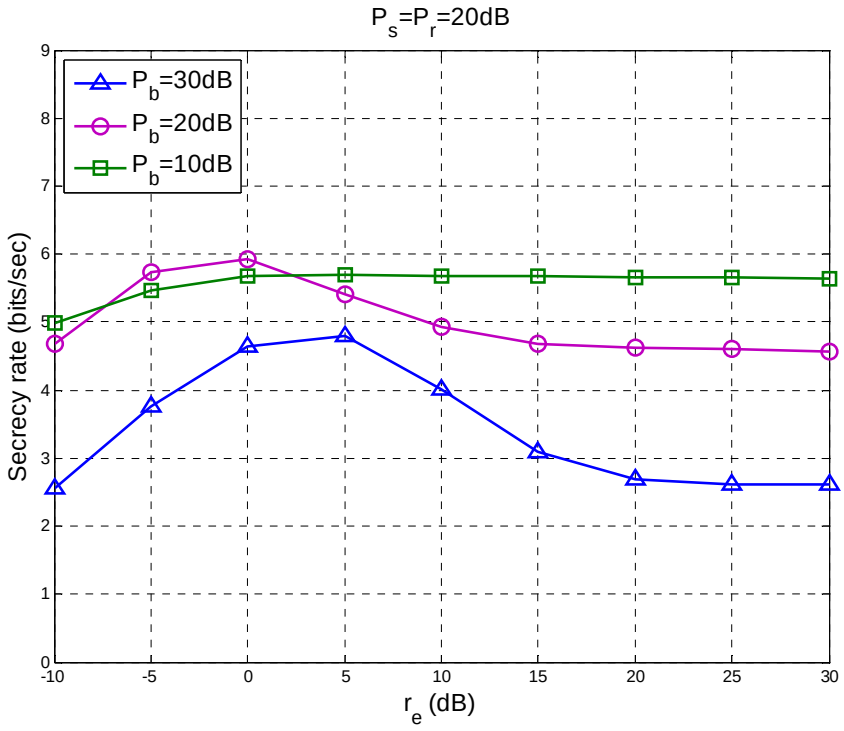

圖 5-10 $P_s = P_r$=20dB 時，觀察中繼端限制條件與保密效能關係圖($N_a = N_b = 3$ ，$k = 3$)

最後圖 5-10 中，觀察中繼端限制條件 γ_e 對系統保密容量的影響，我們比較了三種不同人工雜訊功率的結果，可以發現限制條件放寬時，相當於各中繼端可容許的接收品質更多，造成要減去的中繼端最大通道容量變大，所以計算出來的保密容量也相對降低，而限制條件變嚴格時，因為最佳化問題中，可行的集合也隨之變小，導致找不到最佳的傳送統計特性，其保密容量也跟著受影響，其中人工雜訊功率為 30dB 時，因為此時人工雜訊較大，相對限制的中繼端的接收，導致目的端也無法接收到較佳的訊號，保密效能進而受到限制，並且可以觀察到有部分甚至比人工雜訊功率為 20dB 時還要差。

第六章　結論

本文中我們研究多個具備單天線中繼系統，考慮這些中繼端為潛在竊聽者，他們具有潛在的威脅性，亦即可能擅自解開資料源所傳送的訊息，因此，在使用不可靠的中繼端幫忙傳送訊號的同時，也要避免其進行竊聽，因此我們設計從目的端針對中繼端傳送人工雜訊的策略，以期破壞各個中繼端從資料源獲得的訊號品質，降低這些不可靠中繼端順利解開訊號的機率，為了使系統提供保密的效能，我們提出在資料源與目的端各佈置一個預編碼器，以及調整各中繼端預編碼係數的方案，並且利用確保 QoS 為系統考慮的觀點，將最佳化問題進行化簡，最後利用了迭代的方法，使我們預設計的資料源與人工雜訊統計特性，即 $\mathbf{R}_x$ 與 $\mathbf{Q}$，以及中繼端放大後前送的預編碼係數得到最佳解，進而得到保密的效果。電腦模擬的結果可以看出，當使用人工雜訊干擾潛在的竊聽者時，系統的保密效能確實可以因為竊聽者的接收訊號遭受攻擊而提升，也可以了解經由系統最佳化設計過的訊號與人工雜訊統計特性，以及中繼端的預編碼係數，可以有效抵抗中繼端的竊聽情況，若未經過完善設計，系統保密效能有明顯的降低。

參考文獻

[1] J. Paulraj, D. A. Gore, R. U. Nabar, and H. Bölcskei, “An overview of MIMO communications—A key to gigabit wireless,” *Proc. IEEE*, vol. 92, no. 2, pp. 198–218, Feb. 2004.

[2] A. Nosratinia and A. Hedayat, “Cooperative communication in wireless networks,” *IEEE Commun. Mag*., vol. 42, no. 10, pp. 74–80, Oct. 2004.

[3] A. Sendonaris, E. Erkip, and B. Aazhang, “User cooperation diversity–Part I: System description,” *IEEE Trans. Commun*., vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[4] ——, “User cooperation diversity—Part II: Implementation aspects and performance analysis,” *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1939–1948, Nov. 2003.

[5] T. E. Hunter and A. Nosratinia, “Cooperation diversity through coding,” *in Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, July 2002, pp. 220.

[6] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[7] S. Goel and R. Negi, “Guaranteeing secrecy using artifical noise,” *IEEE Trans.*

[8] R. Negi and S. Goel, “Secret communication using artificial noise,” *in Proc. IEEE VTC*, Sept. 2005, pp. 1906–1910.

[9] X. He and A. Yener, “Two-hop secure communication using an untrusted relay: A case for cooperative jamming,” *in Proc. IEEE Globecom*, New Orleans, USA, Dec. 2008.

[10] A. D. Wyner "The wire-tap channel", *Bell Sys. Tech. J.*, vol. 54, pp.1355–1387 1975.

[11] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[12] A. Khisti and G. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory,* vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[13] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *in Proc. IEEE Int. Symp. Inf. Theory*, pp. 524–528, Jul. 2008.

[14] Y.-L. Liang, Y. Wang, T. Chang, Y.-W. P. Hong, and C. Chi, “On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise ,” in *Proc. IEEE ISIT*, pp. 2351–2355, Seoul, 2009.

[15] 陳信逢(2012)，《在放大後前送多重輸入輸出合作式系統中針對惡意竊聽中繼端之預編碼器設計》。國立中山大學通訊所碩士論文，未出版，高雄市。

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