PRIVATE AND SECURE DATA COMMUNICATION: INFORMATION THEORETIC APPROACH

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University

By

Yuksel Ozan Basciftci, B.S., M.S.

Graduate Program in Electrical and Computer Engineering

The Ohio State University

2016

Dissertation Committee:

Can Emre Koksal, Advisor

Fusun Ozguner

Ness B. Shroff

Facundo Memoli

ABSTRACT

This thesis aims to address privacy concerns in data sharing as well as security concerns in wireless data communication using information theoretic framework. In the first part of the thesis, we build security establishing algorithms that bring unbreakable security to wireless data communication. The broadcast nature of wireless medium makes data communication susceptible to various security attacks. For instance, an adversary can eavesdrop on confidential data traffic without actually tapping a wire or optical fiber, or block the data traffic by transmitting meaningless but powerful radio signals. First, we study point-to-point communication in the presence of a hybrid adversary. The hybrid half-duplex adversary can choose to either eavesdrop or jam the transmitter-receiver channel in arbitrary manner. The goal of the transmitter is to communicate a message reliably to the receiver while keeping it asymptotically secret from the hybrid adversary. We show that, without any feedback from the receiver, the channel capacity is zero if the transmitter-to-adversary channel stochastically dominates the effective transmitter-to-receiver channel. However, the channel capacity is non-zero even when the receiver is allowed to feedback only one bit periodically, that describes the transmitter-to-receiver channel quality. Our novel achievable strategy improves the rates proposed in the literature for the non-hybrid adversarial model.

Then, we study the security of a single-cell downlink massive multiple input multiple output (MIMO) communication in the presence of an adversary capable of jamming and eavesdropping simultaneously. After showing massive MIMO communication is naturally resilient to no training-phase jamming attack in which the adversary jams only the data communication and eavesdrops both the data communication and the training, we evaluate the number of antennas that base station (BS) requires in order to establish information theoretic security without even a need for extra security encoding. Next, we show that things are completely different once the adversary starts jamming the training phase. Specifically, we consider an attack, called training-phase jamming in which the adversary jams and eavesdrops both the training and the data communication. We show that under such an attack, the maximum secure degrees of freedom (DoF) is equal to zero. To counter this attack, we develop a defense strategy in which we use a secret key to encrypt the pilot sequence assignments to hide them from the adversary, rather than encrypt the data. We show that, if the cardinality of the set of pilot signals are scaled appropriately, hiding the pilot signal assignments from the adversary enables the users to achieve secure DoF, identical to the maximum achievable DoF under no attack.

The last part of the thesis is devoted to developing a mathematical framework for privacy-preserving data release mechanisms. The objective of privacy-preserving data release is to provide useful data with minimal distortion while simultaneously minimizing the sensitive data revealed. Dependencies between the sensitive and useful data results in a privacy-utility tradeoff that has strong connections to generalized rate-distortion problems. In this work, we study how the optimal privacy-utility tradeoff region is affected by constraints on the data that is directly available as input to the release mechanism. Such constraints are potentially motivated by applications where either the sensitive or useful data is not directly observable. For example,

the useful data may be an unknown property that must be inferred from only the sensitive data. In particular, we consider the availability of only sensitive data, only useful data, and both (full data). We show that a general hierarchy holds, that is, the tradeoff region given only the sensitive data is no larger than the region given only the useful data, which in turn is clearly no larger than the region given both sensitive and useful data. In addition, we determine the conditions that make the tradeoff region given only the useful data identical with the tradeoff given both sensitive and useful data.

To my dear friend Ozgur Dalkilic, rest in peace...

ACKNOWLEDGMENTS

I would like to express my deepest appreciation and thanks to my advisor, Prof. Can Emre Koksal, for his support and encouragement throughout my graduate studies. I would not be able to complete my studies without his guidance during the difficult times. I would also like to thank my co-advisor, Prof. Fusun Ozguner for her support especially during my first years at my PhD, and the insightful conversations. In addition, I would like to thank Prof. Ness B. Shroff and Prof. Facundo Memoli for agreeing to be in my thesis committee.

I acknowledge the support of National Science Foundation (grants CNS-1054738, CNS-1514260, CIF-0916664), Qatar National Research Fund (grant NPRP 5-559-2-227), and Transportation Research Center (grant 00036949).

VITA

Jun 1986	Born in Ankara, Turkey
Jun 2008	B.Sc. in Electrical & Electronics Engineering, Hacettepe University, Ankara, Turkey
Aug 2010	M.S. in Electrical & Computer Engineering, Bilkent University, Columbus, OH
Sep 2010-Jul. 2016	Grad. Research and Teaching Assoc., The Ohio State University, Columbus, OH
May 2015-Aug 2015	Research Intern, Mitsubishi Electric Research Labs, Cambridge, MA

PUBLICATIONS

Y. O. Basciftci, Y. Wang, and P. Ishwar, "On privacy-utility tradeoff for constrained data release mechanisms", to be submitted to IEEE Trans. on Information Theory

Y. O. Basciftci and C. E. Koksal, "Delay optimal secrecy in two-hop delay networks", to be submitted to IEEE Trans. on Information Theory

Y. O. Basciftci and C. E. Koksal, "Securing massive MIMO at the physical layer", submitted to IEEE Trans. on Information Theory

Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of fading channels with a hybrid adversary", IEEE Trans. on Information Theory, vol. 61, no. 3, pp. 1-19, March 2015

Y. O. Basciftci, Y. Wang, P. Ishwar, "Privacy-utility trade-off in data disclosure", ITA 2016, San Diego, CA

Y. O. Basciftci, C. E. Koksal, A. Ashikhmin "Securing massive MIMO at the physical layer", CNS 2015, Florence, Italy

Y. O. Basciftci, F. Chen, J. Weston, R. Burton, and C. E. Koksal, "How vulnerable is vehicular communication to physical layer jamming attacks?", IEEE VTC 2015, Boston, USA

Y. O. Basciftci and C. E. Koksal, "Delay optimal secrecy in two-hop delay networks", IEEE GlobalSip 2014 , Atlanta, USA

Y. O. Basciftci and C. E. Koksal, "Private broadcasting with probing constraint, IEEE SPAWC 2014, Toronto, Canada

Y. O. Basciftci, C. E. Koksal, and F. Ozguner, "To obtain or not to obtain CSI in the presence of hybrid adversary", IEEE ISIT 2013, Istanbul, Turkey

Y. O. Basciftci and F. Ozguner, "Trust aware particle filters for autonomous vehicles", IEEE ICVES 2012, Istanbul, Turkey.

P. Gong, Y. O. Basciftci, and F. Ozguner, "A parallel resampling algorithm for particle filtering on shared-memory architectures", IEEE PDSEC, 2012, Shanghai, China

Y. O. Basciftci,"A system level simulation of WiMAX," Master's Thesis, Bilkent University, 2010

FIELDS OF STUDY

Major Field: Electrical and Computer Engineering

Specialization: Information Theory, Wireless Communications

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Wireless networks flourishing worldwide enable online services, such as social networks and search engines to serve huge number of users and to collect large amount of data about their users. Sharing of this data has been key driver of innovation and improvement in the quality of these services, but also raised major security and privacy concerns. This thesis aims to address privacy concerns in data sharing as well as security concerns in wireless data communication using information theoretic framework. Wireless networks flourishing worldwide enable online services, such as social networks and search engines to serve huge number of users and to collect large amount of data about their users. Sharing of this data has been key driver of innovation and improvement in the quality of these services, but also raised major security and privacy concerns. This thesis aims to address privacy concerns in data sharing as well as security concerns in wireless data communication using information theoretic framework.

In the first part of the thesis, we build security establishing algorithms that bring unbreakable security to wireless data communication. The broadcast nature of wireless medium makes data communication susceptible to various security attacks. For instance, an adversary can eavesdrop on confidential data traffic without actually tapping a wire or optical fiber, or block the data traffic by transmitting meaningless but powerful radio signals. First, we study point-to-point communication in the presence

of a hybrid adversary. The hybrid half-duplex adversary can choose to either eavesdrop or jam the transmitter-receiver channel, but not both at a given time. The goal of the transmitter is to communicate a message reliably to the receiver while keeping it asymptotically secret from the hybrid adversary. During the communication, the state of the adversary (jamming or eavesdropping) changes in an arbitrary manner and is unknown to the transmitter.

The main challenge in our problem stems from the fact that simultaneously maintaining reliability and security is difficult because of the adversary's arbitrary strategy in choosing its state, i.e., jamming or eavesdropping, at a given time. If we design a scheme focusing on a particular adversary strategy, with a slight change in that particular strategy, the adversary can cause a decoding error or a secrecy leakage. For instance, if our scheme assumes a fully eavesdropping adversary, then jamming even in a small fraction of the time will lead to a decoding error. Likewise, if the scheme is designed against a full jammer, then the adversary will lead to a secrecy leakage even it eavesdrops for a small fraction of time. A robust scheme should take into account the entire set of adversary strategies to maintain reliability and secrecy. We show that, without any feedback from the receiver, the channel capacity is zero if the transmitter-to-adversary channel stochastically dominates the effective transmitter-to-receiver channel. However, the channel capacity is non-zero even when the receiver is allowed to feedback only one bit periodically, that describes the transmitter-to-receiver channel quality. Our novel achievable strategy improves the rates proposed in the literature for the non-hybrid adversarial model.

Finally, we study the security of a single-cell downlink massive MIMO communication in the presence of an adversary capable of jamming and eavesdropping simultaneously. Massive MIMO is one of the highlights of the envisioned 5G communication

systems. In massive MIMO paradigm, the base station is equipped with a number of antennas, typically much larger than the number of users served. Combined with a TDD-based transmission, this solves many of the issues pertaining channel state information. In particular, the base station exploits law-of-large-numbers-like certainties as it serves each user over a combination of a large number of channels. While many issues behind the design of multicellular massive MIMO systems have been studied thoroughly, security of massive MIMO has not been actively addressed. We show that massive MIMO communication is naturally resilient to no training-phase jamming attack in which the adversary jams only the data communication and eavesdrops both the data communication and the training. Further, we evaluate the number of antennas that base station (BS) requires in order to establish information theoretic security without even a need for extra security encoding. Next, we show that things are completely different once the adversary starts jamming the training phase. Specifically, we consider an attack, called training-phase jamming in which the adversary jams and eavesdrops both the training and the data communication. We show that under such an attack, the maximum secure degrees of freedom (DoF) is equal to zero. Furthermore, the maximum achievable rates of users vanish even in the asymptotic regime in the number of BS antennas. To counter this attack, we develop a defense strategy in which we use a secret key to encrypt the pilot sequence assignments to hide them from the adversary, rather than encrypt the data. We show that, if the cardinality of the set of pilot signals are scaled appropriately, hiding the pilot signal assignments from the adversary enables the users to achieve secure DoF, identical to the maximum achievable DoF under no attack.

The last part of the thesis is devoted to developing a mathematical framework for privacy-preserving data release mechanisms. The objective of privacy-preserving data release is to provide useful data with minimal distortion while simultaneously

minimizing the sensitive data revealed. Dependencies between the sensitive and useful data results in a privacy-utility tradeoff that has strong connections to generalized rate-distortion problems. In this work, we study how the optimal privacy-utility tradeoff region is affected by constraints on the data that is directly available as input to the release mechanism. Such constraints are potentially motivated by applications where either the sensitive or useful data is not directly observable. For example, the useful data may be an unknown property that must be inferred from only the sensitive data. In particular, we consider the availability of only sensitive data, only useful data, and both (full data). We show that a general hierarchy holds, that is, the tradeoff region given only the sensitive data is no larger than the region given only the useful data, which in turn is clearly no larger than the region given both sensitive and useful data. In addition, we determine conditions under which the tradeoff region given only the useful data coincides with that given full data.

1.1 Contributions

Chapter 2

We consider a block fading wiretap channel, where a transmitter attempts to send messages securely to a receiver in the presence of a hybrid half-duplex adversary, which arbitrarily decides to either jam or eavesdrop the transmitter-to-receiver channel. We provide bounds to the secrecy capacity for various possibilities on receiver feedback and show special cases where the bounds are tight. We show that, without any feedback from the receiver, the secrecy capacity is zero if the transmitter-to-adversary channel stochastically dominates the *effective* transmitter-to-receiver channel. However, the secrecy capacity is non-zero even when the receiver is allowed to feed back only one bit at the end of each block. Our novel achievable strategy improves the rates proposed in the literature for the non-hybrid adversarial model. We

also analyze the effect of multiple adversaries and delay constraints on the secrecy capacity. We show that our novel time sharing approach leads to positive secrecy rates even under strict delay constraints. We also expand our results to the delay-limited and multiple adversaries setting.

Chapter 3

We consider a single-cell downlink massive MIMO communication in the presence of an adversary capable of jamming and eavesdropping simultaneously. We show that massive MIMO communication is naturally resilient to *no training-phase jamming* attack in which the adversary jams *only* the data communication and eavesdrops *both* the data communication and the training. Specifically, we show that the secure degrees of freedom (DoF) attained in the presence of such an attack is identical to the maximum DoF attained under no attack. Further, we evaluate the number of antennas that base station (BS) requires in order to establish information theoretic security without even a need for Wyner encoding. Next, we show that things are completely different once the adversary starts jamming the training phase. Specifically, we consider an attack, called *training-phase jamming* in which the adversary jams and eavesdrops *both* the training and the data communication. We show that under such an attack, the maximum secure DoF is equal to zero. Furthermore, the maximum achievable rates of users vanish even in the asymptotic regime in the number of BS antennas. To counter this attack, we develop a defense strategy in which we use a secret key to encrypt the pilot sequence assignments to hide them from the adversary, rather than encrypt the data. We show that, if the cardinality of the set of pilot signals are scaled appropriately, hiding the pilot signal assignments from the adversary enables the users to achieve secure DoF, identical to the maximum achievable DoF under no attack. Finally, we discuss how computational cryptography is a legitimate candidate to hide the pilot signal assignments. Indeed, while information

theoretic security is not achieved with cryptography, the computational power necessary for the adversary to achieve a non-zero mutual information leakage rate goes to infinity.

Chapter 4

Privacy-preserving data release mechanisms aim to simultaneously minimize information leakage with respect to sensitive data and distortion with respect to useful data. Dependencies between sensitive and useful data results in a privacy-utility tradeoff that has strong connections to generalized rate-distortion problems. In this work, we study how the optimal privacy-utility tradeoff region is affected by constraints on the data that is directly available as input to the release mechanism. In particular, we consider the availability of only sensitive data, only useful data, and both (full data). We show that a general hierarchy holds, that is, the tradeoff region given only the sensitive data is no larger than the region given only the useful data, which in turn is clearly no larger than the region given both sensitive and useful data. In addition, we determine conditions under which the tradeoff region given only the useful data coincides with that given full data. This is based on the common information between the sensitive and useful data.

CHAPTER 2

ON THE SECRECY CAPACITY OF BLOCK FADING CHANNELS WITH A HYBRID ADVERSARY

2.1 Introduction

We study point-to-point block fading channels, depicted in Figure 3.1, in the presence of a hybrid adversary. The hybrid half-duplex adversary can choose to either eavesdrop or jam the transmitter-receiver channel, but not both at a given block. The goal of the transmitter is to communicate a message reliably to the receiver while keeping it asymptotically secret from the hybrid adversary. During the communication, the state of the adversary (jamming or eavesdropping) changes in an *arbitrary* manner from one block to the next and is *unknown* to the transmitter. We further assume that the transmitter has *no channel state information* (CSI) of the transmitter-to-receiver channel (main channel), the transmitter-to-adversary channel (eavesdropper channel) and the adversary-to-receiver channel (jamming channel). The receiver has perfect causal CSI of the main and jamming channels. We study the secrecy capacity of this setting when (i) there is no receiver-to-transmitter feedback, and (ii) there is 1-bit of receiver-to-transmitter feedback sent at the *end of each block*.

Our technical contributions are summarized as follows:

- We show that the secrecy capacity is zero when the receiver feedback is not available and the eavesdropper channel stochastically dominates the *effective*

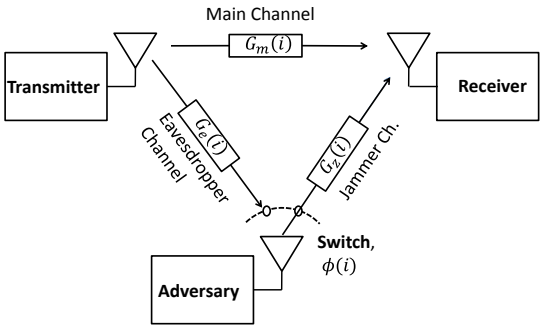

Figure 2.1: System Model

main channel gain. However, we also show that even one bit of receiver feedback at the end of each block is sufficient to make the secrecy capacity positive for almost all possible channel distributions.

- Under an arbitrary adversarial strategy, the receiver cannot employ a well known typical set decoder [1] since it cannot assume a certain distribution for the received signal. To that end, we propose a receiver strategy in which the receiver generates artificial noise and adds it to the received signal (i.e., jams itself to involve typical set decoding [1]). We show special cases in which artificial noise generation at the receiver is an optimal way to achieve the secrecy capacity.

- For the 1-bit receiver feedback case, we propose a proof technique for the equivocation analysis, that is based on renewal theory. By this technique, we can improve the existing achievable secrecy rates in [2], which focus on passive eavesdropping attacks only. Note that our adversary model covers the possibility of a full eavesdropping attack as well since it allows for the adversary to eavesdrop (or jam) for an arbitrary fraction of the time.

- We bound the secrecy capacity when there are multiple hybrid adversaries. The challenge in bounding the secrecy capacity for multiple adversaries scenario stems from the fact that, when an adversary jams the legitimate receiver, it also interferes to the other adversaries as well. However, we show that the impact of the interference of one adversary to another adversary does not appear in the bounds, which results in a tighter upper bound. Furthermore, the bounds we provide are valid for the cases in which the adversaries collude or do not collude. In the non-colluding case, we show that the secrecy capacity bounds are determined by the adversary that has the strongest eavesdropper channel.

In addition to the aforementioned set-up, we also consider a delay limited communication in which a message of fixed size arrives at the encoder at the beginning of each block, and it needs to be transmitted reliably and securely by the end of that particular block. Otherwise, *secrecy outage* occurs at that block. We analyze delay limited capacity subject to a secrecy outage constraint. We employ a time sharing strategy in which we utilize a portion of each block to generate secret key bits and use these key bits as a supplement to secure the delay sensitive messages that are transmitted in the other portion of each block. Our scheme achieves positive delay limited secrecy rates whenever the secrecy capacity without any delay constraint is positive.

Related Work

The wiretap channel, introduced by Wyner [3], models information theoretically secure message transmission in a point-to-point setting, where a passive adversary eavesdrops the communication between two legitimate nodes by wiretapping the legitimate receiver. While attempting to decipher the message, no limit is imposed on the computational resources available to the eavesdropper. This assumption led

to defining (weak) secrecy capacity as the maximum achievable rate subject to zero mutual information rate between the transmitted message and the signal received by the adversary. This work was later generalized to the non-degraded scenario [4] and the Gaussian channel [5]. By exploiting the stochasticity and the asymmetry of wireless channels, the recent works [6, 7] extended the results in [3–5] to a variety of scenarios involving fading channels. However, all of the mentioned works consider a passive adversary that can only eavesdrop.

There is a recent research interest on hybrid adversaries that can either jam or eavesdrop [8–10]. In [9], the authors formulate the wiretap channel as a two player zero-sum game in which the payoff function is an achievable ergodic secrecy rate. The strategy of the transmitter is to send the message in a full power or to utilize some of the available power to produce artificial noise. The conditions under which pure Nash equilibrium exists are studied. In [8], the authors consider fast fading main and eavesdropper channels and a static jammer channel, where the adversary follows an ergodic strategy such that it jams or eavesdrop with a certain probability in each channel use. Under this configuration, they propose a novel encoding scheme, called block-Markov Wyner secrecy encoding. In [10], the authors introduce a pilot contamination attack in which the adversary jams during the reverse training phase to prevent the transmitter from estimating the channel state correctly. The authors show the impact of the pilot contamination attack on the secrecy performance. Note that, neither of these works consider an adversary that has an *arbitrary strategy* to either jam or eavesdrop, which is the focus of this thesis.

Channels under arbitrary jamming (but no eavesdropping) strategies have been studied in the context of arbitrary varying channel (AVC). AVC, the concept of which is introduced in [11], is defined to be the communication channel the statistics of which change in an arbitrary and unknown manner during the transmission

of information. In [12], the authors derive the capacity for Gaussian AVCs, memoryless Gaussian channels disrupted by a jamming signal that changes arbitrarily with unknown statistics. An extensive treatment of AVCs, outlining the challenges and existing approaches can be found in [13]. Recently, discrete memoryless AVCs with a secrecy constraint and no receiver feedback have been studied in [14] [15] [16] where the states of the channels to the both receiver and the eavesdropper remain unknown to the legitimate pair and change in an arbitrary manner under the control of the adversary. In [14] and [15], the achievable secrecy rates the authors propose are zero when the worst possible transmitter-to-receiver channel is a degraded version of the best possible transmitter-to-adversary channel. In [16], the authos investigate the case in which there is a common randomness between the legitimate pair. They study the secrecy capacity when the adversary exploits the common randomness between the legitmate pair. In this thesis, in addition to the jamming signal of the adversary, we consider the fading channels whose states cannot be completely controlled by the adversary. We also do not assume that the legitimate pair shares a common randomness. We show the *secrecy capacity* is zero when the main channel gain is stochastically dominated by the eavesdropper channel gain. Furthermore, under arbitrarily small receiver feedback rate (1-bit at the end of each block), we show that the secrecy capacity is *non-zero*. In [17], the authors consider an (ρ_r, ρ_w) adversary which can see a fraction ρ_r, and modify a fraction ρ_w, of the sent codeword. The adversary chooses which components of the codewords it will observe and modify arbitrarily. The authors characterize the secrecy capacity and provide an explicit code construction method to achieve the secrecy capacity

The rest of this section is organized as follows. In Section 2.2, we explain the system model. In Section 2.3, we present the secrecy capacity bounds for the no feedback case, and in Section 2.4, we consider the 1-bit feedback case. In Section 2.5,

we study the multiple adversaries case. In Section 2.6, we present our results related to the strict delay setting. In Section 2.7, we present our numerical results

2.2 System Model

We study the communication system illustrated in Figure 3.1. In our system a transmitter has a message $w \in \mathcal{W}$ to transmit to the receiver over the main channel. The adversary chooses to either jam the receiver over the jammer channel or eavesdrop it over the eavesdropping channel. The actions of the adversary is parametrized by the state, $\phi(i)$ of a switch, shown in Figure 3.1. Thus, our system consists of three channels: main, eavesdropper and jammer channels, all of which are block fading. In the block fading channel model, time is divided into discrete blocks each of which contains N channel uses. The channel states are assumed to be constant within a block and vary independently from one block to the next. We assume the adversary is half duplex, i.e., the adversary can not jam and eavesdrop simultaneously. The observed signals at the legitimate and the adversary in i-th block are as follows:

$$Y^N(i) = G_m(i)x^N(i) + G_z(i)S_j^N(i)\phi(i) + S_m^N(i) \tag{2.2.1}$$

$$Z^N(i) = \begin{cases} G_e(i)x^N(i) + S_e^N(i) & \text{if } \phi(i) = 0 \\ \emptyset & \text{if } \phi(i) = 1 \end{cases} \tag{2.2.2}$$

where $x^N(i)$ is the transmitted signal, $Y^N(i)$ is the signal received by the legitimate receiver, $Z^N(i)$ is the signal received by the adversary, $S_j^N(i)$, $S_m^N(i)$, and $S_e^N(i)$ are noise vectors distributed as complex Gaussian, $\mathcal{CN}(\mathbf{0}, P_j I_{N\times N})$, $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, and $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, respectively, and P_j is the jamming power. Indicator function $\phi(i) = 1$ if the adversary is in a jamming state in i-th block; otherwise, $\phi(i) = 0$. Channel gains, $G_m(i)$, $G_e(i)$, and $G_z(i)$ are defined to be the complex gains of the main channel, eavesdropper channel, and jammer channel, respectively (as illustrated in Figure 3.1).

Associated power gains are denoted with $H_m(i) = |G_m(i)|^2$, $H_e(i) = |G_e(i)|^2$, and $H_z(i) = |G_z(i)|^2$. For any integer $M > 0$, the joint probability density function (pdf) of $\left(G_m^M, G_e^M, G_z^M\right)$ is

$$p_{G_m^M, G_e^M, G_z^M}\left(g_m^M, g_e^M, g_z^M\right) \tag{2.2.3}$$

$$= \prod_{i=1}^{M} p_{G_m, G_e, G_z}\left(g_m(i), g_e(i), g_z(i)\right). \tag{2.2.4}$$

Here, $g_m(i)$, $g_e(i)$, and $g_z(i)$ are the realizations of $G_m(i)$, $G_e(i)$, and $G_z(i)$, respectively. We assume that the joint pdf of instantaneous channel gains, $p_{G_m, G_e, G_z}(g_m, g_e, g_z)$ is known by all entities. The transmitter does not know the states of any channel, and also cannot observe the strategy of the adversary in any given block. The adversary and the receiver know $g_e(i)$ and $(g_m(i), g_z(i))$, respectively at the end of block i. The receiver can observe the instantaneous strategy of the adversary, $\phi(i)$ in block i (e.g., via obtaining the presence of jamming) only at the end of block i. We generalize some of our results to the case in which the receiver cannot observe $g_z(i)$.

We consider two cases in which feedback from the receiver to the transmitter is not available or some limited feedback is available. In particular, in the latter case, we consider a 1-bit feedback over an error-free public channel at *the end of each block*. Hence, the feedback is available both at the transmitter and the adversary. We denote the feedback sent at j-th time instant as $k(j)$.

For the 1-bit feedback case, $k(j)$ is an element of $\{0, 1\}$ and is a function of $(y^j, g_m^i, g_z^i, \phi^i)$ if time instant j corresponds to the end of a block, i.e., $j = iN$ for any block index $i \geq 1$. For other time instants, the receiver does not send feedback: $k(j) = \emptyset$ if $j \neq iN$ for all $i \geq 1$. For the no feedback case, $k(j) = \emptyset$ for all $j \geq 1$.

The transmitter encodes message w over M blocks. The transmitted signal at j-th instant, $x(j)$ can be written as

$$x(j) = f_j(w, k^{j-1}), \tag{2.2.5}$$

where f_j is the encoding function used at time j. We assume the input signals satisfy an average power constraint such that

$$\frac{1}{NM}\sum_{j=1}^{NM}\mathbb{E}\left[\left|f_j\left(w,K^{j-1}\right)\right|^2\right]\leq P_t \tag{2.2.6}$$

for all $w\in\mathcal{W}$, where $\mathcal{W}$ is the message set. Here, the expectation is taken over $K^{j-1}=[K(1),\ldots,K(j-1)]$, where $K(j)$ is the random variable denoting the feedback signal sent at j-th instant . The channels depicted in Figure 3.1 are memoryless i.e.,

$$\begin{aligned}
&p\left(y^N(i),z^N(i)|x^{Ni},g_m^i,g_e^i,g_z^i,k^{N(i-1)},\phi^i\right)\\
&\quad=p\left(y^N(i),z^N(i)|x^N(i),g_m(i),g_e(i),g_z(i),\phi(i)\right) &(2.2.7)\\
&\quad=p\left(y^N(i)|x^N(i),g_m(i),g_z(i),\phi(i)\right)\times\\
&\qquad\qquad p\left(z^N(i)|x^N(i),g_e(i),\phi(i)\right), &(2.2.8)
\end{aligned}$$

where (2.2.7) follows form the memoryless property and (2.2.8) follows from the fact that the additive noise components in $y^N(i)$ and $z^N(i)$ are independent. Adversary strategy $\phi(i)$ changes arbitrarily from one block to the next. Here, the conditional pdfs $p\left(y^N(i)|x^N(i),g_m(i),g_z(i),\phi(i)\right)$ and $p\left(z^N(i)|x^N(i),g_e(i),\phi(i)\right)$ are governed by the signal models of the main channel (2.2.1) and the eavesdropper channel (2.2.2), respectively.

The transmitter aims to send message $w\in\mathcal{W}=\{1,2,\ldots 2^{NMR_s}\}$ to the receiver over M blocks with rate R_s. By employing a $c\left(2^{NMR_s},NM\right)$ code, the encoder at the transmitter maps message w to a codeword x^{NM}, and the decoder at the receiver, $d(\cdot)$ maps the received sequence Y^{NM} to $\hat{w}\in\mathcal{W}$. The average error probability of a $c\left(2^{NMR_s},NM\right)$ code is defined as

$$\begin{aligned}
&P_e^{NM}(\phi^M,g_m^M,g_z^M,c)\\
&=2^{-NMR_s}\sum_{w\in\mathcal{W}}\mathbb{P}\left(d\left(Y^{NM},\phi^M,g_m^M,g_z^M\right)\neq w|w\text{ was sent}\right) &(2.2.9)
\end{aligned}$$

where $c \triangleq c\left(2^{NMR_s}, NM\right)$.

The secrecy of a transmitted message, w is measured by the equivocation rate at the adversary, which is equal to the entropy rate of the transmitted message conditioned on the adversary's observations.

Definition 1. *A secrecy rate R_s is said to be achievable if, for any $\epsilon > 0$, there exists a sequence of length NM channel codes $c\left(2^{NMR_s}, NM\right)$ and sets $\mathcal{A}_M$ for which the following are satisfied under any strategy of the adversary, ϕ^M:*

$$P_e^{NM}\left(\phi^M, g_m^M, g_z^M, c\right) \leq \epsilon, \tag{2.2.10}$$

$$\frac{1}{MN} H\left(W | Z^{MN}, K^{MN}, \phi^M, g^M, c\right) \geq R_s - \epsilon, , \tag{2.2.11}$$

for sufficiently large N and M and for any $g^M = \left[g_m^M, g_e^M, g_z^M\right] \in \mathcal{A}_M$ such that $\mathbb{P}[\mathcal{A}_M] \geq 1 - \epsilon$.

Note that $K^{MN} = \emptyset$ for the no feedback case. The secrecy capacity is defined to be the supremum of the achievable rates. The secrecy capacities for the no feedback and 1-bit feedback case are denoted as C_s and $C_s^{\text{1-bit}}$, respectively. Our goal is to find secrecy rates, R_s that are achievable under any strategy of the adversary and find the cases in which they are tight.

2.3 No Feedback

In this section, we provide bounds to the secrecy capacity for the no feedback case and evaluate the capacity for special cases. In the sequel, we provide a number of remarks under which we provide the basic insights drawn from the results.

Theorem 2.3.1. ***(Secrecy capacity bounds for the no feedback case)*** *The secrecy capacity, C_s is bounded by*

$$C_s^- \leq C_s \leq C_s^+ \tag{2.3.1}$$

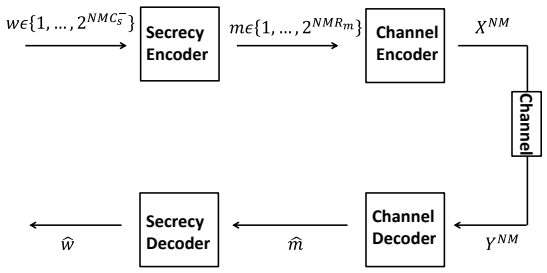

Figure 2.2: Achievability strategy described in the proof sketch of Theorem 2.3.1.

where

$$C_s^- = \left[\mathbb{E}\left[\log\left(1+\frac{P_t H_m}{1+P_j H_z}\right) - \log\left(1+P_t H_e\right)\right]\right]^+ \tag{2.3.2}$$

$$C_s^+ = \min_{p_{\tilde{H}_m,\tilde{H}_e,\tilde{H}_z}} \mathbb{E}\left[\left(\log\left(1+\frac{P_t \tilde{H}_m}{1+P_j \tilde{H}_z}\right) - \log\left(1+P_t \tilde{H}_e\right)\right)^+\right] \tag{2.3.3}$$

$$\textit{subject to}: p_{\tilde{H}_m,\tilde{H}_z} = p_{H_m,H_z},\ p_{\tilde{H}_e} = p_{H_e}$$

□

Notice that in Theorem 2.3.1, the positive operator,[1] $[\cdot]^+$ is outside the expectation in the lower bound, whereas it is inside the expectation in the upper bound. In the upper bound, minimization is over the all possible joint pdfs, $p_{\tilde{H}_m,\tilde{H}_e,\tilde{H}_z}$ that satisfy the following constraints $p_{\tilde{H}_m,\tilde{H}_z} = p_{H_m,H_z}$ and $p_{\tilde{H}_e} = p_{H_e}$. Here, there is no constraint on the dependency of $\left(\tilde{H}_m, \tilde{H}_z\right)$ and $\tilde{H}_e$. Note that if $P_j = 0$ in Theorem 2.3.1, then new bounds are valid for the scenario in which the adversary always eavesdrops the main channel, which is a common scenario in the literature.

The complete proofs for the lower bound and the upper bound in Theorem 2.3.1

[1] $[x]^+ = \min(0, x)$.

are available in Appendix A.1. Here, we provide a proof sketch for the lower bound. We consider the impact of the adversary's arbitrary strategy on both the probability error and secrecy. The secrecy encoder, depicted in Figure 2.2, maps message $w \in \{1, \ldots, 2^{NMC_s^-}\}$ to randomized message $m \in \{1, \ldots, 2^{NMR_m}\}$ as in [3]. The channel encoder, illustrated in Figure 2.2, employs codebook c, where the codebook contains 2^{NMR_m} independently and identically generated codewords, x^{NM} of length NM. The channel encoder maps randomized message m to one of the codewords in c. The probability law of the main channel is $p\left(y^N(i)|x^N(i), g_m(i), g_z(i), \phi(i)\right)$, where $\phi(i)$ changes from one block to the next arbitrarily. To remove the arbitrary nature of the main channel, the decoder artificially generates a noise sequence drawn from $\mathcal{CN}\left(0, h_z P_j I_{N\times N}\right)$, where h_z is picked from $H_z(i)$, and adds the noise sequence to it's received signal $y^N(i)$ when the adversary is in the eavesdropping state, $\phi(i) = 0$. Hence, the decoder can employ typical set decoding [1], which would not have been possible without the artificial noise, due to the lack of the underlying probability distribution for the received signal associated with the arbitrary adversary strategy. We select R_m as

$$R_m = \max_{p(x^N(i))} \frac{1}{N} I(X^N(i), Y^N(i)|G_m(i), G_z(i), \phi(i) = 1) \tag{2.3.4}$$

$$= \mathbb{E}\left[\log\left(1 + \frac{P_t H_m}{1 + P_j H_z}\right)\right], \tag{2.3.5}$$

where the joint distribution of $\left(X^N(i), Y^N(i)\right)$ in (2.3.4) is governed by (2.2.1) for a given $p(x^N(i))$, and (2.3.5) follows from the fact that $X^N(i) \sim \mathcal{C}N(0, P_t I_{N\times N})$ maximizes the optimization in (2.3.4). Therefore, each codeword, x^{NM} is picked from $\mathcal{C}N(0, P_t I_{NM\times NM})$. For the equivocation analysis, the possibility of the adversary eavesdropping at all times should be taken into account. We need to use a conservative secrecy encoder, designed for $\phi(i) = 0$ for all $i \geq 1$; otherwise, we cannot achieve an arbitrarily low mutual information leakage rate to the adversary with high probability.

With the aforementioned techniques, we show that C_s^- satisfies constraints (3.2.10) and (2.2.11) in Appendix A.1. Note that the lower bound C_s^- is valid for any value of block length N. We now provide several remarks related to Theorem 2.3.1.

Remark 2.3.2. ***(Secrecy capacity is zero when the eavesdropper channel power gain stochastically dominates the main channel effective power gain)*** *If H_e stochastically dominates[2] the main channel effective power gain, $H_m^* \triangleq \dfrac{H_m}{1+P_j H_z}$, and H_e and H_m^* have continuous cumulative distribution functions (cdfs), then the secrecy capacity, C_s is zero. To observe this fact, let $\hat{H}_e \triangleq F_{H_e}^{-1}\left(F_{H_m^*}\left(H_m^*\right)\right)$, where F_A and F_A^{-1} stand for the cdf and the inverse cdf[3] of random variable A, respectively. From the definition of stochastic dominance and the definition of $\hat{H}_e$, we have $\hat{H}_e \geq H_m^*$ with probability 1. We now show that $\hat{H}_e$ and H_e have the same cdf the following derivation:*

$$\begin{aligned}
\mathbb{P}\left[\hat{H}_e \leq a\right] &= \mathbb{P}\left[F_{H_e}^{-1}\left(F_{H_m^*}\left(H_m^*\right)\right) \leq a\right] && (2.3.6)\\
&= \mathbb{P}\left[F_{H_m^*}(H_m^*) \leq F_{H_e}(a)\right] && (2.3.7)\\
&= \mathbb{P}\left[H_m^* \leq F_{H_m^*}^{-1}\left(F_{H_e}\left(a\right)\right)\right] && (2.3.8)\\
&= F_{H_m^*}\left(F_{H_m^*}^{-1}\left(F_{H_e}\left(a\right)\right)\right) && (2.3.9)\\
&= F_{H_e}(a), \forall a \geq 0, && (2.3.10)
\end{aligned}$$

where (2.3.7) *follows from the fact that $F_A^{-1}(b) \leq c \iff b \leq F_A(c)$ with $b \in [0,1]$, and* (2.3.8) *and* (2.3.10) *follow from the continuity of the cdf of H_m^*. Hence, $(H_m, \hat{H}_e, H_z)$ satisfy the constraint given in the upper bound* (2.3.3)*. When $(\tilde{H}_m, \tilde{H}_e, \tilde{H}_z) = (H_m, \hat{H}_e, H_z)$, the expectation term in* (2.3.3) *is zero.* □

[2]Random variable A stochastically dominates random variable B if $F_A(a) \leq F_B(a)$ for all a, where $F_A(a) \triangleq \mathbb{P}[A \leq a]$ and $F_B(a) \triangleq \mathbb{P}[B \leq a]$.

[3]$F_A^{-1}(a) \triangleq \inf\{b : F_A(b) = a\}$.

Remark 2.3.2 is easy to state for the fading scenario in which H_m and H_e are exponentially distributed random variables. Condition $\mathbb{E}[H_m] \leq \mathbb{E}[H_e]$ is sufficient for H_e to stochastically dominate H_m^* (defined in Remark 2.3.2).

Remark 2.3.3. ***(Bounds are tight if the power gain of the effective main channel is larger than that of the eavesdropper channel with probability 1)*** *Suppose there exits random variables $\hat{H}_m, \hat{H}_e$, and $\hat{H}_z$ satisfying the following conditions:*

1) $\dfrac{\hat{H}_m}{1+P_j\hat{H}_z} \geq \hat{H}_e$ *with probability 1,*

2) $p_{\hat{H}_m,\hat{H}_z} = p_{H_m,H_z}$, *and*

3) $p_{\hat{H}_e} = p_{H_e}$.

Then, $C_s^- = C_s = C_s^+$. To observe this fact, let $(\tilde{H}_m, \tilde{H}_e, \tilde{H}_z)$ in (2.3.3) be $(\hat{H}_m, \hat{H}_e, \hat{H}_z)$. Then, the positive operator gets out of the expectation in the upper bound, C_s^+. Furthermore, since the lower bound does not depend on p_{H_m,H_e,H_z} but depend on p_{H_m,H_z} and p_{H_e}, we can replace (H_m, H_e, H_z) with $(\hat{H}_m, \hat{H}_e, \hat{H}_z)$. Thus, the upper and lower bounds become equal. □

Remark 2.3.4. ***(The amount of the reduction in the achievable rate in Theorem 2.3.1 can be significant when the jamming channel gain is not available at RX.)*** *In Theorem 2.3.1, the receiver is assumed to know $g_z(i)$. Now, suppose that the receiver is kept ignorant of $g_z(i)$. Then, the following rate*

$$R_s^{'} = [R - \mathbb{E}\left[\log\left(1+P_tH_e\right)\right]]^+ \tag{2.3.11}$$

is achievable, where

$$R = \max_{p_{X^N(i)}(x^N(i))} \frac{1}{N} I(X^N(i), Y^N(i)|G_m(i), \phi(i)=1). \tag{2.3.12}$$

Here, for a given $p_{X^N(i)}(x^N(i))$, the joint distribution of $\left(X^N(i), Y^N(i)\right)$ is governed by (2.2.1)*. We can lower bound R with the following steps:*

$$R \geq \frac{1}{N} I(X_G^N(i), Y^N(i) | G_m(i), \phi(i) = 1) \tag{2.3.13}$$

$$\geq \mathbb{E}\left[\log\left(1 + \frac{P_t H_m}{1 + P_j \mathbb{E}[H_z]}\right)\right], \tag{2.3.14}$$

where $X_G^N(i) \sim \mathcal{CN}(0, P_t I_{N\times N})$ in (2.3.13)*. The covariance matrix of the jamming component in $Y^N(i)$ is $\mathbb{E}\left[H_z(i)\right] I_{N\times N}$. In [18], the authors show that Gaussian noise that has the same covariance matrix with the original additive noise component minimizes $I(X^N(i); Y^N(i))$ when $X^N(i)$ is Gaussian distributed. Hence, we replace $G_z(i) S_j^N(i)$ with $\mathcal{CN}(0, \mathbb{E}\left[H_z(i)\right] I_{N\times N})$, and reach the inequality in* (2.3.14)*. Note that when $\mathbb{E}[H_z] \to \infty$, lower bound $R_s^{'}$ goes to zero, whereas in the original case (Theorem 2.3.1), lower bound C_s^- does not neccesarily goes to zero.* □

Suppose that the transmitter and the adversary power constraints scale in the same order, parametrized by P, i.e., $P_t(P) = \mathcal{O}\left(P_j(P)\right)$ as $P \to \infty$. We show that the secrecy capacity is zero in the no feedback case as $P \to \infty$ in the following corollary.

Corollary 2.3.5. *(**Secrecy capacity goes to zero when the jamming and transmission power constraints scale similarly.**) Suppose that $P_t(P)$ and $P_j(P)$ are continuous functions of P with $\lim_{P\to\infty} P_t(P) = \infty$, $\lim_{P\to\infty} P_j(P) = \infty$ and $P_t(P) = \mathcal{O}\left(P_j(P)\right)$ as $P \to \infty$. When the power gains of the channels have bounded and continuous pdfs and have finite expectations, the secrecy capacity of the no feedback case, C_s is asymptotically*

$$\lim_{P\to\infty} C_s = 0. \tag{2.3.15}$$

□

The proof of Corollary 2.3.5 is available at Appendix A.2. To prove (2.3.15), we investigate the upper bound, C_s^+ as $P \to \infty$ and show that

$$\lim_{P\to\infty} C_s^+ = 0. \tag{2.3.16}$$

2.4 1-Bit Feedback

In this section, we analyze the secrecy capacity for the 1-bit feedback case, i.e., the receiver is allowed to send a 1 bit feedback over a public channel at the end of each block. As we observe in Remark 2.3.2, the secrecy capacity of the no feedback case is zero if H_e stochastically dominates $H_m^* \triangleq \dfrac{H_m}{1+P_jH_z}$. However, in this section, we show that the lower bound for the 1-bit feedback case is non-zero for the most of the joint pdfs of power gains.

Theorem 2.4.1. *(**Secrecy capacity bounds for the 1-bit feedback case**) The secrecy capacity, $C_s^{1\text{-}bit}$ is bounded by*

$$\max\left(C_s^-, R_s^{1\text{-}bit}\right) \le C_s^{1\text{-}bit} \le C_s^{+1\text{-}bit} \tag{2.4.1}$$

where

$$C_s^{+1\text{-}bit} = \mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+\max(P_jH_z, P_tH_e)}\right)\right] \tag{2.4.2}$$

$$R_s^{1\text{-}bit} = \max_R \frac{1}{\mathbb{E}[T]}\mathbb{E}\left[R - \log\left(1+P_t\sum_{i=1}^{T}\tilde{H}_e(i)\right)\right]^+ \tag{2.4.3}$$

where C_s^- is provided in (2.3.2), T is a random variable with probability mass function (pmf), $p_T(t) = \mathbb{P}(\mathcal{D}_t \cap \mathcal{D}_{t-1}^c) = \mathbb{P}(\mathcal{D}_t) - \mathbb{P}(\mathcal{D}_{t-1})$, $t \ge 1$ with

$$\mathcal{D}_t \triangleq \left\{\log\left(1+\sum_{i=1}^{t}\frac{P_tH_m(i)}{1+P_jH_z(i)}\right) \ge R\right\}$$

and $\mathcal{D}_0 = \emptyset$, and

$$p_{\tilde{H}_e(1),\tilde{H}_e(2),\ldots,\tilde{H}_e(T)|T}\left(h_e(1), h_e(2), \ldots, h_e(T)|T=t\right) =$$

$$p_{H_e(1),H_e(2),\ldots,H_e(t)}\left(h_e(1),h_e(2),\ldots,h_e(t)|\mathcal{D}_t,\mathcal{D}_{t-1}^c\right)$$

□

The complete proofs for lower and upper bounds are available in Appendix A.3. Note that the feedback available at the transmitter in block i, $K^{(i-1)N}$ is independent from the channel gains in block i, $G(i)$ since the transmitter observes the feedback at the end of the block, and the channel gains change from one block to the next independently. Hence, the transmission power term in the upper bound is not a function of the channel gains and is equal to the transmission power constraint, P_t. Furthermore, notice that in Theorem 2.4.3, the positive operator is inside the expectation in (2.4.3), that makes the lower bound positive for a wide class of channel statistics.

Remark 2.4.2. *(**Non-zero secrecy capacity**) Note that* $\left\{\log\left(1+\frac{P_tH_m(i)}{1+P_jH_z(i)}\right)\right\}_{i\geq 1}$ *is a sequence of i.i.d non-negative random variables and*

$$T=\inf\left\{t:\sum_{i=1}^{t}\log\left(1+\frac{P_tH_m(i)}{1+P_jH_z(i)}\right)\geq R\right\}.$$

If $\mathbb{P}\left[\frac{P_tH_m}{1+P_jH_z}\neq 0\right]>0$, $\mathbb{E}[T]<\infty$ *for all* $R>0$ *[19]. Furthermore, there exists* $R\geq 0$ *that makes* $\mathbb{E}\left[R-\log\left(1+P_t\sum_{i=1}^{T}\tilde{H}_e(i)\right)\right]^+$ *also positive since* $\mathbb{P}\left[\sum_{i=1}^{T}\tilde{H}_e(i)<\infty\right]>0$. *Hence, we observe that* $C_s^{1\text{-}bit}>0$. □

Here, we provide the proof sketch of the lower bound provided in Theorem 2.4.3. First, C_s^- is achieved with the strategy provided in Theorem 2.3.1 without the feedback. The strategy to achieve $R_s^{\text{1-bit}}$ is as follows. The secrecy encoder, depicted in Figure 2.3, maps message $w\in\left[1:2^{NMR_s^{\text{1-bit}}}\right]$ to bit sequence $B_l\in\{0,1\}^{NM\frac{R}{\mathbb{E}[T]}}$ of size $NM\dfrac{R}{\mathbb{E}[T]}$ with a stochastic mapping as described in [3], where $l\in[1,2,\ldots,2^{NM\frac{R}{\mathbb{E}[T]}}]$. Bit sequence B_l is partitioned into the bit groups $\{B_l(k)\}_{k\in\left[1,2,\ldots,\lceil\frac{M}{\mathbb{E}[T]}\rceil\right]}$ each of which

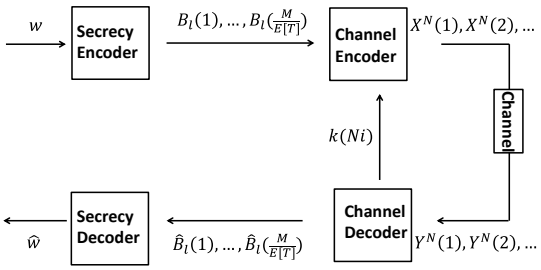

Figure 2.3: Achievability strategy described in the proof sketch of Theorem 2.4.1. The feedback at at the end of block i is denoted as $k(Ni)$, where N is the length of a block.

has size of NR bits such that $B_l = [B_l(1), B_l(2), \ldots, B_l(\lceil \frac{M}{\mathbb{E}[T]} \rceil)]$. The channel encoder, depicted in Figure 2.3, generates Gaussian codebook c of size 2^{NR}, and each bit group $B_l(k)$ is mapped to one of the codewords in the codebook.

To send $B_l(k)$ in block i, the associated codeword $x^N(i)$ is transmitted over the channel. The channel encoder keeps sending the same codeword until $B_l(k)$ is successfully decoded. The channel decoder, depicted in Figure 2.3, employs maximum ratio combining (MRC), and combines all received sequences associated with $B_l(k)$. Specifically, the channel decoder multiples each $y^N(i)$ associated with the bit group with $\frac{g_m^*(i)}{(1+P_j h_z(i))^2}$ and sums them. From the random coding arguments, we can see that $B_l(k)$ will be decoded with arbitrarily low probability error at i-th block if event $\mathcal{S}(i) \triangleq \left\{ \log\left(1 + \sum_{j=1}^{r(i)} \frac{P_t H_m(i-j+1)}{1+P_j H_z(i-j+1)}\right) \geq R \right\}$ occurs, regardless of the adversary strategy ϕ^i, where $r(i)$ is the number of transmissions for $B_l(k)$ until the end of block i. If event $\mathcal{S}(i)$ occurs, the channel decoder sends back positive acknowledgment signal (ACK), and the channel encoder sends the next bit group, i.e., $B_l(k+1)$ on block $i+1$. If event $\mathcal{S}(i)$ does not occur, the channel decoder feeds back a negative acknowledgment signal (NAK) at the end of block i. On next block $i+1$, the channel

encoder sends the same codeword, i.e., $x^N(i+1) = x^N(i)$. This process is repeated until B_l is successfully decoded.

In the derivation for the lower bound for the equivocation rate, we assume that the adversary can observe the transmissions in the jamming state[4]. Consider a renewal process in which a renewal occurs when the accumulated mutual information associated with a bit group exceeds threshold R for the first time. In Appendix A.3, we show that 1-bit feedback case can be considered as a model in which *secure* bits of random size $N\left[R - \log\left(1 + P_t \sum_{i=1}^{T} \tilde{H}_e(i)\right)\right]^+$ are decoded successfully at each renewal point. Here, random variable T defined in Theorem 2.4.1 represents the number of transmissions for a bit group and denotes the inter-renewal time of the renewal process. Thus, $N \log\left(1 + P_t \sum_{i=1}^{T} \tilde{H}_e(i)\right)$ can be considered as a random amount of accumulated mutual information at the adversary corresponding to the transmissions of a bit group. Theorem 2.4.3 follows when we apply the renewal reward theorem [20], where the rewards are the successfully decoded secure bits at each renewal instants. The complete proofs for lower and upper bounds are available in Appendix A.3.

Instead of employing MRC strategy, the receiver can employ a plain automatic repeat request (ARQ) strategy in which the receiver discards the received sequence $y^N(i)$ when the decoding error occurs on i-th block. Impact of plain ARQ on the lower bound is captured with the following corollary.

Corollary 2.4.3. *(**Secrecy capacity lower bound with plain ARQ**) The secrecy capacity, $C_s^{1\text{-}bit}$ is bounded by*

$$\max\left(C_s^-, R_s^{*1\text{-}bit}\right) \leq C_s^{1\text{-}bit} \tag{2.4.4}$$

[4]We will drop this assumption when we analyze the case in which the transmitter has the main channel state information (CSI) in addition to the 1-bit feedback (Corollary 2.4.4).

where

$$R_s^{*1\text{-}bit} = \max_R \; p \times \mathbb{E}\left[R - \log\left(1 + P_t \sum_{i=1}^{T^*} \tilde{H}_e(i)\right)\right]^+ \tag{2.4.5}$$

where C_s^- *is provided in* (2.3.2). *In* (2.4.5), $p \triangleq \mathbb{P}\left(\log\left(1 + \frac{P_t H_M}{1 + P_j H_z}\right) \geq R\right)$, T^* *is a random variable with probability mass function (pmf),* $p_{T^*}(t) = p(1-p)^{t-1}$, $t \geq 1$, *and*

$$\begin{aligned} &p_{\tilde{H}_e(1),\tilde{H}_e(2),\ldots,\tilde{H}_e(T^*)|T^*}\left(h_e(1), h_e(2), \ldots, h_e(T^*)|T^* = t\right) = \\ &\quad \prod_{i=1}^{t-1} p_{H_e}\left(h_e(i)|R > \log\left(1 + \frac{P_t H_m}{1 + P_j H_z}\right)\right) \times \\ &\qquad p_{H_e}\left(h_e(t)|R \leq \log\left(1 + \frac{P_t H_m}{1 + P_j H_z}\right)\right). \end{aligned} \tag{2.4.6}$$

□

The proof of Corollary 2.4.3 can be found at the end of achievability proof of Theorem 2.4.1. It can be observed that the lower bound in Corollary 2.4.3 is not larger than the lower bound in Theorem 2.4.1.

In [2], the authors consider a scenario in which the adversary is a fully eavesdropper, and the transmitter has no information of the states of main and eavesdropper channels, which change from one block to the next randomly as described in our scenario. For the case in which 1-bit feedback is available at the end of each block, the authors employ the plain ARQ strategy mentioned above to achieve the secrecy rate in Theorem 2 of [2]. However, in the secrecy analysis, the authors consider the impact of the bit groups, $B_l(k)$ that are successfully decoded only in a single transmission on the equivocating rate. In this thesis, regardless of the number of the required transmissions for the bit groups, we consider the impact of the each bit group on the equivocation rate with the strategy mentioned in the proof sketch of Theorem 2.4.1. Thus, we improve the achievable secrecy rate in [2] by employing a renewal based analysis and MTC.

In Theorem 2.4.1 and Corollary 2.4.3, we observe that the information corresponding to the retransmissions of a bit group is accumulated at the adversary, which reduces the lower bound. As we will show, we can avoid this situation if the main CSI is available at the beginning of each block at the transmitter in addition to the 1-bit feedback at the end of each block. By using the rate adaptation strategy that we will introduce, the legitimate pair can ensure that information corresponding to the retransmissions of a bit group is not accumulated at the adversary.

Corollary 2.4.4. *(**Achievable secrecy rate with main CSI**) If main CSI is available at the transmitter and the adversary, the secrecy capacity with 1-bit feedback at the end of each block is lower bounded by*

$$R_s^{\textit{1-bit+CSI}} = \max_R \; p \times \mathbb{E}\left[R - \log\left(1 + P_t H_e\right)\right]^+ \leq C_s^{\textit{1-bit+CSI}}, \tag{2.4.7}$$

where $p \triangleq \mathbb{P}\left(\log\left(1 + \dfrac{P_t H_M}{1 + P_j H_z}\right) \geq R\right)$. □

We omit the proof since it follows from an identical line of argument as the proof of Theorem 2.4.1. The only difference is that the legitimate pair employs a plain ARQ strategy as in Corollary 2.4.3, and the transmitter employs a rate adaptation strategy to utilize the main CSI such that $R(i) = R$ if $R \leq \log(1 + Ph_m(i))$; otherwise, $R(i) = 0$, where R is the rate of the Gaussian codebook used in the achievability proof of Theorem 2.4.1. Since the transmitter keeps silent on the blocks in which condition $R > \log(1 + Ph_m(i))$ is satisfied, the decoding error event occurs only when the adversary is in the jamming state. Hence, the adversary cannot hear the retransmissions because of the half duplex constraint, and information that corresponds to the retransmissions of a bit group is not accumulated as seen in (2.4.7).

Note that main CSI combined with 1 bit feedback provides the transmitter *perfect knowledge* of the adversary jamming state (but with one block delay) since an ACK indicates that the adversary is in the eavesdropping state, and a NAK indicates that

the adversary is in the jamming state in the previous block. Therefore, we do not need to employ a conservative secrecy encoder to account for the adversary that eavesdrops at all times.

2.5 Multiple Adversaries

In this section, we study the multiple adversary scenario in which there are V half duplex adversaries each of which has an arbitrary strategy from one block to the next. We focus on the no feedback case. The results given in this section can be extended to the 1-bit feedback case straightforwardly. Since there are multiple adversaries, the message has to be kept secret from each adversary. Moreover, when an adversary jams the receiver, it also jams the other adversaries. Consequently, the observed signals at the legitimate receiver and adversary v in i-th block can be written as follows:

$$Y^N(i) = G_m(i)x^N(i) + \sum_{v=1}^{V} G_{z_v}(i)S_{j_v}^N(i)\phi_v(i) + S_m^N(i) \tag{2.5.1}$$

$$Z_v^N(i) = \begin{cases} G_{e_v}(i)x^N(i) + \\ \sum\limits_{r=1, r\neq v}^{V} G_{f_{rv}}(i)S_{j_v}^N(i)\phi_r(i) + S_e^N(i) & \text{if } \phi_v(i) = 0 \\ \emptyset & \text{if } \phi_v(i) = 1 \end{cases} \tag{2.5.2}$$

where S_{j_v} is the jamming signal of adversary v, and is distributed with $\mathcal{CN}(\mathbf{0}, P_j I_{N\times N})$. As depicted in Figure 2.4, $G_{e_v}(i)$, $G_{z_v}(i)$, and $G_{f_{rv}}(i)$ are defined to be the independent complex gains of transmitter-to-adversary v channel, adversary v-to-receiver channel , and adversary r-to-adversary v channel, respectively. Associated power gains are denoted with $H_{e_v}(i) = |G_{e_v}(i)|^2$, $H_{f_{rv}}(i) = |G_{f_{rv}}(i)|^2$, and $H_{z_v}(i) = |G_{z_v}(i)|^2$. Indicator function $\phi_v(i) = 1$, if the adversary v is in a jamming state in i-th block; otherwise, $\phi_v(i) = 0$.

For the multi adversary scenario, ϕ^M in (2.2.11) is replaced with $\{\phi_v^M\}_{1\leq v\leq V}$, and

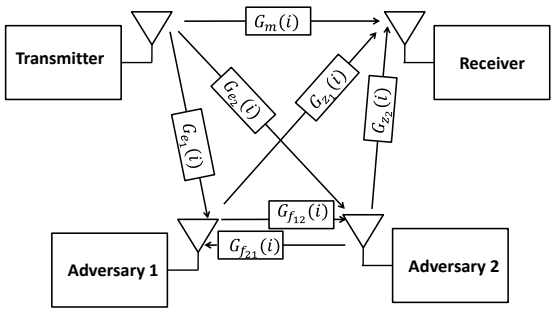

Figure 2.4: System model for multi-adversary scenario including two adversaries.

the constraints (3.2.10)-(2.2.11) have to be satisfied for all $\{\phi_v^M\}_{1\leq v\leq V}$. We study two types of multi-adversary scenarios: colluding and non-colluding. In the colluding scenario, the adversaries share their observations, $\left\{Z_v^{NM}\right\}$ error free whereas in the non-colluding scenario, the adversaries are not aware of the observations of each other. Hence, for the non-colluding scenario, constraint (2.2.11) needs to be satisfied for each adversary and for the colluding scenario, equivocation is conditioned on the adversaries' joint knowledge, i.e., Z^{MN} in (2.2.11) is replaced with $\{Z_v^{MN}\}_{1\leq v\leq V}$. We use notations C_s^C and C_s^{NC} to denote the secrecy capacities for the colluding case and the non-colluding case, respectively. We first analyze the non-colluding scenario.

Theorem 2.5.1. ***(Secrecy capacity bounds for non-colluding adversaries)*** *The secrecy capacity of the non-colluding multiple adversary scenario, C_s^{NC} under the no feedback case is bounded by*

$$C_s^{NC-} \leq C_s^{NC} \leq C_s^{NC+} \tag{2.5.3}$$

where

$$C_s^{NC-} = \min_{1\leq v\leq V} \left[\mathbb{E}\left[\log\left(1+\frac{P_t H_m}{1+P_j\hat{H}_z}\right) - \log\left(1+P_t H_{e_v}\right)\right]\right]^+ \tag{2.5.4}$$

$$C_s^{NC+} = \min_{1\le v\le V} \quad \min_{p_{\tilde{H}_{e_1},\ldots,\tilde{H}_{e_V},\tilde{H}_m,\tilde{H}_{z_1},\ldots,\tilde{H}_{z_V}}}$$
$$\mathbb{E}\left[\left(\log\left(1+\frac{P_t\tilde{H}_m}{1+P_j\tilde{H}_z}\right)-\log\left(1+P_t\tilde{H}_{e_v}\right)\right)^+\right] \tag{2.5.5}$$
$$\textit{subject to: } p_{\tilde{H}_{e_1},\ldots,\tilde{H}_{e_V}} = p_{H_{e_1},\ldots,H_{e_V}}$$
$$p_{\tilde{H}_m,\tilde{H}_{z_1},\ldots,\tilde{H}_{z_V}} = p_{H_m,H_{z_1},\ldots,H_{z_V}}$$

where V is the number of the adversaries, $\hat{H}_z \triangleq \sum_{k=1}^{V} H_{z_v}$, and $\tilde{H}_z \triangleq \sum_{v=1}^{V} \tilde{H}_{z_v}$. □

The proofs of the lower and upper bounds can be found in Appendix A.4.

Theorem 2.5.2. ***(Secrecy capacity bounds for colluding adversaries)*** *The secrecy capacity of the colluding multiple adversary scenario, C_s^C under the no feedback case is bounded by*

$$C_s^{C-} \le C_s^C \le C_s^{C+} \tag{2.5.6}$$

where

$$C_s^{C-} = \mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+P_j\hat{H}_z}\right)-\log\left(1+P_t\sum_{s=1}^{V}H_{e_s}\right)\right]^+$$
$$C_s^{C+} = \min_{p_{\tilde{H}_{e_1},\ldots,\tilde{H}_{e_V},\tilde{H}_m,\tilde{H}_{z_1},\ldots,\tilde{H}_{z_V}}}$$
$$\mathbb{E}\left[\left(\log\left(1+\frac{P_t\tilde{H}_m}{1+P_j\tilde{H}_z}\right)-\log\left(1+P_t\sum_{k=1}^{V}\tilde{H}_{e_v}\right)\right)^+\right] \tag{2.5.7}$$
$$\textit{subject to: } p_{\tilde{H}_{e_1},\ldots,\tilde{H}_{e_V}} = p_{H_{e_1},\ldots,H_{e_V}}$$
$$p_{\tilde{H}_m,\tilde{H}_{z_1},\ldots,\tilde{H}_{z_V}} = p_{H_m,H_{z_1},\ldots,H_{z_V}}$$

where V is the number of the adversaries, $\hat{H}_z \triangleq \sum_{k=1}^{V} H_{z_v}$, and $\tilde{H}_z \triangleq \sum_{v=1}^{V} \tilde{H}_{z_v}$. □

The proof of Theorem 2.5.2 is similar to the proof Theorem 2.3.1 since the colluding scenario can be considered as a single adversary scenario, in which the adversary

observes $\{Z_v^{MN}\}_{1\leq v\leq V}$ instead of Z_v^{NM}. As seen in Theorems 2.5.1 and 2.5.2, colluding strategy severely affects the achievable secrecy rate.

Remark 2.5.3. ***(Independence of upper bound from cross-interference)*** *In* (2.5.2)*, we observe that the received signal at v-th adversary includes the jamming signals of the other adversaries, i.e.,* $\sum_{r=1,r\neq v}^{V} G_{f_{rv}}(i)S_{j_v}^N(i)\phi_r(i)$*. We expect that these cross interference terms at the adversaries help the legitimate pair to communicate at high secrecy rates. However, as seen in Theorem 2.5.1 and 2.5.2, the upper bounds (and also lower bounds) are independent of these jamming terms. Note that the secrecy constraint in the proof of upper bounds makes the minimization of the equivocation rate over the adversary strategies arbitrarily close to the message rate. The strategies that minimize the equivocation rate in the proofs are the ones in which all adversaries eavesdrop the main channel. Hence, the upper bound derivation becomes independent of the cross interference across the adversaries. The detailed information can be found in Appendix A.4.* □

2.6 Strict Delay

In the previous sections, we study the communication of a message without imposing any constraint on the number of blocks it takes for the decoder to decode the message. In this section, we address the problem with the 1-block delay constraint: At the beginning of each block i, $1 \leq i \leq M$, message $w(i) \in \{1, \ldots, 2^{NR_s}\}$ becomes available at the encoder, and it needs to be securely communicated to the receiver by the end of block i. We show that the secrecy capacity under the delay constraint is non-zero as long as the secrecy capacity lower bound provided in Theorem 1 is non-zero.

The transmitter aims to send message $w(i) \in \mathcal{W} = \{1, 2, \ldots 2^{NR_s}\}$ to the receiver over a single block with rate R_s. By employing a $c_i\left(2^{NR_s}, N\right)$ code, the encoder at the

transmitter maps message $w(i)$ to a codeword $x^N(i)$, and the decoder at the receiver, $d(\cdot)$ maps the received sequence Y^{Ni} to $\hat{w}(i) \in \mathcal{W}$. The encoder is not memoryless, i.e., when choosing the current codeword, $x^N(i)$, it uses the previously transmitted codewords, x^{Ni}, as well as the current message. The average error probability of $c_i\left(2^{NR_s}, N\right)$ code is defined as

$$\begin{aligned} &P_e^N(c_i, g^i, \phi^i) \\ &= 2^{-NR_s} \sum_{w \in \mathcal{W}} \mathbb{P}\left(d\left(Y^{Ni}, g^i, \phi^i\right) \neq w(i) | w(i) \text{ was sent}\right) \end{aligned} \tag{2.6.1}$$

where $c_i \triangleq c_i\left(2^{NR_s}, N\right)$ and $g^i = \left[g_m^i, g_e^i, g_z^i\right]$. The secrecy of a transmitted message, $w(i)$ is measured by the equivocation rate[5] at the adversary

$$R_e(c_i, g^M, \phi^M) = \frac{1}{N} H\big(W(i) | Z^{NM}, W^M \backslash W(i), g^M, \phi^M, c_i\big) \tag{2.6.2}$$

Note that, the definition of secrecy capacity needs to be restated with the delay requirement.

Definition 2. *[21] Rate R_s is achievable securely with at most α probability of secrecy outage if, for any fixed $\epsilon > 0$, there exists a sequence of codes of rate no less than R_s such that, for all large enough N, M_1 and M_2 where $M = M_1 M_2$, the conditions*

$$\mathbb{P}(P_e^N(c_i, G^i, \phi^i) \leq \epsilon) \geq 1 - \alpha \tag{2.6.3}$$

$$\mathbb{P}(R_e(c_i, G^M, \phi^M) \geq R_s - \epsilon) \geq 1 - \alpha \tag{2.6.4}$$

are satisfied for all $i > M_1$, and for all possible adversary strategies $\phi^M \in \{0,1\}^M$.

The secrecy capacity with α outage is the supremum of such achievable secrecy rates. We use $C_{s_d}(\alpha)$ to denote α-outage secrecy capacity under no feedback, and use

[5]Although the messages $\{W(i)\}_{i=1}^M$ are mutually independent, they may be dependent conditioned on eavesdroppers' received signal Z^{NM}, therefore equivocation expression includes conditioning on $W^M \backslash W(i)$.

$C_{s_d}^{\text{1-bit}}(\alpha)$ to denote α-outage secrecy capacity under 1-bit feedback at the end of each block.

Theorem 2.6.1. *(**Time sharing lower bound for α-outage secrecy capacity**) For no feedback, $C_{s_d}(\alpha) \geq C_{s_d}^{-}(\alpha)$, where*

$$C_{s_d}^{-}(\alpha) = \max_{\gamma, \tilde{R}_s, R_s} R_s \tag{2.6.5}$$

subject to:

$$\mathbb{P}\Bigg(\left\{ (1-\gamma)\log\left(1+\frac{P_t H_m}{1+P_j H_z}\right) \geq \tilde{R}_s \right\} \bigcap \left\{ \left[\tilde{R}_s - (1-\gamma)\log(1+P_t H_e) \right]^+ \geq R_s - R_{r0} \right\} \Bigg) \geq 1-\alpha \tag{2.6.6}$$

$$R_s \leq \tilde{R}_s, R_{r0} = \gamma C_s^{-}, \gamma \in [0,1], \tag{2.6.7}$$

where C_s^{-} is provided in (2.3.2). □

Similarly, for 1-bit feedback, α-outage secrecy capacity is lower bounded by $C_{s_d}^{-\text{1-bit}}(\alpha)$, where $C_{s_d}^{-\text{1-bit}}(\alpha)$ is in the form (2.6.5-2.6.7), except R_{r0} is replaced with $R_{r1} = \gamma C_s^{-\text{1-bit}}$.

The complete proof can be found in Appendix E. Here, we provide a sketch of achievability. Suppose that the communication lasts M_2 superblocks each of which contains M_1 blocks of N channel uses. In Theorem 5, $\gamma \in [0,1]$ is the time-sharing parameter. We utilize the first γN channel uses of each block to generate keys using the scheme described in proof of Theorem 1: Using a code $(2^{NM_1R_{r0}}, \gamma N M_1)$, we can generate NM_1R_{r0} secret key bits at the end of every superblock, where $R_{r0} \leq \gamma C_s^{-}$. The keys generated in the previous superblock is used in the current superblock to secure the delay sensitive messages. We utilize the rest of the block ($N(1-\gamma)$ channel uses) to send the delay sensitive message. At each block i, $i > M_1$, message $w(i)$ of size NR_s bits is divided to two independent messages $w_1(i)$ and $w_2(i)$, of sizes NR_{r0} and $N(R_s - R_{r0})$, respectively. The encoder secures message $w_1(i)$ by one-time padding

it with the part of the key generated in the previous superblock. Then, the encoder maps one-time padded $w_1(i)$ and $w_2(i)$ to randomized message $m(i) \in [1 \ldots, 2^{N\tilde{R}_s}]$. Message $m(i)$ is mapped to the corresponding codeword in codebook c containing $2^{N\tilde{R}_s}$ independently and identically generated codewords, $x^{(1-\gamma)N}$ of length $(1-\gamma)N$.

Note that we do not impose a secrecy outage constraint on the first M_1 blocks, which is referred to as an initialization phase, used to generate initial common randomness between the legitimate nodes. Note that this phase only needs to appear *once* in the communication lifetime. In other words, when a session (which consists of M blocks) between the associated nodes is over, they would have sufficient number of common key bits for the subsequent session, and would not need to initiate the initialization step again [21].

With the following remark, we demonstrate the relation of the secrecy capacity with a delay constraint and the secrecy capacity without a delay constraint.

Remark 2.6.2. *(**Non-zero delay limited secrecy capacity**) Suppose that* $H_m^* = \dfrac{P_t H_m}{1 + P_j H_z}$ *has a strictly monotone cdf and* $\mathbb{P}(H_m^* \neq 0) > 0$. *If* $\alpha \in (0, 1]$ *and* $C_s^- > 0$, *then* $C_{s_d}(\alpha) > 0$. *We can observe this fact by setting* $\tilde{R}_s = R_s = R_{r0}$ *in Theorem 2.6.1. Furthermore, note that* $C_s^{1\text{-}bit} > 0$ *if* $P(H_m^* \neq 0) > 0$ *(Remark 2.4.2). Hence, by setting* $\tilde{R}_s = R_s = R_{r1}$, *we can get* $C_{s_d}^{1\text{-}bit}(\alpha) > 0$ *for any* $\alpha \in (0, 1]$. □

2.7 Numerical Evaluation

In this section, we conduct Monte Carlo simulations to illustrate our main results. We compare the secrecy capacity lower and upper bounds of the no feedback case with the lower bound of the secrecy capacity with 1-bit feedback. To evaluate the effect of delay constraint, we also plot the lower bound of the α-outage secrecy capacity with no feedback and 1-bit feedback. We consider that the power gains of

the main, eavesdropper, and jamming channels independently follow an exponential distribution.

In Figure 2.5, we fix the outage term $\alpha = 0.2$ and jamming power $P_j = 1$, and we plot the secrecy capacity bounds as a function of the transmission power constraint, P_t. We take $\mathbb{E}[H_m] = 5$, $\mathbb{E}[H_e] = 2$, and $\mathbb{E}[H_z] = 2$. A notable observation is that the lower bound for the no feedback case in Theorem 2.3.1 decreases with P_t beyond a certain point. The reason is that the lower bound, given in Theorem 2.3.1 is not always an increasing function of P_t since the positive operator is outside of the expectation term. The lower bound to the α-outage capacity without feedback, given in Theorem 2.6.1 also decreases with P_t since the achievabilitiy strategy employs a key generation step in which keys are generated with the strategy used in the achievability proof of Theorem 2.3.1 . Let us replace P_t in the lower bounds with dummy variable P. We conclude that the lower bounds in Theorems 2.3.1 and 2.6.1 can be further tightened by maximizing them over $P \in [0, P_t]$. From Figure 2.5, we observe that the secrecy capacity with 1-bit feedback is twice as large as that with no feedback at $P_t/P_j = 10$.

We now numerically illustrate Remark 2.4.2, i.e., even when the eavesdropper channel is better *on average*, we can achieve non-zero secrecy rates with the 1-bit feedback. We take $\mathbb{E}[H_m] = 1$, $\mathbb{E}[H_e] = 2$, and $\mathbb{E}[H_z] = 1$, i.e., the eavesdropper channel *stochastically dominates* the effective main channel. As seen in Figure 2.6, we observe that 1-bit feedback sent at the end of each block is sufficient to make the secrecy capacity non-zero. Furthermore, we observe that the secrecy capacity of the no feedback case is zero (Remark 2.3.2). The importance of the feedback can also be seen in the delay limited set-up, where no feedback strategy results in a zero achievable rate as opposed to the strategy employing 1-bit feedback.

We illustrate Corollary 2.3.5 in Figure 2.7. For each plot in Figure 2.7, we keep

the ratio of transmission power constraint and adversary power same, and we increase the jamming power. As mentioned in Corollary 2.3.5, in Figure 2.7, we observe that the secrecy capacity with no feedback goes to zero, when the transmission power constraint and adversary power increase in the same order.

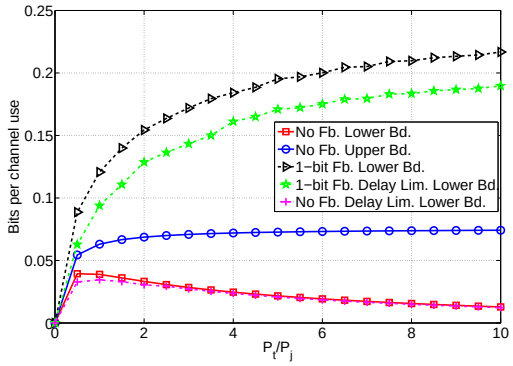

Figure 2.5: The comparison of the lower and upper bounds of the no feedback case with the lower bound of the 1-bit feedback case with $\mathbb{E}[H_m] = 5$, $\mathbb{E}[H_e] = 2$, and $\mathbb{E}[H_z] = 2$.

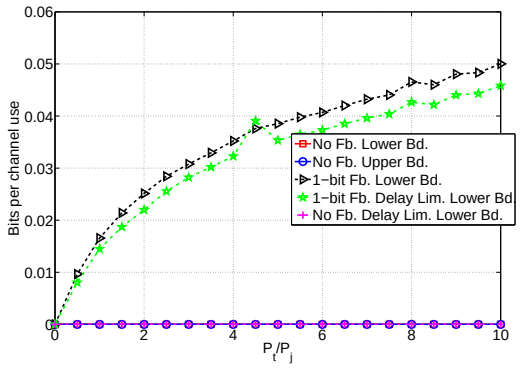

Figure 2.6: The comparison of the lower and upper bounds of the no feedback case with the lower bound of the 1-bit feedback case with $\mathbb{E}[H_m] = 1$, $\mathbb{E}[H_e] = 2$, and $\mathbb{E}[H_z] = 1$.

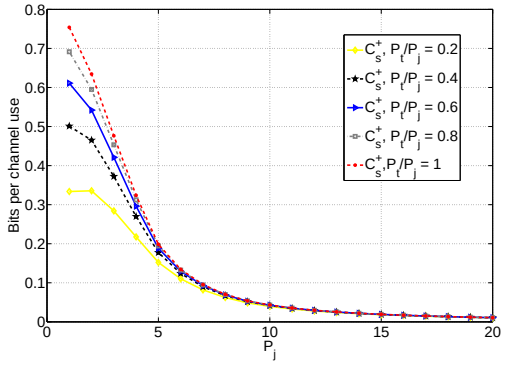

Figure 2.7: The change of the upper bound of the no feedback case when the transmission power constraint and jamming power scale in the same order. $\mathbb{E}[H_m] = 1$, $\mathbb{E}[H_e] = 2$, and $\mathbb{E}[H_z] = 1$.

CHAPTER 3

PHYSICAL LAYER SECURITY OF MASSIVE MIMO

3.1 Introduction

In massive MIMO framework, the base station is equipped with a number of antennas, typically much larger than the number of users served. While many issues behind the design of multicellular massive MIMO systems have been studied thoroughly, security of massive MIMO has not been actively addressed. Part of the reason for this may be the fact that, there is a vast literature on the security of MIMO systems in general, and a common perspective is that massive MIMO is merely an extension of MIMO as it pertains to security. However, we demonstrate that massive MIMO has unique vulnerabilities, and standard approaches to MIMO security do not address them directly. Instead, these approaches focus on issues that massive MIMO is naturally immune to. Furthermore, we argue that, common models used in MIMO security eliminate the need to think on various components of the system that are critical to understanding the vulnerabilities in security. In particular, in massive MIMO, merely making assumptions on available channel state information (CSI) is not sufficient, since the actual technique the system uses to obtain CSI may be the lead cause for some major security issues. For all these reasons, security of massive MIMO calls for a separate treatment of its own.

To that end, we consider the TDD-based single cell downlink massive MIMO system developed in [22] and later readdressed in [23]. The adversary is hybrid, capable of jamming and eavesdropping at the same time with its multiple antennas and we call our system *secure* if secrecy, measured in full equivocation is achieved at the adversary and arbitrarily low probability of decoding error is achieved at the legitimate receiver. We refer to these requirements as **security constraints**. We first show how massive MIMO is naturally resilient to standard jamming and eavesdropping attacks, unless jamming is performed during the training phase when pilot signals are transmitted by the mobile users. We prove that, without pilot jamming, the achievable secure degrees of freedom[1](DoF) is identical to the maximum DoF attained under no attack, even without the need to use a stochastic (e.g., Wyner) secrecy encoder in the massive MIMO limit. On the other hand, as we will show, the adversary can reduce the maximum secure DoF and rate to zero by contaminating the pilot signal of the targeted user via another correlated pilot signal. To address this attack, we develop a defense strategy in which the base station (BS) keeps the assignment of pilot signals to the users hidden from the adversary and informs the assignments to the users reliably. Thus, in our approach, we use computational cryptography for encrypting the pilot assignments in the training phase. We also discuss how the consequences of encryption of pilot assignment is fundamentally different from the consequences of data encryption. In particular, we argue that, even if we use non-information theoretic methods (e.g., Diffie-Hellman) to encrypt the pilot assignments, the level of security we achieve can be as strong as information theoretic secrecy for all practical purposes. Note that, most of our results are **not asymptotic** in the number of antennas and we specify the number of antennas necessary to achieve certain level of security.

[1]Our definition of degrees of freedom is different from the standard definition. Our definition specifies how the achievable rate scales with the log of the number of base station antennas, rather than the log of the transmission power as in the standard definition.

The major ideas developed and demonstrated in this thesis include:

- In information-theoretic secrecy literature, it is often the case that assumptions are made on the CSI available at the adversary. Typically, it is assumed that the adversary has access to the CSI for all channels in the system, with the motivation of making the achievable security robust with respect to the availability of CSI at the adversary. However, we show that, with massive MIMO, *it is not important* **if** *the adversary has full CSI or not.* Indeed, we show that massive MIMO is naturally immune to attacks during data communication phase. Instead, we demonstrate that *the major question is* **how** *the adversary obtains CSI.* In particular, we show that if the adversary is active during the training phase, it substantially degrades the security of data communication.

- Security in computational cryptography is based on the assumptions on the computational power of the attackers. Once data is encrypted, it takes an unreasonable amount of time for a typical adversary to decrypt it without the key. Making such an assumption on the adversary poses a problem for security, since a sophisticated adversary can use various tools and techniques to cut down the time for cryptanalysis applied to recorded encrypted data. We eliminate this shortcoming by encrypting the **pilot assignments** -not the transmitted data,- using keys that are shared via standard Diffie-Hellman. In our scheme, to make an impact, the adversary needs to decrypt the pilot assignment *before* the training phase starts. Note that, the training phase can start immediately after the assignments are made, leaving an arbitrarily low amount of time for the adversary to crack the assignment (i.e., pushing the computational power necessary to infinity). Without the knowledge of the pilot assignment, our scheme achieves perfect secrecy of information transmitted in the data communication phase, **even without** the use of a secrecy encoder. Thus, it is useless

for the adversary to record the received signal for future cryptanalysis, since it is indifferent from noise.

Next, we summarize the technical contributions. Throughout the section, we assume that the adversary is *full-duplex*, i.e., it is capable of eavesdropping and jamming the BS-to-user communication simultaneously. We first study an attack model in which the adversary eavesdrops the entire communication between the BS and users and jams only the downlink data communication (the adversary keeps silent during the training.). Under this attack:

- We show that the maximum secure DoF is identical to the maximum DoF achieved in the presence of no adversary.
- We provide a novel encoding strategy, δ-conjugate beamforming, that provides full security, without the need for Wyner encoding [3].
- We evaluate the number of antennas that the BS requires in order to satisfy the security constraints.

The proposed encoding, δ-conjugate beamforming, utilizes the fact that the correlation between the estimated BS-to-user channel gains and the BS-to-adversary channel gains becomes *zero* when the adversary does not jam during the training phase. We observe that in order to cause a *non-zero* correlation between the estimated BS-to-user channel gains and the BS-to-adversary channel gains, the adversary has to jam the pilots of users.

Next, we consider an attack model in which the adversary eavesdrops and jams the entire communication *(including the training)* between the BS and the users. Under this attack:

- We show that, if the adversary jams the training such that there exists a *non-zero* correlation between the BS-to-adversary channel gain and the estimated

gain of the channel from the BS to a user, the adversary reduces the maximum secure DoF to zero. Further, we show that, if the amount of the correlation is sufficiently large, the maximum achievable rate of the user also vanishes as the number of antennas at the BS grows.

- We propose a counter strategy against the adversary. We show that, if the cardinality of the set of pilot signals scales with the number of antennas at the BS and the BS is able to keep the pilot signal assignments hidden from the adversary, attained secure DoF is arbitrarily close to the maximum DoF attained under no attack.

Related Work: Massive MIMO concept was first proposed in [22, 24]. Since then, there has been a flurry of studies focusing on different aspects of massive MIMO (see survey [25]) such as channel estimation, energy efficiency, and pilot contamination. However, while MIMO security has been an active area of research [26–28], issues specific to massive MIMO have not been considered. Among the very few, in [29], the authors consider downlink multi cell massive MIMO system in the presence of an adversary that only eavesdrops. In order to confuse the adversary, the BS transmits artificial noise from a set of its antennas. The authors conclude that, if the adversary has sufficiently large number of antennas, it is impossible to operate at a positive rate with artificial noise generation at the BS. In our earlier work [30], which sets up the main results in this paper, we have focused on a fairly different model and addressed other questions. For instance, our attack model considers both jamming and eavesdropping, possibly simultaneously by the adversary.

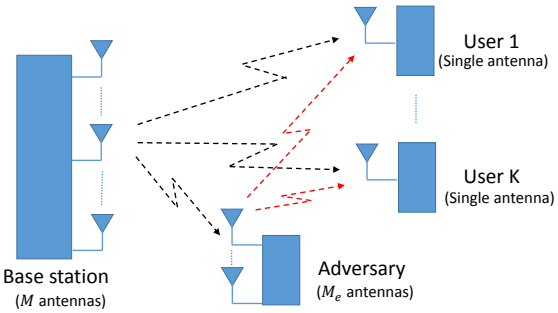

Figure 3.1: System Model

3.2 System Model and Problem Statement

We consider a multi user MIMO downlink communication system, depicted in Figure 3.1, including a base station (BS), K single-antenna users, and an adversary. The BS equipped with M antennas wishes to broadcast K distinct messages $\{W_1, \ldots, W_K\}$ each of which is intended for a different user. The adversary is equipped with M_e antennas.

3.2.1 Channel Model

We assume all the channels in our system, illustrated in Figure 3.1, are block fading. In the block fading channel model, time is divided into discrete blocks each of which contains T channel uses. The channel gains remain constant within a block and the channel gains on different blocks are independent and identically distributed. Furthermore, we assume the channels are reciprocal; the instantaneous gain of the channel connecting the BS to a user is as same as the gain of the channel connecting to the same user to the BS.

We follow a TDD-based two-phase transmission scheme introduced in [31] and is re-adressed in [23]. The signal transmission in a block is separated into two phases:

training phase and data communication phase. On the first T_r channel uses of every block, each user sends a pilot signal to the BS. The BS estimates each BS-to-user channel from the observed pilot signals. On the last T_d channel uses of each block ($T_d \triangleq T - T_r$), the BS transmits data to the users.

The observed signals during a data communication phase at k-th user and at the adversary at a particular channel use of i-th block are as follows[2]:

$$Y_k = H_k(i)X + H_{jam,k}(i)V_{jam} + V_k \tag{3.2.1}$$

$$Z = H_e(i)X + V_e, \tag{3.2.2}$$

where Y_k is a received complex signal at k-th user, Z is a received $M_e \times 1$ complex vector at the adversary, and X denotes $M \times 1$ complex vector of transmitted data symbols. Signals V_k and V_e are additive Gaussian noise components, distributed as $\mathcal{CN}(0,1)$ and $\mathcal{CN}(\mathbf{0}, I_{M_e})$, respectively. Signal V_{jam} denotes $M_e \times 1$ complex vector of jamming signal. Further, $H_k(i)$ and $H_{jam,k}(i)$ denote a $1 \times M$ complex gain vector of the channel connecting the base station to k-th user, a $1 \times M_e$ complex gain vector of the channel connecting the adversary to k-th user, respectively, at i-th block. Similarly, $H_e(i)$ is the $M_e \times M$ complex gain matrix of the MIMO channel connecting the base station to the adversary at i-th block. We assume that all channel gains $H_e(i), H_1(i), \ldots H_K(i), H_{jam,1}(i), \ldots, H_{jam,K}(i)$ are mutually independent for any $i \geq 1$.

The users send pilots in the first T_r channel uses of each block. The received signals at the BS and at the adversary in the training phase of i-th block are as follows:

$$Y^{T_r} = \sum_{k=1}^{K} H_k^{\mathsf{T}}(i)\phi_k + H_e^{\mathsf{T}}(i)W_{jam} + W, \tag{3.2.3}$$

[2]Except for the channel gains, we avoid the block and channel use indices in (3.2.1) and (3.2.2) and the block indicies in (3.2.3) and (3.2.4) for the sake of simplicity.

$$Z^{T_r} = \sum_{k=1}^{K} H_{jam,k}^{\mathsf{T}}(i)\phi_k + W_e, \tag{3.2.4}$$

where Y^{T_r} and Z^{T_r} denote $M \times T_r$ and $M_e \times T_r$ complex matrices of the received signals over T_r channel uses at the BS and at the adversary, respectively. Signals W and W_e are $M \times T_r$ and $M \times T_r$ complex matrices denoting the additive Gaussian noise. Each element of W and W_e are i.i.d $\mathcal{CN}(0,1)$. Signal V_{jam} denotes $M_e \times T_r$ complex matrix of jamming signal. Signal ϕ_k is $1 \times T_r$ complex vector denoting the pilot signal associated with k-th user. The power of pilot signals ρ_r, i.e., $\frac{1}{T_r}\mathrm{tr}\left(\phi_k^*\phi_k\right) = \rho_r$ is identical for all users $k \in \{1, \ldots, K\}$.

We assume that the users do not have the knowledge of the BS-to-user channel gains. Note that the BS, the users, and the adversary know pilot signal set $[\phi_1, \ldots, \phi_K]$. The adversary is assumed to be aware of which pilot signal is assigned to which user. Utilizing the pilot signals, the BS estimates the BS-to-user channel gains. Define $\hat{H}_k(i)$ as $1 \times M$ complex vector of estimated BS-to-k-th user channel gain. Further, for any $B \geq 1$, define H^B, $\hat{H}^B$, H_e^B, and H_{jam}^B as the gains of the BS-to-user channels, the estimated gains of the BS-to-user channels, the gains of the BS-to-adversary channel, and the gains of the adversary-to-user channels over B blocks, respectively, i.e., $H^B \triangleq \left[H_1^B, \ldots, H_K^B\right]$, $\hat{H}^B \triangleq \left[\hat{H}_1^B, \ldots, \hat{H}_K^B\right]$ and $H_{jam}^B \triangleq \left[H_{jam,1}^B, \ldots, H_{jam,K}^B\right]$.

For any $B \geq 1$, the joint probability density function of $\left(H^B, \hat{H}^B, H_e^B, H_{jam}^B\right)$ is

$$p_{H^B,\hat{H}^B,H_e^B,H_{jam}^B}\left(h^B, \hat{h}^B, h_e^B, h_{jam}^B\right) = \prod_{i=1}^{B} p_{H,\hat{H},H_e,H_{jam}}\left(h(i), \hat{h}(i), h_e(i), h_{jam}(i)\right) \tag{3.2.5}$$

where $H \triangleq [H_1, \ldots, H_K]$, $\hat{H} \triangleq \left[H_1, \ldots, \tilde{H}_K\right]$, and $H_{jam} \triangleq [H_{jam,1}, \ldots, H_{jam,K}]$. For any $k \in \{1, \ldots, K\}$, H_k and $H_{jam,k}$ are distributed as $\mathcal{CN}(\mathbf{0}, I_M)$, $\mathcal{CN}(\mathbf{0}, I_{M_e})$, respectively, and each element of matrix H_e is i.i.d $\mathcal{C}N(0,1)$.

The adversary has the perfect knowledge of the BS-to-user channel gains H and the estimated BS-to-user channel gains $\hat{H}$. Define $H_{k,m}$ and $\hat{H}_{k,m}$ as the gain and the estimated gain of the channel connecting m-th BS antenna to k-th user. We assume that for any $k \in \{1, \ldots, K\}$, $\{H_{k,m}\hat{H}_{k,m}\}_{m\geq 1}$ forms an i.i.d process. We also assume that $\hat{H}_k$ are independent from H_l and $\mathbb{E}\left[\hat{H}_k \hat{H}_l^*\right] = 0$ for $k \neq l$ and $k, l \in \{1, \ldots, K\}$. Note that we do not impose these assumptions for the BS-to-adversary channels.

Remark 3.2.1. *When MMSE estimator and mutually orthogonal pilot signals are employed for channel estimation at the BS, these assumptions are satisfied.*

3.2.2 Attack Model

We consider a full duplex adversary that is capable of eavesdropping and jamming simultaneously. In the sequel, we consider two attack models that differ only in the adversary's jamming activity in the training phase.

In Section 3.3, we consider an attack model in which the adversary jams *only* during the data communication phase and eavesdrops both the training and the data communication phases. We call this attack model as *no training-phase jamming*. In the no training-phase jamming, the adversary jams during the communication phase using a Gaussian jamming signal and keeps silent during the training phase. Specifically, signal W_{jam} in (3.2.4) is identical to zero and jamming signal V_{jam} in (3.2.1) is distributed as $\mathcal{CN}(\mathbf{0}, \rho_{jam} I_{M_e})$, where ρ_{jam} is the jamming power.

In Sections 3.4 and 3.5, we consider an attack model in which the adversary jams and eavesdrops both the training and the data communication phases. We call this attack model as *training-phase jamming*. The adversary strategy during the data communication phase in this attack model is the same as that described in the previous attack model (i.e., no training-phase jamming). Instead of jamming with random signals, the adversary jams during the training phase with structured signals.

We provide a detailed description of the signals used for jamming the training phase in Section 3.4 and 3.5.

3.2.3 Code Definition

The BS has random messages $\{W_1, \ldots, W_K\}$ each of which is uniformly distributed on message set $\mathcal{W}_k$, $k = 1, \ldots, K$. We denote $w_k \in \mathcal{W}_k$ as the realization of W_k. The BS aims to send message w_k, $k = 1, \ldots, K$, to k-th user over B blocks with rate R_k, while keeping w_k secret from the adversary. The BS and the users employ code $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ of length BT_d, that contains: **1)** K message sets, $\mathcal{W}_k \triangleq \{1, \ldots, 2^{BTR_k}\}, k = 1, \ldots, K$. **2)** K injective encoding functions, f_k, $k = 1, \ldots, K$, where f_k maps $w_k \in \mathcal{W}_k$ to data signal sequence $s_k^{BT_d} \in \mathbb{C}^{BT_d}$ satisfying an average power constraint such that

$$\frac{1}{BT_d} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} |s_k(i,j)|^2 \leq \rho_k, \quad k = 1, \ldots, K \tag{3.2.6}$$

for all $w_k \in \mathcal{W}_K$, where notation (i, j) indicates the j-th channel use of i-th block, ρ_k denotes the power constraint for k-th user, and $s_k(i, j)$ is the complex data signal of k-th user. Note that $\rho_f \triangleq \sum_{k=1}^{K} \rho_k$ is the cumulative average transmission power. Further, note that encoding functions, f_k, $k = 1, \ldots, K$ can be *deterministic* or *stochastic*. Codes using stochastic encoding functions referred to as stochastic codes and the ones using deterministic encoding functions are referred to as deterministic codes. **3)** Linear beamforming that maps data signals[3] $s_1^{BT_d} \times \cdots \times s_K^{BT_d}$ to channel input[4] X^{BT_d}. Two beamforming strategies are used throughout the section:

[3]Note that $s_k^{BT_d} \triangleq \{s_k(i,j)\}_{i=1:B, j=T_r+1:T}$ and notation $(\cdot)^{BT_d}$ applied to any variable has the same meaning.

[4]Note that the channel input sequence satisfies the following average power constraint

$$\frac{1}{BT_d} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} \mathbb{E}\left[||X(i,j)||^2\right] \leq \rho_f \tag{3.2.7}$$

- **Conjugate beamforming**: When the BS employs conjugate beamforming, channel input at j-th channel use of i-th block can be written as

$$X(i,j) = \sum_{k=1}^{K} s_k(i,j) \frac{\hat{H}_k^*(i)}{\sqrt{M\alpha_k}}, \tag{3.2.8}$$

for any $i \in \{1,\dots,B\}$ and $j \in \{T_\tau + 1,\dots,T\}$, where $\alpha_k \triangleq \mathbb{E}\left[|\hat{H}_{k,m}|^2\right]$.

- **δ-conjugate beamforming**: We introduce a new beamforming strategy, called δ-conjugate beamforming that is slightly modified version of conjugate beamforming. Let δ be a positive real number. When the BS employs δ-conjugate beamforming, the channel input at j-th channel use of i-th block can be written as

$$X(i,j) = \sum_{k=1}^{K} s_k(i,j) \frac{\hat{H}_k^*(i)}{\sqrt{M^{1+\delta}\alpha_k}}. \tag{3.2.9}$$

Note that, when $\delta = 0$, δ-conjugate beamforming becomes identical with conjugate beamforming in (3.2.8).

4) Decoding functions, g_k, $k = 1,\dots,K$, where g_k maps $Y_k^{BT_d}$ to $\hat{w}_k \in \mathcal{W}_k$.

3.2.4 Figures of Merit

We define the average error probability of code $\left(2^{BTR_1},\dots,2^{BTR_K}, BT_d\right)$ as

$$P_e \triangleq \mathbb{P}\left(\bigcup_{k=1}^{K} g_k(Y_k^{BT_d}) \neq W_k\right).$$

We assume that the adversary targets a single user during communication. The secrecy of the transmitted message for k-th user is measured by the equivocation rate at the adversary, which is equal to the entropy rate of transmitted message w_k conditioned on the adversary's observations.

---

for all $w_1 \times \cdots \times w_K \in \mathcal{W}_1 \times \cdots \times \mathcal{W}_K$, where the expectation is over estimated channel gains $\hat{H}$. The inequality (3.2.7) follows from the individual power constraint (3.2.6) and from the fact that $\mathbb{E}\left[\hat{H}_k \hat{H}_l^*\right] = 0$ for $k \neq l$

Definition 3. *A secure rate tuple $R_1, \dots R_K$ is said to be achievable if, for any $\epsilon > 0$, there exists $B(\epsilon) > 0$ and a sequence of codes $\left(2^{BTR_1}, \dots, 2^{BTR_K}, BT_d\right)$ that satisfy the following:*

$$P_e \leq \epsilon, \tag{3.2.10}$$

$$\frac{1}{BT} H\left(W_k | Z^{BT}, H^B, \hat{H}^B, H_e^B\right) \geq R_k - \epsilon \tag{3.2.11}$$

for all $B \geq B(\epsilon)$ and $k \in \{1, \dots, K\}$, where Z^{BT} is the received signal sequence at the adversary over BT channel uses.

We refer to the constraints in (3.2.10) and (3.2.11) as decodability and secrecy constraints, respectively. We also refer to both constraints as security constraints. We call the communication system information theoretically secure if both constraints are satisfied. Notice that the achievable rate tuple definition above is presented for a given M, i.e., M remains constant for a sequence of codes $\left(2^{BTR_1}, \dots, 2^{BTR_K}, BT_d\right)$, $B \geq B(\epsilon)$.

We mainly focus on the massive MIMO limit. Specifically, we study on how achievable rate tuple $R_1, \dots, R_K$ behaves as M goes to infinity. To that end, we use the following notion of degrees of freedom for each user.

Definition 4. *A secure degrees of freedom tuple $d_1, \dots, d_K$ is said to be achievable, if there exists achievable rate tuple $R_1, \dots R_K$ such that*

$$d_k = \lim_{M \to \infty} \frac{R_k}{\log M}, \ k = 1, \dots, K. \tag{3.2.12}$$

In the literature, degrees of freedom is typically defined as the limit $\lim_{\rho_k \to \infty} \frac{R_k}{\log \rho_k}$. Since we aim to understand how R_k changes with M under constant ρ_k, the degree of freedom definition in (3.2.12) is more relevant for our interest.

For a given achievable secure degrees of freedom tuple $d_1, \dots, d_K$, we define the secure degrees of freedom of the downlink communication as the minimum value in the

tuple, i.e., secure $DoF \triangleq \min_{k\in\{1,\ldots,K\}} d_k$. In the rest of the section, when we use secure DoF, we mean secure degrees of freedom attained in the presence of an adversary, and when we use DoF, we mean degrees of freedom attained under no adversary.

We characterize the maximum secure DoF in the presence of various security attacks described in Section 3.2.2. Furthermore, we aim to develop defense strategies that achieve the maximum secure DoF against the security attacks that would limit the maximum secure DoF to zero, otherwise.

3.3 Adversary not jamming The Training Phase

In this section, we show that downlink communication in a single-cell massive MIMO system is resilient to the adversary that jams only the data communication phase and eavesdrops both the communication and training phases. We show that the maximum secure DoF attained under no training-phase jamming is identical to maximum DoF attained under no adversary. Then, we show that we can establish information theoretic security without using stochastic encoding, e.g., Wyner encoding. Finally, we evaluate the number of antennas that BS needs to satisfy the security constraints without a need for Wyner encoding.

3.3.1 Resilience of massive MIMO

In this subsection, we evaluate the maximum secure DoF of the downlink communication in the presence of *no training-phase jamming*. Then, we show that the maximum secure DoF attained in the presence of no training-phase jamming is as same as the maximum DoF attained without an adversary. This result demonstrates the weakness of the no training-phase jamming in the massive MIMO limit.

Theorem 3.3.1. ***(Maximum secure DoF)*** *For given block length T and data*

transmission phase length T_d, the maximum secure DoF under no training-phase jamming is given by $\frac{T_d}{T}$. □

The complete proof is available in Appendix B.1, where we first provide an upper bound on secure DoF and then present a strategy to achieve the upper bound. Here, we provide a proof sketch. In order to find an upper bound on secure DoF, we consider a multiple output single output (MISO) communication system without an adversary, in which the BS communicates to a single user under power constraint ρ_f. Further, we assume that the BS and the user have a perfect information of the channel gains. We show that the supremum of achievable rates leads to a secure DoF of $\frac{T_d}{T}$. Hence, we conclude that $\frac{T_d}{T}$ is an upper bound on secure DoF attained in the multi user downlink communication model in Section 3.2.

We now describe a strategy to attain the maximum secure DoF in Theorem 3.3.1. On the first T_r channel uses of each block, the users send pilot signals that are mutually orthogonal. The BS uses minimum mean square estimator (MMSE) to estimate the BS-to-user channel gains. The BS constructs K codebooks, c_k, $k = 1, \ldots, K$, where codebook c_k contains $2^{BT\hat{R}_k}$ independently and identically generated codewords, $s_k^{BT_d}$ of length BT_d and $\hat{R}_k > R_k$. The BS maps k-th user's message to a codeword with a stochastic mapping function f_k. Specifically, the BS maps message $w_k \in \left\{1, \ldots, 2^{BTR_k}\right\}$ to randomized message $m_k \in \{1, \ldots, 2^{BT\hat{R}_k}\}$ as in [3] and then maps randomized message m_k to one of the codewords in c_k, $k = 1, \ldots, K$. Utilizing the conjugate beamforming in (3.2.8), the BS maps K codewords, $s_k^{BT_d}$, $k = 1, \ldots, K$ to channel input sequence X^{BT_d}. Each user employs typical set decoding [1]. In order to show that secrecy constraint (3.2.11) for a particular user is satisfied, we give the adversary the other users' transmitted codewords. □

In the next couple of remarks, we emphasize the robustness of the downlink communication system against no training-phase jamming.

Remark 3.3.2. ***(The weakness of the adversary not jamming the training phase)*** *In the proof of Theorem 3.3.1, we show that* $\frac{T_d}{T}$ *is indeed an upper bound on the DoF of a downlink communication without the presence of an adversary. Hence, with also showing that the secure DoF of* $\frac{T_d}{T}$ *is attained in the presence of the adversary, we conclude that no training-phase jamming attack does not degrade the performance of the communication in terms of DoF. The reason that secure DoF of* $\frac{T_d}{T}$ *is achieved is that the adversary keeps silent during the training phase; hence the estimated BS-to-user channel gains are independent from* H_e*.*

In the next section, we consider an adversary jamming the training phase. In the presence of such an adversary, the BS-to-user channel gains become correlated with H_e *and the maximum secure DoF is reduced to zero.*

Remark 3.3.3. ***(Resource race between the BS and the adversary)*** *In Appendix B.1, we show that the achievable rate tuple that leads to a secure DoF of* $\frac{T_d}{T}$ *is* $R_k = \frac{T_d}{T}\log\left(1+\frac{M\rho_k a}{\rho_f+\rho_{jam}+1}\right) - \frac{T_d}{T}\log\left(1+M_e\rho_k\right)$*,* $k=1,\ldots,K$*, where* $a \triangleq \frac{\rho_r T_r}{\rho_r T_r+1}$*.*

We next investigate how R_k *varies in* M_e *and* M*. Figure 3.2 illustrates this variation when* $\rho_k = 1$*,* $\rho_f = 10$*,* $\frac{T_d}{T} = 0.99$*,* $\rho_{jam} = 1$*, and* $a = 0.9$*. As seen in Figure 3.2, in the presence of the adversary not jamming the training phase,* ***the achievable secure rates are determined as a result of the arms race between the adversary and the BS.*** *Specifically, we can observe that if* M_e *remains constant, achievable rate* R_k *grows unboundedly as* M *is increasing. Moreover, for a fixed value of* M*, the achievable rates decrease as a function of* M_e*. In the next section, we consider an adversary jamming the training phase instead of keeping silent during the training phase. We will show that, armed with only a single antenna, the adversary is capable of limiting the maximum achievable rate for any user to zero as* $M \to \infty$*.*

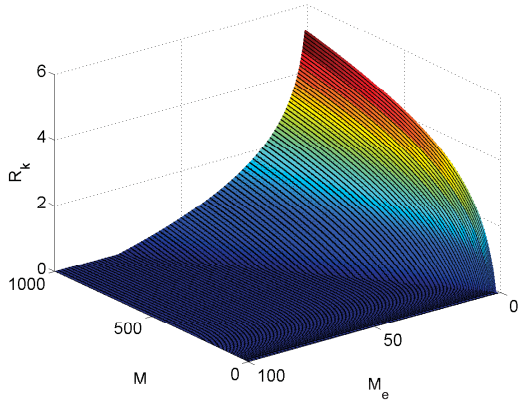

Figure 3.2: The variation of R_k with M and M_e

Hence, by jamming the training phase, the adversary converts the arms race between the BS and itself to the one between an user and itself.

3.3.2 Establishing security without Wyner encoding

In the achievability strategy given in the proof sketch of Theorem 3.3.1, we use a stochastic encoding, a randomized mapping of each message to a codeword with stochastic functions, at the BS. In fact, stochastic encoding, e.g., Wyner encoding [3], is a standard technique in the literature for establishing information theoretic security against the eavesdropping attacks.

In this section, we show that the BS utilizing deterministic encoding, a nonrandom mapping of each message to a codeword with deterministic functions, instead of stochastic encoding is capable of satisfying the security constraints if it is equipped with sufficiently large number antennas. In order to satisfy the security constraints without using stochastic encoding, the BS employs novel beamforming strategy introduced in (3.2.9).

The following theorem shows that, when code $\left(2^{BTR_1},\ldots,2^{BTR_K},BT_d\right)$ of length BT_d utilizes δ-conjugate beamforming instead of conjugate beamforming in (3.2.8), the code satisfies the secrecy constraint in (3.2.11) for any $k\in\{1,\ldots,K\}$ and for any $\epsilon>0$ without a need for stochastic encoding.

Theorem 3.3.4. ***(Establishing secrecy with no stochastic encoding)*** *Let $\delta>0$. Under no training-phase jamming, for any $\epsilon>0$, if $M\geq S(\epsilon)$, then any deterministic code $\left(2^{BTR_1},\ldots,2^{BTR_K},BT_d\right)$ employing δ-conjugate beamforming satisfies*

$$\frac{1}{BT}H\left(W_k|Z^{BT_d},H^B,\hat{H}^B,H_e^B\right)\geq R_k-\epsilon \tag{3.3.1}$$

for all $B\geq 1$ and for all $k\in\{1,\ldots,K\}$, where

$$S(\epsilon)\triangleq\left(\frac{M_e\rho_{max}}{2^{\frac{T}{T_d}\epsilon}-1}\right)^{\frac{1}{\delta}}$$

and $\rho_{max}\triangleq\max\limits_{k\in\{1,\ldots,K\}}\rho_k$. □

We can consider $S(\epsilon)$ in Theorem 3.3.4 as the number of the antennas the BS needs in order to make the conditional entropy ϵ-close to R_k for all $k\in\{1,\ldots,K\}$. Hence the BS equipped with at least $S(\epsilon)$ antennas can satisfy (3.3.1) by harnessing any code $\left(2^{BTR_1},\ldots,2^{BTR_K},BT_d\right)$ that employs deterministic encoding functions and δ-conjugate beamforming.

The proof is available in Appendix B.2.1. The BS constructs K codebooks, c_k, $k=1,\ldots,K$, where codebook c_k contains 2^{BTR_k} codewords, $s_k^{BT_d}$ of length BT_d. The BS maps message w_k to $s_k^{BT_d}$ codeword with a deterministic function, f_k, $k=1,\ldots,K$. Utilizing the δ-conjugate beamforming in (3.2.9), the BS maps K codewords, $s_k^{BT_d}$, $k=1,\ldots,K$ to channel input sequence X^{BT_d}.

In Figure 3.3, we illustrate the variation of $S(\epsilon)$ with ϵ when $\rho_k=1$, $\delta=0.7$, $T/T_d=5/4$, and $M_e=1$. As seen in Figure 3.3, 100 antennas at the BS are sufficient to make the equivocation rate above $R_k-0.05$ for any choice of R_k, $k=1,\ldots,K$.

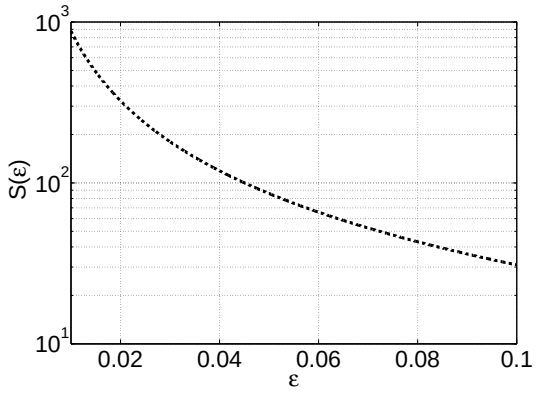

Figure 3.3: The variation of $S(\epsilon)$ with ϵ when $\rho_k = 1$, $\delta = 0.7$, $T/T_d = 5/4$, and $M_e = 1$. As long as $M \geq S(\epsilon)$, $\frac{1}{BT} H\left(W_k | Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right)$ remains ϵ-neighborhood of R_k for any $k \in \{1, \ldots, K\}$.

Theorem 3.3.4 evaluates the number of antennas needed in order to satisfy *only* the secrecy constraint. The following corollary takes both the secrecy and decodability constraints into account.

Corollary 3.3.5. ***(Any rate tuple is achievable with no need to stochastic encoding)*** *Let $0 < \delta < 1$. In the presence of no training-phase jamming, for any $\epsilon > 0$ and any rate tuple $R \triangleq [R_1, \ldots, R_K]$, if $M \geq \max(V(R), S(\epsilon))$, there exists $B(\epsilon) > 0$ and sequence of codes $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right), B \geq B(\epsilon)$ that satisfy the constraints in* (3.2.10) *and* (3.2.11) ***without the use of stochastic encoding****, where*

$$V(R) \triangleq \max_{k \in \{1,\ldots,K\}} \left(\left(2^{R_k \frac{T}{T_d}} - 1\right) \times \frac{\rho_f + \rho_{jam} + 1}{a\rho_k} \right)^{\frac{1}{1-\delta}}.$$

□

The proof of Corollary 3.3.5 can be found in Appendix B.2.2. The sequence of codes in Corollary 3.3.5 utilizes δ-conjugate beamforming. Figure 3.4 illustrates the variation of $\max(V(R), S(\epsilon))$ with δ when $\epsilon = 0.05$, $T/T_d = 5/4$, $M_e = 1$, $\rho_k = 1$, and

$R_k = 0.2$ for any $k \in \{1, \ldots, K\}$. Note that, for these parameters, $\max\left(V(R), S(\epsilon)\right)$ is minimized and identical to 60 when $\delta = 0.78$. When the BS utilizes δ-conjugate beamforming with $\delta = 0.78$, the BS requires at least 60 antennas in order to satisfy the constraints in (3.2.10) and (3.2.11) without the need for a stochastic encoding (e.g., Wyner encoding).

Remark 3.3.6. ***(Achieving secure DoF arbitrarily close the maximum DoF with no Wyner encoding)*** *Theorem 3.3.4 and Corollary 3.3.5 show that it is possible to establish information theoretic security without using stochastic encoding. We next measure the amount of DoF sacrificed as a result of not utilizing stochastic encoding. To that end, we evaluate how number of antennas at the BS* $\max(V(R), S(\epsilon))$ *scales with* R_k *for given* $\epsilon > 0$ *and* $\{R_l\}_{l \neq k}$*. Specifically, we calculate* $\lim\limits_{R_k \to \infty} \dfrac{R_k}{\log \max(V(R), S(\epsilon))}$ *as*

$$\lim_{R_k \to \infty} \frac{R_k}{\log \max(V(R), S(\epsilon))} = \lim_{R_k \to \infty} \frac{R_k}{\log V(R)} \tag{3.3.2}$$

$$= \lim_{R_k \to \infty} \frac{R_k}{\log\left(\left(2^{R_k \frac{T}{T_d}} - 1\right) \times \frac{\rho_f + \rho_{jam} + 1}{a\rho_k}\right)^{\frac{1}{1-\delta}}} \tag{3.3.3}$$

$$= \lim_{R_k \to \infty} \frac{(1-\delta)R_k}{\log\left(2^{R_k \frac{T}{T_d}} - 1\right)}$$

$$= (1-\delta)\frac{T_d}{T} \tag{3.3.4}$$

for all $k \in \{1, \ldots, K\}$*, for any* $\epsilon > 0$ *and for any* $\{R_l\}_{l \neq k}$*. The equalities in* (3.3.2) *and* (3.3.3) *in the above derivation follow from the fact that* $\max(V(R), S(\epsilon))$ *and* $V(R)$ *are increasing functions of* R_k*. We observe from* (3.3.4) *that by choosing* δ *close to* 0*, we can make the difference between* (3.3.4) *and the maximum secure DoF provided in Theorem 3.3.1 arbitrarily small.*

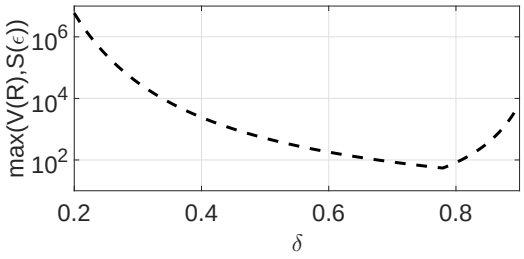

Figure 3.4: The variation of $\max(V(R), S(\epsilon))$ with δ when $\epsilon = 0.05$, $T/T_d = 5/4$, $M_e = 1$, $\rho_k = 1$, and $R_k = 0.2$ for any $k \in \{1, \ldots, K\}$. As long as $M \geq \max(S(\epsilon), V(R))$, constraints in (3.2.10) and (3.2.11) are satisfied for a given ϵ and R **without a need for stochastic encoding.**

3.4 Adversary jamming the training phase

In the previous section, we show that the adversary not jamming during the training phase does not degrade the performance of the multi user communication when the BS has sufficiently large number of antennas. In this section, we aim to find attack model that do degrade the performance. Specifically, we focus on finding an attack strategy capable of limiting secure DoF to an arbitrarily small value. Next theorem sheds light on finding such an attack strategy.

Theorem 3.4.1. ***(A non-zero correlation between the estimated user channel and the adversary channel gains limits the maximum secure DoF to zero)*** *Let the BS use either conjugate beamforming or delta-conjugate beamforming for some $\delta > 0$. Assume that there exists user k such that*

- $\left\{\hat{H}_{k,m} H_{e,m}\right\}_{m \geq 1}$ *is*[5] *an i.i.d random process.*
- *For any $B \geq 1$, there exists a random vector $\tilde{H}_k^B$ that satisfies the following: 1) the joint probability distribution of $H_e^B, \hat{H}^B$ is identical with that of $H_k^B, \tilde{H}^B$,*

[5] H_{e_m} is the gain of the connecting m-th antenna at the BS to the adversary.

where $\tilde{H}^B \triangleq \hat{H}_1^B, \ldots, \tilde{H}_k^B, \ldots, \hat{H}_K^B$ *and 2) the joint probability distribution of* $H(i), \tilde{H}(i)$ *is identical for any* $i \in \{1, \ldots, B\}$.

Then, the maximum secure DoF is zero if $\mathbb{E}\left[H_{e,m}^* \hat{H}_{k,m}\right] \neq 0$. □

Note that random vector $\tilde{H}^B$ is created by replacing $\hat{H}_k^B$ in $\hat{H}^B$ with $\tilde{H}_k^B$. The proof of Theorem 3.4.1 can be found in Appendix B.3.1. In the example given at the end of this section, we show that the assumptions listed in Theorem 3.4.1, that are related to the random variables hold when MMSE and mutually orthogonal pilot signals are used as a channel estimation strategy. Note that such an estimation strategy is quite popular in the multi-user communication [24].

We next give a proof sketch. As indicated in Section 3.2.3, we only focus on codes that use either conjugate beamforming or δ-conjugate beamforming. Hence, upper bound given in Theorem 3.4.1 is valid only for the codes using these beamforming techniques. In the proof sketch, we assume that $M_e = 1$ and the BS employs conjugate beamforming without loss of generality. We convert the communication set-up explained in Section 3.2 to an identical set-up containing a BS equipped with K antennas, where the channel input signal at l-th antenna in the new set-up represents the data signal for l-th user S_l, $l = 1, \ldots, K$. Since conjugate beamforming is used, the gain of the channel connecting l-th antenna to i-th user in the new set-up is $\frac{H_i \hat{H}_l^*}{\sqrt{M\alpha_l}}$ and the gain of the channel connecting l-th antenna to the adversary in the new set-up is $\frac{H_e \hat{H}_l^*}{\sqrt{M\alpha_l}}$, $i, l = 1, \ldots, K$. Following the assumptions in Theorem 3.4.1, we show that the gain of the channel connecting the BS to the adversary can be replaced with $\frac{H_k \hat{H}_1^*}{\sqrt{M\alpha_1}}, \ldots, \frac{H_k \tilde{H}_k^*}{\sqrt{M\alpha_k}}, \ldots, \frac{H_k \hat{H}_K^*}{\sqrt{M\alpha_K}}$. In Appendix B.3.1, we bound R_k as follows

$$R_k \leq \mathbb{E}\left[\left[\max_{\Sigma \in \mathcal{S}} \left(\log\left(1 + A_k \Sigma A_k^*\right)\right.\right.\right.$$
$$\left.\left.\left. - \log\left(1 + A_e \Sigma A_e^*\right)\right)\right]^+\right], \tag{3.4.1}$$

where $A_k \triangleq \left[\frac{H_k\hat{H}_1^*}{\sqrt{M\alpha_1}},\ldots,\frac{H_k\hat{H}_k^*}{\sqrt{M\alpha_k}},\ldots,\frac{H_k\hat{H}_K^*}{M\alpha_K}\right]$ is $1\times K$ complex gain vector of channels connecting the BS to k-th user, and $A_e \triangleq \left[\frac{H_k\hat{H}_1^*}{\sqrt{M\alpha_1}},\ldots,\frac{H_k\tilde{H}_k^*}{\sqrt{M\alpha_k}},\ldots,\frac{H_k\hat{H}_K^*}{\sqrt{M\alpha_K}}\right]$ is $1\times K$ complex gain vector of channels connecting the BS to the adversary. Let Σ be the covariance matrix of input signal $S=[S_1,\ldots,S_K]$ and $\mathcal{S}$ be the feasible set for the maximization problem in (3.4.1). Every matrix Σ in set $\mathcal{S}$ is diagonal due to fact that $S_1,\ldots,S_K$ are independent, and satisfy $\Sigma \preceq diag(\rho_1,\ldots,\rho_k)$ due to the power constraint in (3.2.6).

We show that, if $\mathbb{E}\left[H_{k,m}^*H_{e,m}\right]\neq 0$, then the right hand side (RHS) of (3.4.1) over $\log M$ goes to zero as $M\to\infty$. Hence, the maximum secure DoF becomes zero. □

Remark 3.4.2. *(**Adversary has to jam the training phase**) When the adversary does not jam the training phase, $\hat{H}_k$ and H_e are independent and consequently $\mathbb{E}\left[\hat{H}_{k,m}H_{e,m}^*\right]=\mathbb{E}\left[\hat{H}_{k,m}\right]\mathbb{E}\left[H_{e,m}^*\right]=0$ for all $k\in\{1,\ldots,K\}$. In order to have a non-zero correlation between the gain of the channel connecting itself to the BS H_e with $\hat{H}_k$ for any $k\in\{1,\ldots,K\}$, the adversary has to jam the training phase. Hence, the training-phase jamming is capable of limiting the maximum DoF to zero.* □

In addition to limiting the maximum secure DoF to zero, the adversary can make the maximum achievable rate of k-th user arbitrarily small as $M\to\infty$. We next provide the conditions under which the maximum achievable rate of k-th user goes to a finite value as $M\to\infty$.

Corollary 3.4.3. ***(A user's maximum achievable rate is bounded as** $M\to\infty$**)** *In addition to the assumptions given in Theorem 3.4.1, assume that there exits a finite non negative r such that $p_{K_M}(x)\leq r$ for all $M\geq 1$ and $x\in\mathcal{K}_M$, where p_{K_M} is*

the probability density function of $K_M \triangleq \frac{1}{M^2}||H_e\hat{H}_k^*||^2$ *and* $\mathcal{K}_M$ *is the sample space of* K_M*. Then, the achievable rate of* k*-th user is bounded as*

$$\lim_{M\to\infty} R_k \leq \left[\log\left(\frac{\left|\mathbb{E}\left[H_{k,m}\hat{H}_{k,m}^*\right]\right|^2}{\left|\mathbb{E}\left[H_{e,m}\hat{H}_{k,m}^*\right]\right|^2}\right)\right]^+ .$$

□ The proof of Corollary 3.4.3 can be found in Appendix B.3.2.

As seen in Corollary 3.4.3, if the amount of correlation between the BS-to-k-user channel gain and the estimated BS-to-k-user channel gain, $\left|\mathbb{E}\left[H_{k,m}\hat{H}_{k,m}^*\right]\right|$ is smaller than that between the BS-to-adversary channel gain and estimated BS-to-k-th user channel gain, $\left|\mathbb{E}\left[H_{e,m}\hat{H}_{k,m}^*\right]\right|$, the maximum achievable rate of k-th user vanishes as $M \to \infty$.

Remark 3.4.4. ***(Resource race between the adversary and the user)*** *We show that if there exists a non zero correlation between the BS-to-k-user channel gain and the BS-to-adversary channel gain, then the maximum secure DoF is constrained to zero. Furthermore, we also show that if the amount of this correlation is higher than the amount of the correlation between the BS-to-adversary channel gain and estimated BS-to-k-user channel gain, the maximum achievable rate of k-th user goes to zero as* $M \to \infty$*.*

Hence, in the presence of the training-phase jamming, the achievable rates and the maximum secure DoF are determined as a result of the arms race between the adversary and users. □

Example 1. ***(Using MMSE and mutually orthogonal pilot signals for channel estimation)*** *We study an adversary that chooses to match k-th user's pilot signal on the training phase with one of its antennas when MMSE and mutually orthogonal pilot signals are used for channel estimation. We show that the assumptions given in Theorem 3 are valid under such a jamming attack and a channel estimation strategy. Then, we show that the maximum secure DoF is zero.*

We consider mutually orthogonal pilot signals $\{\phi_l\}_{l\in\{1,\ldots,K\}}$, *i.e.,*

$$\phi_k \times \phi_l^* = \begin{cases} T_r\rho_r & \text{if } k = l \\ 0 & \text{if } k \neq l \end{cases}$$

for any $k, l \in \{1, \ldots, K\}$. *The received signals at the BS in the training phase of* i*-th block is as follows:*

$$Y^{T_r} = \sqrt{\frac{\rho_{jam}}{\rho_r}} H_e^{\mathsf{T}}(i)\phi_k + \sum_{l=1}^{K} H_l^{\mathsf{T}}(i)\phi_l + W,$$

where ρ_{jam} *is the jamming power. Note that we assume that the adversary jams the data communication phase and the training phase with the same power, which is* ρ_{jam}.

In order to validate the assumptions listed in Theorem 3.4.1, we next present the estimated gain of the channel connecting the BS to l*-th user at* i*-th block as*

$$\hat{H}_l(i) = \begin{cases} aH_l(i) + bH_e(i) + cV_l & \text{if } l = k \\ dH_l(i) + eV_l & \text{if } l \neq k, \end{cases}$$

where V_l *is distributed as* $\mathcal{CN}(0, I_M)$ *for any* $l \in \{1, \ldots, K\}$, $a \triangleq \dfrac{T_r\rho_r}{T_r\rho_r + 1 + T_r\rho_{jam}}$, $b \triangleq \dfrac{T_r\sqrt{\rho_r\rho_{jam}}}{T_r\rho_r + 1 + T_r\rho_{jam}}$, $c \triangleq \dfrac{\sqrt{T_r\rho_r}}{T_r\rho_r + 1 + T_r\rho_{jam}}$, $d \triangleq \dfrac{T_r\rho_r}{T_r\rho_r + 1}$ *and* $e \triangleq \dfrac{\sqrt{T_r\rho_r}}{T_r\rho_r + 1}$.

Define $\tilde{H}_k^B$ *stated in Theorem 3.4.1 as* $\tilde{H}_k(i) \triangleq bH_k(i) + aH_e(i) + cV_k$, $i = 1, \ldots, B$. *Further, define* $\hat{H}_l \triangleq aH_l + bH_e + cV_l$ *if* $k = l$, *and otherwise,* $\hat{H}_l \triangleq dH_l + eV_l$. *Note that* $\tilde{H}_k(i), H(i), H_e(i), \hat{H}(i)$ *is an i.i.d process due to* (3.2.5) *and the associated joint distribution is identical with that of* $\tilde{H}_k, H, H_e, \hat{H}$, *where* $\tilde{H}_k \triangleq aH_k + bH_e + cV_k$. *Hence, we conclude that the joint probability distribution of* $H(i), \tilde{H}(i)$ *is identical for any* $i \in \{1, \ldots, B\}$.

We next show that the probability distribution of $H_e^B, \hat{H}^B$ *is identical with that of* $H_k^B, \tilde{H}^B$. *Note that both* $(H_e, \hat{H}_k)$ *and* $(H_k, \tilde{H}_k)$ *are independent frrom* $\{\hat{H}_l\}_{l\neq k}$. *Hence, noting that* H_e *and* H_k *have same probability distributions, it is sufficient to*

show that $\tilde{H}_k|H_k = h_k$ *has the same probability distribution with* $\hat{H}_k|H_e = h_k$ *for any* $h_k \in \mathbb{R}^M$*:*

$$\begin{aligned}
&\mathbb{P}\left(\tilde{H}_k \leq x|H_k = h_k\right) \\
&= \mathbb{P}\left(bh_k + aH_e + cV_k \leq x|H_k = h_k\right) \\
&= \mathbb{P}\left(bh_k + aH_e + cV_k \leq x\right) \qquad (3.4.2) \\
&= \mathbb{P}\left(bh_k + aH_k + cV_k \leq x\right) \qquad (3.4.3) \\
&= \mathbb{P}\left(bH_e + aH_k + cV_k \leq x|H_e = h_k\right) \qquad (3.4.4) \\
&= \mathbb{P}\left(\hat{H}_k \leq x|H_e = h_k\right)
\end{aligned}$$

for any $x \in \mathbb{R}^M$*, where* (3.4.2) *and* (3.4.4) *follow from the fact that* H_e*,* H_k*, and* V_k *are mutually independent and* (3.4.3) *follows from the fact that* (H_e, V_k) *and* (H_k, V_k) *are identically distributed.*

Finally, note that $\{H_{e,m}, \hat{H}_{k,m}\}_{m\geq 1}$ *forms an i.i.d process due to the fact that* H_k, H_e, V_k *are mutually independent random vectors and each is composed of* M *i.i.d complex Gaussian random variables.*

Note that $\mathbb{E}\left[\hat{H}^*_{k,m}H_{e,m}\right] = b$*. Since* $\mathbb{E}\left[\hat{H}^*_{k,m}H_{e,m}\right]$ *is non-zero, we conclude that the maximum secure DoF is zero by Theorem 3.4.1.* □

Combining Remark 3.4.2 and Example 1, we conclude that under the downlink communication set-up in which MMSE estimation and orthogonal pilot signlas are used for channel estimation, if the adversary jams the training phase, it is not possible to achieve non-zero secure *DoF*

3.5 Secure communication under Training-Phase Jamming

In the previous section, we showed that massive MIMO systems are vulnerable to the training-phase jamming. In this section, we first provide a defense strategy against

the training-phase jamming, that expands the cardinality of the set of pilot signals and keeps the pilot signal assignments hidden from the adversary. Then, we show that utilizing the defense strategy and δ-conjugate beamforming, the BS can satisfy the security constraints without using Wyner encoding in the presence of the training-phase jamming. Finally, we discuss that relying only on the computational cryptography, we can secure the communication of pilot signal assignments; hence the entire massive MIMO communication.

3.5.1 Counter strategy against training-phase jamming

We first describe our defense strategy against training-phase jamming attack. Then, in Theorem 3.5.1, we show that the ratio of the achieved rate to the logarithm of number of antennas can be brought arbitrarily close to maximum achievable secure DoF of $\frac{T_d}{T}$ with the proposed defense strategy that will be explained next.

The BS constructs pilot signal set Φ containing L mutually orthogonal pilot signals, i.e., $\Phi = \{\phi_1, \ldots, \phi_L\}$, where L is larger than the number of users in the system, $L \geq K$. Thus, the number the pilot signals is increased. At the beginning of each block, the BS draws K pilot signals from set Φ uniformly at random and assigns each of them to a different user. Let $\Phi_K(i) = [\phi_1(i), \ldots, \phi_K(i)]$ be K pilot signals that the BS picks at the beginning of i-th block, where $\phi_k(i) \in \Phi$ is the pilot signal assigned to k-th user on i-th block.

Throughout sections 3.5.1 and 3.5.2, we assume that the BS communicates to the users the assignments of pilot signals reliably while keeping the assignments hidden from the adversary. In Section 3.5.3, we discuss how this can be achieved. In particular, we consider *computational cryptography* as a way to communicate the pilot signal assignments and discuss the notion of security achieved.

We next describe the attack model in detail, under the lack of knowledge of

the pilot signal assignments. Suppose that the adversary targets k-th user without loss of generality. The adversary eavesdrops the entire communication between user k and the BS and simultaneously jams data communication phase with Gaussian noise as in no training-phase jamming attack model. Furthermore, the adversary, *without knowing which pilot signal is assigned to which user*, picks $J \leq L$ pilot signals uniformly at random from set Φ at the beginning of a block and subsequently jams these pilot signals with an equal power during the training phase. The adversary repeats this process independently at the beginning of each block.

Particularly, the adversary divides its jamming power and transmits an equally weighted combination of J randomly selected pilot signals using all of its M_e antennas with total transmission power $\frac{\rho_{jam}}{J}$. The signal received by the BS during the training phase under this attack model can be written as follows:

$$Y^{T_r} = \sum_{l=1}^{K} H_l^{\mathsf{T}} \phi_l + \sum_{l \in \mathcal{J}} \sum_{n=1}^{M_e} \sqrt{\frac{\rho_{jam}}{M_e J \rho_r}} H_{e_n}^{\mathsf{T}} \phi_l + W, \tag{3.5.1}$$

where Y^{T_r} denotes $M \times T_r$ complex matrix of the received signals over T_r channel uses at the BS, H_{e_n} is $1 \times M$ complex gain vector of the channel connecting n-th antenna at the adversary to the BS, and $\mathcal{J}$ is the set of pilot signals that are selected and transmitted by the adversary at the corresponding block. Note that $\mathcal{J}$ is a random set that can possibly change in each block and $|\mathcal{J}| = J$.

Next theorem shows that when the cardinality, L of pilot signal set is increased as a function of the number of BS antennas in a certain way, the ratio of attained secure rate to $\log M$ for any user can be arbitrarily close to the maximum DoF attained in the presence of no adversary.

Theorem 3.5.1. ***(Achievable rate under training-phase jamming)*** *For given*

block length T and data transmission phase length T_d, the achievable secure rate, R_k under training-phase jamming satisfies

$$\frac{R_k}{\log M} \geq \frac{T_d}{T}\min(1,\gamma) - \epsilon \tag{3.5.2}$$

for any $k \in \{1,\ldots,K\}$, $J \in \{1,\ldots T_r\}$, $\epsilon > 0$, and $\gamma > 0$ if $\max(M^\gamma, K) \leq T_r$ and $M \geq G(\epsilon)$, where

$$G(\epsilon) \triangleq \left(\left(1 + M_e\rho_{max} + \frac{M_e\rho_{max}\rho_{jam}}{\rho_r}\right) \times(\rho_f + \rho_{jam} + 1) \times \frac{\rho_r + \rho_{jam} + 1}{\rho_{min}\rho_r}\right)^{\frac{T_d}{T\epsilon}}, \tag{3.5.3}$$

$\rho_{max} \triangleq \max_{k\in\{1,\ldots,K\}} \rho_k$, *and* $\rho_{min} \triangleq \min_{k\in\{1,\ldots,K\}} \rho_k$. □

Note that the lower bound to $\frac{R_k}{\log M}$ in (3.5.2) does not depend on how many pilot signals the adversary chooses to contaminate. The proof of Theorem 3.5.1 can be found in Appendix B.4.

Remark 3.5.2. ***(Attained $\frac{R_k}{\log M}$ is arbitrarily close to maximum DoF under no attack)*** *We can observe from the statement of Theorem 3.5.1 that when $\gamma = 1$, $\frac{R_k}{\log M}$ that is arbitrarily close to the maximum DoF attained under no attack can be achieved. In order to attain that amount of $\frac{R_k}{\log M}$, the length of the training phase T_r is expanded so that $T_r \geq \max(K, G(\epsilon))$ for given $\epsilon > 0$ and the size of pilot signal set is set to T_r instead of K. Hence, we sacrifice the some of secure throughput by increasing the training overhead. However, as illustrated in the next example, the typical values for the block lengths for mobile wireless communication systems is sufficiently large to keep the overhead ratio, $\frac{T_r}{T}$ reasonably low.*

Example 2. *In this example, we consider massive MIMO downlink transmission to users moving at a speed 10 m/s and the transmitted signal bandwidth is 10 MHz, centered at 1 GHz The associated coherence time corresponds T to as 3×10^5 channel*

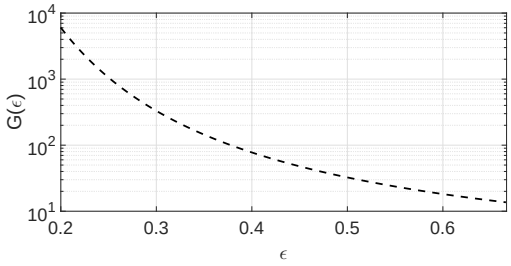

Figure 3.5: The change of $G(\epsilon)$ with ϵ

uses. We first evaluate the number of antennas required to keep R_k in ϵ neighborhood of $\frac{T_d}{T}$ for a given training phase length T_r. To that end, we plot the variation of $G(\epsilon)$ with ϵ in Figure 3.5, when $\gamma = 1$, $T_d = 2 \times 10^5$ channel uses, $p_{jam} = 1$, $K = 5$, $p_f = 5$, $M_e = 1$, $p_r = 10$, $p_k = 1$ for all $k \in \{1, \ldots, K\}$. For these set of parameters, 200 antennas are sufficient to keep $\frac{R_k}{\log M}$ larger than $\frac{T_d}{T} - 0.3$, where $\frac{T_d}{T} = \frac{2}{3}$.

Next we study the trade-off between ϵ and $\frac{T_d}{T}$ for given M, where ϵ is the deviation of achieved $\frac{R_k}{\log M}$ from $\frac{T_d}{T}$ as in (3.5.2). To that end, we plot the variation of ϵ and $\frac{T_d}{T}$ with $\frac{T_r}{T}$ for $M = 200$ as we change $\frac{T_r}{T}$ from $\frac{200}{3 \times 10^5}$ to 1. The values of parameters p_{jam}, K, M_e, ρ_k, and ρ_f are kept same as stated above and we set $\rho_r = \frac{T_d}{T_r}\rho_f$. As seen in Figure 3.6, ϵ vanishes as T_r goes to T and hence $\frac{R_k}{\log M}$ also gets closer to $\frac{T_d}{T}$. However, as T_r increases, the training overhead increases and hence maximum DoF $\frac{T_d}{T}$ decreases.

Remark 3.5.3. ***(Resource race between the adversary and the BS)*** *By keeping the pilot assignments hidden from the adversary and using a pilot signal set that scales with M,* ***the BS converts the arms race between the adversary and the target user (which was the case with known pilot assignments), back***

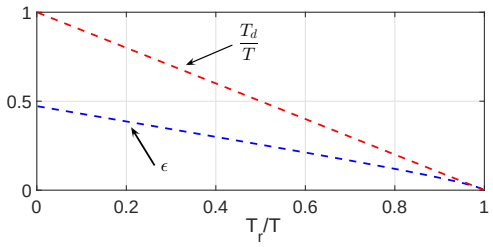

Figure 3.6: The change of ϵ in (3.5.2) and $\frac{T_d}{T}$ with $\frac{T_r}{T}$

to the one between the adversary and itself. *Indeed, the power of the adversary needs to scale with L for it to make an impact.*

3.5.2 Establishing security without Wyner encoding

In this subsection, we show that the BS, when utilizing deterministic encoding instead of stochastic encoding is still capable of satisfying the secrecy and decodability constraints in the presence of training-phase jamming. Hence, this subsection can be considered as the counterpart of Section 3.3.2. There, we assumed no training phase jamming, whereas here we mitigate training-phase jamming by other means.

In order to satisfy the security constraints without using stochastic encoding, the BS employs δ-conjugate beamforming given in (3.2.9) and the strategy explained in Section 3.5.1. Specifically, Theorem 3.5.4 and Corollary 3.5.5 provide the number of antennas that the BS requires in order to satisfy only the secrecy constraint and both the secrecy and decodability constraints, respectively. Note that Theorem 3.5.4 and Corollary 3.5.5 are the counterparts of Theorem 3.3.4 and Corollary 3.3.5.

Theorem 3.5.4. ***(Establishing secrecy with no stochastic encoding)*** *Let δ, $\gamma > 0$, and $\gamma + \delta > 1$. Let block length be T and length of data transmission phase be T_d. In the presence of training-phase jamming, for any $\epsilon > 0$ and any rate tuple*

$R \triangleq [R_1, \ldots, R_K]$, *if* $M \geq S_1(\epsilon)$ *and* $T_r \geq \max(M^\gamma, K)$, *then any deterministic code* $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ *employing* δ*-conjugate beamforming satisfies*

$$\frac{1}{BT} H\left(W_k | Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right) \geq R_k - \epsilon \tag{3.5.4}$$

for any $J \in \{1, \ldots, T_r\}$, $B \geq 1$, *and* $k \in \{1, \ldots, K\}$, *where*

$$S_1(\epsilon) \triangleq \left(\frac{\rho_{max} M_e \max\left(1, \frac{\rho_{jam}}{\rho_r}\right)}{2^{\frac{T}{T_d}\epsilon} - 1} \right)^{\frac{1}{\min(\delta, \delta+\gamma-1)}}$$

and $\rho_{max} \triangleq \max\limits_{k \in \{1,\ldots,K\}} \rho_k$. □

The proof of Theorem 3.5.4 can be found in Appendix B.5.1. Note that when $\gamma = 1$ and $1 \geq \frac{\rho_{\text{jam}}}{\rho_r}$, the necessary number of antennas to meet the secrecy constraint under training phase attack becomes identical to that under no attack. This result demonstrates the effectiveness of the defense strategy, *hiding the pilot signal assignments from the adversary and expanding the pilot signal set.*

There is a tradeoff between the number, M, of antennas and the length, T_r, of the training period necessary to satisfy constraints $M \geq S_1(\epsilon)$ and $T_r \geq \max(M^\gamma, K)$. This tradeoff is controlled by parameter γ. While choosing γ close to 1 minimizes $S_1(\epsilon)$ for any $\epsilon > 0$, it increases the length of the training period, i.e., the overhead. To observe this: First, $S_1(\epsilon)$ is minimum at $\gamma = 1$ due to the fact that $\min(\delta, \delta+\gamma-1) \leq \delta$ and equality occurs when $\gamma = 1$. Second, increasing γ to 1 also increases training overhead as T_r has to be larger than $S_1(\epsilon)^\gamma$.

In Theorem 3.5.4, we provide the number of antennas required to satisfy only the secrecy constraint. Next corollary presents the number of antennas that BS needs in order to satisfy both the secrecy and the decodability constraints without need for stochastic encoding.

Corollary 3.5.5. ***(Any rate tuple is achievable with no need for stochastic encoding)*** *Let* $0 < \delta < 1$, $\gamma + \delta > 1$. *Let block length be* T *and length of data*

transmission phase be T_d *and* J *be any integer in* $\{1, \ldots, T_r\}$. *In the presence of training-phase jamming, for any* $\epsilon > 0$ *and any rate tuple* $R \triangleq [R_1, \ldots, R_K]$, *if* $M \geq \max\left(V_1(R), S_1(\epsilon)\right)$ *and* $T_r \geq M^\gamma$, *then there exists* $B(\epsilon) > 0$ *and a sequence of codes* $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right), B \geq B(\epsilon)$ *that satisfy the constraints in* (3.2.10) *and* (3.2.11) ***without a need for stochastic encoding***, *where*

$$V_1(R) \triangleq \max_{k \in \{1,\ldots,K\}} \left(\left(2^{R_k \frac{T}{T_d}} - 1\right) \times \frac{(\rho_f + \rho_{jam} + 1) \times (\rho_r + \rho_{jam} + 1)}{\rho_r \rho_k} \right)^{\frac{1}{1-\delta}}.$$

□

The proof of Corollary 3.5.5 can be found in Appendix B.5.2.

3.5.3 How do we hide the pilot signal assignments?

So far, we have demonstrated that, if pilot signal assignments can be kept secret from the adversary, the impact of training-phase jamming can be mitigated by increasing the cardinality of the pilot signal set at the expense of some increase in training overhead. Next, we discuss how to keep the assignments secret from the adversary.

In order to communicate the pilot signal assignments securely, at the beginning of each block, the BS shares with each user a secret key of size $\log L$ bits, that is unknown to the adversary. In the literature, by far the most popular way to generate an information-theoretically secure secret key across a wireless channels is via the use of reciprocal channel gains [32–34]. However, we cannot use such channel-gain based methods, since for those methods we need to observe the channel gains. However, our objective of generating the keys is to secure the training phase, whose sole purpose is to observe the channel gains in the first place, leaving us with a "chicken or the egg" dilemma.

With this observation, let us consider the methods in which these keys are generated and shared by standard private key based methods (e.g., Diffie-Hellman [35]) or public key based methods (e.g., RSA [36]). Thus, it only relies on existing standard computational cryptographic techniques and does not rely on information-theoretic techniques for secure key sharing. Note that a shared key between the BS and a user is used to hide the pilot signal assigned to that user from the adversary. With the shared key, pilot signal assignments are encrypted with the shared key (for instance; index k is encrypted if ϕ_k is assigned to the user) and these assignments are communicated to the users immediately after key sharing.

Despite the use of computational cryptographic methods for key generation, the security we provide has the "same flavor" as information theoretic secrecy, as we clarify next. The main drawback of computational cryptographic methods such as Diffie-Hellman is that, they make assumptions on the computational power of the adversaries. This kind of security is based on the supposition that, given that the key is hidden from an adversary via a difficult puzzle[6], it takes an unreasonable amount of time for an adversary to crack it. Nevertheless, given enough time, the adversary will eventually decrypt the message (possibly quickly, given a quantum computer, for instance). This constitutes the main motivation for information-theoretic security, which makes no assumptions on the computational powers of the attackers.

In our approach, we have a hybrid scheme, combining information theoretic security and computational cryptography. We are using cryptography to hide the pilot sequence assignments, **not the message**. Encrypting the pilot signal assignments is fundamentally different from encrypting the message. In message encryption, the signal received by the adversary remains vulnerable to cryptanalysis, long after the message is transmitted. On the other hand, with pilot signal assignment encryption,

[6]For example, RSA is based on an NP problem: prime factorization of a large number.

this window of time for cryptanalysis can be arbitrarily small: unless the adversary figures out the pilot sequence assigned to the targeted user before the training phase starts, the knowledge of the assignment becomes useless. But, we know that the training phase starts immediately after the encrypted assignment is communicated to the users. If we define the computational power required for the adversary as the ratio of amount of computation needed to decrypt the key via cryptanalysis to the time required to solve the problem, the computational power necessary for the adversary to make a damage on the targeted user goes to infinity. This addresses the shortcoming of existing cryptographic methods due to their assumptions on computational powers of adversaries. Note that, if the adversary cannot act during the training phase, the message transmission is "perfectly secure" as shown in Theorem 4.

It is important to emphasize that, in the above discussion, we did **not** show that the aforementioned defense strategy achieves information-theoretic security. Instead, we argued that, utilizing our defense strategy of encrypting training signals, we can avoid one of the main drawbacks of the existing computational-cryptographic methods, i.e., assumptions on the computational power of adversaries.

CHAPTER 4

ON PRIVACY-UTILITY TRADEOFFS FOR CONSTRAINED DATA RELEASE MECHANISMS

4.1 Introduction

The objective of privacy-preserving data release is to provide useful data with minimal distortion while simultaneously minimizing the sensitive data revealed. Dependencies between the sensitive and useful data results in a privacy-utility tradeoff that has strong connections to generalized rate-distortion problems [37]. In this work, we study how the optimal privacy-utility tradeoff region is affected by constraints on the data that is directly available as input to the release mechanism. Such constraints are potentially motivated by applications where either the sensitive or useful data is not directly observable. For example, the useful data may be an unknown property that must be inferred from only the sensitive data. Alternatively, the constraints may be used to capture the limitations of a particular approach, such as *output-perturbation* data release mechanisms that take only the useful data as input, while ignoring the remaining sensitive data.

The general challenge of privacy-preserving data release has been the aim of a broad and varied field of study. Basic attempts to anonymize data have led to widely publicized leaks of sensitive information, such as [38, 39]. These have subsequently motivated a wide variety of statistical formulations and techniques for preserving

privacy, such as k-anonymity [40], L-diversity [41], t-closeness [42], and differential privacy [43]. Our work concerns a non-asymptotic, information-theoretic treatment of this problem, such as in [37,44], where the sensitive data and useful data are modeled as random variables X and Y, respectively, and mechanism design is the problem of constructing channels that obtain the optimal privacy-utility tradeoffs. While we consider a non-asymptotic, single-letter problem formulation, there are also related asymptotic coding problems that additionally consider communication efficiency in a rate-distortion-privacy tradeoff, as studied in [45, 46].

In this work, we generalize the framework of [37, 44] to address scenarios with data constraints and allow for general utility metrics. In particular, we compare three scenarios, where only the sensitive data, only the useful data, or both (full data) are available. We show that a general hierarchy holds, that is, the tradeoff region given only the sensitive data is no larger than the region given only the useful data, which in turn is clearly no larger than the region given both sensitive and useful data. We also show that if the common information and mutual information between the sensitive and useful data are equal[1], then the tradeoff region given only the useful data coincides with that given full data, indicating when output perturbation is optimal despite unavailability of the sensitive data. Conversely, when the common information and mutual information are not equal, there exist distortion metrics where the tradeoff regions are not the same, indicating that output perturbation can be strictly suboptimal compared to the full data scenario.

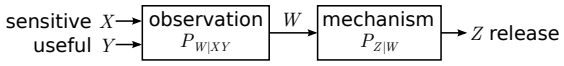

Figure 4.1: The observation W of the sensitive data X and useful data Y is input to the data release mechanism which produces the released data Z.

4.2 Privacy-Utility Tradeoff Problem

Let X, Y, and W be discrete random variables (RVs) distributed on finite alphabets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{W}$, respectively. Let X denote the sensitive information that the user wishes to conceal, Y the useful information that the user is willing to reveal, and W the directly observable data, which may represent a noisy observation of X and/or Y. The target application dictates (or imposes a specific structure upon) the *data model* P_{XY} and *observation constraints* $P_{W|XY}$ so that $(X, Y, W) \sim P_{XY}P_{W|XY}$. The *data release mechanism* takes W as input and (randomly) generates output Z in a given finite alphabet $\mathcal{Z}$ dictated by the target application (perhaps implicitly via the distortion metric). Note that Z must satisfy the Markov chain $(X, Y) \to W \to Z$ and the mechanism can be specified by the conditional distribution $P_{Z|W}$. A diagram of the overall system is shown in Figure 4.1.

The mechanism should be designed such that Z provides application-specific utility through the information it reveals about Y while protecting privacy by limiting the information it reveals about X.

A commonly used information-theoretic measure of privacy-leakage which quantifies the amount of information about X leaked by Z (on average) is the mutual information $I(X; Z)$ between them. We adopt this privacy-leakage measure in our

[1]This statement applies for both the Wyner [47] and Gács-Körner [48] notions of common information.

work. *Privacy* is inversely related to $I(X;Z)$: privacy is stronger if the privacy-leakage $I(X;Z)$ is smaller. We have perfect privacy if $I(X;Z)=0$. Thus, the aim is to minimize $I(X;Z)$ in order to maximize privacy.

The amount of *utility* that the mechanism-output Z provides about the useful information represented by Y can be quantified through a general distortion metric $D(P_{YZ})$, which is a functional that assigns values in $[0,\infty)$ to input joint distributions of Y and Z. Utility and distortion have an inverse relationship to each other: smaller the distortion, greater the utility. Thus, the aim is to minimize $D(P_{YZ})$. The specification of the distortion metric is dictated by the target application. Example distortion metrics include: 1) *expected distortion*, where $D(P_{YZ}) = E[d(Y,Z)]$ for some distortion function $d : \mathcal{Y} \times \mathcal{Z} \to [0,\infty)$, 2) *conditional entropy*, where $D(P_{YZ}) = H(Y|Z)$ which corresponds to the goal of maximizing the mutual information between Y and Z. Note that probability of error $\mathbb{P}(Y \neq Z)$ is an example within the class of expected distortion metrics where $d(y,z)$ is equal to zero when $y=z$ and equal to one otherwise.

Given a target application that specifies a particular instance of the problem by dictating the data model P_{XY}, observation model $P_{W|XY}$ and distortion metric $D(P_{YZ})$, the goal of the system designer is to construct mechanisms $P_{Z|W}$ that provide the desired levels of privacy and utility while achieving the optimal tradeoff. We say that particular privacy-utility pair $(\epsilon,\delta) \in [0,\infty)^2$ is *achievable* if there exists a mechanism $P_{Z|W}$ with privacy leakage $I(X;Z) \leq \epsilon$ and distortion $D(P_{YZ}) \leq \delta$. The set of all achievable privacy-utility pairs forms the *achievable region* of privacy-utility tradeoffs. Particularly, we are interested the *optimal boundary* of this region, which can be expressed by the optimization problem

$$\begin{aligned} \pi(\delta) \triangleq \inf_{P_{Z|W}} \; & I(X;Z) \\ \text{s.t. } & D(P_{YZ}) \leq \delta, \end{aligned} \tag{4.2.1}$$

which determines the optimal privacy leakage as a function of the allowable distortion δ.

The distortion constraint, $D(P_{YZ}) \leq \delta$, can be equivalently expressed as a constraint on the conditional distribution $P_{Z|Y}$ given that P_Y is fixed by the data model. Note that a mechanism specified by $P_{Z|W}$ determines the corresponding $P_{Z|Y}$ through the linear relationship[2]

$$P_{Z|Y}(z|y) = \sum_{w \in \mathcal{W}, x \in \mathcal{X}} P_{Z|W}(z|w) P_{W|XY}(w|x,y) P_{X|Y}(x|y). \tag{4.2.2}$$

Similarly, $P_{Z|X}$ is determined by $P_{Z|W}$ through the linear relationship

$$P_{Z|X}(z|x) = \sum_{w \in \mathcal{W}, y \in \mathcal{Y}} P_{Z|W}(z|w) P_{W|XY}(w|x,y) P_{Y|X}(y|x). \tag{4.2.3}$$

While general observation models $P_{W|XY}$ can be considered within this framework, particular structures may be of interest for certain applications. We highlight and explore the relationship between three specific cases for W, while allowing a general distribution P_{XY} between the sensitive and private data.

Full Data: In this case, P_{XY} is general but $W = (X, Y)$, capturing the situation when the mechanism has direct access to both the sensitive and useful information. For this case, the privacy-utility optimization problem of (4.2.1) reduces to

$$\begin{aligned} \pi_{\mathrm{FD}}(\delta) \triangleq \inf_{P_{Z|XY}} \; & I(X;Z) \\ \text{s.t. } & D(P_{YZ}) \leq \delta. \end{aligned} \tag{4.2.4}$$

Output Perturbation: In this case, P_{XY} is general but $W = Y$, capturing the

[2]This and all other statements involving conditional distributions are defined only for symbols in the support of the conditioned random variables.

situation when the mechanism only has direct access to the useful information. For this case, the privacy-utility optimization problem of (4.2.1) reduces to

$$\begin{aligned} \pi_{\mathrm{OP}}(\delta) \triangleq \inf_{P_{Z|Y}} \; & I(X;Z) \\ \text{s.t. } & D(P_{YZ}) \leq \delta, \end{aligned} \tag{4.2.5}$$

where $P_{Z|X}(z|x) = \sum_{y \in \mathcal{Y}} P_{Z|Y}(z|y) P_{Y|X}(y|x)$. Note: this optimization is equivalent to that of (4.2.4), with the Markov chain $X \to Y \to Z$ imposed as an additional constraint.

Inference: In this case, P_{XY} is general but $W = X$, capturing the situation when the mechanism only has direct access to the sensitive information and the useful information, such as a discrete hidden state, is not directly available or observable and needs to be *inferred* indirectly by processing the sensitive information. For this case, the privacy-utility optimization problem of (4.2.1) reduces to

$$\begin{aligned} \pi_{\mathrm{INF}}(\delta) \triangleq \inf_{P_{Z|X}} \; & I(X;Z) \\ \text{s.t. } & D(P_{YZ}) \leq \delta, \end{aligned} \tag{4.2.6}$$

where $P_{Z|Y}(z|y) = \sum_{x \in \mathcal{X}} P_{Z|X}(z|x) P_{X|Y}(x|y)$. Note: this optimization is equivalent to that of (4.2.4), with the Markov chain $Y \to X \to Z$ imposed as an additional constraint.

4.3 Convexity and Rate-Distortion Connections

Here we discuss how for certain combinations of utility metrics and data constraints, the resulting tradeoff problem is equivalent to generalized rate-distortion and privacy-utility problems encountered in the literature. We also indicate how the tradeoff optimizations of (4.2.4), (4.2.5), and (4.2.6) will become convex for certain utility metrics.

Note that in the general tradeoff optimization problem (4.2.1), the distributions $P_{Z|X}$ and $P_{Z|Y}$ are *linear* functions of the optimization variable $P_{Z|W}$ as shown by (4.2.2) and (4.2.3), while P_{XYW} and its marginals are fixed. Thus, the convexity properties of the problem will follow from the convexity properties of the privacy and distortion metrics as functions of $P_{Z|X}$ and $P_{Z|Y}$, respectively. The mutual information privacy metric $I(X;Z)$ is a *convex* objective function of $P_{Z|X}$ and hence also of the optimization variable in each of the three scenarios given by (4.2.4), (4.2.5), and (4.2.6). Thus, for all convex distortion functionals, the overall optimization problem will be convex. For example, any expected distortion utility metric $D(P_{YZ}) = E[d(Y,Z)]$ is a linear and therefore a convex functional.

The privacy-utility tradeoff problem as considered by [37, 44] assumes the output perturbation constraint (see (4.2.5)), while using expected distortion $D(P_{YZ}) = E[d(Y,Z)]$ as the utility metric, and mutual information $I(X;Z)$ as the privacy metric. Additionally, [44] also considers maximum information leakage,

$$\max_{z \in \mathcal{Z}} [H(X) - H(X|Z=z)]$$

as an alternative privacy metric. As noted by [44], the optimization problem for the full data scenario (see (4.2.4)) can be recast as an optimization with the output perturbation constraint, by redefining the useful data as $Y' := (X,Y)$ and the distortion function as $d'(Y',Z) := d(Y,Z)$. This approach allows one to solve the optimization problem for the full data scenario using an equivalent optimization problem appearing in the output perturbation scenario. However, the distinction between these two scenarios should not be overlooked, as the output perturbation scenario represents a fundamentally different problem where the sensitive data is not available, which in general results in a strictly smaller privacy-utility tradeoff region (see Theorem 4.4.3).

The inference scenario given by (4.2.6) with expected distortion $D(P_{YZ}) = E[d(Y,Z)]$ as the utility metric is equivalent to an indirect rate-distortion problem [49]. As shown

by Witsenhausen in [49], indirect rate-distortion problems can be converted to direct ones with the modified distortion metric $d'(x,z) := E[d(Y,Z)|X=x,Z=z] = \sum_{y\in\mathcal{Y}} d(y,z)P_{Y|X}(y|x)$ since $Y \to X \to Z$ forms a Markov chain.

When the utility metric is conditional entropy, i.e., $D(P_{YZ}) = H(Y|Z)$, the equivalent utility objective is to maximize the mutual information $I(Y;Z)$, and the distortion constraint can be equivalently written as $I(Y;Z) \geq \delta'$, where $\delta' := H(Y) - \delta$. Thus, this results in the optimization problem of choosing Z to minimize $I(X;Z)$ subject to a lower bound on $I(Y;Z)$. This problem in the inference scenario, where the additional Markov chain constraint $Y \to X \to Z$ is imposed, is equivalent to the Information Bottleneck problem considered in [50], which also provides a generalization of the Blahut-Arimoto algorithm [51] to perform this optimization. For the output perturbation scenario, where the additional Markov chain constraint $X \to Y \to Z$ is imposed, this problem is called the Privacy Funnel and was proposed by [52]. In all three scenarios, the optimization problems are non-convex as the feasible regions are non-convex, specifically, they are complements of convex regions.

4.4 Results

For a given (fixed) distribution P_{XY} between the sensitive and private data, we can study how the optimal privacy-utility tradeoff changes across the aforementioned three different cases of W. This is of practical interest, since the restrictions on W in the inference and output perturbation mechanisms might be considered not just for when these situations inherently arise in the given application, but also for simplifying mechanism design and optimization.

Since the optimization problems of (4.2.5) and (4.2.6) are equivalent to (4.2.4) with an additional Markov chain constraint, we immediately have that $\pi_{\mathrm{FD}}(\delta) \leq$

$\pi_{\mathrm{OP}}(\delta)$ and $\pi_{\mathrm{FD}}(\delta) \leq \pi_{\mathrm{INF}}(\delta)$ for any δ. This implies that the achievable privacy-utility regions of both the inference mechanism and output perturbation mechanism are contained within the achievable privacy-utility region of the full data mechanism, which intuitively follows since the full data mechanism only has more input data available. The next theorem establishes the general relationship between the inference and output perturbation tradeoff regions.

Theorem 4.4.1. ***(Output Perturbation better than Inference)*** *For any data model P_{XY} and distortion metric $D(P_{YZ})$, the achievable privacy-utility region for the output perturbation mechanism (when $W = Y$) contains the achievable privacy-utility region for the inference mechanism (when $W = X$), that is, $\pi_{OP}(\delta) \leq \pi_{INF}(\delta)$ for any δ.*

Combining the preceding theorem with the earlier observations, we have that $\pi_{\mathrm{FD}}(\delta) \leq \pi_{\mathrm{OP}}(\delta) \leq \pi_{\mathrm{INF}}(\delta)$ for any δ. Thus, in general, full data offers a better privacy-utility tradeoff than output perturbation, which in turn offers a better privacy-utility tradeoff than inference.

The next theorem establishes that for a certain class of joint distributions P_{XY}, the full data and output perturbation mechanisms achieve the same optimal privacy-utility tradeoff. Thus, for this class of P_{XY}, the full data mechanism design can be simplified to the design of output perturbation mechanism, which can ignore the sensitive data X without degrading the privacy-utility performance. Specifically, this class is a characterized by the joint distributions P_{XY} where the common information $C(X;Y) = I(X;Y)$. See Appendix C.1 for properties of common information.

Theorem 4.4.2. ***(Sufficient Conditions for the General Optimality of Output Perturbation)*** *For any distortion metric $D(P_{YZ})$ and any data model P_{XY}*

where $C(X;Y) = I(X;Y)$, the achievable privacy-utility region for the output perturbation mechanism (when $W = Y$) is the same as the achievable privacy-utility region for the full data mechanism (when $W = (X,Y)$), that is, $\pi_{OP}(\delta) = \pi_{FD}(\delta)$ for any δ.

Theorem 4.4.2 establishes that $C(X;Y) = I(X;Y)$ is a sufficient condition on P_{XY} such that, for any general distortion metric, full data mechanisms cannot provide better privacy-utility tradeoffs than the output perturbation mechanisms. Our next theorem gives the converse result, establishing that for data models where $C(X;Y) \neq I(X;Y)$, output perturbation mechanisms are generally suboptimal, that is, there exists a distortion metric such that the full data mechanisms provide a strictly better privacy-utility tradeoff.

Theorem 4.4.3. ***(Necessary Conditions for the General Optimality of Output Perturbation)*** *For any data model P_{XY} where $C(X;Y) \neq I(X;Y)$, there exists a distortion metric $D(P_{YZ})$ such that the achievable privacy-utility region for the output perturbation mechanism (when $W = Y$) is strictly smaller than the achievable privacy-utility region for the full data mechanism (when $W = (X,Y)$), that is, there exists $\delta \geq 0$ such that $\pi_{OP}(\delta) > \pi_{FD}(\delta)$.*

CHAPTER 5

CONCLUSIONS

This dissertation focuses on information theoretic formulation of secure data communication and private data sharing. In Chapter 2, we study the impact of a hybrid adversary, that arbitrarily jams or eavesdrops at a given block, on the secrecy capacity of point to point Gaussian block fading channels. We illustrate the necessity of receiver-to-transmitter feedback by considering two cases: 1) no feedback and 2) 1-bit feedback at the end of each block. For both cases, we bound the secrecy capacities. We show that, without any feedback, the secrecy capacity is zero if the eavesdropper channel power gain stochastically dominates the effective main channel power gain. We also observe that, the secrecy capacity vanishes asymptotically when the transmit power constraint and jamming power increase in the same order. However, even with 1-bit receiver feedback at the end of each block, the secrecy capacity is non-zero for the wide class of channel statistics as described in Remark 2.4.2. We also analyze the effects of multiple colluding/non-colluding adversaries and delay. We show that, with no feedback, multiple adversaries can hurt the secrecy capacity even more, as the secrecy capacity bounds are not affected by the cross-interference across the adversaries. Finally, we provide a novel time-sharing approach for the delay limited setting, and we show that α-outage secrecy capacity is positive whenever the secrecy capacity without any delay limitation is positive.

In Chapter 3, we study the physical-layer security of massive MIMO downlink

communication. We first consider *no training-phase jamming* attack in which the adversary jams *only* the data communication and eavesdrops *both* the data communication and training. We show that secure DoF attained in the presence of no training-phase jamming is as same as the DoF attained under no attack. This result shows the resilience of the massive MIMO against adversaries not jamming the training phase. Further, we propose a joint power allocation and beamforming strategy, called δ-conjugate beamfoming, using which we can establish information theoretic security without even a need for Wyner encoding as long as the number of antennas is above a certain threshold, evaluated in the sequel.

We next show the vulnerability of massive MIMO systems against the attack, called training-phase jamming in which the adversary jams and eavesdrops *both* the training and data communication. We show that the maximum secure DoF attained in the presence of training-phase jamming is zero. We then develop a defense strategy against training-phase jamming. We show that if the BS keeps the pilot signal assignments hidden from the adversary and extends the cardinality of the pilot signal set, a secure DoF equal to the maximum DoF attained under no attack can be achieved. We finally provide a discussion why standard computational-cryptographic key sharing methods can be considered as strong candidates to encrypt the pilot signal assignments and how they achieve a level of security that is comparable to information-theoretically secure key-generation methods.

In Chapter 4, we formulate the privacy-utility tradeoff problem when the data release mechanism has limited access to the entire data composed of useful and sensitive parts. Based on the information theoretic formulation, we compare the privacy-utility tradeoff regions attained by full data, output perturbation, and inference mechanisms, which have an access to entire data, only useful data, and only sensitive data, respectively.

We first observe that the full data mechanism provides the best privacy-utility tradeoff and then show that the output perturbation mechanism provides better privacy-utility tradeoff than the inference mechanism. We draw connections between common information and privacy-utility tradeoffs by providing a condition that results in the privacy-utility tradeoff regions attained by full data and output perturbation mechanisms equal. Specifically, we show that if the common and mutual information between useful and sensitive data are identical, the full data mechanism simplifies to the output perturbation mechanism. Conversely, we show that if the common information is not equal to mutual information, the tradeoff region achieved by full data mechanism is strictly larger than the one achieved by the output perturbation mechanism.

In this thesis, we attack privacy and security problems separately. Specifically, we do not take privacy of data at the receiver into account in our security research. Similarly, we do not consider the security of data against the adversary in our privacy research. In the future, we aim to develop algorithms that jointly establish privacy and security in wireless communications. Further research directions can be listed as follows:

- Deriving secrecy capacity of broadcast and multi access channels in the presence of hybrid half-duplex adversary
- Understanding the performance of zero-forcing beam forming under pilot contamination attack in the massive MIMO limit.
- Investigating the privacy-utility tradeoff problem for general privacy metrics and observation models, and evaluating the tradeoff regions attainable for non-trivial data models.

APPENDIX A: PROOFS IN CHAPTER 2

A.1 Proof of Theorem 2.3.1

Codebook Generation: Pick $R_s = C_s^-$ and $R_m = \mathbb{E}\left[\log\left(1+\frac{P_t H_m}{1+P_j H_z}\right)\right] - \epsilon$ for some $\epsilon > 0$. Generate codebook c containing independently and identically generated codewords $x_l^{NM}, l \in [1 : 2^{NMR_m}]$, each of which are drawn from $\prod_{k=1}^{NM} p_X(x_{lk})$. Here, $p_X(x)$ is the probability density function of complex Gaussian random variable with zero mean and variance P_t.

Encoding: To send message $w \in [1 : 2^{NMR_s}]$, the secrecy encoder draws index l from the uniform distribution whose sample space is $\left[(w-1)2^{NM(R_m-R_s)}+1 : w2^{NM(R_m-R_s)}\right]$. The channel encoder then transmits corresponding codeword, x_l^{NM}.

Decoding: Let y^{NM} be the received sequence. If the adversary is in the eavesdropping state, i.e, $\phi(i) = 0$, the channel decoder draws $g_z(i)$ from $G_z(i)$ and a noise sequence $s_j^N(i)$ from $S_j^N(i)$ to obtain

$$\hat{y}^N(i) = y^N(i) + g_z(i)s_j^N(i).$$

The channel decoder looks for a unique message $l \in [1 : 2^{NMR_m}]$ such that

$$\left(x_l^{NM}, (\hat{y}^{NM}, g_m^M, g_z^M)\right) \in \mathcal{A}_\epsilon^{NM}$$

, where $\mathcal{A}_\epsilon^{NM}\left(X^N, (\hat{Y}^N, G_m, G_z)\right)$ is the set of jointly typical $\left(x^{NM}, (\hat{y}^{NM}, g_m^M, g_e^M)\right)$ sequences with

$$\hat{Y}^N = G_m X^N + G_z S_j^N + S_m^N \tag{A.1.1}$$

Analysis of the probability error and secrecy: Random coding argument is used to show that there exists sequences of codebooks that satisfy the constraint (3.2.10) and (2.2.11) simultaneously. Since $R_m < \frac{1}{N} I\left(X^N; \hat{Y}^N, G_m, G_z\right) = \mathbb{E}\left[\log\left(1 + \frac{P_t H_m}{1 + P_j H_z}\right)\right]$, by the channel coding theorem [1], we have $\mathbb{E}_{\mathcal{C}}(P_\epsilon^{NM}(\mathcal{C})) \to 0$ as $M \to \infty$, where the expectation is over all random codebooks.

Define $R_e(c) \triangleq \frac{1}{NM} H(W|Z^{NM}, g^M, K^{NM}, \phi^M, c)$. Note that $R_e(c)$ represents the equivocation rate. Since we are studying the no feedback case, K^{NM} is null set, and we will omit feedback term K^{MN} from the equivocation terms in the rest of the section. In the secrecy analysis below, we show that the expectation of the equivocation rate over random codebooks, $\mathbb{E}_{\mathcal{C}}[R_e(\mathcal{C})]$ goes to R_s as $M \to \infty$, where

$$\mathbb{E}_{\mathcal{C}}[R_e(\mathcal{C})] = \frac{1}{NM} H(W|Z^{NM}, g^M, \phi^M, \mathcal{C}). \tag{A.1.2}$$

Note that

$$\begin{aligned}
&\frac{1}{NM} I(W; Z^{NM}|g^M, \phi^M, \mathcal{C}) \\
&= \frac{1}{NM} H(W) - \frac{1}{NM} H(W|Z^{NM}, g^M, K^{NM}, \phi^M, \mathcal{C}) \\
&= R_s - \mathbb{E}_{\mathcal{C}}[R_e(\mathcal{C})]
\end{aligned}$$

since W is uniformly distributed random variable on $[1 : 2^{NMR_s}]$. We observe that $\frac{1}{NM} I(W; Z^{NM}|g^M, \phi^M, \mathcal{C}) \to 0$ as $M \to \infty$. Hence, there exists a sequence of codebooks that satisfy both (3.2.10) and (2.2.11) since we have

$$\mathbb{E}_{\mathcal{C}}\left[P_\epsilon^{NM}(\mathcal{C}) + \frac{1}{NM} I(W; Z^{NM}|g^M, \phi^M, \mathcal{C})\right] \to 0$$

as $M \to 0$.

For the secrecy analysis, let's define $\hat{Z}^N(i) = X^N(i) g_e(i) + S_e^N(i)$, $1 \leq \forall i \leq M$. The equivocation analysis averaged over codebooks is as follows.

$$MNR_e(\mathcal{C}) = H(W|Z^{NM}, g^M, \mathcal{C})$$

$$
\begin{aligned}
&\overset{(a)}{=} H(W|Z^{NM}, g_e^M, \mathcal{C}) \\
&\overset{(b)}{\geq} H(W|\hat{Z}^{NM}, g_e^M, \mathcal{C}) \\
&= H(W, X^{NM}|\hat{Z}^{NM}, g_e^M, \mathcal{C}) - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&= H(X^{NM}|\hat{Z}^{NM}, g_e^M, \mathcal{C}) + H(W|X^{NM}, \hat{Z}^{NM}, g_e^M, \mathcal{C}) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&\geq H(X^{NM}|\hat{Z}^{NM}, g_e^M, \mathcal{C}) - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&= H(X^{NM}|g_e^M) - I(X^{NM}; \hat{Z}^{NM}|g_e^M, \mathcal{C}) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&\overset{(c)}{=} MNR_m - I(X^{NM}; \hat{Z}^{NM}|g_e^M, \mathcal{C}) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&\geq MNR_m - I(X^{NM}, \mathcal{C}; \hat{Z}^{NM}|g_e^M,) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&\overset{(d)}{=} MNR_m - I(X^{NM}; \hat{Z}^{NM}|g_e^M) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}) \\
&\geq MNR_m - N\sum_{i=1}^{M} \log(1 + P_t h_e(i)) \\
&\qquad\qquad - H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C})
\end{aligned}
$$

where (a) follows from the fact that $W \to Z^{NM}, G_e^M, \mathcal{C} \to G_m^M, G_z^M$ forms a Markov chain, (b) follows from the fact that conditioning reduces the entropy, (c) follows from the fact that codeword X^{NM} is uniformly distributed over a set of size 2^{NMR_m}, and (d) follows from the fact that

$$\mathcal{C} \to X^{NM} \to \hat{Z}^{NM} \tag{A.1.3}$$

forms Markov chain. We continue with the following steps.

$$
\begin{aligned}
&\frac{1}{MN} H\left(W|Z^{NM}, g_e^M, \mathcal{C}\right) \\
&\geq R_m - \sum_{i=1}^{M} \frac{1}{M} \log(1 + P_t h_e(i)) \\
&\qquad\qquad - \frac{1}{MN} H\left(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}\right) \\
&\overset{(e)}{\geq} R_m - \mathbb{E}\left[\log(1 + P_t H_e)\right] - \epsilon_1 \\
&\qquad\qquad - \frac{1}{MN} H\left(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}\right) \\
&\overset{(f)}{\geq} R_m - \mathbb{E}\left[\log(1 + P_t H_e)\right] - \epsilon_1 - \epsilon_2 \qquad \text{(A.1.4)} \\
&= R_s - \epsilon - \epsilon_3,
\end{aligned}
$$

where $\epsilon_3 = \epsilon_1 + \epsilon_2$. Here, for any $\epsilon_1 > 0$, (e) is satisfied for any $h_e^M \in B_M$ with $Pr[B_M] = 1$ and for sufficiently large M since

$$\lim_{M\to\infty} \frac{1}{M} \sum_{i=1}^{M} \log(1 + P_t H_e(i)) = \mathbb{E}\left[\log(1 + P_t H_e)\right]$$

with probability 1.

To have the inequality in (A.1.4), we need to bound equivocation term

$$\frac{1}{NM} H(X^{NM}|\hat{Z}^{NM}, W, g_e^M, \mathcal{C}).$$

In the encoding part, we mention that the secrecy encoder draws an index from the uniform distribution whose sample space is $\left[(w-1)2^{NM(R_m-R_s)} + 1 : w2^{NM(R_m-R_s)}\right]$ to send message w, and the channel encoder then maps the index to corresponding codeword, x^{NM}. Hence, the number of the candidate codewords corresponding to message w is $2^{NM(R_m-R_s)}$. Let us define $R_{me} \triangleq R_m - R_s$. Note that from the definitions of R_m and R_s, it easy to observe that $R_{me} = \mathbb{E}\left[\log(1 + P_t H_e)\right] - \epsilon$, where $\mathbb{E}\left[\log(1 + P_t H_e)\right]$ is the capacity of the eavesdropper channel. Thus, the adversary can find the transmitted codeword with a low error probability when message w

chosen by the encoder is revealed to the adversary. Let us define a probability of the event that the adversary cannot decode the transmitted codeword as: $E^{NM}(c) \triangleq \left[P\left(X^{NM} \neq \hat{X}^{NM} \middle| W = w, h_e^M, \mathcal{C} = c\right)\right]$, where $\hat{X}^{NM} = f(\hat{Z}^{NM}, g_e^M, W = w, \mathcal{C} = c)$ is the decoded codeword at the adversary. Also, define average of $E^{NM}(c)$ over random codebooks: $E^{NM} \triangleq \mathbb{E}_{\mathcal{C}}\left[E^{NM}(\mathcal{C})\right]$. Inequality (f) follows from the fact that

$$\frac{1}{MN} H\left(X^{NM} \middle| \hat{Z}^{NM}, W = w, g_e^M, \mathcal{C}\right) \overset{(a)}{\leq} E^{NM} R_{me} + \frac{1}{MN} H(E^{NM}) \overset{(b)}{\leq} \epsilon_2$$

for any $\epsilon_2 > 0$ and for sufficiently large M, where (a) follows from Fano's inequality and (b) follows the fact that $E^{NM} \to 0$ as $M \to \infty$ from the random coding argument since $R_{me} \leq \mathbb{E}\left[\log(1 + P_t H_e)\right]$. □

We now provide the proof of the upper bound in Theorem 2.3.1. Suppose that R_s is achievable rate. From definition (3.2.10)-(2.2.11) and Fano's inequality, we have

$$\min_{\phi(i):1\leq i\leq M} \frac{1}{NM} H\left(W | Z^{NM}, g^M, \phi^M\right) \geq R_s - a_{NM} \tag{A.1.5}$$

$$\max_{\phi(i):1\leq i\leq M} \frac{1}{NM} H\left(W | Y^{NM}, g^M, \phi^M\right) \leq b_{NM} \tag{A.1.6}$$

for any $h^M \in \mathcal{A}_M$ with $\mathbb{P}(\mathcal{A}_M) \geq 1 - c_{NM}$. Here, a_{NM}, b_{NM}, and c_{NM} go to zero as $N \to \infty$ and $M \to \infty$.

Adversary strategy $\phi(i) = 0,\ 1 \leq \forall i \leq M$ solves LHS of (A.1.5) and strategy $\phi(i) = 1,\ 1 \leq \forall i \leq M$ solves LHS of (A.1.6). Hence, we have

$$\frac{1}{NM} H\left(W | \hat{Z}^{NM}, g^M\right) \geq R_s - a_{NM} \tag{A.1.7}$$

$$\frac{1}{NM} H\left(W | \hat{Y}^{NM}, g^M\right) \leq b_{NM} \tag{A.1.8}$$

where

$$\hat{Y}^N(i) = g_m(i) X^N(i) + g_z(i) S_j^N(i) + S_m^N(i), \text{ and} \tag{A.1.9}$$

$$\hat{Z}^N(i) = g_e(i)X^N(i) + S_e^N(i), \qquad 1 \leq \forall i \leq M. \tag{A.1.10}$$

Here, the LHS of (A.1.5) equals to that of (A.1.7) since conditioning reduces the entropy and the LHS of (A.1.6) equals to that of (A.1.8) since $W \to Y^{NM} \to \hat{Y}^{NM}$ forms a Markov chain.

We now show that if R_s is achievable, we have

$$\frac{1}{NM} H(W|\hat{Z}^{NM}, G^M) \geq \tag{A.1.11}$$
$$\int_{\mathcal{A}_M} \frac{1}{NM} H(W|\hat{Z}^{NM}, g^M) f_{G^M}(g^M)\, dg^M$$
$$\geq \int_{\mathcal{A}_M} (R_s - a_{NM}) f_{G^M}(g^M)\, dg^M \tag{A.1.12}$$
$$\geq R_s - \delta_{NM}, \tag{A.1.13}$$

where $G^M = \left[G_m^M, G_e^M, G_z^M\right]$, $\delta_{NM} = -R_s c_{NM} - a_{NM} + a_{NM}c_{NM}$, and $\delta_{NM} \to 0$ as $N \to \infty$ and $M \to \infty$. Here, (A.1.12) follows from (A.1.7), and (A.1.13) follows from the fact that $P[\mathcal{A}_M] \geq 1 - c_{NM}$. Note that here, the message W is conditioned on random vector, G^M instead of g^M in (A.1.7). With the similar steps, we can show that

$$\frac{1}{NM} H(W|\hat{Y}^{NM}, G^M) \leq \epsilon_{NM}, \tag{A.1.14}$$

where $\epsilon_{NM} \to 0$ as $N \to \infty$ and $M \to \infty$. The upper bound, C_s^+ follows when we combine (A.1.13) and (A.1.14) with the following steps:

$$R_s \leq \frac{1}{NM} H(W|\hat{Z}^{NM}, G^M)$$
$$- \frac{1}{NM} H(W|\hat{Y}^{NM}, G^M) + \gamma_{NM} \tag{A.1.15}$$
$$\overset{(a)}{=} \frac{1}{NM} H(W|\tilde{Z}^{NM}, \tilde{G}_m^M, \tilde{G}_e^M, \tilde{G}_z^M)$$
$$- \frac{1}{NM} H(W|\tilde{Y}^{NM}, \tilde{G}_m^M, \tilde{G}_e^M, \tilde{G}_z^M) + \gamma_{NM} \tag{A.1.16}$$
$$= \frac{1}{NM} I(W; \tilde{Y}^{NM}|\tilde{Z}^{NM}, \tilde{G}_m^M, \tilde{G}_e^M, \tilde{G}_z^M) + \gamma_{MN}$$

$$\overset{(b)}{\leq} \frac{1}{NM} I(X^{NM}; \tilde{Y}^{NM} | \tilde{Z}^{NM}, \tilde{G}_m^M, \tilde{G}_e^M, \tilde{G}_z^M) + \gamma_{MN} \tag{A.1.17}$$

$$\overset{(c)}{\leq} \frac{1}{NM} \sum_{i=1}^{M} I(X^N(i), \tilde{Y}^N(i) | \tilde{Z}^N(i), \tilde{G}_m(i), \tilde{G}_e(i), \tilde{G}_z(i)) + \gamma_{NM} \tag{A.1.18}$$

$$\overset{(d)}{\leq} \frac{1}{NM} \sum_{i=1}^{M} \sum_{j=1}^{N} I\left(X(i,j), \tilde{Y}(i,j) \middle| \tilde{Z}(i,j), \tilde{G}_m(i), \tilde{G}_e(i), \tilde{G}_z(i)\right) + \gamma_{NM} \tag{A.1.19}$$

$$\overset{(e)}{\leq} \frac{1}{NM} \sum_{i=1}^{M} \sum_{j=1}^{N} \mathbb{E}\left[\left(\log\left(1 + \frac{P_{t_{ij}} \tilde{H}_m}{1 + P_j \tilde{H}_z}\right) - \log\left(1 + P_{t_{ij}} \tilde{H}_e\right)\right)^+\right] + \gamma_{NM} \tag{A.1.20}$$

$$\overset{(f)}{\leq} \mathbb{E}\left[\left(\log\left(1 + \frac{\frac{1}{NM}\sum_{i=1}^{M}\sum_{j=1}^{N} P_{t_{ij}} \tilde{H}_m}{1 + P_j \tilde{H}_z}\right) - \log\left(1 + \frac{1}{NM}\sum_{i=1}^{M}\sum_{j=1}^{N} P_{t_{ij}} \tilde{H}_e\right)\right)^+\right] + \gamma_{NM} \tag{A.1.21}$$

$$\overset{(g)}{\leq} \mathbb{E}\left[\left(\log\left(1 + \frac{P_t \tilde{H}_m}{1 + P_j \tilde{H}_z}\right) - \log\left(1 + P_t \tilde{H}_e\right)\right)^+\right] + \gamma_{NM}, \tag{A.1.22}$$

where the notation (i, j) indicates the j-th channel use of i-th block and $\gamma_{NM} = \delta_{NM} + \epsilon_{NM}$. Note that $\gamma_{NM} \to 0$ as N and $M \to \infty$. In (A.1.16), we define new random variables, i.e.,

$$\tilde{Y}^N(i) = \tilde{G}_m(i) X^N(i) + \tilde{G}_z(i) S_j^N(i) + S_m^N(i), \text{ and} \tag{A.1.23}$$

$$\tilde{Z}^N(i) = \tilde{G}_e(i) X^N(i) + S_e^N(i), \qquad 1 \leq \forall i \leq M. \tag{A.1.24}$$

and $\tilde{H}_m(i) = |\tilde{G}_m(i)|^2$, $\tilde{H}_e(i) = |\tilde{G}_e(i)|^2$, and $\tilde{H}_z(i) = |\tilde{G}_z(i)|^2$. Here,

$$\left\{\tilde{G}_e(1), \tilde{G}_e(2), \ldots, \tilde{G}_e(M)\right\}$$

are i.i.d random variables with $\tilde{G}_e(i) \sim p_{G_e}$, and G_e^M is independent from

$$\left(W, S_e^{NM}, S_j^{NM}, S_m^{NM}\right)$$

. In a similar way,

$$\left\{\left(\tilde{G}_m(1), \tilde{G}_z(1)\right), \left(\tilde{G}_m(2), \tilde{G}_z(2)\right), \ldots, \left(\tilde{G}_m(M), \tilde{G}_z(M)\right)\right\}$$

are i.i.d random vectors with $\left(\tilde{G}_m(i), \tilde{G}_z(i)\right) \sim p_{G_m,G_z}$, and $\left(G_m^M, G_z^M\right)$ are independent from $\left(W, S_e^{NM}, S_j^{NM}, S_m^{NM}\right)$.

For the derivation above, (a) follows from the fact $\left(W, Z^{NM}, G_e^M\right)$ and $\left(W, Y^{NM}, G_e^M\right)$ have the same joint pdf with $\left(W, \tilde{Z}^{NM}, \tilde{G}_e^M\right)$ and $\left(W, \tilde{Y}^{NM}, \tilde{G}_e^M\right)$, respectively. Furthermore, note that $W \to \hat{Z}^{NM}, G_e^M \to G_m^M, G_z^M$ and $W \to \tilde{Z}^{NM}, \tilde{G}_e^M \to \tilde{G}_m^M, \tilde{G}_z^M$ form Markov chain. In a similar way, $W \to \hat{Y}^{NM}, G_m^M, G_z^M \to G_e^M$ and $W \to \tilde{Y}^{NM}, \tilde{G}_m^M, \tilde{G}_z^M \to \tilde{G}_e^M$ form Markov chain. (b) follows from the fact that $W \to X^{NM}, \tilde{Z}^{NM}, \tilde{G}_m^M, \tilde{G}_e^M, \tilde{G}_z^M \to \tilde{Y}^{NM}$ forms a Markov chain. (c) and (d) follows from the memoryless property of the channel and from the fact conditioning reduces the entropy.

The power constraint in (2.2.6) implies that $\frac{1}{NM}\sum_{i=1}^{M}\sum_{j=1}^{N}\mathbb{E}\left[|X(i,j)|^2\right] \leq P_t$, where the expectation is taken over W. Also, note that $\tilde{G}(i) = \left[\tilde{G}_m(i), \tilde{G}_e(i), \tilde{G}_z(i)\right]$ and $X(i,j)$ are independent random variables. Define

$$P_{t_{ij}} \triangleq \mathbb{E}\left[|X(i,j)|^2\right] = \mathbb{E}\left[|X(i,j)|^2 | \tilde{G}(i) = g(i)\right]$$

. Then, (e) follows from the fact that Gaussian distribution maximizes the conditional mutual information [5]. In (A.1.21), (f) follows from the fact that

$$\left(\log(1 + P_{t_{ij}}x) - \log(1 + P_{t_{ij}}y)\right)^+$$

is a concave function of $P_{t_{ij}}$ for any $x \geq 0$ and $y \geq 0$ and from Jensen's inequality. Finally, (g) follows from the fact that

$$(\log(1 + Px) - \log(1 + Py))^+$$

is a non-decreasing function in P for any $x \geq 0$ and $y \geq 0$. . $\square$

A.2 Proof of Corollary 2.3.5

We have the following analysis:

$$\begin{aligned}
&\lim_{P\to\infty} C_s^+ \\
&\leq \lim_{P\to\infty} \mathbb{E}\left[\left(\log\left(1+\frac{P_t(P)H_m}{1+P_j(P)H_z}\right)-\log\left(1+P_t(P)H_e\right)\right)^+\right] \\
&\overset{(a)}{=} \mathbb{E}\left[\lim_{P\to\infty}\left(\log\left(1+\frac{P_t(P)H_m}{1+P_j(P)H_z}\right)-\log\left(1+P_t(P)H_e\right)\right)^+\right] \\
&= 0. \qquad \text{(A.2.1)}
\end{aligned}$$

Here, (a) follows from the dominant convergence theorem. To apply dominant convergence theorem, we need to show that

$$\begin{aligned}
&g_P(H_m, H_e, H_z) \\
&= \left(\log\left(1+\frac{P_t(P)H_m}{1+P_j(P)H_z}\right)-\log\left(1+P_t(P)H_e\right)\right)^+ \qquad \text{(A.2.2)}
\end{aligned}$$

is upper and lower bounded by random variables that have a finite expectation. Note that $g_P(H_m, H_e, H_z)$ is lower bounded by zero and upper bounded by $\log\left(1+\frac{P_t(P)H_m}{P_j(P)H_z}\right)$ with probability 1.

Since $P_t(P) = \mathcal{O}(P_j(P))$ as $P \to \infty$, there exists finite B and p_0 such that $P_t(P) \leq B \times P_j(P)$ for all $P > p_0$. We now show that $\mathbb{E}[g_P(H_m, H_e, H_z)]$ has a finite expectation for all $P > p_o$ with the following analysis:

$$\begin{aligned}
&\mathbb{E}[g_P(H_m, H_e, H_z)] \leq \mathbb{E}\left[\log\left(1+\frac{BH_m}{H_z}\right)\right] \qquad \text{(A.2.3)} \\
&= \mathbb{E}[\log(H_z + BH_m)] - \mathbb{E}[\log(H_z)] \\
&\leq \log\left(B\mathbb{E}[H_m] + \mathbb{E}[H_z]\right) - \mathbb{E}[\log(H_z)] \qquad \text{(A.2.4)}
\end{aligned}$$

$$\leq \log\left(B\mathbb{E}[H_m] + \mathbb{E}[H_z]\right) - \int_0^1 \log(h_z) f_{H_z}(h_z)\, dh_z \tag{A.2.5}$$

$$\leq \log\left(B\mathbb{E}[H_m] + \mathbb{E}[H_z]\right) - A\int_0^1 \log(h_z)\, dh_z \tag{A.2.6}$$

$$= \log\left(B\mathbb{E}[H_m] + \mathbb{E}[H_z]\right) + A\log(e) \tag{A.2.7}$$

$$< \infty, \tag{A.2.8}$$

for all $P > p_0$, where $A = \sup_{h_z} f_{H_z}(h_z)$. Here, (A.2.4) follows from the Jensen's inequality, (A.2.7) follows from the fact that $\int_0^1 \log(h_z) = -\log(e)$, and (A.2.8) follows from the fact that $\mathbb{E}[H_m], \mathbb{E}[H_z] < \infty$ and the pdf of H_z is bounded.

Since $\log\left(1 + \dfrac{P_t(P)H_m}{P_j(P)H_z}\right)$ is a continuous function of P, it is a bounded function on the closed interval $[0, p_0]$ with probability 1. Hence, $\mathbb{E}[g_P(H_m, H_e, H_z)] < \infty$ for all $P \geq 0$. □

A.3 Proof of Theorem 2.4.1

Codebook Generation: Fix $R > 0$ and $\epsilon > 0$. Pick $R_m = \dfrac{R}{\mathbb{E}[T]} - \epsilon$, where T is defined in Theorem 2.4.1. Generate codebook c containing independently and identically generated codewords $x_l^N, l \in [1 : 2^{NR}]$, each are drawn from $\prod_{k=1}^{N} p_X(x_{lk})$. Here, $p_X(x)$ is the distribution of complex Gaussian random variable with zero mean and variance P_t.

Encoding: To send message $w \in [1 : 2^{NMR_s^{\text{1-bit}}}]$, the secrecy encoder draws an index l from the uniform distribution whose sample space is

$$\left[(w-1)2^{NM(R_m - R_s^{\text{1-bit}})} + 1 : 2^{NM(R_m - R_s^{\text{1-bit}})}\right]$$

. Then, the secrecy encoder maps l into NMR_m bits and decompose NMR_m bits into groups of NR bits. To send the index l, the channel encoder transmits NR in each block by using codebook c. When NAK is received, the channel encoder sends the same bit group transmitted at the previous block.

We first define several terms. Define $r(i)$ as the required number of transmissions for the bit group that is successfully decoded on i-th block, $\mathcal{A}$ as the set of blocks on which decoding occurs successfully, i.e.,

$$\mathcal{A} \triangleq \left\{ i : \log\left(1 + \sum_{j=1}^{r(i)-1} \frac{P_t h_m(i-j)}{1 + P_j h_z(i-j)}\right) < R \right.$$
$$\left. \leq \log\left(1 + \sum_{j=1}^{r(i)} \frac{P_t h_m(i-j+1)}{1 + P_j h_z(i-j+1)}\right) \text{ and } 1 \leq i \leq M \right\}$$

and $R_w^*(M) \triangleq NR \sum_{i \in \mathcal{A}} 1$.

Consider a renewal process in which a renewal occurs when the accumulated mutual information associated with a bit group exceeds threshold R for the first time. Note that $R_w^*(M)$ is the accumulated reward (i.e., the number of sucessfully bits) at the receiver up to M-th block for the renewal process, where the reward at each renewal is NR bits.

We choose M such that $|\frac{1}{MN} R_w^*(M) - \frac{R}{\mathbb{E}[T]}| \leq \epsilon$ is satisfied for channel gains $(g_m^M, g_z^M) \in \mathcal{G}$ where $\mathcal{G}$ is a set with probability 1, i.e., $\mathbb{P}(\mathcal{G}) = 1$. A similar renewal-based approach for the ARQ transmission scheme was also used in [20].

Decoding: Let $y^N(i)$ be the received sequence. If the adversary is in the eavesdropping state, i.e., $\phi(i) = 0$, the channel decoder draws $g_z(i)$ from $G_z(i)$ and a noise sequence $s_j^N(i)$ from $S_j^N(i)$ to obtain

$$\hat{y}^N(i) = y^N(i) + g_z(i) s_j^N(i).$$

The channel decoder collects $y^N(i)$'s that correspond to the same bit group and apply MRC to these observations as explained in the proof sketch. Then, the channel decoder employs joint typicality decoding as in the no feedback case (mentioned in the Appendix A.1).

Secrecy Analysis: For the secrecy analysis, let's define $\hat{Z}^N(i) = X^N(i)g_e(i)+S_e^N(i)$, $1 \leq \forall i \leq M$. The equivocation analysis averaged over codebooks is as follows:

$$\mathbb{E}_{\mathcal{C}}[R_e(\mathcal{C})] = \frac{1}{MN} H(W|\{Z^N(i)\}_{i:\phi(i)=0}, g^M, \mathcal{C}) \tag{A.3.1}$$

$$\begin{aligned}
&\overset{(a)}{\geq} \frac{1}{MN} H(W|\hat{Z}^{NM}, g^M, \mathcal{C}) \\
&= \frac{1}{MN} H\left(W, \{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, g^M, \mathcal{C}\right) \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \qquad \text{(A.3.2)} \\
&\geq \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\mathcal{C}\right) \\
&\quad - \frac{1}{MN} I\left(\{X^N(i)\}_{i:i\in\mathcal{A}}; \hat{Z}^{NM}|g^M, \mathcal{C}\right) \\
&\qquad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \\
&= \frac{1}{MN} \sum_{i\in\mathcal{A}} H\left(X^N(i)|\hat{Z}^{NM}, \mathcal{C}, g^M\right) \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \\
&= \frac{1}{MN} \sum_{i\in\mathcal{A}} \left[H(X^N(i)) - I\left(X^N(i); \hat{Z}^{NM}|\mathcal{C}, g^M\right)\right]^+ \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \\
&\overset{(b)}{=} \frac{1}{MN} \sum_{i\in\mathcal{A}} \left[NR - I\left(X^N(i); \hat{Z}^N(i-r(i)+1:i)|\mathcal{C}, g^M\right)\right]^+ \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \qquad \text{(A.3.3)} \\
&\geq \frac{1}{MN} \sum_{i\in\mathcal{A}} \left[NR - I\left(X^N(i), \mathcal{C}; \hat{Z}^N(i-r(i)+1:i)|g^M\right)\right]^+ \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \\
&\overset{(c)}{=} \frac{1}{MN} \sum_{i\in\mathcal{A}} \left[NR - I\left(X^N; \hat{Z}^N(i-r(i)+1:i)|g^M\right)\right]^+ \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}}|\hat{Z}^{NM}, W, g^M, \mathcal{C}\right) \qquad \text{(A.3.4)} \\
&\overset{(d)}{=} \frac{1}{M} \sum_{i\in\mathcal{A}} \left[R - I\left(X; \hat{Z}_{(i-r(i)+1)\ldots,\hat{Z}_i}|g^M\right)\right]^+
\end{aligned}$$

$$
\begin{aligned}
&- \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}} | \hat{Z}^{NM}, W, g^M, \mathcal{C}\right) && \text{(A.3.5)}\\
&= \frac{1}{M}\sum_{i\in\mathcal{A}}\left[R - \log\left(1 + P_t \sum_{j=1}^{r(i)} h_e\left(i-j+1\right)\right)\right]^+ \\
&- \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}} | \hat{Z}^{NM}, W, g^M, \mathcal{C}\right) && \text{(A.3.6)}\\
&\overset{(e)}{\geq} C_s^{-1\text{-bit}} \\
&\quad - \frac{1}{MN} H\left(\{X^N(i)\}_{i:i\in\mathcal{A}} | \hat{Z}^{NM}, W, g^M, \mathcal{C}\right) - \epsilon && \text{(A.3.7)}\\
&\geq C_s^{-1\text{-bit}} - 2\epsilon && \text{(A.3.8)}
\end{aligned}
$$

for any $\epsilon > 0$ and for sufficiently large M. Here, (a) follows from the fact that conditioning reduces the entropy. In (A.3.3),

$$\hat{Z}^N(i-r(i)+1:i) = \left[\hat{Z}^N(i)\ldots, \hat{Z}^N(i-r(i)+1)\right]$$

is the vector of the observed signals at the adversary that corresponds to successfully received codeword $X^N(i)$. Here, (b) follows from the fact that $X^N(i)$ and $\{Z^N(j)\}_{j\notin(i-r(i)+1,\ldots,i)}$ are independent. In (A.3.4), (c) follows from the fact that $\mathcal{C} \to X^N(i) \to \hat{Z}^N(i), \ldots \hat{Z}^N(i-k+1)$ forms Markov chain. Here, $X^N(i)$ is not conditioned to codebook $\mathcal{C}$, hence $X^N(i) = X^N \sim \mathcal{CN}(0, P_t I_{N\times N})$. In (A.3.5),

$$\hat{Z}_k \triangleq X + N_k,\ k \in \{i-r(i)+1, \ldots, i\} \tag{A.3.9}$$

where N_k's are i.i.d and X and N_k are distributed with $\mathcal{CN}(0, P_t)$ and $\mathcal{CN}(0,1)$, respectively. In (A.3.5), (d) follows from the fact that

$$
\begin{aligned}
&p_{X^N, \hat{Z}^N(i-k+1:i)}\left(x^N, z^N(i-k+1:i)\right) = \\
&\prod_{j=1}^{N} p_X(x_j) p_{\hat{Z}_{(i-k+1:i)}}\left(z_j\left(i-k+1:i\right)|x_j, g\left(i-k+1:i\right)\right)
\end{aligned}
$$

where $z_j(i)$ denotes j-th element of i-th block. In (A.3.7), (e) follows from the renewal reward theorem, i.e., for sufficently large M, we have the following inequality

$$\left| \frac{1}{M} \sum_{i \in \mathcal{A}} \left[R - \log \left(1 + P_t \sum_{j=1}^{r(i)} h_e \left(i - j + 1 \right) \right) \right]^+ - \frac{1}{\mathbb{E}[T]} \mathbb{E} \left[R - \log \left(1 + P_t \sum_{i=1}^{T} \tilde{H}_e(i) \right) \right]^+ \right| \leq \epsilon \tag{A.3.10}$$

for all chanel gains (g_m^M, g_e^M, g_z^M) that construct a set with probability 1.

We can show that the second term in (A.3.7) goes to zero as $M \to \infty$ with the list decoding argument used in the proof of Theorem 2 of [7]. This concludes the proof. □

We now give the proof for Corollary 2.4.3. Since the proof is similar to the achievability proof of Theorem 2.4.1, we only present the differences in codebook generation, encoding, decoding, and secrecy analysis steps. In the codebook generation, R_m is selected as $R_m = Rp - \epsilon$, where p is defined in Theorem 2.4.1. Note that $p = 1/\mathbb{E}[T^*]$.

In the encoding step, we select M such that $|\frac{1}{MN} R_w^{**}(M) - \frac{R}{\mathbb{E}[T^*]}| \leq \epsilon$. Here, $R_w^{**}(M)$ is the accumulated reward (i.e., the number of sucesfully bits) at the receiver up to M-th block for the renewal process whose inter-renewal time is distributed with T^* and whose rewards at each renewal are NR bits.

In the decoding step, as opposed to the MRC approach, the receiver discards the received sequence, $y^N(i)$ if event $\mathcal{S}^c(i) = \left\{ \log \left(1 + \frac{P_t h_m(i)}{1 + P_j h_z(i)} \right) < R \right\}$ occurs. Consequently, the transmitter sends back a NAK signal. The receiver successfully decodes a bit group on i-th block if event $\mathcal{S}(i)$ occurs.

The secrecy analysis is same with the secrecy analysis in Theorem 2.4.1. □

We now provide the proof of the upper bound in Theorem 2.4.3. Instead of an arbitrary adversary strategy, we assume the adversary strategy on a block, $\phi(i)$ is a deterministic function of the instantaneous channel gains on the block, i.e., $\phi(i) =$

$f\left(g_m(i), g_e(i), g_z(i)\right)$. Since we constrain the adversary strategy, the secrecy capacity upper bound for this case is also the upper bound of the secrecy capacity of the original case in which the adversary strategy arbitrarily changes from one block to the next.

Suppose that R_s is an achievable secrecy rate. From definition (2.2.11), Fano's inequality and the analysis (A.1.11-A.1.13), we have

$$\frac{1}{NM} H(W|Z^{NM}, K^{MN}, G_m^M, G_e^M, G_z^M, \Phi^M) \geq R_s - \delta_{NM} \tag{A.3.11}$$

$$\frac{1}{NM} H(W|Y^{NM}, K^{MN}, G_m^M, G_e^M, G_z^M, \Phi^M) \leq \epsilon_{NM} \tag{A.3.12}$$

for any deterministic function, $f : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to [0, 1]$.

Here, $\Phi(i) = f\left(H_m(i), H_e(i), H_z(i)\right)$ and ϵ_{NM} and δ_{NM} go to zero as $N \to \infty$ and $M \to \infty$. The upper bound follows with following steps.

$$\begin{aligned} R_s &\leq \frac{1}{MN} \min_f H\left(W|Z^{NM}, K^{MN}, G_m^M, G_e^M, G_z^M, \Phi^M\right) \\ &\quad - H\left(W|Y^{NM}, K^{MN}, G_m^M, G_e^M, G_z^M, \Phi^M\right) + \gamma_{NM} \qquad \text{(A.3.13)} \\ &\leq \frac{1}{MN} \min_f I\left(W; Y^{NM}|Z^{NM}, K^{MN}, G_m^M, G_e^M, G_z^M, \Phi^M\right) \\ &\qquad\qquad + \gamma_{NM} \\ &\leq I\left(W; Y^{NM}, G_m^{MN}, G_z^{MN}|Z^{NM}, K^{MN}, G_e^{MN}, \Phi^M\right) + \gamma_{NM} \qquad \text{(A.3.14)} \end{aligned}$$

where $\gamma_{NM} = \delta_{NM} + \epsilon_{NM}$ and $\gamma_{NM} \to 0$ as $N \to \infty$ and $M \to \infty$. By using the following lemmas, we can reduce the mutual information term in (A.3.14) to a simplier form. Since Lemma A.3.1 and Lemma A.3.2 are similar to Lemma 1 and Lemma 2 of [**?**], respectively, we omit the proofs.

Lemma A.3.1. *For each block $i \in \{1, \ldots, M\}$, we have that*

$$\begin{aligned} &I\left(W; Y^{Ni}, G_m^M, G_z^M|Z^{Ni}, K^{Ni}, G_e^M, \Phi^M\right) \leq \\ &\quad I\left(W; Y^{Ni}, G_m^M, G_z^M|Z^{Ni}, K^{N(i-1)}, G_e^M, \Phi^M\right) \qquad \text{(A.3.15)} \end{aligned}$$

□

Lemma A.3.2. *For each block $i \in \{1, \ldots, M\}$, we have that*

$$
\begin{aligned}
&I\left(W; Y^{Ni}, G_m^M, G_z^M | Z^{Ni}, K^{N(i-1)}, G_e^M, \Phi^M\right) \leq \\
&I\left(W; Y^{N(i-1)}, G_m^M, G_z^M | Z^{N(i-1)}, K^{N(i-1)}, G_e^M, \Phi^M\right) \\
&+ I\left(X^N(i); Y^N(i) | Z^N(i), G_m(i), G_e(i), G_z(i), \Phi(i)\right)
\end{aligned} \tag{A.3.16}
$$

□

As in [**?**], by successively applying Lemma 1 and Lemma 2, we can show the following inequality.

$$
\begin{aligned}
&I\left(W; Y^{NM}, G_m^{MN}, G_z^{MN} | Z^{NM}, K^{MN}, G_e^{MN}, \Phi^M\right) \leq \\
&\sum_{i=1}^{M} I\left(X^N(i); Y^N(i) | Z^N(i), G_m(i), G_e(i), G_z(i), \Phi(i)\right).
\end{aligned}
$$

Hence, we have

$$
\begin{aligned}
&R_s - \gamma_{NM} \qquad\qquad (A.3.17)\\
&\leq \frac{1}{MN} \min_f \sum_{i=1}^{M} I\left(X^N(i); Y^N(i) | Z^N(i), G(i), \Phi(i)\right) \\
&\leq \frac{1}{MN} \min_f \sum_{i=1}^{M} \sum_{j=1}^{N} I\left(X(i,j); Y(i,j) | Z(i,j), G(i), \Phi(i)\right) \\
&\overset{(a)}{\leq} \min_f \\
&\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(\mathbb{E}\left[\log\left(1 + \frac{P_{t_{ij}} H_m(i)}{1 + P_j H_z(i)}\right) \middle| f(G(i)) = 1 \right] \times \right. \\
&\qquad\qquad \mathbb{P}\left(f(G(i)) = 1\right) + \\
&\left. \mathbb{E}\left[\log\left(1 + \frac{P_{t_{ij}} H_m(i)}{1 + P_{t_{ij}} H_e(i)}\right) \middle| f(G(i)) = 0 \right] \mathbb{P}(f(G(i)) = 0) \right) \\
&\overset{(b)}{\leq} \min_f \left(\mathbb{E}\left[\log\left(1 + \frac{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} P_{t_{ij}} H_m}{1 + P_j H_z}\right) \middle| f(G) = 1 \right] \right.
\end{aligned}
$$

$$\times \mathbb{P}\left(f(G)=1\right)+$$

$$\mathbb{E}\left[\log\left(1+\frac{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}P_{t_{ij}}H_m}{1+\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}P_{t_{ij}}H_e}\right)\middle| f(G)=0\right]$$

$$\times \mathbb{P}(f(G)=0)) \tag{A.3.18}$$

$$\overset{(c)}{\leq} \min_{f}\left(\mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+P_jH_z}\right)\middle| f(G)=1\right]\mathbb{P}\left(f(G)=1\right)\right.$$

$$\left.+\,\mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+P_tH_e}\right)\middle| f(G)=0\right]\mathbb{P}(f(G)=0)\right) \tag{A.3.19}$$

$$=\min_{f}\mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+P_jH_zf(G)+P_tH_e(1-f(G))}\right)\right] \tag{A.3.20}$$

$$\overset{(d)}{=}\mathbb{E}\left[\log\left(1+\frac{P_tH_m}{1+\max\left(P_tH_e,P_jH_z\right)}\right)\right], \tag{A.3.21}$$

where the notation (i,j) indicates the j-th channel use of i-th block, $G=[G_m,G_e,G_z]$, $H=[H_m,H_e,H_z]$, and $G(i)=[G_m(i),G_e(i),G_z(i)]$. The power constraint in (2.2.6) implies that $\frac{1}{NM}\sum_{i=1}^{M}\sum_{j=1}^{N}\mathbb{E}\left[|X(i,j)|^2\right]\leq P_t$, where the expectation is taken over W and $K^{(i-1)N}$. Also, note that $G(i)=[G_m(i),G_e(i),G_z(i)]$ and $X(i,j)$ are independent random variables. Define $P_{t_{ij}}\triangleq\mathbb{E}\left[|X(i,j)|^2\right]=\mathbb{E}\left[|X(i,j)|^2|G(i)=g(i)\right]$. Then, (a) follows from the fact that Gaussian distribution maximizes the conditional mutual information [**?**] for both values of $\Phi(i)$. In (A.3.18), (b) follows from Jensen's inequality and from the fact that $\log\left(1+P_{t_{ij}}x\right)$ and $\log\left(1+\frac{P_{t_{ij}}x}{1+P_{t_{ij}}y}\right)$ are concave functions of $P_{t_{ij}}$ for any $x\geq 0$ and $y\geq 0$. In (A.3.19), (c) follows from the fact that $(\log(1+Px)$ and $\log\left(1+\frac{Px}{1+Py}\right)$ are non-decreasing functions in P for any $x\geq 0$ and $y\geq 0$. In (A.3.21), (d) follows from the fact that $f(G)=I_{P_jH_z\geq P_tH_e}$ minimizes the expectation in (A.3.20), where $I_{x\geq a}=1$ if $x\geq a$; otherwise, $I_{x\geq a}=0$. □

A.4 Proof of Theorem 2.5.1

The decoding and encoding strategies are the same with the strategies used in the proof of Theorem 2.3.1. Therefore, we omit the probability error analysis and only

focus on the secrecy analysis. We pick $R_m = \mathbb{E}\left[\log\left(1+\frac{P_t H_m}{1+P_j\hat{H}_z}\right)\right] - \epsilon$ for some $\epsilon > 0$.

For the secrecy analysis, let's define $\hat{Z}_s^N(i) = X^N(i)g_{e_v}(i) + S_{e_v}^N(i)$, $1 \leq \forall v \leq V$, $1 \leq \forall i \leq M$. With the same steps used in the secrecy analysis of the proof of Theorem 2.3.1, we can get

$$\frac{1}{MN}H\left(W\middle|\left\{Z_v^N(i), g_{e_v}(i), \phi_v(i)\right\}_{1\leq i\leq M}, \mathcal{C}\right) \tag{A.4.1}$$

$$\geq L_s - \epsilon_1 - \frac{1}{MN}H\left(X^{NM}|\hat{Z}_v^{NM}, W, g_{e_v}^M, \mathcal{C}\right) \tag{A.4.2}$$

for any $\epsilon_1 > 0$ and sufficiently large M, where

$$L_v = \mathbb{E}\left[\log\left(1+\frac{P_t H_m}{1+P_j\hat{H}_z}\right) - \log\left(1+P_t H_{e_v}\right)\right].$$

We now show that, for any $\epsilon_2 > 0$,

$$\frac{1}{MN}H\left(X^{NM}|\hat{Z}_v^{NM}, W, g_e^M, \mathcal{C}\right) \leq L_v - C_s^{NC-} + \epsilon_2 \tag{A.4.3}$$

for sufficiently large M. To prove (A.4.3), suppose that codewords correspond to message W is partitioned into $2^{NM(L_v - C_s^{NC-})}$ groups. Let's define random variable T that represents the group index of X^{NM}. Then, we have

$$\frac{1}{MN}H\left(X^{NM}|\hat{Z}_v^{NM}, W, g_{e_v}^M, \mathcal{C}\right) \tag{A.4.4}$$

$$\leq \frac{1}{MN}H\left(X^{NM}, T|\hat{Z}_v^{NM}, W, g_{e_v}^M, \mathcal{C}\right) \tag{A.4.5}$$

$$\leq \frac{1}{MN}H\left(X^{NM}|T, \hat{Z}_v^{NM}, W, g_{e_v}^M, \mathcal{C}\right) + \frac{1}{MN}H(T) \tag{A.4.6}$$

$$\leq \epsilon_2 + L_v - C_s^{NC-}, \tag{A.4.7}$$

for any $\epsilon_2 > 0$ and sufficiently large M. Here, (A.4.7) follows from the random coding argument as in (A.1.4)) of the proof of Theorem 2.3.1. The proof follows when we combine (A.4.2) and (A.4.3). □

We now provide the upper bound. Suppose that R_s is achievable rate. From definition (3.2.10)-(2.2.11) and Fano's inequality, we have

$$\min_{1\le v\le V} \min_{\substack{\phi_j^M \\ 1\le j\le V}} \frac{1}{NM} H\left(W|Z_v^{NM}, g^M, \{\phi_j^M\}_{1\le j\le V}\right)$$

$$\geq R_s - a_{NM} \tag{A.4.8}$$

$$\max_{\substack{\phi_j^M \\ 1\le j\le V}} \frac{1}{NM} H\left(W|Y^{NM}, g^M, \{\phi_j^M\}_{1\le j\le V}\right)$$

$$\leq b_{NM} \tag{A.4.9}$$

for any $g^M \in \mathcal{A}_M$ where $g^M = \left[g_m^M, g_{e_1}^M, \dots g_{e_V}^M, g_{z_1}^M, \dots g_{z_V}^M, \{g_{f_{vj}}^M\}_{1\le v,j\le V}\right]$ with $\mathbb{P}(\mathcal{A}_M) \geq 1 - c_{NM}$. Here, a_{NM}, b_{NM}, and c_{NM} go to zero as $N \to \infty$ and $M \to \infty$.

For each adversary v, the adversary strategy $\phi_j(i) = 0$, $1 \le \forall i \le M, 1 \le \forall j \le V$ solves the inner minimization problem in the LHS of (A.4.8). The strategy $\phi_j(i) = 1$, $1 \le \forall i \le M, 1 \le \forall j \le V$ solves LHS of (A.4.9). Hence, we have

$$\min_{1\le v\le V} \frac{1}{NM} H\left(W|\hat{Z}_v^{NM}, g^M\right) \geq R_s - a_{NM} \tag{A.4.10}$$

$$\frac{1}{NM} H\left(W|\hat{Y}^{NM}, g^M\right) \leq b_{NM} \tag{A.4.11}$$

where

$$\hat{Y}^N(i) = g_m(i)X^N(i) + \sum_{v=1}^{V} g_{z_v}(i)S_{j_v}^N(i) + S_m^N(i) \tag{A.4.12}$$

$$\hat{Z}_v^N(i) = g_{e_v}(i)X^N(i) + S_e^N(i) \tag{A.4.13}$$

for $1 \le \forall i \le M$ and $1 \le \forall v \le V$. Here, the LHS of (A.4.8) equals to that of (A.4.10) since $W \to \hat{Z}_v^{NM} \to Z_v^{NM}$ and the LHS of (A.4.9) equals to that of (A.4.11) since $W \to Y^{NM} \to \hat{Y}^{NM}$ forms a Markov chain. Furthermore, note that

$$W \to \hat{Y}^{NM}, G_m^M, \{G_{z_v}\}_{1\le v\le V} \to G^M \backslash G_m^M, \{G_{z_v}\}_{1\le v\le V}$$

and

$$W \to \hat{Z}^{NM}, \{G_{e_v}\}_{1\leq v\leq V} \to G^M \backslash \{G_{e_v}\}_{1\leq v\leq V}$$

form Markov chains. The rest of the proof is similar to the proof of the upper bound given in Theorem 2.3.1. □

A.5 Proof of Theorem 2.6.1

Fix $\gamma \in [0,1]$, $\bar{\gamma} = 1-\gamma$, $\epsilon > 0$. Each consecutive M_1 blocks is called a superblock. Suppose that communication lasts $M = M_1 M_2$ blocks. Let us denote $x^{NM_1}(j)$, $y^{NM_1}(j)$, and $z^{NM_1}(j)$ as the transmitted signal, the received signal at the receiver, and the received signal at the adversary in superblock j, respectively. Denote $x^{\gamma N}(j,i)$ and $x^{\bar{\gamma}N}(j,i)$ as the transmitted signals in the first γN channel uses and in the next $\bar{\gamma}N$ channel uses of i-th block of j-th superblock, respectively. Signals $y^{\gamma N}(j,i)$, $y^{\bar{\gamma}N}(j,i)$, $z^{\gamma N}(j,i)$ and $z^{\bar{\gamma}N}(j,i)$ are defined in a similar way. Let $w(j,i)$ be the message to be transmitted in i-th block of j-th superblock. Finally, let $x^{\gamma NM_1}(j) \triangleq [x^{\gamma N}(j,1),\ldots,x^{\gamma N}(j,M_1)]$, and $y^{\gamma NM_1}(j), z^{\gamma NM_1}(j), x^{\bar{\gamma}NM_1}(j), y^{\bar{\gamma}NM_1}(j),$ and $x^{\bar{\gamma}NM_1}(j)$ are defined in a similar way. Through this appendix, (j,i) indicates i-th block of j-th superblock.

Encoding and decoding strategies are summarized in Figure A.1 and Figure A.2. We begin with key generation. Let $R_{r0} > 0$. At the beginning of superblock j, the transmitter picks key $k(j)$ from random variable $K(j)$ which is uniformly distributed in $\{1,\ldots,2^{NR_{r0}}\}$. By using the encoding strategy in the proof of Theorem 1, the transmitter maps $k(j)$ to codeword $x^{\gamma NM_1}(j)$. This process is repeated for every superblock $j \geq 1$. Next lemma provides a lower bound to achievable key rates.

Lemma A.5.1. *For any $\epsilon > 0$, there exit $N' > 0$, $M_1' > 0$ and a sequence of length*

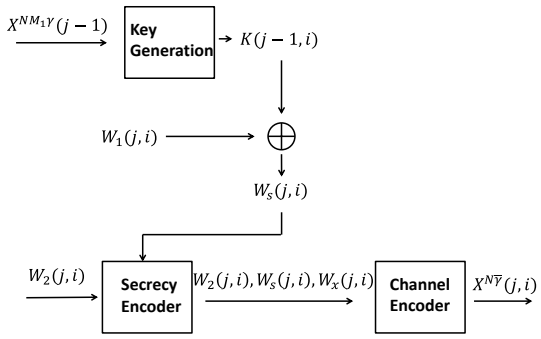

Figure A.1: Encoder structure.

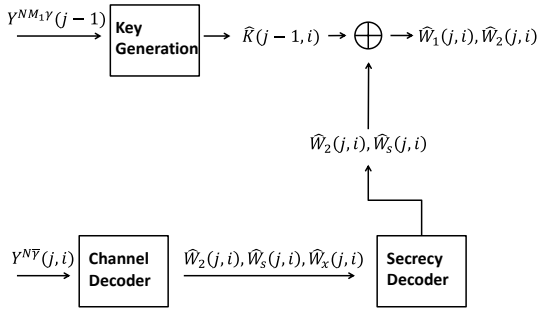

Figure A.2: Decoder structure.

γNM_1 channel codes $\left(\gamma NM_1, 2^{\gamma R_{r0} NM_1}\right)$ for which the following are satisfied under any strategy of the adversary, $\phi^{M_1}(j)$:

$$\mathbb{P}\left(K(j) \neq \hat{K}(j)\right) < \epsilon/3 \tag{A.5.1}$$

$$\frac{1}{NM_1} H\left(K(j) | \{Z^{\gamma NM_1}(j)\}, g^{M_1}(j), \phi^{M_1}(j)\right) > R_{r0} - \epsilon/2 \tag{A.5.2}$$

for any superblock $j \in \{1, 2, \ldots, M_2\}$, for any $N \geq N'$, and for any $M_1 \geq M_1'$ where $R_{r0} \leq \gamma C_s^-$. □

The proof follows from Theorem 1. Now, we describe the transmission of delay

limited message $w(j,i)$[1], illustrated in Figure A.1. Let $R_s \geq R_{r0}$ and $\tilde{R}_s \geq R_s$. Message $w(j,i)$ of size NR_s bits is divided[2] to two messages $w_1(j,i)$ and $w_2(j,i)$, of size NR_{r0} and $N(R_s - R_{r0})$, respectively. We also divide key $k(j-1)$, generated in previous superblock $j-1$, into M_1 equivalent size chunks such that $k(j-1) = [k(j-1,1)\ldots, k(j-1,M_1)]$, where $k(j-1,i)$ is of size NR_{r0} bits.

Let $w_s(j,i) = w_1(j,i) \oplus k(j-1,i)$. Suppose $w_x(j,i)$ is picked from random variable $W_x(j,i)$ which is uniformly distributed on sample space $\{1,\ldots,2^{N(\tilde{R}_s - R_s - \epsilon)}\}$ and independent from $W(j,i)$. We generate a Gaussian codebook consisting of $2^{N(\tilde{R}_s-\epsilon)}$ codewords each of which is independently drawn from $\prod_{k=1}^{\bar{\gamma}N} p_X(x_k)$. Here, $p_X(x)$ is the probability density function of complex Gaussian random variable with zero mean and variance P_t. To transmit $w(j,i) = (w_1(j,i), w_2(j,i))$, the codeword indexed by $(w_1(j,i), w_s(j,i), w_x(j,i))$ is transmitted.

Error and Equivocation Analysis:

Lemma A.5.2. *For any $\epsilon > 0$, there exit $N'' > 0$ and a sequence of length $\bar{\gamma}N$ channel codes $(\bar{\gamma}N, 2^{\bar{\gamma}\tilde{R}_s N})$ for which the following are satisfied*

$$\mathbb{P}\big((W_2(j,i), W_s(j,i), W_x(j,i)) \neq (\hat{W}_2(j,i), \hat{W}_s(j,i), \hat{W}_x(j,i))\big) < \epsilon/3 \tag{A.5.3}$$

for any $j \in \{1,2,\ldots M_2\}$, for any $i \in \{1,2,\ldots M_1\}$ and for any $N \geq N''$ when the channel conditions satisfy

$$\bar{\gamma}\log\left(1 + \frac{P_t h_m(j,i)}{1 + P_j h_z(j,i)}\right) \geq \tilde{R}_s. \tag{A.5.4}$$

□

[1]Due to Definition 2, we skip the message transmission at first M_1 blocks, and declare *secrecy outage*.

[2]Note that in this process, the messages are converted to binary form.

The proof follows from standard arguments, and is omitted. Assume for the error and equivocation analysis that N and M_1 are chosen such that $N = \max(N', N'', N''')$, and $M_1 = M_1'$, where N''' will be defined later. Then, error probability is bounded as

$$\begin{aligned}
&\mathbb{P}(\mathcal{E}(j,i)) \triangleq \mathbb{P}\big((W_1(j,i), W_2(j,i)) \neq (\hat{W}_1(j,i), \hat{W}_2(j,i))\big) \\
&\leq \mathbb{P}\left(\Big(W_2(j,i) \neq \hat{W}_2(j,i)\Big) \bigcup \Big(W_1(j,i) \neq \hat{W}_1(j,i)\Big)\right) \\
&\leq \frac{\epsilon}{3} + \mathbb{P}\left(W_1(j,i) \neq \hat{W}_1(j,i)\right) && \text{(A.5.5)} \\
&\leq \frac{\epsilon}{3} + \mathbb{P}\left(W_s(j,i) \neq \hat{W}_s(j,i) \bigcup K(j,i) \neq \hat{K}(j,i)\right) && \text{(A.5.6)} \\
&\leq \epsilon, && \text{(A.5.7)}
\end{aligned}$$

where (A.5.5) follows from Lemma A.5.2, (A.5.6) follows from the fact that $W_1(j,i) = W_s(j,i) \oplus K(j,i)$ and (A.5.7) follows from Lemma A.5.1 and Lemma A.5.2.

For the secrecy analysis, let's define $\hat{Z}^N(j,i) = X^N(j,i)g_e(j,i) + S_e^N(j,i)$, $1 \leq \forall j \leq M_1$, $1 \leq \forall i \leq M_2$. Equivocation analysis averaged over codebooks is as follows. Note that all the equivocation terms below are conditioned on the channel gains g^M, and we omit them for the sake of simplicity.

$$\begin{aligned}
&H(W_1(j,i), W_2(j,i) | Z^{NM}, W^M \backslash W(j,i), \mathcal{C}) \\
&\geq H(W_1(j,i), W_2(j,i) | \hat{Z}^{NM}, W^M \backslash W(j,i), \mathcal{C}) && \text{(A.5.8)} \\
&= H(W_2(j,i) | \hat{Z}^{NM}, W^M \backslash W(j,i), \mathcal{C}) \\
&\quad + H(W_1(j,i) | \hat{Z}^{NM}, W^M \backslash W(j,i), W_2(j,i), \mathcal{C}) && \text{(A.5.9)}
\end{aligned}$$

We now bound the first term in (A.5.9).

$$\begin{aligned}
&H(W_2(j,i) | \hat{Z}^{NM}, W^M \backslash W(j,i), \mathcal{C}) \\
&= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{NM}, W^M \backslash W(j,i) | \mathcal{C}) && \text{(A.5.10)} \\
&= H(W_2(j,i)) \\
&- I(W_2(j,i); \hat{Z}^{N\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j) \backslash W(j,i) | \mathcal{C}) && \text{(A.5.11)}
\end{aligned}$$

$$= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C})$$

$$- I(W_2(j,i); \hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j)\backslash\hat{Z}^{N\bar{\gamma}}(j,i),$$

$$W^{M_1}(j)\backslash W(j,i)|\hat{Z}^{N\bar{\gamma}}(j,i), \mathcal{C}) \tag{A.5.12}$$

$$\geq H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C})$$

$$- I(W_2(j,i); K(j-1,i), \hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j)\backslash\hat{Z}^{N\bar{\gamma}}(j,i),$$

$$W^{M_1}(j)\backslash W(j,i)|\hat{Z}^{N\bar{\gamma}}(j,i), \mathcal{C}) \tag{A.5.13}$$

$$= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C})$$

$$- I(W_2(j,i); K(j-1,i), \hat{Z}^{NM_1\gamma}(j-1)|\hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C}) \tag{A.5.14}$$

$$= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C})$$

$$- I(W_2(j,i); K(j-1,i)|\hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C})$$

$$- I(W_2(j,i); \hat{Z}^{NM_1\gamma}(j-1)|K(j-1,i), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C}) \tag{A.5.15}$$

$$= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C})$$

$$- I(W_2(j,i); \hat{Z}^{NM_1\gamma}(j-1)|K(j-1,i), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C}) \tag{A.5.16}$$

$$= H(W_2(j,i)) - I(W_2(j,i); \hat{Z}^{N\bar{\gamma}}(j,i)|\mathcal{C}) \tag{A.5.17}$$

$$= H(W_2(j,i)|\hat{Z}^{N\bar{\gamma}}(j,i), \mathcal{C})$$

$$\geq R_s - R_{r0} - N\epsilon/2, \tag{A.5.18}$$

where (A.5.11) follows from the fact that

$$\hat{Z}^{NM}\backslash\left(\hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j)\right), W^{M}\backslash W^{M_1}(j)$$

are independent from the rest of the random variables in (A.5.10) for every codebook.

(A.5.16) follows from the fact that $K(j-1,i)$ and

$$\Big(W_2(j,i), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C}\Big)$$

are independent due to the fact that $K(j-1,i) \rightarrow W_1(j,i) \oplus K(j-1,i), \mathcal{C} \rightarrow W_2(j,i), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), \mathcal{C}$ forms Markov chain, and $K(j-1,i)$ and

$$(W_1(j,i) \oplus K(j-1,i), \mathcal{C})$$

are independent. (A.5.17) follows from the fact $\hat{Z}^{NM_1\gamma}(j-1) \rightarrow K(j-1,i), \mathcal{C} \rightarrow W_2(j,i), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}\backslash W(j,i)$ forms Markov chain. Following the same steps in the equivocation analysis in Theorem 2.3.1, we can show that (A.5.18) is satisfied for any $N \geq N^{'''}$ if $\tilde{R}_s - (R_s - R_{r0}) \geq \log(1 + Ph_e(j,i))$. Next, we bound the second term in (A.5.9).

$$\begin{aligned}
&H(W_1(j,i)|\hat{Z}^{NM}, W^M\backslash W(j,i), W_2(j,i), \mathcal{C}) \\
&= H(W_1(j,i)|\hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j), W^{M_1}(j)\backslash W(j,i), W_2(i,j), \mathcal{C}) && \text{(A.5.19)} \\
&\geq H(W_1(j,i)|\hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j), A) && \text{(A.5.20)} \\
&= H(K(j-1,i)|\hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j), A) && \text{(A.5.21)} \\
&= H(K(j-1,i)) - I(K(j-1,i); \hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j), A) && \text{(A.5.22)} \\
&= H(K(j-1,i)) - I(K(j-1,i); \hat{Z}^{NM_1\gamma}(j-1), \hat{Z}^{NM_1\bar{\gamma}}(j)|A) && \text{(A.5.23)} \\
&= H(K(j-1,i)) - I(K(j-1,i); \hat{Z}^{NM_1\gamma}(j-1)|A) \\
&- I(K(j-1,i); \hat{Z}^{NM_1\bar{\gamma}}(j)|\hat{Z}^{NM_1\gamma}(j-1), A) && \text{(A.5.24)} \\
&= H(K(j-1,i)) - I(K(j-1,i); \hat{Z}^{NM_1\gamma}(j-1)|\mathcal{C}) \\
&- I(K(j-1,i); \hat{Z}^{NM_1\bar{\gamma}}(j)|\hat{Z}^{NM_1\gamma}(j-1), A) && \text{(A.5.25)} \\
&= H(K(j-1,i)) - N\epsilon/2 \\
&- I(K(j-1,i); \hat{Z}^{NM_1\bar{\gamma}}(j)|\hat{Z}^{NM_1\gamma}(j-1), A) && \text{(A.5.26)} \\
&= NR_{r0} - N\epsilon/2, && \text{(A.5.27)}
\end{aligned}$$

where $A = \left(W^{M_1}(j)\backslash W(j,i), W_2(j,i), W_s(j,i), \mathcal{C}\right)$. Here, (A.5.20) follows from the fact in (A.5.11), (A.5.21) follows from the fact that $W_s(j,i) = W_1(j,i) \oplus K(j-1,i)$, (A.5.23) follows from the fact that $K(j-1,i)$ and A are independent, and (A.5.25) follows from the fact that $\left(K(j-1), \hat{Z}^{NM_1\gamma}(j-1), \mathcal{C}\right)$ are independent of $\left(W^{M_1}(j)\backslash W(j,i), W_2(j,i), W_s(j,i)\right)$. From Lemma A.5.1, we observe that (A.5.26) is satisfied for any $N \geq N^{'}$ and for any $M \geq M_1^{'}$ if $R_{r0} \leq \gamma C_s^-$. (A.5.27) follows from the fact that $K(j-1,i) \rightarrow \hat{Z}^{NM_1\gamma}(j-1), A \rightarrow \hat{Z}^{NM_1\bar{\gamma}}(j)$ forms Markov chain. Combining (A.5.18) and (A.5.27), we can observe

$$H(W_1(i), W_2(i)|Z^{NM}, W^{NM}\backslash W(i)) \geq N(R_s - \epsilon), \tag{A.5.28}$$

if $\tilde{R}_s - (R_s - R_{r0}) \leq \log(1 + Ph_e(j,i))$ and $R_{r0} \leq \min(\gamma C_s^-, R_s)$.

We can observe that α-outage secrecy capacity is lower bounded by R_s if there exists $\left(R_s, \tilde{R}_s, R_{r0}, \gamma\right)$ that satisfy the following conditions: 1)

$$\mathbb{P}\left(\left\{(1-\gamma)\log\left(1+\frac{P_t H_m}{1+P_j H_z}\right) \geq \tilde{R}_s\right\} \bigcap \left\{\tilde{R}_s - R_s + R_{r0} \geq (1-\gamma)\log(1+P_t H_e) I_{R_s \neq R_{r0}}\right\}\right) \geq 1-\alpha, \tag{A.5.29}$$

2) $R_{r0} \leq \min\left(R_s, \gamma C_s^-\right)$, 3) $R_s \leq \tilde{R}_s$, and 4) $\gamma \in [0,1]$. Notice that the second event in the probability term is equal to $\left\{\left[\tilde{R}_s - (1-\gamma)\log(1+P_t H_e)\right]^+ \geq R_s - R_{r0}\right\}$.

Let's define set $\mathcal{A}$ containing $\left(R_s, \tilde{R}_s, R_{r0}, \gamma\right)$'s that satisfy these four conditions. The lower bound to α outage secrecy capacity can be written as $C_{s_d}^-(\alpha) = \max_{R_s, \tilde{R}_s, R_{r0}, \gamma \in A} R_s$. It is easy to observe that if $R_s = C_{s_d}^-(\alpha)$, the corresponding R_{r0} has to be equal to γC_s^-. Then, the lower bound can be written as

$$C_{s_d}^-(\alpha) = \max_{R_s, \tilde{R}_s, R_{r0}, \gamma \in \mathcal{A}} R_s \tag{A.5.30}$$

$$\text{subject to } R_{r0} = \gamma C_s^-$$

(A.5.31)

which concludes the proof. □

APPENDIX B: PROOFS IN CHAPTER 3

B.1 Proof of Theorem 3.3.1

We first evaluate an upper bound on the secure DoF. In order to derive an upper bound, we assume that there is a single user and no adversary in the system. Further, we assume that the user and the BS have a perfect information of the channel gains. As a last assumption, the user is assumed to know the received pilot signals at the BS. Hence, with these assumptions, the communication model in Section 2 reduces to a multiple input single output (MISO) communication set-up in which the channel gains and pilot signals are available at the BS and the user. Note that the capacity, the supremum of the achievable rates, of this new set-up upper bounds the secrecy rates achieved under the communication set-up explained in Section 3.2. We derive the capacity with the following analysis:

$$C = \max_{p\left(x^{T_d}|h_1,y^{T_r}\right),\mathbb{E}\left[tr\left(X^{T_d}X^{T_d*}\right)\right]\leq\rho_f T_d} \frac{1}{T} I\left(X^{T_d}; Y_1^{T_d}|Y^{T_r}, H_1\right) \tag{B.1.1}$$

$$= \max_{p\left(x^{T_d}|h_1\right),E\left[tr\left(X^{T_d}X^{T_d*}\right)\right]\leq\rho_f T_d} \frac{1}{T} I\left(X^{T_d}; Y_1^{T_d}|H_1\right) \tag{B.1.2}$$

$$= \max_{p(x|h_1),\mathbb{E}[tr(XX^*)]\leq\rho_f} \frac{T_d}{T} I(X;Y|H_1) \tag{B.1.3}$$

$$= \max_{\mathbb{E}[P(H_1)]\leq\rho_f} \frac{T_d}{T}\mathbb{E}\left[\log\left(1+P\left(H_1\right)||H_1||^2\right)\right] \tag{B.1.4}$$

where X^{T_d} is a complex $T_d \times M$ matrix and $P(\cdot) : \mathbb{C}^M \to \mathbb{R}^+ \cup \{0\}$ is a power allocation function. In the derivation above, (B.1.1) follows from Section 7.4.1 of [53] where the capacity of a communication system in which the channel gains are available at both encoder and decoder is stated. The equality in (B.1.2) follows from the fact that $Y_1^{T_r} \to X^{T_d}, H_1 \to Y_1^{T_d}$ forms a Markov chain and the equality in (B.1.3) follows from the fact that

$$I\left(X^{T_d}; Y_1^{T_d} | H_1\right) \leq \sum_{i=1}^{T_d} I(X_i; Y_i | H_1) \tag{B.1.5}$$

and from the fact that the equality is attained in (B.1.5) if $p_{X^{T_d}|H_1}\left(x^{T_d}|h_1\right) = \prod_{i=1}^{T_d} p_{X|H_1}(x_i|h_1)$. Then, the RHS and the LHS of (B.1.5) becomes $I(X; Y|H_1)$.

In (B.1.4), the equality follows from Section of [54], where the capacity of MISO system is evaluated. In [54], the power allocation function maximizing (B.1.4) is given as

$$P\left(h_1\right) = \left(\lambda_M - \frac{1}{||h_1||^2}\right)^+,$$

where λ_M is a non-negative real number and is chosen such that $\mathbb{E}[P(H_1)] = \rho_f$. We next find an upper bound on λ_M with the following analysis:

$$\begin{aligned}
\rho_f &= \mathbb{E}\left[\left(\lambda_M - \frac{1}{||H_1||^2}\right)^+\right] \\
&\geq \lambda_M - \mathbb{E}\left[\frac{1}{||H_1||^2}\right] &\text{(B.1.6)} \\
&= \lambda_M - \frac{1}{M-1} &\text{(B.1.7)}
\end{aligned}$$

where (B.1.6) follows from the fact that $\frac{1}{||H_1||^2}$ is distributed with inverse Gamma distribution and has a mean of $\frac{1}{M-1}$. Hence, we have $\lambda_M \leq \frac{1}{M-1} + \rho_f$ for $M > 1$. We next bound the DoF of the MISO communication system as

$$\lim_{M\to\infty} \frac{T_d}{T} \frac{E\left[\log\left(1 + P\left(H_1\right)||H_1||^2\right)\right]}{\log M}$$

$$\leq \lim_{M\to\infty} \frac{T_d}{T} \frac{E\left[\log\left(1+\lambda_M||H_1||^2\right)\right]}{\log M} \tag{B.1.8}$$

$$\leq \lim_{M\to\infty} \frac{T_d}{T} \frac{\log\left(1+\lambda_M E\left[||H_1||^2\right]\right)}{\log M} \tag{B.1.9}$$

$$= \lim_{M\to\infty} \frac{T_d}{T} \frac{\log\left(1+\lambda_M M\right)}{\log M}$$

$$\leq \lim_{M\to\infty} \frac{T_d}{T} \frac{\log\left(1+\frac{M}{M-1}+M\rho_f\right)}{\log M} \tag{B.1.10}$$

$$= \frac{T_d}{T} + \lim_{M\to\infty} \frac{T_d}{T} \frac{\log\left(\frac{1}{M}+\frac{1}{M-1}+\rho_f\right)}{\log M}$$

$$= \frac{T_d}{T}, \tag{B.1.11}$$

where (B.1.8) follows from the fact that $P(\cdot) \leq \lambda_M$ for all realizations of H_1, (B.1.9) follows from Jensen's inequality, and (B.1.10) follows from (B.1.7). In (B.1.11), we show that secure DoF can be at most $\frac{T_d}{T}$. □

Next, we describe an achievability strategy to attain secure DoF of $\frac{T_d}{T}$.

Channel estimation: Pilot signals are mutually orthogonal, i.e.,

$$\phi_k \times \phi_l^* = \begin{cases} T_r\rho_r & \text{if } k = l \\ 0 & \text{if } k \neq l \end{cases}$$

for any $k, l \in \{1, \ldots, K\}$. The BS employs MMSE for channel estimation. The estimated gain of the channel connecting the BS to k-th user is as follows:

$$\hat{H}_k = aH_k + bV_k \tag{B.1.12}$$

for $k \in \{1, \ldots, K\}$, where $a \triangleq \frac{\rho_r T_r}{\rho_r T_r + 1}$, $b \triangleq \frac{\sqrt{\rho_r T_r}}{\rho_r T_r + 1}$, and V_k is additive Gaussian noise distributed with $\mathcal{CN}(0, I_M)$. Note that $\mathbb{E}\left[\hat{H}_k\right] = 0_{1\times M}$, $\mathbb{E}\left[||\hat{H}_k||^2\right] = Ma$. Further, for any $k \in \{1, \ldots, K\}$ and for any $m, n \in \{1, \ldots, M\}$, $\mathbb{E}\left[\left|\hat{H}_{k,n}^* H_{k,m}\right|^2\right] = a^2 + a$ if $m = n$, otherwise; $\mathbb{E}\left[\left|\hat{H}_{k,m}^* H_{k,n}\right|^2\right] = a^2$.

Codebook generation: Pick $R_k = \frac{T_d}{T}\log\left(1+\frac{M\rho_k a}{\rho_f+\rho_j+1}\right) - \frac{T_d}{T}\log\left(1+M_e\rho_k\right)$

and $\hat{R}_k = \frac{T_d}{T}\log\left(1+\frac{M\rho_k a}{\rho_f+\rho_j+1}\right)-\epsilon_1$ for some $\epsilon_1>0$ and for $k=1,\ldots,K$. Generate K codebooks, c_k, $k=1,\ldots,K$, where K is the number of users. Codebook c_k contains independently and identically generated codewords, $s_{kl}^{BT_d}$, $l\in\{1,\ldots,2^{BT\hat{R}_k}\}$, each is drawn from $\mathcal{CN}(\mathbf{0},\rho_k I_{BT_d})$.

Encoding: In order to send k-th user's message $w_k\in\mathcal{W}_k$, the encoder draws index l_k from the uniform distribution that has a sample space of

$$\left\{(w_k-1)\,2^{BT\left(\hat{R}_k-R_k\right)}+1,\ldots,w_k 2^{BT\left(\hat{R}_k-R_k\right)}\right\}$$

. Note that this mapping makes the encoder *stochastic*. The encoder then maps index l_k to the corresponding codeword $s_{kl_k}^{BT_d}$ in codebook c_k.

The encoder employs a conjugate beamforming to map codewords to channel input sequence X^{BT_d}. The channel input at j-th channel use of i-th block can be written as follows:

$$X(i,j)=\sum_{k=1}^{K} s_{kl_k}(i,j)\frac{1}{\sqrt{M\alpha_k}}\hat{H}_k^*(i)$$

where $\alpha_k=a$ for all $k\in\{1,\ldots,K\}$ due to the fact that $\mathbb{E}\left[|\hat{H}_{k,m}|^2\right]=a$ for all $k\in\{1,\ldots,K\}$.

Decoding Each user employs typical set decoding [1]. Let $y_k^{BT_d}$ be the received signal at k-th user over BT_d channel uses. The decoder at k-th user looks for an unique index $l_k\in\left\{1,\ldots,2^{BT_dR_k}\right\}$ such that $\left(s_{kl_k}^{BT_d},y_k^{BT_d}\right)\in\mathcal{A}_\epsilon^{BT_d}\left(S_k^{T_d},Y_k^{T_d}\right)$, where $\mathcal{A}_\epsilon^{BT_d}\left(S_k^{T_d},Y_k^{T_d}\right)$ is the set of jointly typical sequences $(s_k^{BT_d},y_k^{BT_d})$ with

$$\begin{aligned}Y_k^{T_d}&=\frac{1}{\sqrt{Ma}}H_k\hat{H}_k^*S_k^{T_d}\\&\quad+\frac{1}{\sqrt{Ma}}\sum_{j=1,j\neq k}^{K}H_j\hat{H}_j^*S_j^{T_d}+H_{jam,k}V_{jam}+V_k\end{aligned}$$

where $S_j^{T_d}$ is distributed with $\mathcal{CN}\left(\mathbf{0},\rho_k I_{T_d}\right)$, $j=1,\ldots,K$ and V_k is distributed with $\mathcal{CN}\left(\mathbf{0},I_{T_d}\right)$.

Probability error and equivocation analysis By the channel coding theorem [1], $\mathbb{E}[P_e] \to 0$ as $B \to \infty$ if $\hat{R}_k < \frac{T_d}{T} I\left(S_k^{T_d}, Y_k^{T_d}\right)$, $k = 1, \ldots, K$, where expectation is over random codebooks, $\mathcal{C}_1, \ldots, \mathcal{C}_K$. Note that codebook c_k is the realization of $\mathcal{C}_k$. Define

$$
\begin{aligned}
T_0 &\triangleq \frac{1}{\sqrt{Ma}} S_k \mathbb{E}\left[H_k \hat{H}_k^*\right] \\
T_1 &\triangleq \frac{1}{\sqrt{Ma}} S_k \left(\mathbb{E}\left[H_k \hat{H}_k^*\right] - H_k \hat{H}_k^*\right) \\
T_2 &\triangleq \frac{1}{\sqrt{Ma}} \sum_{j=1, j\neq k}^{K} H_k \hat{H}_j^* S_j \\
T_3 &\triangleq H_{jam,k} V_{jam} + V_k.
\end{aligned}
$$

Note that $\mathbb{E}[T_0] = \mathbb{E}[T_1] = \mathbb{E}[T_2] = \mathbb{E}[T_3] = 0$ and $\mathbb{E}[T_0 T_1^*] = \mathbb{E}[T_0 T_2^*] = \mathbb{E}[T_0 T_3^*] = 0$. We can bound $\frac{T_d}{T} I\left(S_k^{T_d}, Y_k^{T_d}\right)$ as

$$
\begin{aligned}
&\frac{T_d}{T} I\left(S_k^{T_d}, Y_k^{T_d}\right) \\
&\geq \frac{T_d}{T} \log\left(1 + \frac{\mathbb{V}ar[T_0]}{\mathbb{V}ar[T_1 + T_2 + T_3]}\right) && \text{(B.1.13)} \\
&= \frac{T_d}{T} \log\left(1 + \frac{\mathbb{V}ar[T_0]}{\mathbb{V}ar[T_1] + \mathbb{V}ar[T_2] + \mathbb{V}ar[T_3]}\right) && \text{(B.1.14)} \\
&= \frac{T_d}{T} \log\left(1 + \frac{M\rho_k a}{\rho_f + \rho_{jam} + 1}\right), && \text{(B.1.15)}
\end{aligned}
$$

where (B.1.13) follows from Theorem 1 of [55] and (B.1.14) follows from the fact that T_1, T_2, and T_3 are uncorrelated random variables. The equality in (B.1.15) follows from the fact that $\mathbb{V}ar[T_0] = M\rho_k a$, $\mathbb{V}ar[T_1] = \rho_k$, $\mathbb{V}ar[T_2] = \sum_{j\neq k} \rho_j$, and $\mathbb{V}ar[T_3] = \rho_{jam} + 1$. From (B.1.15), we conclude that $\hat{R}_k \leq \frac{T_d}{T} I\left(S_k^{T_d}, Y_k^{T_d}\right)$. Hence, $\mathbb{E}[P_e] \to 0$ as $B \to \infty$.

We next analyze the secrecy constraint in (3.2.11). Let $H\left(W_k | Z^{TB}, H^B, \hat{H}^B, H_e^B, \mathcal{C}\right)$ be the expectation of the conditional entropy in (3.2.11) over random codebooks

$\mathcal{C} \triangleq [\mathcal{C}_1, \ldots, \mathcal{C}_K]$. We show that the expectation satisfies the constraint in (3.2.11) for k-th user with the following analysis:

$$
\begin{aligned}
& H\left(W_k \middle| Z^{BT}, G^B, \mathcal{C}\right) \geq H\left(W_k \middle| Z^{BT}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& = H\left(W_k \middle| Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.16)} \\
& = H\left(W_k, S_k^{BT_d} \middle| Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad - H\left(S_k^{BT_d} \middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& \geq H\left(S_k^{BT_d} \middle| Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad - H\left(S_k^{BT_d} \middle| W_k, Z^{TB}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& = H\left(S_k^{BT_d} \middle| S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad\quad - I\left(S_k^{BT_d}; Z^{BT_d} \middle| S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad\quad - H\left(S_k^{BT_d} \middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) \\
& = H\left(S_k^{BT_d} \middle| \mathcal{C}_k\right) - I\left(S_k^{BT_d}; Z^{BT_d} \middle| S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad\quad - H\left(S_k^{BT_d} \middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.17)} \\
& = BT\hat{R}_k - I\left(S_k^{BT_d}; Z^{BT_d} \middle| S^{BT_d}, G^B, \mathcal{C}\right) \\
& \qquad\quad - H\left(S_k^{BT_d} \middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.18)} \\
& \geq BT\hat{R}_k - I\left(S_k^{BT_d}, \mathcal{C}; Z^{BT_d} \middle| S^{BT_d}, G^B\right) \\
& \qquad\quad - H\left(S_k^{BT_d} \middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.19)}
\end{aligned}
$$

where $G^B \triangleq \left[H^B, \hat{H}^B, H_e^B\right]$. Signal set $S^{BT_d} \triangleq \left\{S_i^{BT_d}\right\}_{i \neq k}$ is defined to be the transmitted codewords of the users except k-th user. Signals Z^{BT_r} and Z^{BT_d} are the received signals at the adversary over the training phases and data communication phases, respectively. Note that $Z^{BT} \triangleq \left[Z^{BT_r},\ Z^{BT_d}\right]$.

In the above derivation (B.1.16) follows from the fact that Z^{BT_r} and

$$(G^B, W_k, S^{BT_d}, Z^{BT_d}, \mathcal{C})$$

are independent, (B.1.17) follows from the fact that $(S_k^{BT_d}, \mathcal{C}_k)$ are independent from $(G^B, \{\mathcal{C}_i\}_{i\neq k})$, and (B.1.18) follows from the fact that $S_k^{BT_d}$ is uniformly distributed on a set of size $2^{BT\hat{R}_k}$. We continue the derivation as

$$\begin{aligned}
\text{(B.1.19)} &= BT\hat{R}_k - I\left(S_k^{BT_d}; Z^{BT_d}\middle| S^{BT_d}, G^B\right) \\
&\quad - H\left(S_k^{BT_d}\middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.20)} \\
&\geq BT\hat{R}_k \\
&\quad - \sum_{i=1}^{B}\sum_{j=T_r+1}^{T} I\left(S_k(i,j); Z(i,j)\middle| S(i,j), G(i)\right) \\
&\quad - H\left(S_k^{BT_d}\middle| W_k, Z^{BT_d}, S^{BT_d}, G^B, \mathcal{C}\right) \\
&\geq BT\hat{R}_k \\
&\quad - \sum_{i=1}^{B}\sum_{j=T_r+1}^{T} \mathbb{E}\left[\log\left(1+\frac{\rho_k}{Ma}\sum_{m=1}^{M_e}\left|\hat{H}_k H_{e,m}^*\right|^2\right)\right] \\
&\quad - H\left(S_k^{BT_d}\middle| W_k, Z^{BT}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.21)} \\
&\geq BT\hat{R}_k - BT_d\log\left(1+\frac{\rho_k}{Ma}\sum_{m=1}^{M_e}\mathbb{E}\left[\left|\hat{H}_k H_{e,m}^*\right|^2\right]\right) \\
&\quad - H\left(S_k^{BT_d}\middle| W_k, Z^{BT}, S^{BT_d}, G^B, \mathcal{C}\right) \\
&= BT\hat{R}_k - BT_d\log\left(1+M_e\rho_k\right) \\
&\quad - H\left(S_k^{BT_d}\middle| W_k, Z^{BT}, S^{BT_d}, G^B, \mathcal{C}\right) && \text{(B.1.22)} \\
&\geq BT\left(\hat{R}_k - \frac{T_d}{T}\log\left(1+M_e\rho_k\right)\right) - BT\epsilon_2 && \text{(B.1.23)} \\
&= BT\left(R_k - \epsilon\right) && \text{(B.1.24)}
\end{aligned}$$

for any $\epsilon_2 > 0$ and sufficiently large B, where $\epsilon \triangleq \epsilon_1 + \epsilon_2$ and $H_{e,m}$ in (B.1.21) denotes the gain of the channel connecting m-th antenna at the BS to the adversary. The equality in (B.1.20) follows from the fact that $\mathcal{C} \to S_k^{T_d B}, S^{T_d B}, G^B \to Z^{T_d B}$ forms a Markov chain. The equality in (B.1.22) is due to the fact that $\mathbb{E}\left[\left|\hat{H}_k^* H_{e,m}\right|^2\right] = Ma$, $m = 1, \ldots, M_e$.

To get the inequality in (B.1.23), we need to bound

$$\frac{1}{BT}\, H\left(S_k^{BT_d}\middle|\, W_k, Z^{TB}, S^{BT_d}, G^B, \mathcal{C}\right).$$

Define $R_e \triangleq \hat{R}_k - R_k$. Note that $R_e < \frac{1}{T}\, I\left(S_k^{T_d}; Z^{T_d}\middle|\, S^{T_d}, G\right) = \frac{T_d}{T}\log\left(1 + M_e\rho_k a\right)$. Hence, as in (52) of [56], utilizing Fano's inequality and the channel coding theorem, we show that $\lim_{B\to\infty} \frac{1}{BT}\, H\left(S_k^{BT_d}\middle|\, W_k, Z^{TB}, S^{BT_d}, G, \mathcal{C}\right) = 0$.

From the fact that $\mathbb{E}\left[P_e\right] \to 0$ as $B \to \infty$ and from (B.1.24), we conclude that there exists a sequence of codes satisfying constraints (3.2.10) and (3.2.11). We now evaluate degree of freedom d_k associated with R_k as

$$\begin{aligned} d_k = \lim_{M\to\infty} \frac{R_k}{\log M} &= \frac{T_d}{T} + \lim_{M\to\infty} \frac{T_d}{T}\log\left(1 + M_e\rho_k\right) \\ &= \frac{T_d}{T} \end{aligned}$$

for $k = 1, \ldots, K$. Hence, the attained secure DoF is equal to $\frac{T_d}{T}$. □

B.2

B.2.1 Proof of Theorem 3.3.4

Note that since the adversary keeps silent during the training phases, the received signals at the BS over training phases are independent from H_e^B. Hence, we conclude that $\hat{H}^B \triangleq \left[\hat{H}_1^B, \ldots, \hat{H}_K^B\right]$ and H_e^B are independent.

The BS picks message rates $R_k > 0$, $k = 1, \ldots, K$. The equivocation rate for a code $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ utilizing deterministic encoding mapping functions, f_k, $k = 1, \ldots, K$ and δ-conjugate beamforming is as follows:

$$\begin{aligned} &\frac{1}{BT}\, H\left(W_k\middle|\, Z^{BT}, G^B\right) \\ &= \frac{1}{BT}\, H\left(W_k\middle|\, Z^{BT_d}, G^B\right) \\ &\geq \frac{1}{BT}\, H\left(W_k\middle|\, Z^{BT_d}, S^{BT_d}, G^B\right) \end{aligned} \tag{B.2.1}$$

$$
\begin{aligned}
&= \frac{1}{BT} H\left(W_k \middle| S^{BT_d}, G^B\right) \\
&\qquad - \frac{1}{BT} I\left(W_k; Z^{BT_d} \middle| S^{BT_d}, G^B\right) \\
&= R_k - \frac{1}{BT} I\left(W_k; Z^{BT_d} \middle| S^{BT_d}, G^B\right) && \text{(B.2.2)} \\
&\geq R_k - \frac{1}{BT} I\left(S_k^{BT_d}; Z^{BT_d} \middle| S^{BT_d}, G^B\right) && \text{(B.2.3)} \\
&\geq R_k - \frac{1}{BT} \sum_{i=1} \sum_{j=1} I\left(S_k(i,j); Z(i,j) \middle| S(i,j), G(i)\right) \\
&\geq R_k - \frac{1}{BT} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} \\
&\qquad \log\left(1 + \frac{P_k(i,j)}{M^{1+\delta}\alpha_k} \sum_{m=1}^{M_e} \mathbb{E}\left[\left|\hat{H}_k^* H_{e,m}\right|^2\right]\right) && \text{(B.2.4)} \\
&\geq R_k - \frac{T_d}{T} \log\left(1 + \frac{\rho_k}{M^{1+\delta}\alpha_k} \sum_{m=1}^{M_e} \mathbb{E}\left[\left|\hat{H}_k^* H_{e,m}\right|^2\right]\right) && \text{(B.2.5)} \\
&= R_k - \frac{T_d}{T} \log\left(1 + \frac{M_e \rho_k}{M^{\delta}}\right) && \text{(B.2.6)} \\
&\geq R_k - \epsilon
\end{aligned}
$$

for any $\epsilon > 0$ and for sufficiently large M, where $G \triangleq \left[H^B, \hat{H}^B, H_e^B\right]$. Particularly, for a given $\epsilon > 0$ if $M \geq \left(\frac{M_e \rho_k}{2^{\frac{T}{T_d}\epsilon} - 1}\right)^{\frac{1}{\delta}}$, then there exists a code that satisfies the constraint in (3.2.12).

In the above derivation, (B.2.1) follows from the fact that Z^{BT_r} and (Z^{BT_d}, G^B, W_k) are independent, (B.2.2) follows from the facts that W_k is independent from S^{BT_d}, G^B and uniformly distributed on $[1 : 2^{BTR_k}]$. In (B.2.3), the inequality follows from the fact that $W_k \to S_k^{BT_d} \to Z^{BT_d}, S^{BT_d}, G^B$.

In (B.2.4), $P_k(i,j) \triangleq \mathbb{E}\left[||S_k(i,j)||^2\right]$, where the expectation is over W_k. In (B.2.5), the inequality follows from Jensen's inequality and from the fact that

$$
\frac{1}{BT_d} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} P_k(i,j) \leq \rho_k.
$$

In (B.2.6), the equality follows from the fact $\hat{H}_k$ and $H_{e,m}$ are independent and $\mathbb{E}\left[\left|\hat{H}_k^* H_{e,m}\right|^2\right] = M\alpha_k$, $k = 1, \ldots, K$.

B.2.2 Proof of Corollary 3.3.5

Pick $0 < \delta < 1$. Pick arbitrary $\epsilon > 0$ and rate tuple $R = [R_1, \ldots, R_K]$. Let $M \geq \max(V(R), S(\epsilon))$. Note that inequality $M > V(R)$ implies that

$$R_k < \frac{T_d}{T} \log\left(1 + \frac{M^{1-\delta} a \rho_k}{M^{-\delta}\rho_f + \rho_j + 1}\right)$$

, $k = 1, \ldots, K$. We first show that there exists $B(\epsilon) > 0$ and a sequence of codes $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ utilizing δ-beamforming and deterministic mapping, that satisfy the decodability constraint in (3.2.10) for $B \geq B(\epsilon)$.

The same channel estimation strategy in Appendix A is used. Codebook generation is as same as the one in Appendix B.1. The BS generates K codebooks, c_k, $k = 1, \ldots, K$, where c_k contains 2^{BTR_k} codewords, $s_{kl}^{BT_d}$, $l \in \{1, \ldots, 2^{BTR_k}\}$.

To send k-th user's message $w_k \in \mathcal{W}_k = \left\{1, \ldots, 2^{BTR_k}\right\}$, the BS maps message w_k to the corresponding codeword $s_{kw_k}^{BT_d}$ in codebook c_k. Note that there is no randomization in the mapping as opposed to the mapping in the encoding in Appendix B.1, where the codeword is a stochastic function of the message. The BS employs δ-conjugate beamforming to map codewords to channel input sequence X^{BT_d}. The channel input at j-th channel use of i-th block can be written as

$$X(i,j) = \sum_{k=1}^{K} s_{kw_k}(i,j) \frac{1}{\sqrt{M^{1+\delta}\alpha_k}} \hat{H}_k^*(i) \tag{B.2.7}$$

where $\alpha_k = a$ and a is defined in (B.1.12).

The typical set decoding is used at each user as in the proof of Theorem 3.3.1 in Appendix B.1. Hence, since $R_k < \frac{1}{T} I\left(S_k^{BT_d}; Y_k^{BT_d}\right)$, $k = 1, \ldots, K$, by the channel coding theorem, there exists a sequences of codes that satisfy constraint (3.2.10).

In addition, since $M \geq S(\epsilon)$, the sequence of codes mentioned above satisfy the secrecy constraint in (3.2.11) due to Theorem 3.3.4. Hence, the proof of Corollary 3.3.5 follows. □

B.3

B.3.1 Proof of Theorem 3.4.1

Throughout the proof, we assume that the BS employs conjugate beamforming without loss of generality. Suppose that R_k is an achievable rate. From the constraints (3.2.10)-(3.2.11) and Fano's inequality, we have

$$\frac{1}{BT} H\left(W_k | Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right) \geq R_k - \delta_B \tag{B.3.1}$$

$$\frac{1}{BT}\, H\left(W_k |\, Y_k^{BT_d}\right) \leq \epsilon_B \tag{B.3.2}$$

where ϵ_B and δ_B go to zero as $B \to \infty$.

The LHS of (B.3.1) can be written as follows

$$\begin{aligned}
&\frac{1}{BT} H\left(W_k | Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right) \\
&= \frac{1}{BT} H\left(W_k | Z^{BT_d}, \hat{H}^B, H_e^B\right) && \text{(B.3.3)} \\
&= \frac{1}{BT} H\left(W_k | \tilde{Z}^{BT_d}, \tilde{H}^B, H_k^B\right) && \text{(B.3.4)} \\
&= \frac{1}{BT} H\left(W_k | \tilde{Z}^{BT_d}, \tilde{H}^B, H^B\right) && \text{(B.3.5)}
\end{aligned}$$

where $\tilde{H}(i) \triangleq \left[\hat{H}_1(i), \ldots, \tilde{H}_k(i), \ldots, \hat{H}_K(i)\right]$ and

$$\begin{aligned}
\tilde{Z}(i,j) \triangleq\ & \frac{1}{\sqrt{M\alpha_k}} H_k(i) \tilde{H}_k^*(i) S_k(i,j) \\
& + \sum_{l=1, l\neq k}^{K} \frac{1}{\sqrt{M\alpha_l}} H_l(i) \tilde{H}_l^*(i) S_l(i,j) + W
\end{aligned} \tag{B.3.6}$$

for $1 \leq i \leq B$ and $T_d + 1 \leq j \leq T$. The equality in (B.3.3) follows from the fact that $H^B \to Z^{BT_d}, \hat{H}^B, H_e^B \to W_k$ forms a Markov chain and the equality in (B.3.4)

follows from the fact that the joint distribution of $W_k, Z^{BT_d}, H_e^B, \hat{H}_1^B, \ldots, \hat{H}_k^B, \ldots \hat{H}_K^B$ is identical with that of $W_k, \tilde{Z}^{BT_d}, H_k^B, \hat{H}_1^B, \ldots, \tilde{H}_k^B, \ldots, \hat{H}_K^B$. The equality in (B.3.5) follows from the fact that $H^B/H_k^B \to \tilde{Z}^{BT_d}, \hat{H}_1^B, \tilde{H}^B \to W_k$ forms a Markov chain.

The upper bound on R_k can be derived with the following steps:

$$
\begin{aligned}
R_k &\leq \frac{1}{BT} H\left(W_k \middle| Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right) \\
&\qquad - \frac{1}{BT} H\left(W_k \middle| Y_k^{BT_d}\right) + \gamma_B && \text{(B.3.7)} \\
&= \frac{1}{BT} H\left(W_k \middle| \tilde{Z}^{BT_d}, \tilde{H}^B, H^B\right) \\
&\qquad - \frac{1}{BT} H\left(W_k \middle| Y_k^{BT_d}\right) + \gamma_B && \text{(B.3.8)} \\
&\leq \frac{1}{BT} H\left(W_k \middle| \tilde{Z}^{BT_d}, \tilde{H}^B, H^B\right) \\
&\quad - \frac{1}{BT} H\left(W_k \middle| \tilde{Z}^{BT_d}, \tilde{H}^B, H^B\right) + \gamma_B && \text{(B.3.9)} \\
&= \frac{1}{BT} I\left(W_k; Y_k^{BT_d} \middle| \tilde{Z}^{BT_d}, \tilde{H}^B, H^B\right) \\
&\leq \frac{1}{BT} I\left(S^{BT_d}; Y_k^{BT_d} \middle| \tilde{Z}^{BT_d}, G^B\right) + \gamma_B && \text{(B.3.10)} \\
&\leq \frac{1}{BT} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} I\left(S(i,j); Y_k(i,j) \middle| \tilde{Z}(i,j), G\right) + \gamma_B && \text{(B.3.11)} \\
&= \int \frac{1}{BT} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} I\left(S(i,j); Y_k(i,j) \middle| Z(i,j), g\right) \\
&\qquad\qquad p_G(g)\, \mathrm{d}g + \gamma_B, && \text{(B.3.12)}
\end{aligned}
$$

where $\gamma_B \triangleq \epsilon_B + \delta_B$, $G^B \triangleq \left[H^B, \tilde{H}^B\right]$, and $G \triangleq \left[H, \tilde{H}\right]$. In the derivation above, (B.3.7) follows from (B.3.1) and (B.3.2), and (B.3.9) follows from the fact that conditioning reduces the entropy. The inequality in (B.3.10) follows from the fact that $W_k \to S^{BT_d} \to Y_k^{BT_d}, \tilde{Z}^{T_d}, G^B$. The inequality in (B.3.11) follows from the memoryless property of the channel and from the assumption in Theorem 3.4.1, stating that $\left(\tilde{H}(i), H(i)\right)$ have an identical probability distribution for any $i \geq 1$. We continue

the upper bound derivation with the following steps:

$$(\text{B.3.12}) \leq \int \frac{1}{BT} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} I\left(S_G(i,j); Y_k(i,j) |\, \tilde{Z}(i,j), g\right)$$

$$p_G(g)\, \mathrm{d}g + \gamma_B \tag{B.3.13}$$

$$\leq \frac{T_d}{T} \int I\left(S_G; Y_k |\, Z, g\right) p_G(g)\, \mathrm{d}g + \gamma_B \tag{B.3.14}$$

$$\leq \frac{T_d}{T} \int \Bigg[\max_{\Sigma \in \mathcal{S}} \left(\log\left(1 + c_k \Sigma c_k^*\right) - \right.$$

$$\left. \log\left(1 + c_e \Sigma c_e^*\right) \right)^+ p_G(g)\, \mathrm{d}g + \gamma_B \tag{B.3.15}$$

$$\leq \frac{T_d}{T} \mathbb{E} \Bigg[\max_{\Sigma \in \mathcal{S}} \left(\left[\log\left(1 + C_k \Sigma C_k^*\right) - \right.\right.$$

$$\left.\left. \log\left(1 + C_e \Sigma C_e^*\right) \right]^+ \right) \Bigg] + \gamma_B, \tag{B.3.16}$$

where C_k and C_e are $1 \times K$ random vectors and are defined as

$$C_k \triangleq \left[\frac{H_k \hat{H}_1^*}{\sqrt{M\alpha_1}}, \ldots, \frac{H_k \hat{H}_k^*}{\sqrt{M\alpha_k}}, \ldots \frac{H_k \hat{H}_K^*}{\sqrt{M\alpha_K}} \right]$$

and $C_e \triangleq \left[\frac{H_k \hat{H}_1^*}{\sqrt{M\alpha_1}}, \ldots, \frac{H_k \tilde{H}_k^*}{\sqrt{M\alpha_k}}, \ldots, \frac{H_k \hat{H}_K^*}{\sqrt{M\alpha_K}} \right]$. Further, c_k and c_e are the realizations of C_k and C_e, respectively. Define Σ_{ij} as $K \times K$ covariance matrix of $S_k(i,j)$. Note that Σ_{ij} is a diagonal matrix due to the fact that each component of $S(i,j)$ are independent. The inequality (B.3.13) follows from (41) of [57], where $S_G(i,j)$ in (B.3.13) is distributed with $\mathcal{CN}\left(\mathbf{0}, \Sigma_{ij}\right)$.

Define $f(\Sigma_{ij}) \triangleq I\left(S_G(i,j); Y_k(i,j) |\, \tilde{Z}(i,j), g\right)$. The inequality in (B.3.14) follows from Jensen's inequality and Proposition 5 of [57] that states $f(\Sigma_{ij})$ is a concave function of Σ_{ij}. Note that S_G in (B.3.14) is distributed with $\mathcal{CN}\left(0, \frac{1}{BT_d} \sum_{i=1}^{B} \sum_{j=T_r+1}^{T} \Sigma_{ij}\right)$. The inequality in (B.3.15) follows from (139) of [57], where $\mathcal{S}$ is a set of covariance matrices and defined as

$$\mathcal{S} \triangleq \{\Sigma : \Sigma \preceq diag\left(\rho_1, \ldots, \rho_K\right)$$

$$\text{and } \Sigma \text{ is a diagonal matrix}\} \tag{B.3.17}$$

We can rewrite the random variable inside the expectation as

$$\max_{\Sigma\in\mathcal{S}}\left(\left[\log\left(1+\frac{1}{M}C_k\Sigma C_k^*\right)-\log\left(1+\frac{1}{M}C_e\Sigma C_e^*\right)\right]^+\right) \tag{B.3.18}$$

$$=\max_{\Sigma\in\mathcal{S}}\left(\left[\log\left(\frac{1}{M}+\rho_k(G)v_k(G)+\sum_{l\neq k}^{K}\rho_l(G)v_l(G)\right)-\log\left(\frac{1}{M}+\rho_k(G)w_k(G)+\sum_{l\neq k}^{K}\rho_l(G)v_l(G)\right)\right]^+\right) \tag{B.3.19}$$

with probability 1, where $\rho_k(G)$ is defined to be k-th element on the diagonal of Σ, i.e., $\Sigma \triangleq diag\left(\rho_1(G),\ldots,\rho_K(G)\right)$. Note that

$$0\leq\rho_l(G)\leq\rho_l,\ l=1,\ldots,K,$$

due to (B.3.17). In (B.3.19), we define

$$v_l(G)\triangleq\frac{1}{\alpha_l M^2}\left|H_k\hat{H}_l^*\right|^2$$

for $l=1,\ldots,K$ and $w_k(G)\triangleq\frac{1}{\alpha_k M^2}\left|H_k\tilde{H}_k^*\right|^2$. We continue to simplify (B.3.18) with the following:

$$\text{(B.3.19)}=\left[\max_{\rho_k(G):0\leq\rho_k(G)\leq\rho_k}\left(\log\left(\frac{1}{M}+\rho_k(G)v_k(G)\right)-\log\left(\frac{1}{M}+\rho_k(G)w_k(G)\right)\right)\right]^+ \tag{B.3.20}$$

$$=\left[\left(\log\left(\frac{1}{M}+\rho_k v_k(G)\right)-\log\left(\frac{1}{M}+\rho_k w_k(G)\right)\right)\right]^+ \tag{B.3.21}$$

with probability 1, where (B.3.20) follows from the fact that

$$f(x)=\left[\log(a+x)-\log(b+x)\right]^+$$

is a non-increasing function if $x \geq 0$, where a and b are positive real numbers. The equality in (B.3.21) follows from the fact $g(x) = \left[\log\left(\frac{1}{M} + ax\right) - \log\left(\frac{1}{M} + bx\right)\right]^+$ is non-decreasing if $x \geq 0$ where a and b are non-negative real numbers and $M \geq 1$.

We now bound R_k as follows:

$$\begin{aligned} R_k &\leq \frac{T_d}{T}\mathbb{E}\left[\left[\log\left(\frac{1}{M} + \rho_k v_k(G)\right)\right.\right. \\ &\qquad \left.\left. - \log\left(\frac{1}{M} + \rho_k w_k(G)\right)\right]^+\right] + \gamma_B \qquad \text{(B.3.22)} \\ &= \frac{T_d}{T}\mathbb{E}\left[\left[\log\left(\frac{1}{M} + \rho_k v_k(G)\right)\right.\right. \\ &\qquad \left.\left. - \log\left(\frac{1}{M} + \rho_k w_k(G)\right)\right]^+\right] \qquad \text{(B.3.23)} \end{aligned}$$

where (B.3.22) follows from (B.3.16) and from the fact that (B.3.18) = (B.3.21) with probability 1 and (B.3.23) follows from the fact that $\lim_{B\to\infty} \gamma_B = 0$.

We now bound the secure degree of freedom of k-th user as follows

$$\begin{aligned} d_k &= \lim_{M\to\infty} \frac{R_k}{\log M} \\ &\leq \lim_{M\to\infty} \frac{T_d}{T}\mathbb{E}\left[\left[\frac{\log\left(1 + M\rho_k v_k(G)\right)}{\log M}\right.\right. \\ &\qquad \left.\left. - \frac{\log\left(1 + M\rho_k w_k(G)\right)}{\log M}\right]^+\right] \qquad \text{(B.3.24)} \\ &= \frac{T_d}{T}\mathbb{E}\left[\lim_{M\to\infty}\left[\frac{\log\left(1 + M\rho_k v_k(G)\right)}{\log M}\right.\right. \\ &\qquad \left.\left. - \frac{\log\left(1 + M\rho_k w_k(G)\right)}{\log M}\right]^+\right], \qquad \text{(B.3.25)} \end{aligned}$$

where (B.3.24) follows from (B.3.23) and (B.3.25) follows form the dominant convergence theorem. To apply the dominant convergence theorem, we need to show that random variable

$$\begin{aligned} t(M) \triangleq &\left[\frac{\log\left(1 + M\rho_k v_k(G)\right)}{\log M}\right. \\ &\left. - \frac{\log\left(1 + M\rho_k w_k(G)\right)}{\log M}\right]^+ \qquad \text{(B.3.26)} \end{aligned}$$

is upper and lower bounded by random variables that have a finite limit for $M > 1$. Note that $t(M)$ is lower bounded by zero and upper bounded by

$$t^+(M) \triangleq \frac{\log\left(1 + M\rho_k v_k(G)\right)}{\log M}$$

for any $M > 1$ since the second $\log(\cdot)$ term in (B.3.26) is non-negative. We next upper bound $\mathbb{E}\left[t^+(M)\right]$ as follows:

$$\begin{aligned}
&\mathbb{E}\left[t^+(M)\right] \\
&= \mathbb{E}\left[\frac{\log\left(\frac{1}{M} + \rho_k v_k(G)\right)}{\log M}\right] + 1 && \text{(B.3.27)} \\
&\leq \mathbb{E}\left[\log\left(\frac{1}{M} + \rho_k v_k(G)\right)\right] + 1 \\
&\leq \log\left(1 + \rho_k \mathbb{E}\left[v_k(G)\right]\right) + 1 && \text{(B.3.28)} \\
&\leq \log\left(1 + \rho_k\left(\gamma_k + \pi_k\right)\right) + 1 && \text{(B.3.29)} \\
&< \infty, && \text{(B.3.30)}
\end{aligned}$$

where $\gamma_k \triangleq \left|\mathbb{E}\left[H_{k,m}\hat{H}^*_{k,m}\right]\right|^2$ and $\pi_k \triangleq \mathbb{E}\left[\left|H_{k,m}\hat{H}^*_{k,m}\right|^2\right]$. In the derivation above, (B.3.28) follows from Jensen's inequality and (B.3.29) follows from the fact that $\mathbb{E}\left[\left|H_k\hat{H}^*_k\right|^2\right] = \left(M^2 - M\right)\left|\mathbb{E}\left[H_{k,m}\hat{H}^*_{k,m}\right]\right|^2 + M\mathbb{E}\left[\left|H_{k,m}\hat{H}^*_{k,m}\right|^2\right] = \left(M^2 - M\right)\gamma_k + M\pi_k$.

We continue the derivation of the upper bound on d_k with the following:

$$\begin{aligned}
\text{(B.3.25)} &= \frac{T_d}{T}\mathbb{E}\left[\left[\lim_{M\to\infty}\frac{\log\left(\frac{1}{M} + \rho_k v_k(G)\right)}{\log M}\right.\right. \\
&\qquad \left.\left. - \lim_{M\to\infty}\frac{\log\left(\frac{1}{M} + \rho_k w_k(G)\right)}{\log M}\right]^+\right] && \text{(B.3.31)} \\
&= 0, && \text{(B.3.32)}
\end{aligned}$$

where (B.3.31) follows from the fact $[\cdot]$ is a continuous function. In order to show the equality in (B.3.32), first note that

$$\lim_{M\to\infty} v_k(G) = \lim_{M\to\infty}\frac{1}{\alpha_k M^2}\left|H_k\hat{H}^*_k\right|^2$$

$$= \lim_{M\to\infty} \frac{1}{\alpha_k M} \sum_{m=1}^{M} H_{k,m}\hat{H}_{k,m}^{*} \times \lim_{M\to\infty} \frac{1}{M} \sum_{m=1}^{M} H_{k,m}^{*}\hat{H}_{k,m}$$

$$= \frac{1}{\alpha_k} \left| \mathbb{E}\left[H_{k,m}\hat{H}_{k,m}^{*} \right] \right|^2, \tag{B.3.33}$$

with probability 1, where (B.3.33) follows from the strong law of large numbers. In a similar way we can show that

$$\lim_{M\to\infty} w_k(G) = \frac{1}{\alpha_k} \mathbb{E}\left[\left| H_{k,m}\tilde{H}_{k,m}^{*} \right|^2 \right]$$

$$= \frac{1}{\alpha_k} \left| \mathbb{E}\left[H_{e,m}\hat{H}_{k,m}^{*} \right] \right|^2 \tag{B.3.34}$$

with probability 1, where (B.3.34) follows from the fact that the joint probability distribution of $\left(H_e, \hat{H}_k\right)$ is identical with that of $\left(H_k, \tilde{H}_k\right)$. Hence, we have

$$\lim_{M\to\infty} \log\left(\frac{1}{M} + \rho_k v_k(G) \right) = \log\left(\lim_{M\to\infty} \rho_k v_k(G) \right)$$

$$= \log\left(\frac{\rho_k}{\alpha_k} \left| \mathbb{E}\left[H_{k,m}\hat{H}_{k,m}^{*} \right] \right|^2 \right) \tag{B.3.35}$$

with probability 1. Further, we have

$$\lim_{M\to\infty} \log\left(\frac{1}{M} + \rho_k w_k(G) \right) = \log\left(\lim_{M\to\infty} \rho_k w_k(G) \right)$$

$$= \log\left(\frac{\rho_k}{\alpha_k} \left| \mathbb{E}\left[H_{e,m}\hat{H}_{k,m}^{*} \right] \right|^2 \right) \tag{B.3.36}$$

with probability 1. The equality in (B.3.32) follows by combining (B.3.35) and (B.3.36). Hence, the proof ends.

The proof of Theorem 3.4.1 for the case in which the BS employs δ-conjugate beamforming can be done in the similar way. One only needs to replace $c_k\Sigma c_k^{*}$ and $c_e\Sigma c_e^{*}$ in (B.3.15) with $\frac{1}{M^{\delta}} c_k\Sigma c_k^{*}$ and $\frac{1}{M^{\delta}} c_e\Sigma c_e^{*}$, respectively and change the rest of the proof accordingly.

□

B.3.2 Proof of Corollary 3.4.3

Assume that the BS employs conjugate beamforming without loss of generality. Note that from (B.3.23), we have following upper bound:

$$\begin{aligned}\lim_{M\to\infty} R_k &= \lim_{M\to\infty} \frac{T_d}{T}\mathbb{E}\left[\left[\log\left(\frac{1}{M}+\rho_k v_k(G)\right)\right.\right.\\ &\qquad \left.\left.-\log\left(\frac{1}{M}+\rho_k w_k(G)\right)\right]^+\right]\\ &= \frac{T_d}{T}\mathbb{E}\left[\lim_{M\to\infty}\left[\log\left(\frac{1}{M}+\rho_k v_k(G)\right)\right.\right.\\ &\qquad \left.\left.-\log\left(\frac{1}{M}+\rho_k w_k(G)\right)\right]^+\right] \qquad \text{(B.3.37)}\end{aligned}$$

where (B.3.37) follows from the dominant convergence theorem. To apply the dominant convergence theorem, we need to show that random variable

$$\begin{aligned}g(M) \triangleq &\left[\log\left(\frac{1}{M}+\rho_k v_k(G)\right)\right.\\ &\left.-\log\left(\frac{1}{M}+\rho_k w_k(G)\right)\right]^+\end{aligned}$$

is upper and lower bounded by random variables that have a finite limit for $M > 1$. Note that $g(M)$ is lower bounded by zero and upper bounded by

$$\begin{aligned}g(M) &\le \left[\log\left(\frac{1}{M}+\rho_k v_k(G)\right)\right.\\ &\qquad \left.-\log\left(\frac{1}{M}+\rho_k w_k(G)\right)\right]^+\\ &\le \log\left(2+\rho_k v_k(G)+\rho_k w_k(G)\right)-\log\left(\rho_k w_k(G)\right) \qquad \text{(B.3.38)}\end{aligned}$$

with probability 1 for any $M > 1$. Noting the analysis in (B.3.27)-(B.3.30), in order to show (B.3.38) is upper bounded by a random variable that has a finite expectation, it is sufficient to show the expectation of second $\log(\cdot)$ term in (B.3.38) has a finite lower bound. Hence,

$$\mathbb{E}\left[\log\left(\rho_k w_k(G)\right)\right] = \log\rho_k + \mathbb{E}\left[\log\left(w_k(G)\right)\right]$$

$$
\begin{aligned}
&= \log \rho_k + \mathbb{E}\left[\log\left(w_k(G)\right)\right] \\
&= \log \rho_k - \log \alpha_k + \mathbb{E}\left[\log\left(K_M\right)\right] && \text{(B.3.39)} \\
&\geq \log \rho_k - \log \alpha_k + \int \log(x) p_{K_M}(x)\, \mathrm{d}x \\
&\geq \log \rho_k - \log \alpha_k + \int_0^1 \log(x) p_{K_M}(x)\, \mathrm{d}x \\
&\geq \log \rho_k - \log \alpha_k + \int_0^1 \log(x) r\, \mathrm{d}x && \text{(B.3.40)} \\
&= \log \rho_k - \log \alpha_k - r \log e \\
&> -\infty,
\end{aligned}
$$

where r is defined in the statement of Corollary 3.4.3. In (B.3.39), the equality follows from the definition of K_M in Corollary 3.4.3 and from the fact that the joint probability distribution of $\left(H_e, \hat{H}_k\right)$ is identical with that of $\left(H_k, \tilde{H}_k\right)$. In (B.3.40), the inequality follows from the assumption in Corollary 3.4.3. The rest of the proof follows from Appendix B.3.1

The proof for the case the BS employs δ-conjugate beamforming follows from the same argument at the end of Appendix B.3.1 □

B.4 Proof of Theorem 3.5.1

The length, T_r of training phase has to be identical to at least the size of the pilot signal set L so that the BS can generate $L \geq K$ mutually orthogonal pilot signals. Let J be any integer in set $\{1, \ldots, T_r\}$. In order to estimate k-th user's channel, the BS first projects the received signal during the training phase Y^{T_r} indicated in (3.5.1) to ϕ_k. Then, the BS normalizes the projected signal and estimates the gain of the channel connecting the BS to k-th user at i-th block as

$$
\hat{H}_k(i) = x_1 \left(\sqrt{T_r \rho_r} H_k(i)
$$

$$+\Pi_i \sum_{n=1}^{M_e} \sqrt{\frac{T_r \rho_{jam}}{M_e J}} H_e(i) + V_k \Bigg) \tag{B.4.1}$$

for any $k \in \{1, \ldots, K\}$, where $\mathbb{E}\left[||\hat{H}_k(i)||^2\right] = 1$, V_k is distributed as $\mathcal{CN}(0, I_M)$ for any $k \in \{1, \ldots, K\}$, $x_1 \triangleq \dfrac{1}{\sqrt{M}\sqrt{T_r\rho_r + 1 + T_r \frac{\rho_{jam}}{J}}}$ and $\{\Pi_i\}_{i \geq 1}$ is an i.i.d Bernoulli process, where $\mathbb{P}(\Pi_i = 1) = \dfrac{J}{L}$. Event $\{\Pi_i = 1\}$ indicates that the set of pilot signals the adversary contaminates at i-th block contains k-th user's pilot signal.

Utilizing stochastic encoding and conjugate beamforming as in the proof Theorem 3.3.1, we can show that rate

$$\begin{aligned} R_k = \Bigg[& \frac{T_d}{T} \log\left(1 + \frac{M\rho_k a}{\rho_f + \rho_{jam} + 1}\right) \\ & - \frac{T_d}{T} \log\left(1 + M_e\rho_k + \frac{M M_e \rho_k \rho_{jam} a}{L\rho_r}\right)\Bigg]^+ \end{aligned} \tag{B.4.2}$$

for any $k \in \{1, \ldots, K\}$ is achievable, where $a \triangleq \dfrac{T_r\rho_r}{T_r\rho_r + 1 + T_r\frac{\rho_{jam}}{L}}$. Notice that the rate in (B.4.2) does not depend on J. We can rewrite R_k as

$$\begin{aligned} R_k = \Bigg[& \frac{T_d}{T} \log\left(1 + \frac{M\rho_k\rho_r T_r}{(\rho_f + \rho_{jam} + 1)(\rho_r T_r + \rho_{jam} + 1)}\right) \\ & - \frac{T_d}{T} \log\left(1 + M_e\rho_k + \frac{M_e M \rho_k \rho_{jam}}{\rho_r T_r + \rho_{jam} + 1}\right)\Bigg]^+ \end{aligned} \tag{B.4.3}$$

due to the fact that $L = T_r$. Suppose $\gamma \leq 1$. We bound R_k as follows

$$\begin{aligned} R_k \geq & \frac{T_d}{T}\Bigg[\log\left(1 + \frac{M\rho_k\rho_r M^\gamma}{(\rho_f + \rho_{jam} + 1)(\rho_r M^\gamma + \rho_{jam} + 1)}\right) \\ & - \log\left(1 + M_e\rho_k + \frac{M_e M\rho_k\rho_{jam}}{\rho_r M^\gamma + \rho_{jam} + 1}\right)\Bigg]^+ \end{aligned} \tag{B.4.4}$$

$$\begin{aligned} \geq & \frac{T_d}{T}\Bigg[\log M + \log\left(\frac{\rho_k\rho_r}{(\rho_f + \rho_{jam} + 1)(\rho_r + \rho_{jam} + 1)}\right) \\ & - (1-\gamma)\log M - \log\left(1 + M_e\rho_k + \frac{M_e\rho_k\rho_{jam}}{\rho_r}\right)\Bigg]^+ \\ = & \frac{T_d}{T}\Bigg[\gamma \log M - \log\Bigg(\left(1 + M_e\rho_k + \frac{M_e\rho_k\rho_{jam}}{\rho_r}\right) \\ & \times (\rho_f + \rho_{jam} + 1)\frac{\rho_r + \rho_{jam} + 1}{\rho_k\rho_r}\Bigg)\Bigg]^+ \end{aligned} \tag{B.4.5}$$

where (B.4.4) follows from the fact that $T_r \geq M^{\gamma}$. Notice that the second logarithm term in (B.4.5) does not depend on M. Hence, we observe that $\dfrac{R_k}{\log M} \geq \dfrac{T_d}{T}\gamma - \epsilon$ if $M \geq G(\epsilon)$. In a similar way, for $\gamma > 1$, we can show that $\dfrac{R_k}{\log M} \geq \dfrac{T_d}{T} - \epsilon$ if $M \geq G(\epsilon)$.

B.5

B.5.1 Proof of Theorem 3.5.4

We set the size of the pilot signal set L to T_r. Let J be any integer in set $\{1, \ldots, T_r\}$. The BS uses the same strategy explained in the proof of Theorem 3.5.1 in order to estimate the gains of channels connecting the BS to users.

The BS picks arbitrary message rates $R_k > 0$, $k = 1, \ldots, K$. The equivocation rate for a code $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ utilizing deterministic encoding mapping functions, f_k, $k = 1, \ldots, K$ and δ-conjugate beamforming is as follows:

$$\begin{aligned}
&\frac{1}{BT} H\left(W_k | Z^{BT_d}, H^B, \hat{H}^B, H_e^B\right) \\
&\geq R_k - \frac{T_d}{T} \log\left(1 + \frac{M_e \rho_k}{M^{\delta}} + \frac{M^{1-\delta} M_e \rho_k \rho_{jam} a}{L \rho_r}\right) && \text{(B.5.1)} \\
&= R_k - \frac{T_d}{T} \log\left(1 + \frac{M_e \rho_k}{M^{\delta}} + \frac{M^{1-\delta} M_e \rho_k \rho_{jam}}{\rho_r T_r + T_r + 1}\right) && \text{(B.5.2)} \\
&\geq R_k - \frac{T_d}{T} \log\left(1 + \frac{M_e \rho_k}{M^{\delta}} + M^{1-\delta-\gamma} \frac{M_e \rho_k \rho_{jam}}{\rho_r}\right) && \text{(B.5.3)}
\end{aligned}$$

for all $k \in \{1, \ldots, K\}$, where a is defined in (B.4.2) and $\hat{H}_k(i)$ for any $k \in \{1, \ldots, K\}$ and $i \in \{1, \ldots, B\}$ is given in (B.4.1). In the above derivation, (B.5.1) follows from a derivation that is similar to (B.2.1)-(B.2.6) in Appendix B.2.1, (B.5.2) follows from the fact the cardinality of pilot signal set L is chosen as T_r and (B.5.3) follows from the fact that $T_r \geq M^{\gamma}$.

As $\delta + \gamma > 1$, the RHS of (B.5.3) goes to zero as $M \to \infty$. For any $\epsilon > 0$,

$M \geq S_1(\epsilon)$ implies that right hand side of (B.5.3) is smaller than ϵ, completing the proof.

B.5.2 Proof of Corollary 3.5.5

We set the size of the pilot signal set L to T_r. Let J be any integer in set $\{1, \ldots, T_r\}$. The BS uses the same strategy explained in the proof of Theorem 3.5.1 in order to estimate the gains of channels connecting the BS to users.

Pick δ and γ such that $0 < \delta < 1$ and $\gamma + \delta > 1$. Pick any arbitrary $\epsilon > 0$ and arbitrary rate tuple $R = [R_1, \ldots, R_K]$. Choose M such that $M \geq \max(V_1(R), S_1(\epsilon))$. Note that inequality $M \geq V_1(R)$ implies that $R_k \leq \frac{T_d}{T} \log\left(1 + \frac{M^{1-\delta}\rho_k a}{M^{-\delta}\rho_f + \rho_{jam} + 1}\right)$ for all $k \in \{1, \ldots, K\}$, where a is defined in (B.4.2). As in the proof of Corollary 3.3.5, we can show that there exists $B(\epsilon) > 0$ and a sequence of codes $\left(2^{BTR_1}, \ldots, 2^{BTR_K}, BT_d\right)$ that satisfy the decodability constraint in (3.2.10) for $B \geq B(\epsilon)$, when δ-beamforming, combined with deterministic mapping is used. In addition, since $M \geq S_1(\epsilon)$ and $T_r \geq M^\gamma$, following Theorem 3.5.4, the sequence of codes mentioned above satisfy the constraint in (3.2.11), completing the proof.

APPENDIX C: PROOFS IN CHAPTER 4

C.1 Properties of Common Information

The *graphical representation* of P_{XY} is the bipartite graph with an edge between $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ if and only if $P_{XY}(x, y) > 0$. The *common part* U of two random variables (X, Y) is defined as the (unique) label of the connected component of the graphical representation of P_{XY} in which (X, Y) falls. Note that U is a deterministic function of X alone and also a deterministic function of Y alone.

The Gács-Körner common information of two random variables (X, Y) is given by entropy of the common part, that is, $C(X;Y) := H(U)$, and has the operational significance of being the maximum number of common bits per symbol that can be independently extracted from X and Y [48]. In general, $C(X;Y) \leq I(X;Y)$, with equality if and only if $X \to U \to Y$ forms a Markov chain [58]. Since our results are only concerned with whether $C(X;Y) = I(X;Y)$, our theorem statements are unchanged if we use instead the Wyner notion of common information (see [47]), since it is also equal to mutual information if and only if $X \to U \to Y$ forms a Markov chain [58].

We give the following lemma which aids our proof of Theorem 4.4.3 in Appendix C.4.

Lemma C.1.1. *If $C(X;Y) \neq I(X;Y)$, then there exist $x_0, x_1 \in \mathcal{X}$ and $y_0, y_1 \in \mathcal{Y}$, such that $y_0 \neq y_1$, $P_{XY}(x_0, y_0) > 0$, $P_{XY}(x_0, y_1) > 0$, and $P_{X|Y}(x_1|y_0) \neq P_{X|Y}(x_1|y_1)$.*

Proof. We will prove this lemma by showing the contrapositive, that is, if there does not exist $x_0, x_1 \in \mathcal{X}$ and $y_0, y_1 \in \mathcal{Y}$ satisfying the conditions stated in the lemma, then $C(X;Y) = I(X;Y)$. First, note that if for all $x_0 \in \mathcal{X}$ and $y_0, y_1 \in \mathcal{Y}$, either $y_0 = y_1$, $P_{XY}(x_0, y_0) = 0$, or $P_{XY}(x_0, y_1) = 0$, then Y is a deterministic function of X, which would result in $C(X;Y) = I(X;Y)$. Thus, we are left with showing that for all $x_0 \in \mathcal{X}$ and $y_0, y_1 \in \mathcal{Y}$, with $y_0 \neq y_1$, $P_{XY}(x_0, y_0) > 0$, and $P_{XY}(x_0, y_1) > 0$, if we also have that for all $x_1 \in \mathcal{X}$, $P_{X|Y}(x_1|y_0) = P_{X|Y}(x_1|y_1)$, then $C(X;Y) = I(X;Y)$. This follows since these conditions would imply that for the common part U of (X, Y), $X \to U \to Y$ forms a Markov chain. □

C.2 Proof of Theorem 4.4.1

It is sufficient to show that for any mechanism $P_{Z|X}$ that is a feasible solution in the inference optimization of (4.2.6), there is a corresponding mechanism $P_{Z'|Y}$ for the output perturbation optimization of (4.2.5) that achieves the same distortion and only lesser or equal privacy-leakage.

Let $P_{Z|X}$ be a mechanism in the feasible region of the inference optimization problem of (4.2.6). Define the corresponding mechanism for the output perturbation optimization of (4.2.5) by

$$P_{Z'|Y}(z|y) := \sum_{x \in \mathcal{X}} P_{Z|X}(z|x) P_{X|Y}(x|y).$$

Let $(X, Y, Z, Z') \sim P_{XY} P_{Z|X} P_{Z'|Y}$. Note that by construction, (Y, Z) and (Y, Z') have the same distribution $P_Y P_{Z'|Y}$. Thus, both mechanisms achieve the same distortion $D(P_Y P_{Z'|Y})$ and $I(Y;Z) = I(Y;Z')$. Further, by construction, $Y \to X \to Z$ and $X \to Y \to Z'$ form Markov chains. Thus, by the data processing inequality,

$$I(X;Z') \leq I(Y;Z') = I(Y;Z) \leq I(X;Z),$$

showing that the output perturbation mechanism has only lesser or equal privacy-leakage.

C.3 Proof of Theorem 4.4.2

Since $\pi_{\mathrm{FD}}(\delta) \leq \pi_{\mathrm{OP}}(\delta)$ is immediate, we only need to show that $\pi_{\mathrm{OP}}(\delta) \leq \pi_{\mathrm{FD}}(\delta)$. It is sufficient to show that for any mechanism $P_{Z|XY}$ that is a feasible solution in the full data optimization of (4.2.4), there is a corresponding mechanism $P_{Z'|Y}$ for the output perturbation optimization of (4.2.5) that achieves the same distortion and only lesser or equal privacy-leakage.

Let $P_{Z|XY}$ be a mechanism in the feasible region of the full data optimization problem of (4.2.4). Define the corresponding mechanism for the output perturbation optimization of (4.2.5) by

$$P_{Z'|Y}(z|y) := \sum_{x \in \mathcal{X}} P_{Z|XY}(z|x,y) P_{X|Y}(x|y).$$

Let $(X, Y, Z, Z') \sim P_{XY} P_{Z|XY} P_{Z'|Y}$, and let U be the common part of (X, Y), where, by construction, U is a deterministic function of either X alone or Y alone. Since $C(X;Y) = I(X;Y)$, we have that $X \to U \to Y$ forms a Markov chain, i.e., $I(X;Y|U) = 0$. By construction, $X \to Y \to Z'$ also forms a Markov chain, and hence $I(X;Z'|UY) = I(X;Z'|Y) = 0$, since U is deterministic function of Y. Given these two Markov chains, we have

$$\begin{aligned}
0 &= I(X;Y|U) + I(X;Z'|UY) \\
&= I(X;YZ'|U) \\
&= I(X;Z'|U) + I(X;Y|UZ') \\
&\geq I(X;Z'|U),
\end{aligned}$$

and hence $I(X;Z'|U) = 0$, i.e., $X \to U \to Z'$ also forms a Markov chain. Continuing, we can show the desired privacy-leakage inequality,

$$\begin{aligned} I(X;Z') &\overset{(a)}{=} I(XU;Z') \\ &= I(U;Z') + I(X;Z'|U) \\ &\overset{(b)}{=} I(U;Z) \\ &\leq I(U;Z) + I(X;Z|U) \\ &= I(XU;Z) \\ &\overset{(c)}{=} I(X;Z), \end{aligned}$$

where (a) and (c) follow from U being a deterministic function of X, and (b) follows from the fact that $P_{YZ} = P_{YZ'}$ (and hence $P_{UZ} = P_{UZ'}$) by construction and the Markov chain $X \to U \to Z'$.

C.4 Proof of Theorem 4.4.3

We will show the following result, which is key to the proof.

Lemma C.4.1. *If $C(X;Y) \neq I(X;Y)$ then there exist random variables Z and Z' with $P_{YZ} = P_{YZ'}$, such that $X \to Y \to Z'$ forms a Markov chain, $I(X;Z) = 0$, and $I(X;Z') > 0$.*

The proof of Theorem 4.4.3 then follows by defining the distortion functional (metric) $D(P_{YZ})$ to equal 1 for the particular choice of $P_{YZ'}$ in Lemma C.4.1 and to equal 2 otherwise, and choosing $\delta = 1$. This choice for the distortion metric and distortion level restricts the feasible output perturbation mechanism to only $P_{Z'|Y}$, which by Lemma C.4.1 results in $\pi_{OP}(\delta) = I(X;Z') > 0$. However, Lemma C.4.1 also ensures the existence of Z produced by a full data mechanism $P_{Z|XY}$ that results in $\pi_{FD}(\delta) = I(X;Z) = 0$.

Using the symbols (x_0, x_1, y_0, y_1) shown to exist by Lemma C.1.1, we can prove Lemma C.4.1 by constructing a binary Z with alphabet $\mathcal{Z} = \{0, 1\}$ as follows. Choose any $s \in (0, 1)$ and any $t \in \big(0, \min\{s'/P_{Y|X}(y_1|x_0), s/P_{Y|X}(y_0|x_0)\}\big)$, where $s' := (1 - s)$. Define Z with $(X, Y, Z) \sim P_{XY}P_{Z|XY}$, where

$$P_{Z|XY}(0|x, y) := \begin{cases} s + tP_{Y|X}(y_1|x_0), & \text{if } (x, y) = (x_0, y_0), \\ s - tP_{Y|X}(y_0|x_0), & \text{if } (x, y) = (x_0, y_1), \\ s, & \text{otherwise.} \end{cases}$$

The choice of s and t ensures that $P_{Z|XY}(0|x, y) \in (0, 1)$ for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$. This construction of $P_{Z|XY}$ makes Z independent of X, since for all $x \in \mathcal{X}$ in the support of P_X,

$$P_{Z|X}(0|x) = \sum_{y \in \mathcal{Y}} P_{Z|XY}(0|x, y)P_{Y|X}(y|x) = s.$$

With the above construction, we have

$$\begin{aligned} P_{Z|Y}(0|y) &= \sum_{x \in \mathcal{X}} P_{Z|XY}(0|x, y)P_{X|Y}(x|y) \\ &= \begin{cases} s + tP_{Y|X}(y_1|x_0)P_{X|Y}(x_0|y_0), & \text{if } y = y_0, \\ s - tP_{Y|X}(y_0|x_0)P_{X|Y}(x_0|y_1), & \text{if } y = y_1, \\ s, & \text{otherwise.} \end{cases} \end{aligned}$$

Next, we construct binary Z' such that $X \to Y \to Z'$ forms a Markov chain, with $(X, Y, Z') \sim P_{XY}P_{Z'|Y}$, where we set $P_{Z'|Y} := P_{Z|Y}$. Then, consider

$$\begin{aligned} P_{Z'|X}(0|x) &= \sum_{y \in \mathcal{Y}} P_{Z'|Y}(0|y)P_{Y|X}(y|x) \\ &= \sum_{y \in \mathcal{Y}} P_{Z|Y}(0|y)P_{Y|X}(y|x) \\ &= s + tP_{Y|X}(y_1|x_0)P_{X|Y}(x_0|y_0)P_{Y|X}(y_0|x) \end{aligned}$$

$$
\begin{aligned}
&\quad - tP_{Y|X}(y_0|x_0)P_{X|Y}(x_0|y_1)P_{Y|X}(y_1|x) \\
&= s + tP_X(x_0)P_{Y|X}(y_0|x_0)P_{Y|X}(y_1|x_0) \\
&\quad \times [P_{X|Y}(x|y_0) - P_{X|Y}(x|y_1)]/P_X(x).
\end{aligned}
$$

Finally, we show that $P_{Z'|X}(0|x)$ is not constant for all $x \in \mathcal{X}$ in the support of P_X, which implies that Z' is not independent of X, i.e., $I(X;Z') > 0$. This can be proved by contradiction, by supposing that $P_{Z'|X}(0|x)$ is constant for all $x \in \mathcal{X}$ in the support of P_X. Then, for all $x \in \mathcal{X}$,

$$P_{X|Y}(x|y_0) - P_{X|Y}(x|y_1) = cP_X(x),$$

for some constant c. By summing over all $x \in \mathcal{X}$, we have that $c = 0$. This would imply that $P_{X|Y}(x|y_0) = P_{X|Y}(x|y_1)$ for all $x \in \mathcal{X}$, contradicting the existence of $x_1 \in \mathcal{X}$ given by Lemma C.1.1 for the choice of y_0 and y_1.

BIBLIOGRAPHY

[1] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[2] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3364–3379, 2014.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, 1975.

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[7] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[8] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: a block-markov wyner secrecy encoding scheme," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4660–4677, 2012.

[9] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the mimo wiretap channel with an active eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82–91, 2013.

[10] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

[11] D. Blackwell, L. Breiman, and A. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, vol. 31, no. 3, pp. 558–567, 1960.

[12] I. Csiszár and P. Narayan, "Capacity of the gaussian arbitrarily varying channel," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 18–26, 1991.

[13] A. Lapidoth, P. Narayan *et al.*, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.

[14] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary jamming can preclude secure communication," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on.* IEEE, 2009, pp. 1069–1075.

[15] I. Bjelaković, H. Boche, and J. Sommerfeld, "Strong secrecy in arbitrarily varying wiretap channels," in *Information Theory Workshop (ITW), 2012 IEEE.* IEEE, 2012, pp. 617–621.

[16] H. Boche and R. F. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1482–1496, 2013.

[17] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 970–983, 2016.

[18] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081, 2001.

[19] S. M. Ross *et al.*, *Stochastic processes.* John Wiley & Sons New York, 1996, vol. 2.

[20] G. Caire and D. Tuninetti, "The throughput of hybrid-arq protocols for the gaussian collision channel," *IEEE Transactions on Information Theory*, vol. 47, no. 5, pp. 1971–1988, 2001.

[21] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5379–5397, 2013.

[22] T. Marzetta, "Multi-cellular wireless with base stations employing unlimited numbers of antennas," in *Proc. UCSD Inf. Theory Applicat. Workshop*, 2010.

[23] H. Yang and T. L. Marzetta, "Performance of conjugate and zero-forcing beamforming in large-scale antenna systems," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 2, pp. 172–179, 2013.

[24] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.

[25] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive mimo: Benefits and challenges," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 742–758, 2014.

[26] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell tdd systems," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2640–2651, 2011.

[27] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser mimo systems," *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436–1449, 2013.

[28] R. R. Müller, L. Cottatellucci, and M. Vehkaperä, "Blind pilot decontamination," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 773–786, 2014.

[29] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive mimo systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[30] Y. O. Basciftci and C. E. Koksal, "How different is security with massive mimo?" *UCSD Information Theory Applications (ITA)*, 2015.

[31] T. L. Marzetta, "How much training is required for multiuser mimo?" in *2006 Fortieth Asilomar Conference on Signals, Systems and Computers*. IEEE, 2006, pp. 359–363.

[32] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[33] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, 2010.

[34] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, 2012.

[35] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[36] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[37] D. Rebollo-Monedero, J. Forné, and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 11, pp. 1623–1636, 2010.

[38] L. Sweeney, "Simple demographics often identify people uniquely," *Carnegie Mellon University, Data Privacy Working Paper*, 2000.

[39] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *IEEE Symp. on Security and Privacy*. IEEE, 2008, pp. 111–125.

[40] L. Sweeney, "k-anonymity: A model for protecting privacy," *Intl. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[41] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Trans. on Knowledge Discovery from Data*, vol. 1, no. 1, p. 3, 2007.

[42] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *IEEE Intl. Conf. on Data Eng.* IEEE, 2007, pp. 106–115.

[43] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Springer, 2006, pp. 265–284.

[44] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Allerton Conf. on Comm., Ctrl., and Comp.*, 2012, pp. 1401–1408.

[45] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Trans. on Information Theory*, vol. 29, no. 6, pp. 918–923, 1983.

[46] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 6, pp. 838–852, 2013.

[47] A. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[48] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, vol. 2, no. 2, pp. 149–162, 1973.

[49] H. S. Witsenhausen, "Indirect rate distortion problems," *IEEE Transactions on Information Theory*, vol. 26, no. 5, pp. 518–521, 1980.

[50] N. Tishby, F. C. Pereira, and W. Bialek, "The information bottleneck method," in *Allerton Conf. on Comm., Ctrl., and Comp.*, 1999, pp. 368–377.

[51] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. John Wiley & Sons, 2012.

[52] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in *IEEE Information Theory Workshop*, 2014, pp. 501–505.

[53] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.

[54] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[55] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 951–963, 2003.

[56] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1325–1343, 2015.

[57] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[58] R. Ahlswede and J. Körner, "On common information and related characteristics of correlated information sources," in *Proc. Prague Conf. on Information Theory*, 1974.