DISTRIBUTED SECRECY FOR INFORMATION THEORETIC SENSOR NETWORK MODELS

A Dissertation

by

WILLIAM LUH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

August 2008

Major Subject: Electrical Engineering

DISTRIBUTED SECRECY FOR INFORMATION THEORETIC SENSOR NETWORK MODELS

A Dissertation

by

WILLIAM LUH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Deepa Kundur
Committee Members,	Don R. Halverson
	Jim Xiuquan Ji
	Dezhen Song
Head of Department,	Costas N. Georghiades

August 2008

Major Subject: Electrical Engineering

ABSTRACT

Distributed Secrecy for Information Theoretic Sensor Network Models.

(August 2008)

William Luh, B.A.Sc., University of Toronto;

M.S., Texas A&M University

Chair of Advisory Committee: Dr. Deepa Kundur

This dissertation presents a novel problem inspired by the characteristics of sensor networks. The basic setup through-out the dissertation is that a set of sensor nodes encipher their data without collaboration and without any prior shared secret materials. The challenge is dealt by an eavesdropper who intercepts a subset of the enciphered data and wishes to gain knowledge of the uncoded data. This problem is challenging and novel given that the eavesdropper is assumed to know *everything*, including secret cryptographic keys used by both the encoders and decoders. We study the above problem using information theoretic models as a necessary first step towards an understanding of the characteristics of this system problem.

This dissertation contains four parts. The first part deals with noiseless channels, and the goal is for sensor nodes to both source code and encipher their data. We derive inner and outer regions of the capacity region (i.e the set of all source coding and equivocation rates) for this problem under general distortion constraints. The main conclusion in this part is that unconditional secrecy is unachievable unless the distortion is maximal, rendering the data useless. In the second part we thus provide a practical coding scheme based on distributed source coding using syndromes (DISCUS) that provides secrecy beyond the equivocation measure, i.e. secrecy on each symbol in the message. The third part deals with discrete memoryless channels, and

the goal is for sensor nodes to both channel code and encipher their data. We derive inner and outer regions to the secrecy capacity region, i.e. the set of all channel coding rates that achieve (weak) unconditional secrecy. The main conclusion in this part is that interference allows (weak) unconditional secrecy to be achieved in contrast with the first part of this dissertation. The fourth part deals with wireless channels with fading and additive Gaussian noise. We derive a general outer region and an inner region based on an equal SNR assumption, and show that the two are partially tight when the maximum available user powers are admissible.

To My Family

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor, Prof. Deepa Kundur, for her support, encouragement, and generosity. I would also like to thank my committee members, Prof. Don Halverson, Prof. Jim Ji, Prof. Dezhen Song, and former committee member Prof. Prasad Enjeti, for their encouragement and support of this research. I would like to thank Prof. Takis Zourntos and Prof. Tie Liu whom I have had the pleasure of knowing at Texas A&M. Finally, I would like to thank Alexandra Czarlinska for helping me throughout the years.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

FIGURE Page

CHAPTER I

INTRODUCTION

A. Sensor Networks and Security

Cryptography is a well-studied field that has evolved significantly from its World War II renaissance to address more modern goals and challenges. Particularly since the advent of computer networks and the digital and mobile age, the goal of cryptography has been diversified from providing the critical confidentiality service, to the additional study of key exchange and management, authentication and digital signatures, secret sharing, protocols and algorithms for E-commerce and E-voting, (casino) games over the Internet, quantum cryptography, and many more.[1] As new needs continue to arise and to be identified, existing cryptographic schemes must be evaluated to determine whether or not they are appropriate in the new setting, whether they can be modified for the new scenario, or whether a new shift in paradigm is required.

The recent introduction and study of sensor networks illustrates this important point. Sensor networks are generally envisioned as low-cost, low-complexity networks where the ubiquity and density of deployed nodes compensates for their lack of computational power and battery life [1]. Due to the limited and sometimes unpredictable lifetimes of many of the nodes, traditional cryptographic services such as key exchange and key management may not provide a sufficiently light-weight and efficient solution for these networks [2]. The difficulty of designing and implementing suitable key exchange and management protocols for sensor networks only becomes

---

The journal model is *IEEE Transactions on Automatic Control*.

[1]In the recent IEEE International Conference on Communications, 57 different security topics were listed under the Computer and Communications Network Security symposium.

more apparent when one considers the random initial deployment of the nodes as well as the topology changes which occur in such networks due to mobility, node depletion and the addition of new nodes. When such variability in topology exists, the task of re-establishing keys with neighboring nodes may become prohibitive in terms of the percentage of time and energy spent on node management [3]. It is thus desirable to develop light-weight methodologies that exploit the inherent characteristics of sensor nodes, such as any redundancies that result from the physical proximity of nodes to their neighbors. Ideally however, any new proposed methodology should also be compatible with the existing key exchange and management protocols.

As a further consideration for sensor network design, nodes are often assumed to operate unattended in possibly harsh and hostile environments [4]. Such extreme scenarios often result in low bandwidth communications due to interference noise or intentional jamming. Thus it is of utmost importance that sensor nodes perform their duties with as little need for *explicit* communication as possible, since such communication consumes valuable power and bandwidth resources [3]. At the same time, nodes within close proximity of one another (i.e. a cluster of nodes) may sample correlated readings from their environment. This suggests that collaboration among these nodes would be beneficial towards the accomplishment of their shared goal of sensing and data reporting. This apparent conflict between the need to collaborate and the need to minimize inter-cluster communication is one of the central themes in the first half of our research. Thus in a similar flavor to the field of distributed source coding (where the goal is compression instead of confidentiality), we will explore the possibility of providing confidentiality to all the nodes within a cluster *without* the need to explicitly communicate and *without* the use of costly key exchange and management services.

In lieu of using cryptographic keys to provide confidentiality in a communications

network, an alternative paradigm based on exploiting the ambient environmental and communications noise to conceal the secret forms the central theme in the second half of our research. This paradigm allows us to model distributed secrecy in a sensor network such that the system exhibits the desirable properties outlined above, i.e. a keyless and inter-communicationless sensor network.

B. Contributions

As will be detailed, most of our contributions are information theoretic in nature. Thus the sensor network characteristics summarized above inspire the abstract models that this dissertation analyzes. The ultimate goal is thus to provide a solid foundation towards addressing these issues in a more practical light. For example we study the tradeoffs between the fundamental parameters of secrecy, compression, and channel coding redundancy, with the overall aim of providing guidance for future design and implementations of practical codes for sensor networks and with possible significance for other distributed networks. To achieve this goal, this dissertation consists of four main parts. We first study the tradeoffs between secrecy and compression with the assumption of noiseless channels. The second part of our research is the derivation of practical coding schemes for the first problem. Next we study the above problem under the assumption of discrete memoryless interference channels (DMIC), and derive tradeoffs between secrecy and the channel coding rates. The last part of our research extends the DMIC to the wireless setting (fading channels and Gaussian noise), thus making the results more applicable to practical wireless networks.

We now provide a more detailed outline of our contributions. For the first part of our dissertation we analyze the interaction between source coding and secrecy using multiterminal source coding theorems [5]–[7]. We derive inner and outer regions for

the set of all source coding and equivocation (measure of secrecy) rates (which we call the capacity region) for user-defined distortion criteria. We show that unconditional secrecy is only achievable if the distortion is maximal, which means no information is sent. We then show that feedback from the base station to the legitimate users does not improve equivocation. We do this by deriving an upper bound on the secret key rate that can be achieved *without* feedback, and comparing this to an upper bound on the secret key rate using feedback [8], [9].

In the second part of our research, we extend the existing distributed source coding using syndromes (DISCUS) Slepian-Wolf coding scheme. DISCUS is the practical implementation of the multitermianl source coding problem without distortion. We show that using equivocation as the measure of secrecy leaks too much information to the eavesdropper. This can be understood from our first result where unconditional secrecy is unachievable and thus equivocation is not maximal. Thus this motivates the definition of a set of additional secrecy requirements. We show how these additional requirements can be implemented by modifying DISCUS. One of the main results is that the subcodes in DISCUS should be maximum distance separable, and furthermore we show how to partition a Reed-Solomon code to meet the subcode and supercode requirements of DISCUS.

In the third part of our research we study the interaction between channel coding and secrecy in the context of the general discrete memoryless interference channel. We derive inner and outer regions of the secrecy capacity region, which is the set of all channel coding rates such that unconditional secrecy is achieved. Surprisingly, the secrecy capacity region is not empty, thus in contrast with the first part of our research, interference permits unconditional secrecy. The proof utilizes the random coding technique of Wyner's wiretap channel [10] and its generalization [11].

In the final part of our research, we study the interference problem under wire-

less settings by assuming that the interference channel has additive white Gaussian noise, and later augmenting this model with the additional challenge of slow Rayleigh fading. Again we derive inner and outer regions of the secrecy capacity region for this special case. Significantly we show that the inner region can be simplified to such an extent that its description is merely a *single* region based on an optimal power allocation scheme without the need for pre-coding (as is the case with the DMIC); for our problem at hand, this simplification is not trivial. Next, our extension of the interference channel to slow and flat Rayleigh fading demonstrates that interference and random fading are not only friends rather than foes, but are in fact necessary enablers of unconditional secrecy.

If asked for one main important result in this dissertation, it would be the surprising result that independent noisy channels do not give the encoders any advantage in terms of their ability to achieve unconditional secrecy; however, if the noisy channels are dependent in the form of interference, then although the encoders cannot communicate with one another, they can rely on the dependence afforded by the interference to help them collaborate in the "post-coding" sense.

Finally we point out that based on the need for a unified theme and a coherent structure, this dissertation focuses only on the information theoretic results that we have obtained for sensor network security. For additional and somewhat orthogonal results on privacy and security in (visual) sensor networks, the interested reader is referred to our earlier work in [12], [13].

C. Organization of Dissertation

In Chapter II we compare and contrast this dissertation to existing works in cryptography research and more specifically, to information theoretic secrecy. In Chapter III

we look at the source coding and secrecy problem, specifically, we examine the capacity region and the effect of feedback on equivocation. In Chapter IV we look at practical coding for the problem in Chapter III. In Chapter V we study the secrecy problem in the context of the discrete memoryless interference channel, thus switching gears to the channel coding problem. In Chapter VI we study the wireless setting involving additive white Gaussian noise and the extension to slow and flat Rayleigh fading.

CHAPTER II

BACKGROUND

A. Challenges and Beneficial Characteristics of Sensor Networks

Before embarking on the specifics of our research, we examine some general challenges in sensor networks and identify beneficial characteristics which we exploit in our formulation. As noted, resource constraints such as limited computation, memory and battery life result in part from the envisioned miniaturized size of the nodes [3]. The limited (battery) power and antenna size in turn impact the signal-to-noise ratio (SNR) thus limiting the available bandwidth. In addition, the environment may also present communication obstacles in the form of incidental interference or intentional jamming due to the presence of attackers [2]. The dynamic network topology resulting from node depletion and replenishment presents a further challenge in that it alters the routing topologies. Such routing changes inadvertently add to the difficulties of achieving reliable and timely inter-node communication. Fig. 1 presents a more detailed categorization of the various challenges that exist in sensor networks [1]. Importantly, these challenges can be addressed by considering the beneficial characteristics which arise in sensor networks, such as the potential for decentralized processing, node ubiquity (i.e. large-scale deployment) and the presence of natural randomness which can be utilized for security purposes. The model which we propose in the next section aims to inherently exploit such beneficial characteristics to achieve a novel and clean modeling solution. As an example, the dynamic routing topology present in sensor networks is not only a challenge, but also a characteristic which may be exploited since it also poses problems for the potential eavesdropper. The eavesdropper is forced to either discover and visit all the dynamic routes, or to settle

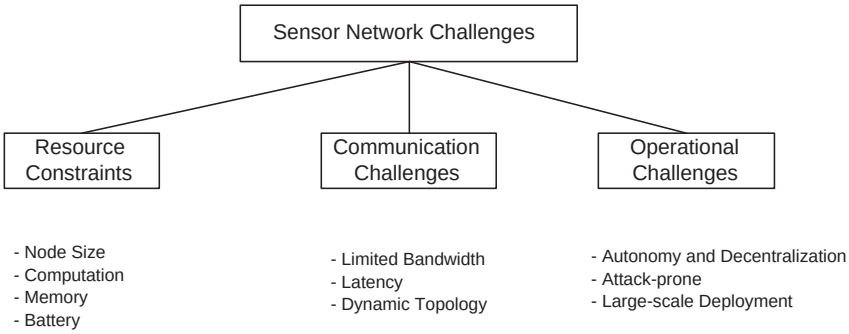

Fig. 1. Sensor Network Challenges

for an opportunistic strategy by remaining relatively stationary and waiting for the packets to arrive. This implies that the eavesdropper may only intercept a fraction of all the messages being communicated from the sensor nodes to the base station, particularly when the number of sensors is large. Thus the dynamic routing topology is a characteristics which may be exploited to the sensor network's advantage.

B. Sensor Network Architecture and Security Model

Although we have cast our research in the light of sensor network secrecy, it is important to note that our results may have broader applicability to networks in which many low-cost and low-power nodes share a common goal of protecting data as it is transmitted to a more powerful central authority (base station).[1] Fig. 2 summarizes the general setup of our sensor network problem which is based upon a considera-

[1]We note that although the structure of this network may resemble that of a cellular network with uplink communication, the goal of a sensor network differs greatly from the cellular network case. In cellular networks, individual users are independent of one another and are interested in optimizing their own throughput. In contrast, in the networks that we describe the nodes work collectively towards the achievement of one central goal: the collection and efficient relaying of data back to the base station.

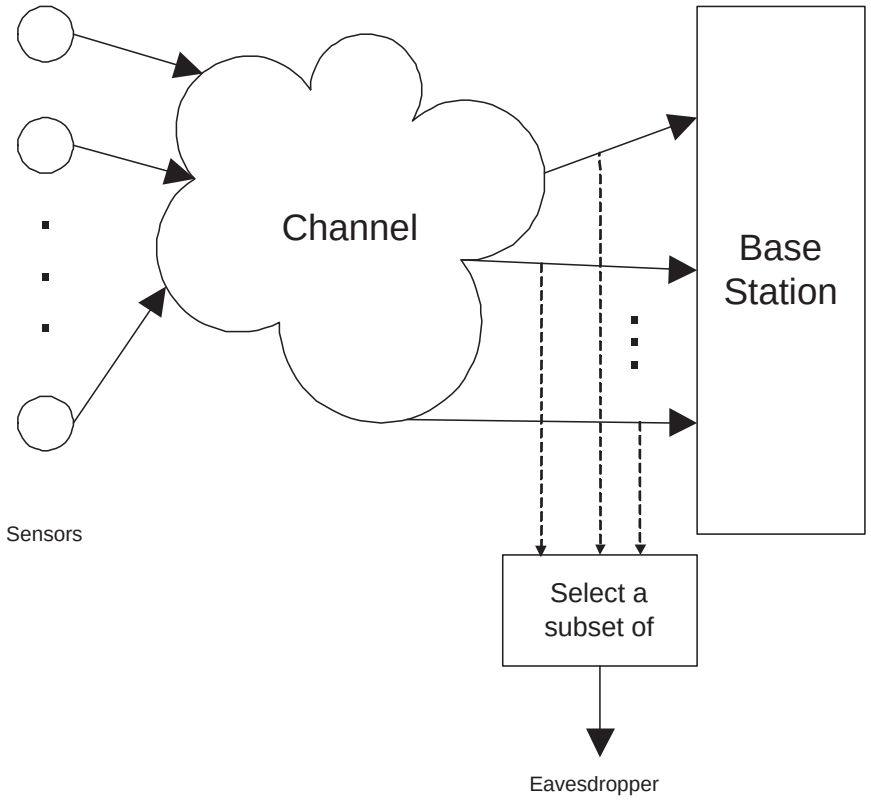

Fig. 2. General Sensor Network

tion of the sensor network challenges and opportunities as discussed in Section II-A. As shown in Fig. 2, we consider the case where many sensor nodes collect (possibly correlated) data and wish to encode their messages separately to alleviate the communication burden. At the same time, the challenge of a dynamic routing topology limits the eavesdropper's interception rate to a fraction of the total messages. This point is illustrated in Fig. 2 via the block titled "select a subset of" nodes, referring to the attacker's limitations. It is important to note that in this formulation we do not consider intermediate node processing (such as aggregation), since our approach enables the nodes to encode their data locally with efficiency (i.e. with near maximum achievable compression). However, since the data from all the nodes is available

at the base station (or cluster-head in the case of hierarchical topologies), additional processing may be performed at that stage with the benefit of shifting the processing away from the power-limited nodes towards the more powerful unit.

We now outline and discuss the main features of our assumed security model. In the terminology of our work, once a node's message is *encoded*, it is referred to as a *share* or *encoded message*. Our problem formulation states that the adversary only has access to a small subset (to be defined) of shares generated by the nodes as shown in Fig. 2. This is a reasonable assumption and requirement, especially if the environment is so large that the adversary cannot cover all possible paths back to the base station. We note that this assumption has also been made in the secret sharing literature [14], though it has not been previously exploited in an information theoretic consideration of sensor networks. The "limited shares" model of the eavesdropping attacker may thus be a far more suitable model in the context of sensor networks.

In the event that the limited shares requirement is *not* satisfied however, the methodology presented in our work is still applicable to sensor networks via *limited* integration with key-based methods. Specifically, if the condition is not satisfied, the eavesdropper has access to all shares generated by the nodes. In this scenario, confidentiality based purely on our methods is not achievable. However, if conventional key-based encryption is used at a *limited* number of nodes, the eavesdropper's situation returns to the case where he is missing shares. In other words, if some shares are additionally encrypted with keys, they become useless to the eavesdropper and thus he has in his possession only a subset of usable shares (satisfying the original limited shares assumption). Thus our model complements existing cryptographic schemes efficiently. We also note that the overarching goal of encoding in our problem is to jointly (and optimally) achieve secrecy and compression, or error correction. Thus even if additional (limited) encryption via keys is required, our encoding stage is not

wasted as it performs compression and error correction coding.

C. Information Theoretic Approach to Secrecy

In Section II-E we provide a full review of the state-of-the-art concerning the use of information theory in cryptography. The aim of the current section is to provide an efficient background summary with some key definitions, in preview of the full literature review.

Shannon [15] was the first to propose the concept of *conditional* entropy (equivocation), which measures the number of bits of plaintext (the unencrypted message) that is protected when the eavesdropper has in his possession the ciphertext (the encrypted message). He defined *unconditional* secrecy as the condition where an eavesdropper with unlimited computational time and complexity is unable to learn anything regarding the plaintext by intercepting the ciphertext alone. Importantly, he showed that in order to achieve unconditional secrecy, a secret key with the same number of bits as the plaintext is *necessary*. Unfortunately this result effectively states that to completely protect a message, one may as well just send this message through a completely protected channel, since the establishment of a secret key mimics this action. Whereas the secret key gives the legitimate party an advantage over the eavesdropping adversary, the subsequent work of Wyner's wiretap channel [10] gives the legitimate party a better channel than that of the eavesdropper, thus creating an advantage for the legitimate party [16]. Since its inception, the wiretap channel has been developed fundamentally by leading authorities [17]–[19], [11], [20], [21]. All recent works are based on these fundamental works including our research.

D. Differences from the Key Exchange & Management Approach to Secrecy

Traditional key-based cryptography is not the focus of our research, however we wish to briefly list some differences between the security considered in this dissertation and the paradigms explored in the key-based literature.

Traditional key-based security solutions generally require:

- The periodic refreshing of keys
- The off-line creation of keys (with the exception of information-theoretic key exchange)
- The possession of matching keys by the base station (either the same keys in the symmetric ciphers case, or different/private keys in the asymmetric ciphers case)
- The safe-guarding of keys against an adversary (i.e. the keys must not be disclosed)

In contrast, the physical layer security considered in this research mimics the *effect* of a key by exploiting the inherent noise or randomness already present in the environment in the form of channel noise and interference from other nodes. In other words, it is the inherent randomness already present in the sensor network setting that is utilized to encipher the contents of the data. This signifies that the manual refreshing of keys is no longer required. Furthermore, since the noise-based randomness is readily available in the environment, the "key" is generated and available in real-time. However the most significant drawback of the key-based approach which we resolve in our method, is the requirement for the intended receiving party to have a matching key. In our work, the intended recipient must have a matching *codebook* instead. However the

required codebooks may be disclosed publically, even to the adversary, and thus they do not need to be refreshed or kept secret. In contrast, the key-based solution in sensor networks requires that keys must be refreshed often due to the removal and addition of nodes. Thus in the key-based approach, the base station must keep track of the corresponding deletion and creation of keys which is less efficient than in our approach.

E. Literature Review and Classification

The extensive field of cryptography may be classified into five main areas based on the objectives under consideration as shown in Fig. 3. These five main areas consist of confidentiality (protection from eavesdropping), data integrity (protection from alteration), authentication (protection from false identity), non-repudiation (protection against non-commitment), and availability (protection against denial of service) [22]–[25]. The focus of our research is the core *confidentiality* service which is of central importance in sensor networks and other distributed networks. Within the area of confidentiality, there are two main well-developed paradigms in cryptography and two related areas which we mention for completeness. The two main areas of confidentiality are computational number theory (for public-key cryptography) and information theory. The former has been used not only for analysis purposes but also for practical implementation, while the latter has mainly been used for theoretical analysis. The adjoining paradigm of signal processing shown in Fig. 3 does not itself provide security, however it is often used in combination with asymmetric or symmetric key cryptographic schemes and it is listed for perspective and completeness [26]. The algebra paradigm also shown in Fig. 3 refers to symmetric-key cryptography or block ciphers such as the Data Encryption Standard (DES) or the Advanced Encryption

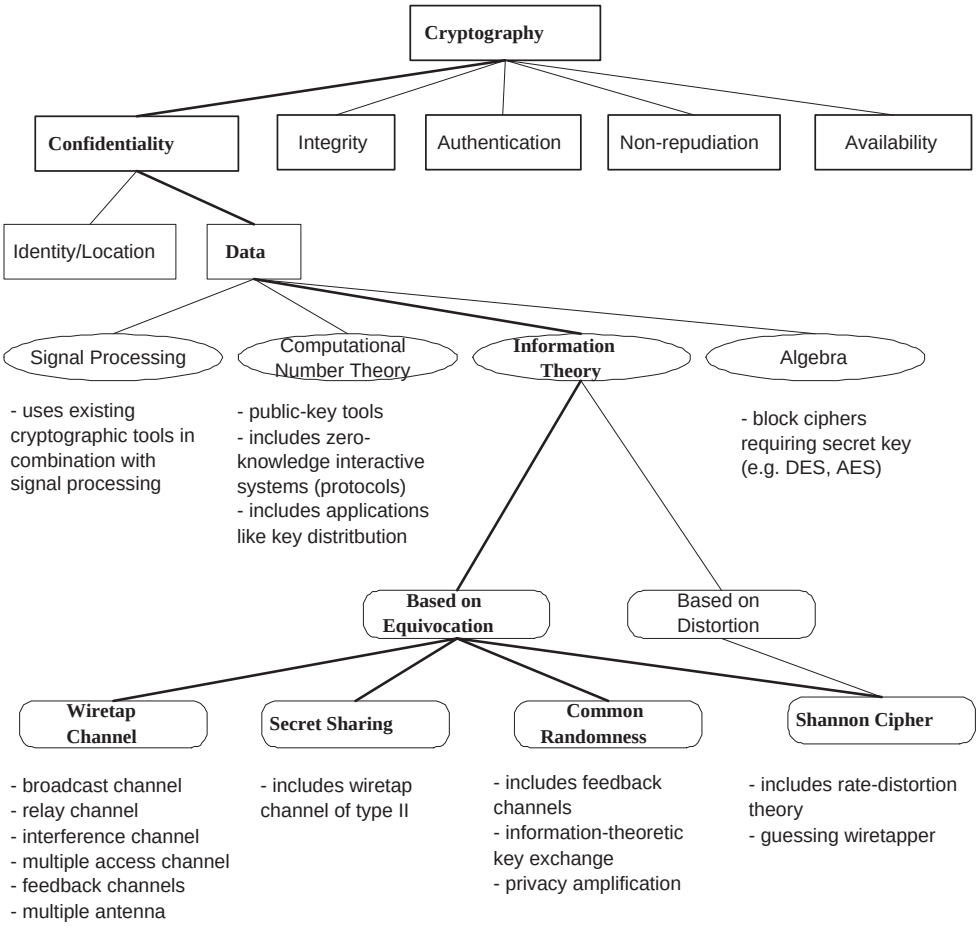

Fig. 3. Classification of Research (Bold Indicates Elements in Research)

Standard (AES). In our research we focus solely on the use of the information theoretic approach. We employ Fig. 3 both as a classification mechanism and as a means of visualizing the intended depth and breadth of our proposed research. The text which appears in bold letters in Fig. 3 indicates areas explored in our research. We note that the bottom layer of the classification scheme which reflects our research is quite broad, covering many areas in the realm of information theory. Thus we refrain from confining our research to a single area within the information theoretic approach in hopes of offering a broader and more complete solution.

Finally we would like to point out that the information theoretic security research belongs to the physical network layer, whereas the other security paradigms and approaches are typically formulated and explored at the other network layers as depicted in Fig. 4. The benefit of physical layer security is that it is performed

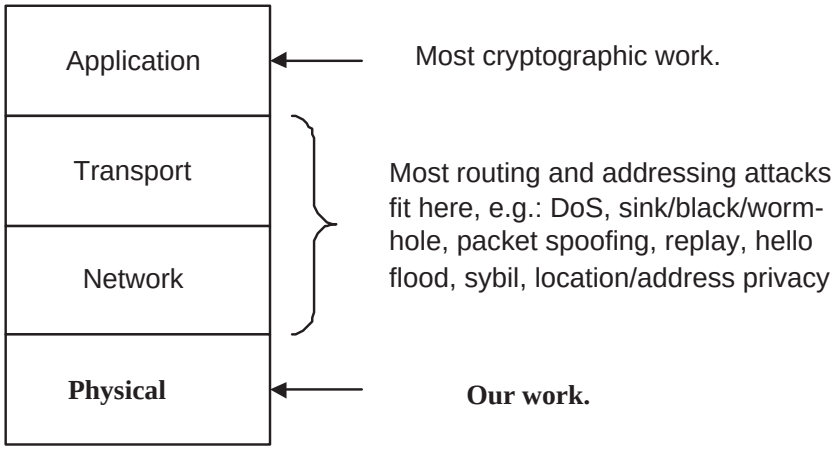

Fig. 4. Information-theoretic Security in the Physical Layer

jointly with either source or channel coding. This signifies that overall, the physical layer approach should perform more efficiently (faster) than other approaches and thus achieve performance which is more typical of cross-layer algorithms.

We now provide a description intended to further place our problem within the existing information theoretic cryptography community. Within this community, a wide range of problems have been extensively studied. The wiretap channel mentioned in Section II-B is the most popular current area of research in information theoretic security. Researchers working in this area have analyzed the tradeoff between secrecy/equivocation and channel coding for all the classical channels. In contrast, the area of secret sharing experienced its highlight in the 1990's, and thus most of the work in this area has been completed. Finally, the area of common randomness

and privacy amplification continues to be examined and has yielded an information-theoretically secure protocol to exchange secret keys, which may then be used in block and Shannon ciphers. We now provide an overview of these areas shown as the bottom layer in Fig. 3.

1. The Wiretap Channel

We summarize some of the most important definitions and results within this well-studied area of research. Due to the volume of work in this area, we will only describe the problems and their similarities or differences to our problem.

a. Relay Channel

The relay channel with confidential messages is studied in the works of [27]–[29]. In the setup, one party communicates with another party directly, as well as through a relay node, which is used to help increase the capacity between the two parties. In the case where a relay node is used, a requirement is placed which mandates that the relay be kept ignorant of the secret message being transmitted. In a slightly different setup [30], the relay node, which is usually used to help increase the capacity between the legitimate parties, is used to increase the capacity for the eavesdropper instead.

b. Distributed Encryption

This area introduces a model similar to ours in that the attacker is allowed to eavesdrop on a subset of the encoded messages [31]. However the authors *only* showed that unconditional secrecy is unachievable when the encoders are determinstic and when the channels are noiseless. In contrast, we derive the *entire* capacity region (tradeoff between secrecy and compression) without such an assumption (i.e. by including stochastic encoders). Thus part of our research generalizes and completely

characterizes the problem in [31]. Finally we provide codes that achieve the promised tradeoffs, whereas [31] does not provide a practical implementation.

c. Multiple Access Channel

In [32]–[34] the multiple access channel with confidential messages is studied. The two senders can also listen to the channel, thus receiving a noisy version of the other sender's message. Each sender would like to keep the other sender ignorant regarding his or her own secret message.

d. Interference Channel

In [35]–[37], the interference channel with confidential messages is considered. Two transmitters wish to send to two different base stations, however their signals interfere with one another. The base stations thus receive not only the intended message, but also a noisy message from the unintended sender. The goal is to keep each base station ignorant of the unintended secret messages. In our work we have one base station that receives both messages, thus the base station performs joint decoding. The interference wiretap channel is also specialized to the case when one of the transmitter's role is to interfere or jam one of the base stations, which belongs to the eavesdropper [38]–[42].

e. Broadcast Channel

In [10], [17]–[19], [11], [20], [21], [43], [35], [36], [44] the broadcast channel with confidential messages is studied under several setups and assumptions. The most general setup is that one sender broadcasts signals containing multiple messages to multiple base stations. The goal is for each base station to be kept ignorant of those secret messages not intended for that base station. In [45]–[50] the broadcast channels are

considered with random fading, thus making these results appropriate for wireless communications.

f. MIMO Channel

The multiple-input multiple-output (MIMO) wiretap channel has recently received much attention [51]–[62]. In this setting, the sender, receiver, and eavesdropper may each be equipped with multiple antennas. The characterization of the secrecy capacity under this setting is difficult, and two different schools of thought have arisen. In [57], [61], a Sato-like argument is applied in which the legitimate receiver is given the wiretap output as well (i.e. genie-aided), and the secrecy capacity for this upper bound is minimized. It is shown that the resulting minimized upper bound is actually the secrecy capacity region of the MIMO wiretap channel. In [62] a different approach is used in which the legitimate receiver's channel is enhanced such that the secrecy capacity is preserved while permitting results from degraded wiretap channel to be applied. In [63], [64] the MIMO wiretap channel is generalized to the case in which both receivers are to receive legitimate messages intended for each receiver, but to be kept ignorant of each other's messages.

g. Feedback Channel

The presence of feedback provides the wiretap channel with several advantages. First, when the legitimate channel is more noisy than the wiretap channel, feedback may permit unconditional secrecy, whereas without feedback this is not possible [65], [66], [8]. In addition when both forward and feedback channels are noisy, it may be possible to increase the secrecy capacity to the usual one-way capacity without secrecy [67], [68]. Finally the role of feedback in multiple user channels has be explored and found to aid secrecy [69]. In contrast, feedback will be shown to provide no advantage in

our problem.

2. Secret Sharing and the Wiretap Channel II

Secret sharing [14], [70]–[72] is a well-studied research area in which one node with one secret creates and distributes several shares to distinct nodes. Each node alone is incapable of knowing the secret, however a certain combination of the shares allows the secret to be reconstructed. A bibliography containing more than 200 publications dealing with secret sharing from its inception to 1998 is presented in [73]. The wiretap channel II [74]–[77] problem is similar to the secret sharing problem in that each of the letters in a wiretap channel II codeword can be viewed as an individual share. An eavesdropper is given a subset of these shares via nature (erasure channel), thus there is either a chance that the eavesdropper will receive many shares or only a few.

3. Common Randomness and Privacy Amplification

The general setup of the works of [66], [78], [8], [9], [79]–[82] is that two parties, A and B, share a pair of correlated random vectors while a third eavesdropping party also has a vector correlated with the two. The goal is for the two parties to distill a secret key from their correlated random vectors that the eavesdropper is completely oblivious to. The steps taken are: (1) reconciliation, in which party A sends additional information to party B (and thus to the eavesdropper as well) through a noisy channel so that party B can reproduce party A's vector; (2) privacy amplification, in which party A sends to party B (and to the eavesdropper) a hash function from the class of universal hash functions; (3) key distillation in which both parties apply the hash to their common vectors, thus producing a secret key completely unknown to the eavesdropper. The secret key can thus be used as a one-time-pad to completely secure any confidential message of the same length. In [83], the setup is similar

except instead of exchanging a key between A and B, the goal is for A to securely transmit its random vector (correlated with B and the eavesdropper) to B, such that it is secure from the eavesdropper; thus in this case the message itself should be protected.

4. Comparison of Our Research to Related Work

We now compare our work to the literature briefed above. Table I shows the different criteria (rows) being compared against the different information theory secrecy works (columns). An entry of Yes/No means that only in certain cases has the criterion been considered. For the first seven criteria, answering No does not signify a weakness in the work, but rather an inappropriateness for a wireless sensor network.

Table I. Comparison with Related Work

	Ours	Relay	MAC	Int.	Br./MIMO	SS
1. Separate Encoding	Yes	No	Yes	Yes	No	No
2. Joint Decoding	Yes	Yes	Yes/No	No	No	Yes
3. Coop. Enc. Nodes	Yes	No	Yes/No	Yes/No	N/A	N/A
4. Multiple Messages	Yes	No	Yes	Yes	Yes	Yes/No
5. Multiple Routes	Yes	Yes	Yes/No	Yes	Yes	Yes
6. Keyless	Yes	Yes	Yes	Yes	Yes	Yes
7. Random Fading	Yes	-	-	-	Yes/No	N/A
8. Rate-Distortion	Yes	-	-	-	-	-

First the following non-standard abbreviations are explained: MAC (multiple access channel), Int. (interference channel), Br. (broadcast channel), SS (secret sharing). The Separate Encoding criterion is essential in sensor networks to reduce

network traffic, as well as to save power and communication resources. Furthermore, nodes should perform the encoding locally to avoid transmitting unprotected data to a central authority for processing. The Joint Decoding criterion means that there is one base station that receives all message from the sensors including those intercepted by the eavesdropper. We assume that the eavesdropper may acquire a subset of the base station's received signals since there may be insider attacks at the base station; thus this models a worst case scenario in which most wiretap channel problems do not consider. The Cooperative Encoding Nodes criterion means that all encoding nodes are working towards the same objective and are thus collaborative. This is in contrast with a cellular network where all the users wish to achieve a high throughput but do not necessarily collaborate. The Multiple Messages criterion arises from the fact that each node sends a different (but possibly correlated message). The Keyless Criterion was motivated at the beginning of this dissertation as an efficient alternative sensor network approach. The Random Fading criterion is suitable for wireless communications in various outdoor settings such as in sensor networks. Finally, the Rate-Distortion criterion is relevant to visual sensor networks since media such as video or images are typically compressed in a lossy manner. We thus consider the use of rate-distortion theory in our work as presented in [84]. We note that the use of rate-distortion theory with secrecy has been studied by Yamamoto [85]–[87]. Also in [88], a source coding and secrecy problem is considered in which the legitimate receiver also receives side information, whereas the eavesdropper receives the same encoded message as the legitimate receiver, but without any additional side information.

We would like to point out that the above literature survey includes only theoretical results. Practical coding research for the wiretap channel is growing in the following three areas: (1) wiretap channel coding [89], [82], [90], 2) source coding and secrecy, which have not been widely studied to-date [91] rendering our work in

Chapter IV pioneering in nature, and finally (3), the wiretap channel II, which is the most extensively-studied of the three listed coding problems [92].

5. Relationship of Existing Literature to Our Work

Our research takes on elements of all the above reviewed works and we now further elaborate on how they are related. From a problem point-of-view, our security model is similar to the secret sharing and wiretap channel II problem in that an eavesdropper is only permitted to eavesdrop on a small subset of all encoded messages, whereas the base station receives all the encoded messages. The difference is that in our work we require that all nodes encode their messages separately without communicating with one another, whereas in the secret sharing and wiretap channel II problem one central authority encodes all the messages. Furthermore in most wiretap channels (such as the broadcast channel), one node broadcasts messages to several nodes. In our problem we consider the reverse scenario: several nodes send messages to one node, namely the base station. In the setup of other wiretap channels such as the multiple access channel (MAC) and the interference channel (Int.), several nodes send to one base station. However the base station does not receive the encoded messages that are intercepted by the eavesdropper. In other words the eavesdropper and the legitimate base station have different channels, which is not the case in our problem setup. In our work elements of secret sharing, as well as the wiretap channel (MAC and interference) will be combined in a novel way and used in our solution.

CHAPTER III

MULTITERMINAL SOURCE CODING AND DISTRIBUTED SECRECY*

In this chapter we analyze the interaction between source coding and secrecy using multiterminal source coding theorems [5]–[7]. We derive inner and outer regions for the set of all source coding and equivocation (measure of secrecy) rates (which we call the capacity region) for user-defined distortion criteria. We show that unconditional secrecy is only achievable if the distortion is maximal, which means no information is sent. We then show that feedback from the base station to the legitimate users does not improve equivocation. We do this by deriving an upper bound on the secret key rate that can be achieved *without* feedback, and by comparing this to an upper bound on the secret key rate using feedback [8], [9].

The system model studied in this chapter is motivated by the idea that a cluster of sensors within close proximity of one another is likely to record correlated readings. In keeping with the inter-node communicationless and keyless requirements introduced and motivated in Chapter I, our sensor nodes encode independently and without using any secret materials (e.g. cryptographic keys). On the other hand, the eavesdropper faces the challenge of a large world that makes it difficult to collect many encoded messages (i.e. only a proper subset of encoded messages can be intercepted by the eavesdropper), which was motivated in Chapter II.

---

*Part of the material in this chapter is reprinted with permission from W. Luh and D. Kundur, "Distributed Keyless Security for Correlated Data with Applications in Visual Sensor Networks" in *Proc. ACM Multimedia and Security Workshop*, Dallas, Texas, September 2007, pp. 75-86. http://doi.acm.org/10.1145/1288869.128881

A. System Model

For clarity in presentation, we consider a two-node sensor network. Fig. 5 summarizes the source coding aspect of our problem in this chapter. Let $S_A^k \in \mathcal{S}_A^k$ and $S_B^k \in \mathcal{S}_B^k$ denote Alice's and Bob's messages, respectively. Alice's and Bob's messages are generated by a joint discrete memoryless source (DMS) given by Eq. 3.1.

$$P_{S_A,S_B}^k(s_A^k, s_B^k) = \prod_{i=1}^{k} P_{S_A,S_B}(s_{A,i}, s_{B,i}) \tag{3.1}$$

Alice and Bob are to encipher their S_A^k, S_B^k *separately without cooperation* creating $W_A \in \mathcal{W}_A$ and $W_B \in \mathcal{W}_B$, respectively, where $\mathcal{W}_A, \mathcal{W}_B$ are finite sets.

The base station (BS) receives both W_A and W_B, and its goal is to reconstruct S_A^k and S_B^k within some fidelity criterion to be discussed below. Let the quadruple $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$ denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the BS's decoders to reconstruct Alice's and Bob's messages, respectively. Here $f_A^k : \mathcal{S}_A^k \to \mathcal{W}_A$, $f_B^k : \mathcal{S}_B^k \to \mathcal{W}_B$, $\varphi_A^k : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}_A^k$, and $\varphi_B^k : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}_B^k$, where $\hat{\mathcal{S}}_A^k$ and $\hat{\mathcal{S}}_B^k$ are the finite reconstruction alphabets for Alice and Bob, respectively.

If the encoders f_A^k, f_B^k are stochastic, they can be defined without loss of generality by deterministic encoders f'^k_A, f'^k_B, where the randomness comes from locally generated RVs T_A, T_B, respectively as shown below.

$$W_A = f_A^k(S_A^k) = f'^k_A(S_A^k, T_A) \tag{3.2}$$

$$W_B = f_B^k(S_B^k) = f'^k_B(S_B^k, T_B) \tag{3.3}$$

The random variables T_A, T_B may for example simulate choosing a codeword randomly from the subsets of $\mathcal{W}_A, \mathcal{W}_B$, respectively.

Let $\rho_A^k : \mathcal{S}_A^k \times \hat{\mathcal{S}}_A^k \to \mathbb{R}^+$ be the *block* distortion measure between Alice's original

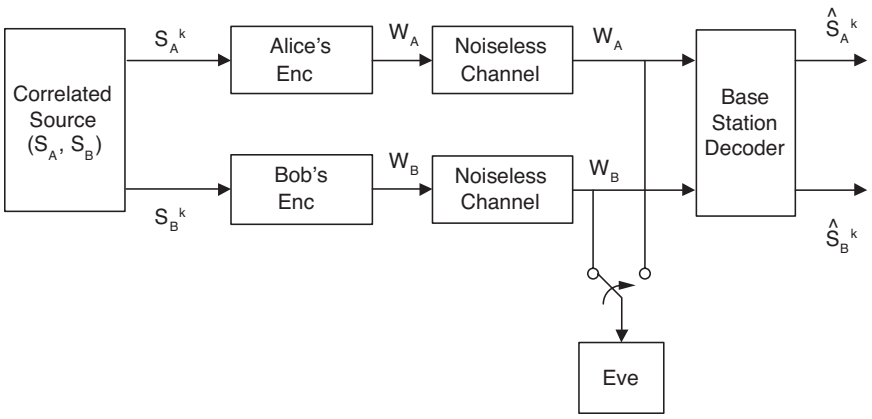

Fig. 5. Distributed Source Coding for Secrecy with Distortion Criteria Model

message block s_A^k and the BS's reconstruction $\hat{s}_A^k$; similarly $\rho_B^k : \mathcal{S}_B^k \times \hat{\mathcal{S}}_B^k \to \mathbb{R}^+$ is the block distortion measure for Bob's message. Following Shannon rate-distortion theory, the block distortion measures are defined by *single-letter* distortion measures $\rho_j : \mathcal{S}_j \times \hat{\mathcal{S}}_j \to \mathbb{R}^+$ for $j = A, B$ so that the block distortion measure is an average of the single-letter distortion measures as in Eq. 3.4.

$$\rho_j^k(s_j^k, \hat{s}_j^k) = \frac{1}{k} \sum_{i=1}^{k} \rho_j(s_{j,i}, \hat{s}_{j,i}), \quad j = A, B \tag{3.4}$$

Hence the BS's reconstruction distortion criteria can be specified by two real non-negative numbers representing Alice's and Bob's messages, $D_A > 0$ and $D_B > 0$, respectively, such that the expected distortion is bounded by these two numbers as in Eqs. 3.5 and 3.6 for $\epsilon > 0$ arbitrarily small. The expectation is taken over all random quantities, such as the original message blocks S_A^k, S_B^k, as well as the possibly stochastic encoders f_A^k, f_B^k via T_A, T_B, respectively.

$$\mathbb{E}[\rho_A^k(S_A^k, \hat{S}_A^k)] \leq D_A + \epsilon \tag{3.5}$$

$$\mathbb{E}[\rho_B^k(S_B^k, \hat{S}_B^k)] \leq D_B + \epsilon \tag{3.6}$$

In other words, for a distortion pair (D_A, D_B), the encoders and decoders $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$ satisfying Eqs. 3.5 and 3.6 are said to satisfy the distortion criteria (D_A, D_B).

The (source coding) rates of Alice's and Bob's enciphered messages are defined as

$$R_A \triangleq \frac{\log_2 |\mathcal{W}_A|}{k} \tag{3.7}$$

$$R_B \triangleq \frac{\log_2 |\mathcal{W}_B|}{k}. \tag{3.8}$$

In Fig. 5, the eavesdropper, referred to as Eve, is allowed to select either W_A or W_B, but not both. To justify our definition of secrecy we require $H(S_A) = H(S_B)$, which is equivalent to Alice and Bob sensing the same phenomenon in the same physical space. Depending on which enciphered message Eve selects, the equivocation rates of Eve w.r.t. Alice and Bob are defined as

$$\Delta_A \triangleq \frac{H(S_A^k|W_A)}{k} \tag{3.9}$$

$$\Delta_B \triangleq \frac{H(S_B^k|W_B)}{k}. \tag{3.10}$$

A stronger definition of secrecy would be to replace the numerators in Eqs. 3.9 and 3.10 with $H(S_A^k, S_B^k|W_i)$, however Eqs. 3.9 and 3.10 are defined to simplify the model, and can be justified as follows. Assume Eve intercepts W_A, then $S_B^k \leftrightarrow S_A^k \leftrightarrow W_A$ form a Markov chain and by the data processing inequality, Eve learns less about S_B^k than she does of S_A^k. Formally we can write

$$\begin{aligned} H(S_A^k, S_B^k|W_A) &\overset{(a)}{=} H(S_B^k|W_A) + H(S_A^k|W_A, S_B^k) \\ &= H(S_A^k|W_A) + H(S_B^k|W_A, S_A^k) \\ &\overset{(b)}{=} H(S_A^k|W_A) + H(S_B^k|S_A^k) \\ &\overset{(c)}{=} H(S_A^k|W_A) + H(S_A^k|S_B^k) \end{aligned}$$

where (b) follows from the Markov chain $S_B^k \leftrightarrow S_A^k \leftrightarrow W_A$, and (c) from the assumption $H(S_A) = H(S_B)$. Thus we then have $H(S_A^k|W_A) \leq H(S_B^k|W_A)$ by comparing (a) and (c).[1]

Definition 1 *A quadruple* (d_A, d_B, r_A, r_B) *corresponding to* $(\Delta_A, \Delta_B, R_A, R_B)$ *is* achievable *w.r.t* (D_A, D_B) *if there exists a sequence of encoders and decoders* $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$ *such that as* $k \to \infty$

$$\begin{aligned} R_A &\leq r_A + \epsilon && (3.11)\\ R_B &\leq r_B + \epsilon && (3.12)\\ d_A - \epsilon \leq \Delta_A &\leq d_A && (3.13)\\ d_B - \epsilon \leq \Delta_B &\leq d_B && (3.14) \end{aligned}$$

for $\epsilon > 0$ *arbitrarily small and such that Eqs. 3.5 and 3.6 are also satisfied. In addition, all parties, Alice, Bob, and Eve, have complete knowledge of* f_A^k, f_B^k *(except for the possibly locally generated RVs* T_A, T_B*), and any cryptographic keys used.*

B. Capacity Region

The capacity region $\mathcal{R}(D_A, D_B)$ is defined to be the set of *all* quadruples (d_A, d_B, r_A, r_B) that are achievable w.r.t to the distortion criteria (D_A, D_B). Outer and inner regions, $\mathcal{R}_{out}(D_A, D_B)$ and $\mathcal{R}_{in}(D_A, D_B)$ are defined to be sets such that

$$\mathcal{R}_{in}(D_A, D_B) \subseteq \mathcal{R}(D_A, D_B) \subseteq \mathcal{R}_{out}(D_A, D_B).$$

[1] Since we are deriving a negative result, by showing unconditional secrecy is unachievable under this weaker definition of secrecy (Eqs. 3.9 and 3.10), we are necessarily implying that unconditional secrecy is also unachievable under the stronger definition.

The inner region is any set of equivocation and source coding rates in which one can find some coding scheme to *achieve* these equivocation and source coding rates. On the other hand the outer region is any set of equivocation and source coding rates such that any such rates *not* in this set are necessarily *not* achievable, i.e. there exists no coding scheme to achieve rates outside the outer region. Of course the goal is to find inner and outer regions equal to one another, which equals the capacity region $\mathcal{R}(D_A, D_B)$ itself. Generally

$$\mathcal{R}_{in}(D_A, D_B) \neq \mathcal{R}_{out}(D_A, D_B),$$

due to the existing gap between the outer and inner regions for the multiterminal source coding (MSC) problem [5]–[7]. However, in some special cases, the inner and outer regions converge.

Definition 2 *Define $\mathcal{P}(D_A, D_B)$ as the set of auxiliary RVs (Q_A, Q_B) jointly distributed with (S_A, S_B) such that:*

(i) $Q_A \leftrightarrow S_A \leftrightarrow S_B$ and $S_A \leftrightarrow S_B \leftrightarrow Q_B$;

(ii) there exist functions $F_A : \mathcal{Q}_A \times \mathcal{Q}_B \to \hat{\mathcal{S}}_A$ and $F_B : \mathcal{Q}_A \times \mathcal{Q}_B \to \hat{\mathcal{S}}_B$ such that

$$\mathbb{E}[\rho_A(S_A, \hat{S}_A)] \leq D_A \tag{3.15}$$

$$\mathbb{E}[\rho_B(S_B, \hat{S}_B)] \leq D_B \tag{3.16}$$

where

$$\hat{S}_A = F_A(Q_A, Q_B) \tag{3.17}$$

$$\hat{S}_B = F_B(Q_A, Q_B). \tag{3.18}$$

Theorem 1 (Outer Region) *For a fixed $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$ define $\mathcal{R}_o(Q_A, Q_B)$*

to be the set of all (d_A, d_B, r_A, r_B) *that satisfy*

$$\begin{aligned} 0 \le d_A &\le H(S_A) && (3.19)\\ 0 \le d_B &\le H(S_B) && (3.20)\\ d_A + d_B &\le H(S_A) + H(S_B) - I(S_A, S_B; Q_A, Q_B) && (3.21) \end{aligned}$$

$$\begin{aligned} r_A &\ge I(Q_A; S_A, S_B|Q_B) && (3.22)\\ r_B &\ge I(Q_B; S_A, S_B|Q_A) && (3.23)\\ r_A + r_B &\ge I(S_A, S_B; Q_A, Q_B) && (3.24)\\ r_A + d_A &\ge H(S_A) && (3.25)\\ r_B + d_B &\ge H(S_B). && (3.26) \end{aligned}$$

Then

$$\mathcal{R}_{out}(D_A, D_B) \triangleq \bigcup_{(Q_A,Q_B)\in\mathcal{P}(D_A,D_B)} \mathcal{R}_o(Q_A, Q_B)$$

is an outer region.

Theorem 1 is proved in Section III-D-1.

Theorem 2 (Inner Region) *For a fixed* $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$ *define* $\mathcal{R}_i(Q_A, Q_B)$ *to be the set of all* (d_A, d_B, r_A, r_B) *that satisfy*

$$\begin{aligned} 0 \le d_A &\le H(S_A) && (3.27)\\ 0 \le d_B &\le H(S_B) && (3.28)\\ d_A + d_B &\le I(S_A; S_B) + H(S_A|S_B, Q_A) + H(S_B|S_A, Q_B) && (3.29) \end{aligned}$$

$$
\begin{aligned}
r_A &\geq I(S_A; S_B, Q_A|Q_B) && (3.30)\\
r_B &\geq I(S_B; S_A, Q_B|Q_A) && (3.31)\\
r_A + r_B &\geq H(S_A, S_B) - H(S_A|S_B, Q_A) - H(S_B|S_A, Q_B) && (3.32)\\
r_A + d_A &\geq H(S_A) && (3.33)\\
r_B + d_B &\geq H(S_B). && (3.34)
\end{aligned}
$$

Then

$$\mathcal{R}_{in}(D_A, D_B) \triangleq \bigcup_{(Q_A,Q_B)\in\mathcal{P}(D_A,D_B)} \mathcal{R}_i(Q_A, Q_B)$$

is an inner region.

Theorem 2 is proved in Section III-D-2.

1. Discussion

From Theorems 1 and 2 we can conclude that unconditional secrecy is in general impossible. Also in general, the outer and inner regions do not match. The capacity region is a 4-dimensional hyper-polygon. Since we are interested in the amount of equivocation (secrecy) that is achievable, Fig. 6 depicts a 2-dimensional projection of the general hyper-polygon onto the variables of interest: Δ_A, Δ_B; the polygons are the achievable equivocation rates for Alice and Bob parametrized by their source coding rates R_A, R_B (this relation is not shown in Fig. 6) for various cases.

The worst case (corresponding to the smallest triangle region) occurs when Alice and Bob process different (but correlated) messages under a zero-distortion criterion (that is the base station is required to reconstruct each of Alice's and Bob's messages S_A^k, S_B^k perfectly). Neither Alice nor Bob can achieve unconditional secrecy since the diagonal line corresponds to $I(S_A, S_B)$, which is strictly less than $H(S_i)$ for $i = A, B$ required for unconditional secrecy. Also, the less correlated S_A^k, S_B^k, the smaller the

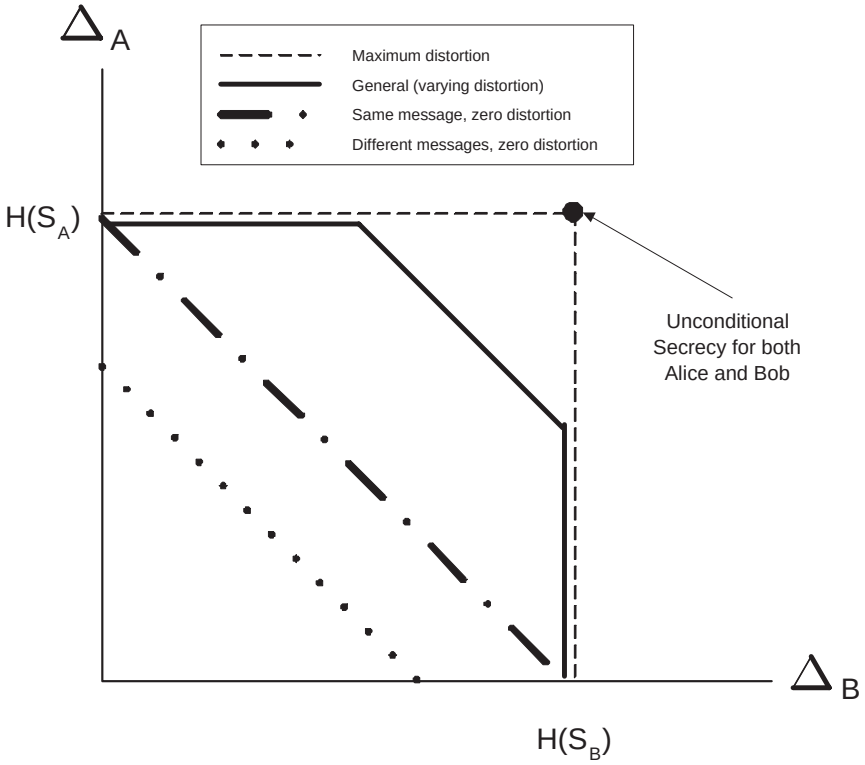

Fig. 6. Equivication Rate Regions

equivocation rate region.

When the correlation is "perfect" in the sense that Alice and Bob are processing the *same* message, i.e. $S_A^k = S_B^k$, the corresponding equivocation rate region is the largest triangular region. In this case Alice or Bob may achieve unconditional secrecy, but not simulatenously; if Alice achieves unconditional secrecy, then Bob has no secrecy (zero equivocation). The interpretation of this scenario is that Alice sends nothing to the base station, while Bob sends the entire unenciphered message to the base station. Alice and Bob's secrecy can be thought of as being "shared" on the diagonal line of the triangular equivocation rate region. What is interesting about this result is not the achievability (sufficiency result), but rather the impossibility

of achieving any pair of equivocation rates that do not follow this "shared" secrecy interpretation, i.e. the diagonal line.

By allowing distortion upon decoding at the base station, the equivocation rate region becomes a pentagon. Increasing distortion increases the vertical and horizontal lines in the pentagon, while reducing the length of the diagonal line. When the distortion is maximal, the pentagon degenerates (diagonal disappears) to the square in which case, the desired maximum equivocation for Alice and Bob (i.e. unconditional secrecy) is included in the outer region. Whereas in the above two cases the inner and outer regions match, in general, given distortion criteria the inner and outer regions do not match.

The above discussion shows that unconditional secrecy may be achieved only when the distortion is maximal, which implies nothing useful is sent from Alice and Bob. This also suggests that adding (independent) noise alone, either by the encoders or via independent channels gives no secrecy advantages as it usually does in other wiretap channels.

C. Feedback and Equivocation Rate

We show that feedback from the receiver (base station) to the legitimate encoding parties (Alice and Bob) generally does not increase secrecy if all channels including Eve's channel are noiseless, even if Eve is permitted to eavesdrop on *only* one of the feedback streams. This is in contrast with the wiretap channel with feedback results in [65], [66], [8], [9], [80], [68] in which public feedback does increase secrecy.

We consider different types of feedback that can occur based on the three criteria listed in Table II. These three criteria are True Feedback (as opposed to Artificial Feedback), Knowledge of Previous Eavesdrop, and Knowledge of Future Feedback

Table II. Different Types of Base Station Feedback

	Yes	No
True Feedback (as opposed to artificial feedback)?	1	0
Knowledge of Previous Eavesdrop?	1	0
Knowledge of Future Feedback Eavesdrop?	1	0

Eavesdrop. In the first criterion, the receiver can send information to Alice and Bob, Z_A and Z_B, respectively, based on the $\hat{s}_A^k$ or $\hat{s}_B^k$ reconstructed from W_A and W_B (true feedback), or the BS can send arbitrary information independent from what it received from Alice and Bob (artificial feedback). In the second criterion, the receiver may either have knowledge of which W_j, for $j = A$ or $j = B$, Eve *previously* intercepted, or have no such knowledge. Finally in the third criterion, the receiver may have knowledge of which Z_j, $j = A$ or $j = B$ Eve *will* intercept, or have no such knowledge. These three criteria thus result in eight possible types of feedback. We can systematically analyze all the different feedback cases succinctly since we are only interested in whether secrecy capacity may be increased or not. Using Table II, the case 101 corresponds to: true feedback, no knowledge of previous eavesdrop, and knowledge of future feedback eavesdrop. The case *00 corresponds to either true or artificial feedback, no knowledge of previous eavesdrop, and knowledge of future feedback eavesdrop. We now summarize the salient results obtained for the various types of feedback:

- Case **1: If the BS knows Eve will not be eavesdropping on Z_B for instance, then the BS can add a tag to Z_B informing Bob that Z_B may be used as a one-time pad for Bob's future transmission to the BS, thus secrecy for Bob is increased via the one-time pad cipher.

- Case 110: Feedback either does not help or can actually decrease secrecy. The proof is given in Section III-D-3.
- Case 100: Without knowledge of what Eve possess, this case performs worst than the case 110.
- Case 0*0: Artificial feedback does not improve secrecy, nor does it decrease secrecy. The proof is given in Section III-D-3.

Note that although feedback does not improve secrecy in the Shannon equivocation sense, feedback can improve computational secrecy, e.g. BS sends the parties its public-key for asymmetric ciphers [25].

D. Proofs and Ancillary Results

1. Proof of Theorem 1

Assume that some (d_A, d_B, r_A, r_B) is achievable such that Eqs. 3.11 to 3.14 are satisfied along with the Markov constraint in Eq. 3.35.

$$W_B \leftrightarrow S_B^k \leftrightarrow S_A^k \leftrightarrow W_A \tag{3.35}$$

Then we shall show that the following bounds of Eqs. 3.19 to 3.26 for *all* $\epsilon > 0$ are necessarily true for fixed encoders and decoders $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$. Note that Eqs. 3.19 and 3.20 are trivial bounds. Eqs. 3.22 to 3.24 are multiterminal source coding bounds [5], [6].

First we prove Eq. 3.21. Before proceeding, we state a well known lemma.

Lemma 1 *If $X \leftrightarrow Y \leftrightarrow Z$ forms a Markov chain, then*

$$I(X;Y|Z) = I(X;Y) - I(X;Z). \tag{3.36}$$

Our goal is to upper and lower bound $I(S_A^k, S_B^k; W_A, W_B)$. First we derive the upper bound.

$$\begin{aligned} I(S_A^k, S_B^k; W_A, W_B) &= I(S_A^k; W_A, W_B) + I(S_B^k; W_A, W_B | S_A^k) \\ &= I(S_A^k; W_A) + I(S_A^k; W_B | W_A) + I(S_B^k; W_A, W_B | S_A^k) \\ &= I(S_A^k; W_A) + I(S_A^k; W_B | W_A) + I(S_B^k; W_A | S_A^k) \\ &\qquad + I(S_B^k; W_B | S_A^k, W_A) \\ &= I(S_A^k; W_A) + I(S_A^k; W_B | W_A) + I(S_B^k; W_B | S_A^k, W_A) \quad (3.37) \end{aligned}$$

since $I(S_B^k; W_A | S_A^k) = 0$. The original Markov chain of Eq. 3.35 induces $W_B \leftrightarrow S_B^k \leftrightarrow (S_A^k, W_A)$, and using Lemma 1 gives

$$\begin{aligned} I(S_B^k; W_B | S_A^k, W_A) &= I(S_B^k; W_B) - I(W_B; S_A^k, W_A) \\ &= I(S_B^k; W_B) - I(W_A; W_B) - I(S_A^k; W_B | W_A) \quad (3.38) \end{aligned}$$

where the final equality made use of the chain rule again. Therefore applying Eq. 3.38 to Eq. 3.37 gives

$$\begin{aligned} I(S_A^k, S_B^k; W_A, W_B) &= I(S_A^k; W_A) + I(S_B^k; W_B) - I(W_A; W_B) \\ &= H(S_A^k) - H(S_A^k | W_A) + H(S_B^k) - H(S_B^k | W_B) - I(W_A; W_B) \\ &\leq H(S_A^k) - H(S_A^k | W_A) + H(S_B^k) - H(S_B^k | W_B). \quad (3.39) \end{aligned}$$

The lower bound of $I(S_A^k, S_B^k; W_A, W_B)$ is stated in the following lemma, which is proved in [5], [6].

Lemma 2 *For a fixed* $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$

$$I(S_A^k, S_B^k; W_A, W_B) \geq k I(S_A, S_B; Q_A, Q_B). \quad (3.40)$$

where $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$ *is determined by the source statistics and* $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$.

Although Lemma 2 is derived for determinstic encoders, the lower bound also applies to stochastic encoders. Essentially the sum of the source coding rates is lower bounded by $I(S_A, S_B; Q_A, Q_B)$ for fixed encoders and decoders; using stochastic encoders would not lower this bound (i.e. stochastic encoders do not achieve better compression rates).

Now combining Eqs. 3.39 and 3.40, and then rearranging yields

$$H(S_A^k|W_A) + H(S_B^k|W_B) \leq H(S_A^k) + H(S_B^k) - kI(S_A, S_B; Q_A, Q_B). \tag{3.41}$$

Next, dividing by k and using the definitions in Eqs. 3.9, 3.10 and Eqs. 3.13, 3.14 gives

$$d_A + d_B \leq H(S_A) + H(S_B) - I(S_A, S_B; Q_A, Q_B) + 2\epsilon \tag{3.42}$$

proving Eq. 3.21.

Next we prove Eqs. 3.25 and 3.26, which follow simply from the chain rule:

$$\begin{aligned} H(S_A^k) &= kH(S_A) \leq H(S_A^k, W_A) = H(W_A) + H(S_A^k|W_A) \\ &\leq \log_2 |\mathcal{W}_A| + H(S_A^k|W_A). \end{aligned} \tag{3.43}$$

Now dividing by k and using the definitions for rate and equivocation rate (see Eqs. 3.7 and 3.9), and then using the definition of achievability of these rates (see Eqs. 3.11 and 3.13) results in

$$H(S_A) \leq R_A + \Delta_A \leq (r_A + \epsilon) + d_A \tag{3.44}$$

which proves Eq. 3.25. Eq. 3.26 may be proved in the same way.

2. Proof of Theorem 2

Eqs. 3.30 to 3.32 are directly from [7]. One can achieve Eq. 3.29 without any secrecy coding simply by (determinstic) source coding. If Alice and Bob each compress their messages to the boundaries promised by Eqs. 3.30 to 3.32 for some $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$, then it is easy to see that

$$\begin{aligned} \Delta_A + \Delta_B &= H(S_A) - R_A + H(S_B) - R_B \\ &= H(S_A) + H(S_B) - H(S_A, S_B) \\ &\qquad + H(S_A|S_B, Q_A) + H(S_B|S_A, Q_B) \end{aligned} \tag{3.45}$$

where the first equality follows since approximately $k(H(S_A) - R_A)$ bits (for k sufficiently large) are unknown to Eve given she possess the kR_A bits of W_A, and similarly $k(H(S_B) - R_B)$ bits for Bob. The second equality follows by using Eq. 3.32 with equality. The reader can verify that Eq. 3.45 is equivalent to Eq. 3.29.

3. Derivation of Feedback Bounds

a. Case 110

For the following discussion, suppose the BS knows Eve intercepted W_A, which we will denote as $\tilde{W}_A$, where the tilde is used to indicate a previous round (the reader can prove the other case when the BS knows Eve intercepted $\tilde{W}_B$ using the same method). We put forth a lemma which helps us show there is no advantage in feedback from the **BS to Alice**.

Lemma 3 *If*

$$I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B | \tilde{W}_A) \leq k\tilde{\Delta}_A - H(\tilde{S}_A^k | \tilde{W}_A, \tilde{W}_B) \tag{3.46}$$

then feedback from BS to Alice provides no advantage, given the BS knows Eve pos-

sesses $\tilde{W}_A$.

Proof: Without feedback, Alice can distill a secret key (from $\tilde{S}_A^k$ and $\tilde{W}_A$) of length $k\tilde{\Delta}_A$ bits that is independent of $\tilde{W}_A$. However since the BS reconstruction is distorted, Alice's secret key must be reduced by $H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B)$, which represents the unrecoverable distortion. Thus Alice and the BS can distill a secret key of length given by the right hand side (RHS) of Eq. 3.46 without the need for feedback from the BS.

Theorem 3 of [9] shows that through feedback from the BS to Alice, a secret key of *maximum* length $I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A)$ bits can be established. Thus feedback from the BS to Alice given the BS knows Eve posses Alice's $\tilde{W}_A$ results in a secret key of maximum length given by the left hand side (LHS) of Eq. 3.46.

Clearly, if a secret key derived using feedback has length less than or equal to a secret key derived without feedback, then feedback offers no advantage; this is the significance of Eq. 3.46. Furthermore, both keys cannot be used at the same time since they are both derived from $\tilde{S}_A^k$ and $\tilde{W}_A$. This concludes the proof of Lemma 3.

We can now explicitly show that Lemma 3 is true, and thus feedback provides no advantage.

$$\begin{aligned} I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A) &= H(\tilde{S}_A^k|\tilde{W}_A) - H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B) \\ &= k\tilde{\Delta}_A - H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B) \end{aligned} \tag{3.47}$$

Thus Lemma 3 is true and feedback from the BS to Alice provides no advantage.

Next, under the same assumption that the BS knows Eve has $\tilde{W}_A$, we show that feedback from the **BS to Bob** has no advantage either. Let

$$m \triangleq I(\tilde{S}_B^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A) \tag{3.48}$$

where m is the maximum number of bits of secret key that can be established between the BS and Bob through feedback, given the BS knows Eve posses $\tilde{W}_A$ [9]. In this case, it can be shown that m does *not* satisfy a modified Lemma 3 (for Bob instead of Alice). However Lemma 3 (and a modified version for Bob) provides a sufficient condition only, and thus failure to satisfy the condition in Lemma 3 does not imply there is an advantage using feedback.

Again, let tilde variables represent the previous round, while non-tilde variables represent the current round. To analyze the benefits of feedback, let $kR_B \geq m$, which allows the secret key derived through feedback to be fully used. Let W_B denote Bob's current enciphered message *without* feedback, and let W_B^F denote Bob's current enciphered message *using* feedback Z_B. Then

$$k\Delta_B^F = k\Delta_B + m \tag{3.49}$$

which results because the m bits of the secret key can be used as a one-time pad. For example, suppose W_B is in binary form, and $W_{B,1}$ is the first m bits of W_B, while $W_{B,2}$ is the last $kR_B - m$ bits of W_B. Then

$$W_B^F = (W_{B,1} \oplus K_B, W_{B,2}) \tag{3.50}$$

where K_B is the m-bit key created from feedback.

In order for an improvement in equivocation using feedback, we must show

$$\begin{aligned} H(S_B^k, \tilde{S}_B^k | Z_B, W_B^F, \tilde{W}_A) &> H(S_B^k, \tilde{S}_B^k | W_B, \tilde{W}_A) \\ &= H(\tilde{S}_B^k | \tilde{W}_A) + H(S_B^k | W_B). \end{aligned} \tag{3.51}$$

The previous message block $\tilde{S}_B^k$ must be considered since the feedback Z_B is a function of $\tilde{S}_B^k$. Next we upper bound the LHS of Eq. 3.51.

$$\begin{aligned} H(S_B^k, \tilde{S}_B^k | Z_B, W_B^F, \tilde{W}_A) &= H(\tilde{S}_B^k | Z_B, W_B^F, \tilde{W}_A) + H(S_B^k | \tilde{S}_B^k, Z_B, W_B^F, \tilde{W}_A) \\ &\leq H(\tilde{S}_B^k | Z_B, \tilde{W}_A) + H(S_B^k | \tilde{S}_B^k, Z_B, W_B^F, \tilde{W}_A) \\ &= \Big(H(\tilde{S}_B^k | \tilde{W}_A) - I(\tilde{S}_B^k; Z_B | \tilde{W}_A) \Big) \\ &\quad + \Big(H(S_B^k | W_B^F) - I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A | W_B^F) \Big) \\ &= H(\tilde{S}_B^k | \tilde{W}_A) - I(\tilde{S}_B^k; Z_B | \tilde{W}_A) + \big(H(S_B^k | W_B) + m \big) \\ &\quad - I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A | W_B^F) \end{aligned} \tag{3.52}$$

The last equality follows from Eq. 3.49. Next we bound the final term in Eq. 3.52.

$$\begin{aligned} I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A | W_B^F) &\overset{(a)}{\geq} I(S_B^k; K_B | W_B^F) \\ &\overset{(b)}{=} H(K_B | W_{B,1} \oplus K_B, W_{B,2}) \\ &\quad - H(K_B | S_B^k, W_{B,1} \oplus K_B, W_{B,2}) \\ &\overset{(c)}{=} H(K_B | W_{B,1} \oplus K_B) \\ &\quad - H(K_B | S_B^k, W_{B,1}, K_B, W_{B,2}) \\ &\overset{(d)}{=} H(K_B) = m \end{aligned} \tag{3.53}$$

The explanations are: (a) from the fact that K_B can be derived from $\tilde{S}_B^k$ and Z_B by Bob; (b) from Eq. 3.50; (c) $W_{B,2}$ is assumed to be independent of K_B and $W_{B,1}$, and $W_{B,1}$ can be derived from S_B^k (determinstic encoding); (d) K_B is used as a one-time pad [9].

Combining Eq. 3.53 into Eq. 3.52 shows Eq. 3.51 is not satisfied, thus feedback does not offer any advantage. In fact when $I(\tilde{S}_B^k; Z_B | \tilde{W}_A) > 0$ in Eq. 3.52, feedback strictly performs worst than no feedback.

This proves the case when the BS knows Eve possesses $\tilde{W}_A$. The other case when the BS knows Eve posses $\tilde{W}_B$ can be proved in the same way.

b. Case 0*0

We analyze the 010 case, while the result for the 000 case follows from the 010 case. Suppose the BS knows Eve possess W_A. Theorem 3 of [9] shows that a secret key of maximum length $I(S_j^k; M|W_A)$ bits may be distilled, where M is a RV generated by the BS independent of all messages and received material. This quantity is 0 since M is independent, and thus artificial feedback produces no shared secret key.

E. Summary of Results

In this chapter we studied the source coding and secrecy tradeoffs for the sensor network model of Fig. 5. From our analysis, we summarize the following conclusions. First unconditional secrecy (or maximum secrecy) cannot simultaneously be achieved by all parties in general unless the distortion is necessarily maximal, which implies that no information is disclosed to the base station as well. Furthermore, since the encoders may be stochastic, this implies independent noisy channels cannot improve secrecy, otherwise such virtual channels may be included inside the encoders, which contradicts the results. Next, the inner and outer regions only match for the case when distortion is *not* permitted at the base station, while the inner and outer regions do not match for the case when distortion is permitted at the base station. In the former case, this implies that we have completely characterized the capacity region for the distortionless case. An outcome of this characterization is that source coding alone is enough to achieve the highest equivocation rates possible. In the latter case (i.e. allowing distortion at the base station), the capacity region is not fully characterized

due to the gap between the inner and outer regions, which suggests that perhaps additional coding (other than source coding) may improve secrecy. Finally, a natural question we asked is whether public feedback from the more powerful base station can improve secrecy. Unfortunately, we have shown that feedback from the base station offers no improvement in secrecy in most realistic scenarios unless the base station unrealistically knows *a priori* a specific feedback channel will be free of eavesdropping.

CHAPTER IV

SECURE DISCUS*

Although in the absence of distortion Slepian-Wolf encoding alone suffices to achieve the optimal equivocation rates (see Chapter III), and therefore any distributed source code may be applied, in practice the resulting secrecy is mediocre, giving the eavesdropper too much information concerning the message without the eavesdropper having to do any work.

Thus we define additional secrecy requirements that not only resolves the shortcomings of simply using equivocation as the measure of secrecy, but also account for the possible scenario in which the eavesdropper has access to uncoded symbols from the message in addition to intercepting the corresponding encoded message (similar threat model as [76]).

While the exploration of the capacity of various wiretap channel models has recently received much attention, practical coding for these models is only beginning to emerge [91], [89]. The contribution of this chapter is the extension of DISCUS (distributed source coding using syndromes) to include the practical measure of secrecy briefed above.

A. System Model

We define the problem for m users who have random messages (column vectors) $U_1^k, \ldots, U_m^k \in (GF(q))^k$ with each Galois field element equally likely, and the correla-

*Part of the material in this chapter is reprinted with permission from W. Luh and D. Kundur, "Secure Distributed Source Coding with Side-Information," *IEEE Communication Letters*, vol. 12, no. 4, pp. 310-312, April 2008. © 2008 IEEE.

tion between the messages modeled by

$$w(U_1^k + \cdots + U_m^k) \leq t, \tag{4.1}$$

where $w(\cdot)$ is the Hamming weight, and addition is over $GF(q)$.[1] The m users are to separately and linearly encode (jointly encipher and source code) their realizations $u_1^k, \ldots, u_m^k$, resulting in Galois vectors $x_1^{n_1}, \ldots, x_m^{n_m}$, respectively, via the relationship

$$x_i^{n_i} \quad = \quad \mathbf{H}_i u_i^k \tag{4.2}$$

for $i = 1, \ldots, m$ such that $\mathbf{H}_i$s are $n_i \times k$ matrices.[2] Given all $x_i^{n_i}$, $i = 1, \ldots, m$, the decoder is to reproduce all u_i^k, $i = 1, \ldots, m$ without error.

The eavesdropper is permitted to have at his disposal only one $x_i^{n_i}$; we later generalize this to include the case when the eavesdropper has multiple $x_i^{n_i}$. In addition the eavesdropper is also permitted to have α_i uncoded symbols from u_i^k if he intercepts $x_i^{n_i}$. These extra uncoded symbols (similar threat assumptions as in [76]) are the eavesdropper's side-information. The goal is to design an encoding and decoding scheme for the above system model, such that the eavesdropper cannot uniquely solve for any other symbols in u_i^k given that he has $x_i^{n_i}$ and the corresponding side-information. This level of secrecy is not unconditional, but may be satisfactory for certain applications, e.g. lightweight video encryption [94].

---

[1] This correlation model can be found in [93].

[2] Consideration of nonlinear codes is beyond the scope of this dissertation. In practice nonlinear codes may offer better protection against a wide assortment of cryptanalysis attacks. However the security of nonlinear codes is in general difficult to prove mathematically, while linear codes are amenable to analysis.

B. Coding Scheme

Our codes belong to the class of distributed source coding using syndromes (DISCUS) [95]. In the DISCUS scheme, a supercode with the capability of correcting t-errors (the same t as in Eq. 4.1) is partitioned into m (where m is the number of users) subcodes in which the parity check matrices of these subcodes are used in Eq. 4.2 to encode each of the user's messages. We now present the components and properties of our codes with the relevant proofs stated in Section IV-C.

1. Code Construction

We have at our disposal conditions on the supercode (error correction capability equal to correlation [95]) and the subcodes (MDS from Theorem 5) for DISCUS with secrecy. However, simply choosing MDS subcodes will often result in unacceptable supercodes. Similarly, choosing an acceptable supercode and arbitrarily partitioning the supercode into subcodes will often result in non-MDS codes, e.g. in [96] we showed this is the case for the DISCUS codes in [93]. This section derives codes that satisfy both conditions.

Algorithm 1 (found near the end of this chapter) provides a method of constructing DISCUS codes that are *both* decodable (zero errors), and secure in the sense developed in Section IV-A.[3]

Theorem 3 *If* $\mathbf{H}_i$, $i = 1, \ldots, m$ *are selected using Algorithm 1 and the eavesdropper has side-information restricted to* $\alpha_i < a_i$ *(*a_i *from Algorithm 1), then the encoding scheme is secure and uniquely decodable.*

[3] As in the original DISCUS, the drawback is that these codes do not always exist for all parameters.

2. Decoding

Algorithm 2 (found near the end of this chapter) outlines a fast approach to decoding (as opposed to an exhaustive search), when the decoder has all $x_i^{n_i}$, $i = 1, \ldots, m$. The systematic version of this algorithm is sketched (via an example) in [95]. Algorithm 2 is more general in that it also decodes some non-systematic forms by adding Line 1. We include the entire algorithm for completeness.

Theorem 4 *Algorithm 2 decodes without error, i.e.* $\hat{u}_i^k = u_i^k$ *for all* $i = 1, \ldots, m$.

3. Multiple Eavesdropping

Algorithm 1 only allows the eavesdropper to have access to *one* encoded message with some corresponding side-information. We now analyze the above code for the case when the eavesdropper has access to multiple encoded messages.

Proposition 1 *If the eavesdropper has access to* μ *encoded messages* $\{x_{j_1}^{n_{j_1}}, \ldots, x_{j_\mu}^{n_{j_\mu}}\}$ *for* $1 < \mu < m$*, and any amount of side-information, then the scheme of Algorithm 1 is* not *secure. If the eavesdropper has* no *side-information, then the scheme of Algorithm 1 is secure.*

4. Discussion

a. Intuition on MDS Subcodes

We give an (informal) intuition on the MDS subcode condition. The SW (Slepian-Wolf) coding scheme basically partitions each user's message space into disjoint bins. The encoded result is the syndrome of the message, which also characterizes the bin, i.e. the syndrome can be thought of as a bin index that uniquely identifies that bin. If the eavesdropper intercepts only one of these bin indices, then the eavesdropper must guess the actual message belonging to this bin.

In DISCUS, for decodability reasons, the bins are cosets of a linear code. Our additional condition is that this linear code should be a MDS code to provide security. We motivate this informally by looking at a counter-example. Suppose the bin in consideration contains the actual linear code. Suppose the messages in this bin have very low minimum distance. Then this means that many symbols in the same symbol coordinate may be identical. If the eavesdropper is given a few uncoded symbols, then the number of possible messages from this bin is reduced. It may then be possible to guess other symbols of the actual message if there is some symbol-coordinate such that the symbols are all identical in this reduced message set. For example if the eavesdropper is given one bit resulting in the reduced message set $\{0010, 0011, 0111\}$, then the eavesdropper knows the first and third bits are 0 and 1, respectively. Thus the eavesdropper learns at least one additional bit.

If the linear code is a MDS code, then the codewords in the linear code are separated as far as possible. The phenomenon described in the counter-example is less likely to occur, unless the eavesdropper is given more uncoded symbols than allowed by our theorem. Since cosets of a linear code share the same minimum distance properties, this holds whether the eavesdropper intercepts a bin index corresponding to the actual linear code or one of its cosets.

b. Type of Security

Shannon's lesser known landmark paper on secrecy systems [15] is divided into three parts: the first part is on the algebra of secrecy systems, the second part on perfect secrecy, and the third part on practical secrecy (diffusion-confusion, and statistical attacks). Most secrecy papers deal with either the second part (information-theoretic

works) or third part (DES, AES, etc.).[4] In this section we show that our scheme shares the same type of secrecy as a *pure cipher* from the first part of [15] if the messages are uniformly distributed.

A (Shannon) cipher can be represented by a bipartite graph, such that one set of nodes corresponds to the messages, while the other set of nodes corresponds to the encoded messages (ciphertexts). The edges connecting nodes in both sets represent a message being encoded into the ciphertext, and vice versa in decoding. The edges are associated with a key. In our keyless problem, we can also represent the encoding by a bipartite graph, but the edges do not represent the use of any keys. Furthermore, this graph would *not* describe decoding, since decoding in our case is performed jointly over all encoded messages.

Informally a pure cipher is one in which its bipartite graph can be partitioned such that each partition (called residue class) can be regarded as a sub-cipher that has "perfect" secrecy in the sense that given a ciphertext, any message in that residue class is equally likely. In our scheme, given that the messages are all equally likely, an eavesdropper with a bin index of a coset essentially must consider all messages in that coset. This anology is illustrated in Fig. 7. Of course if the messages are not equally likely, then the analogy to pure ciphers does not hold. Thus the level of security in our scheme is determined by the size of each bin, which is related to the length k of the input messages.

c. Duality

In [97] a direct duality between the channel coding and source coding (rate-distortion) theorems is presented. The channel encoder and decoder are constructed together.

[4]Even more papers deal with the computational number theory paradigm commonly referred to as the public-key paradigm, which is not part of Shannon's paper.

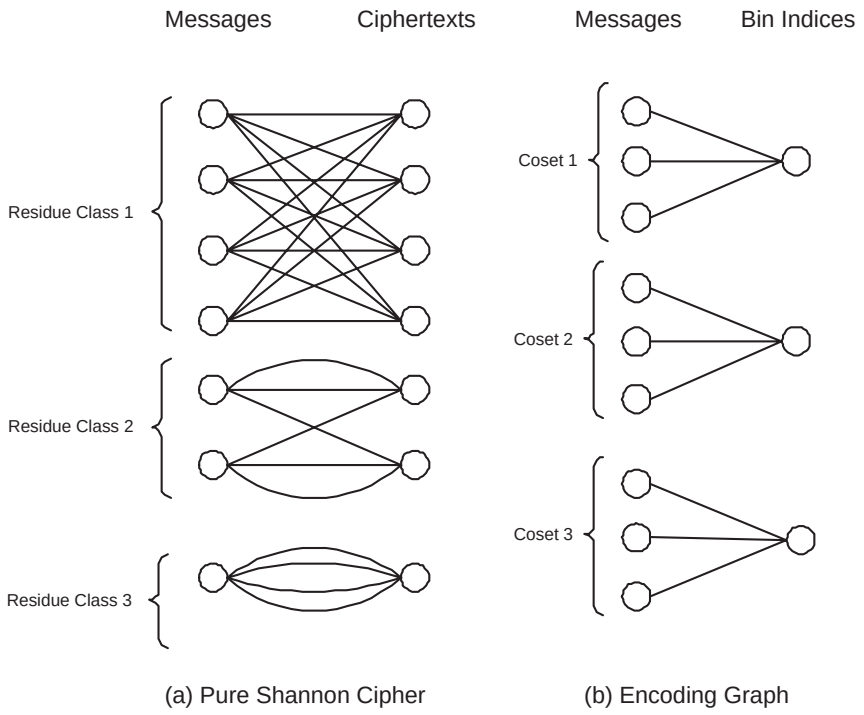

Fig. 7. Analogy Between Pure Shannon Cipher and Our Encoding Scheme: (a) In Each Residue Class Given a Ciphertext, Any Message in That Residue Class Is a Possibility; (b) Given a Bin Index, Any Message in That Coset Is a Possibility

The idea is to select codewords such that their decoding regions $\{\mathcal{D}_i\}$ are optimal. On the other hand, source encoding operates by mapping all words inside a $\mathcal{D}_i$ to the index i, thus resulting in compression. Therefore in the channel coding setup, the messages (*input* to encoder) are the indices i for $\{\mathcal{D}_i\}$, whereas in the source coding setup, the message space is the entire $\bigcup_i \mathcal{D}_i$, and the is are the *outputs* of the source encoder.

We point out a similar duality in our codes and those of the wiretap channel II. The wiretap channel II (and more generally the wiretap channel) concerns secrecy and channel coding, whereas the problem we presented concerns secrecy and source coding. In the wiretap channel II, the encoder partitions a set of codewords into

bins, and a codeword from a bin is randomly selected if the message corresponding to that bin index is to be transmitted. Although the legitimate channel is usually noiseless in the wiretap channel II, the wiretapper's channel is considered as an erasure channel. In our code, the messages are partitioned into bins (as outlined in the previous subsection). We send the bin index instead of a codeword from the bin.

Our problem setup has similarities and differences to [76]. In both cases the eavesdropper is allowed some uncoded symbols of the messages that need to be protected. Interestingly, [76] also shows that MDS codes may be used. The main difference is that in our problem, the two users cannot collaborate, and there is no shared keys or random variables between the two users. The restriction causes unconditional secrecy to *not* be achievable (see Chapter III).

C. Proofs and Ancillary Results

While the supercode requirement of being t-error-correctable aids decodability [95], the secrecy requirement is satisfied when the subcodes are maximum distance separable (MDS) codes; this is stated explicitly in Theorem 5 along with restrictions on the quantity of side-information available to the eavesdropper.

Theorem 5 *Let $\alpha_i < k - n_i$. The eavesdropper cannot solve for any symbols other than those given as side-information in u_i^k for each $i = 1, \ldots, m$ if and only if the subcodes are each maximum distance separable.*

Thus Theorem 5 is the driving force behind the validity of Algorithm 1.

1. Proof of Theorem 5

Theorem 5 is proved using two lemmas. The proof of Lemma 4 is adapted from [98]; we have included a version of the proof that clarifies many subtle points. We state

Lemma 4 for one of the subcodes, therefore we drop the subscripts 1 or 2.

Lemma 4 (Adapted from [98]) *Let* $\mathbf{H}$ *be a* $n \times k$ *matrix with* $n < k$*. Define the* $1 \times k$ *vector*

$$I_i = (0 \ \cdots \ 0 \ \underbrace{1}_{i^{th} \ entry} \ 0 \ \cdots \ 0).$$

If $\alpha < k - n$ *and*

$$\dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{k-n}}\}) = k \tag{4.3}$$

for any *set of unique* $\{I_{j_1}, \ldots, I_{j_{k-n}}\}$*, then given* $x^n = \mathbf{H}u^k$*, and any* α *symbols from* u^k*, no other symbols in* u^k *can be solved for uniquely.*

Proof: We prove the contrapositive, i.e. given x^n and $\alpha < k-n$ uncoded symbols in u^k, if we can solve for an additional $\beta > 0$ uncoded symbols in u^k then there exists *some* set of unique $\{I_{j_1}, \ldots, I_{j_{k-n}}\}$ such that

$$\dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{k-n}}\}) < k. \tag{4.4}$$

Suppose $\{u_{j_1}, \ldots, u_{j_{\alpha+\beta}}\}$ is the set of uncoded symbols including both those given to the eavesdropper, and the extra β that can be solved. Without loss of generality, assume that $\{u_{j_1}, \ldots, u_{j_\alpha}\}$ are given as side-information, while $\{u_{j_{\alpha+1}}, \ldots, u_{j_{\alpha+\beta}}\}$ can be solved for given the side-information and given x^n. This implies that for each u_{j_m}, $m = \alpha + 1, \ldots, \alpha + \beta$, there exists a row vector $(b_{m,1}, \ldots, b_{m,n+\alpha})$ such that

$$(b_{m,1}, \ldots, b_{m,n+\alpha}) \begin{pmatrix} x^n \\ \hline u_{j_1} \\ \vdots \\ u_{j_\alpha} \end{pmatrix} = u_{j_m}, \tag{4.5}$$

i.e. $(b_{m,1}, \ldots, b_{m,n+\alpha})$ applied to what is given to the eavesdropper reveals the symbol u_{j_m}, $m = \alpha+1, \ldots, \alpha+\beta$, which is equivalent to

$$(b_{m,1}, \ldots, b_{m,n+\alpha}) \left(\begin{array}{c} \mathbf{H} \\ \hline I_{j_1} \\ \hline \vdots \\ \hline I_{j_\alpha} \end{array}\right) u^k = I_{j_m} u^k. \tag{4.6}$$

Thus each I_{j_m}, $m = \alpha+1, \ldots, \alpha+\beta$ is in the rowspace of $\left(\begin{array}{c} \mathbf{H} \\ \hline I_{j_1} \\ \hline \vdots \\ \hline I_{j_\alpha} \end{array}\right)$. This implies

$$\dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{\alpha+\beta}}\}) \leq n + \alpha. \tag{4.7}$$

Next there are two cases to consider. First consider the case when $\alpha + \beta > k - n$. In this case it easily follows that

$$\begin{aligned} & \dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{k-n}}\}) \\ \overset{(a)}{\leq} \; & \dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{\alpha+\beta}}\}) \\ \overset{(b)}{\leq} \; & n + \alpha \overset{(c)}{<} k \end{aligned} \tag{4.8}$$

where (a) follows since $\alpha+\beta > k-n$ (first case), (b) from Eq. 4.7, (c) from assumption of lemma: $\alpha < k - n$. Thus the first case satisfies the contrapositive of the lemma.

Consider the second case when $\alpha + \beta \leq k - n$. In this case it easily follows that

$$\begin{aligned} & \dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{I_{j_1}, \ldots, I_{j_{k-n}}\}) \\ = \; & \dim(\text{rowspace}(\mathbf{H}) \cup \text{span}\{ \underbrace{I_{j_1}, \ldots, I_{j_{\alpha+\beta}}}_{\text{correspond to solved symbols}}, \\ & \qquad \underbrace{I_{j_{\alpha+\beta+1}}, \ldots, I_{j_{k-n}}}_{\text{correspond to any unsolved symbols}} \}) \\ \overset{(a)}{\leq} \; & (n + \alpha) + (k - n - (\alpha + \beta)) \\ = \; & k - \beta \overset{(b)}{<} k \end{aligned} \tag{4.9}$$

where the $n + \alpha$ term in (a) follows from Eq. 4.7, while (b) follows since $\beta > 0$ by the assumption of the contrapositive. Therefore the second case also satisfies the contrapositive of the lemma.

The second lemma is the link between Lemma 4 and Theorem 5.

Lemma 5 (From [96]) *Eq. 4.3 is satisfied if and only if any n columns of $\mathbf{H}$ have a non-zero determinant.*

The proof we gave in [96] was succinct and lacked clarity concerning many subtle points due to space limitation. We now give a complete proof.

Proof: Assume that $\mathbf{H}$ fails Lemma 4. Then there exists some $\{I_{j_1}, \ldots, I_{j_{k-n}}\}$ such that Eq. 4.4 is true. In particular this implies

$$(a_1, \ldots, a_n)\mathbf{H} = b_1 I_{j_i} + \cdots + b_{k-n} I_{j_{k-n}} \tag{4.10}$$

for some $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ and $(b_1, \ldots, b_{k-n}) \neq (0, \ldots, 0)$. For example, if I_{j_1} is a culprit, i.e. it is in the rowspace of $\mathbf{H}$ (thus Eq. 4.4 is true), then $(b_1, \ldots, b_{k-n}) = (1, 0, \ldots, 0)$ is a possibility. Let $\mathbf{H}^{[\{1,\ldots,k\} - \{j_1,\ldots,j_{h_{k-n}}\}]}$ represent the n columns of $\mathbf{H}$

whose column indices are *not* from $\{j_1, \ldots, j_{k-n}\}$. Then from Eq. 4.10

$$(a_1, \ldots, a_n)\mathbf{H}^{[\{1,\ldots,k\}-\{j_1,\ldots,j_{k-n}\}]} = (0, \ldots, 0). \tag{4.11}$$

Since $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$, this implies $\det \mathbf{H}^{[\{1,\ldots,k\}-\{j_1,\ldots,j_{k-n}\}]} = 0$.

Conversely, suppose there exist n columns of $\mathbf{H}$ that have a zero determinant. Let $\mathbf{H}^n$ represent these n columns. We use the following fact concerning the nullspace of a square matrix $\mathbf{A}$:

$$\text{nullspace}(\mathbf{A}) = \{(0, \ldots, 0)\} \text{ iff } \mathbf{A} \text{ full rank.} \tag{4.12}$$

Thus since $\det \mathbf{H}^n = 0$, $\mathbf{H}^n$ is not full rank, and the nullspace of $\mathbf{H}^n$ contains more than just $(0, \ldots, 0)$, i.e. there exists a $(c_1, \ldots, c_n) \in \text{nullspace}(\mathbf{H}^n)$ such that $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$. This is equivalent to

$$(c_1, \ldots, c_n)\mathbf{H}^n = (0, \ldots, 0), \tag{4.13}$$

which implies

$$(c_1, \ldots, c_n)\mathbf{H} = d_1 I_{j_1} + \cdots + d_{k-n} I_{j_{k-n}} \tag{4.14}$$

where now the indices $\{j_1, \ldots, j_{k-n}\}$ are those indices that *do not* correspond to the column indices of $\mathbf{H}^n$. We now show that since $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$, this implies that there exists some $1 \leq l \leq k - n$ such that $d_l \neq 0$. To prove this we consider the contrapositive of this statement; suppose $d_l = 0$ for all l, which is equivalent to $(c_1, \ldots, c_n)\mathbf{H} = (0, \ldots, 0)$. Since the rows of $\mathbf{H}$ are independent, the definition of independence implies that $(c_1, \ldots, c_n) = (0, \ldots, 0)$ necessarily. Thus the contrapositive is that $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$ implies there exists at least one $d_l \neq 0$. This proves that there exists some $d_l \neq 0$. Thus some linear combination of $\{I_{j_1}, \ldots, I_{j_{k-n}}\}$ is in the rowspace of $\mathbf{H}$ implying the dimension in Eq. 4.3 is less than

k.

Using the two lemmas, we can finally prove Theorem 5.

Proof of Theorem 5: We prove that if $\mathbf{H}$ satisfies Lemma 5, then it is a parity check matrix of a MDS code. We use the fact that the minimum distance of a linear code is equivalent to the smallest number of columns of $\mathbf{H}$ that are linearly dependent. Since every n columns in $\mathbf{H}$ are full rank if $\mathbf{H}$ satisfies Lemma 5, the minimum distance is at least

$$d_{min} \geq n + 1. \tag{4.15}$$

Note that the generator matrix corresponding to parity check matrix $\mathbf{H}$ would be a $(k-n) \times k$ matrix, and thus by the Singleton bound $d_{min} \leq k - (k-n) + 1 = n + 1$, which implies $d_{min} = n+1$ by Eq. 4.15. Since d_{min} satisfies the Singleton bound with equality, the code with parity check matrix $\mathbf{H}$ is a MDS code. This concludes the proof of Theorem 5.

Finally we note that the above two lemmas can be generalized such that the conditions are sufficient *and* necessary. See [98] and [96] for the converse proofs. Therefore the condition of MDS is necessary and sufficient as stated in Theorem 5.

2. Proof of Theorem 3

The matrix $\mathbf{A}$ is a general *parity check matrix* of a Reed-Solomon code (when the decoder and channel alphabets are equal, which is the case here, i.e. the alphabets are all $GF(k+1)$), which are MDS codes. Since the dual of a MDS code is also MDS, we consider $\mathbf{A}$ as a *generator matrix* of a MDS code. This implies the minimum distance equals the Singleton bound $d_{min} = k - (2s) + 1$. Therefore the linear code with generator matrix $\mathbf{A}$ can correct $\left\lfloor \frac{k}{2} - s \right\rfloor \triangleq t$ errors. Therefore if $\mathbf{A}$ is the generator matrix of the supercode, then unique decodability is possible given the correlation

model, Eq. 4.1, and the Slepian-Wolf (SW) constraints are satisfied [99]. Since $\mathbf{H}_i$ is a $(k - a_i) \times k$ matrix from Algorithm 1, the side-information constraint $\alpha_i < k - (k - a_i) = a_i$ follows from Theorem 5. Furthermore, since U_is are each uniformly distributed over $GF(k+1)$, the source coding rate given by Eq. 4.28 and constrained by Eq. 4.29 is simply the Slepian-Wolf theorem. Therefore we have proved that zero-error decodability is achieved given the above constraints are satisfied.

Next we must check that the $\mathbf{H}_i$s are parity check matrices of MDS codes for all $i = 1, \ldots, m$ (to satisfy Theorem 5). In general, partitioning a MDS code may not result in MDS subcodes. However, the choice of starting with $\mathbf{A}$ in Algorithm 1 facilitates the generation of MDS subcodes as we show. Since $\mathbf{A}_i$ is a BCH parity check matrix, which corresponds to a cyclic code, and since the dual code of a cylic code is also cyclic, we can consider $\mathbf{A}_i$ as a generator matrix of a cyclic code. Thus the parity check polynomial corresponding to the generator matrix $\mathbf{A}_i$ is equal to

$$h_i(x) = \prod_{l=a_i^-}^{a_i^+} (x - \xi^{-l}) = \prod_{l=a_i^-}^{a_i^+} (x - \xi^{k-l}) = \prod_{l=k-a_i^+}^{k-a_i^-} (x - \xi^l) \tag{4.16}$$

where

$$a_i^- = \left(\sum_{j=1}^{i-1} a_j \right) + 1, \qquad a_i^+ = \sum_{j=1}^{i} a_j. \tag{4.17}$$

Therefore the generator polynomial corresponding to generator matrix $\mathbf{A}_i$ is given by

$$g_i(x) \;=\; \frac{x^k - 1}{h_i(x)} = \prod_{l=1}^{k-a_i^+-1} (x - \xi^l) \prod_{l=k-a_i^-+1}^{k} (x - \xi^l) = \prod_{l=k-a_i^-+1}^{2k-a_i^+-1} (x - \xi^l) \tag{4.18}$$

where the final equality follows since $\xi^{k+l} = \xi^l$. Since the generator polynomial has roots that are consecutive powers of the primitive element ξ, the code it generates is by definition Reed-Solomon, which is MDS.

3. Proof of Theorem 4

For succinctness we prove Theorem 4 for two users, i.e. $m = 2$. Left-side multiplication of Eq. 4.2 $\mathbf{E}_i$ yields

$$\tilde{w}_i^{n_i} = \bar{\mathbf{H}}_i u_i^k \tag{4.19}$$

for $i = 1, \ldots, m$ (see Line 1). We claim

$$u_i^k = \mathbf{G}_i^{\mathrm{T}} v_i + \begin{pmatrix} \tilde{w}_i^{n_i} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{4.20}$$

which can be verified by left-side multiplication with $\bar{\mathbf{H}}_i$ (see Eq. 4.30) resulting in Eq. 4.19. Defining $e^k = u_1^k + u_2^k$ yields

$$\mathbf{G}_1^{\mathrm{T}} v_1 + \mathbf{G}_2^{\mathrm{T}} v_2 + \begin{pmatrix} \tilde{w}_1^{n_1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} \tilde{w}_2^{n_2} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e^k \tag{4.21}$$

or

$$r^k = \left(\begin{array}{c} \mathbf{G}_1 \\ \hline \mathbf{G}_2 \end{array}\right)^{\mathrm{T}} \left(\begin{array}{c} v_1 \\ \hline v_2 \end{array}\right) + e^k \tag{4.22}$$

referring to Line 2 for the definition of r^k. Eq. 4.22 can be interpreted as follows: r^k is a noisy codeword from the code generated by $\left(\begin{array}{c} \mathbf{G}_1 \\ \hline \mathbf{G}_2 \end{array}\right)$. Note that the rowspace of $\left(\begin{array}{c} \mathbf{G}_1 \\ \hline \mathbf{G}_2 \end{array}\right)$ is identical to the rowspace of $\mathbf{A}$ from Algorithm 1 since the operations on $\mathbf{H}_i$s are elementary row operations. Therefore we can use a Reed-Solomon decoder

(Line 3), corresponding to the code with generator matrix $\mathbf{A}$. The decoder will return a unique codeword c^k since the error $e^k = u_1^k + u_2^k$ has weight less than t given by the correlation model, and the code generated by $\mathbf{A}$ corrects t errors or less. Since there is a unique message corresponding to each codeword of a linear code, we can solve for the vector in Line 5. Substituting back into Eq. 4.20 yields the decoded messages u_1^k, u_2^k.

4. Proof of Proposition 1

Given $\{x_{j_1}^{n_{j_1}}, \ldots, x_{j_\mu}^{n_{j_\mu}}\}$, we can write

$$\left(\begin{array}{c} x_{j_1}^{n_{j_1}} \\ \hline \vdots \\ \hline x_{j_\mu}^{n_{j_\mu}} \end{array}\right) = \left(\begin{array}{c|c|c} \mathbf{H}_{j_1} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \ddots & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{H}_{j_\mu} \end{array}\right) \left(\begin{array}{c} u_{j_1}^k \\ \hline \vdots \\ \hline u_{j_\mu}^k \end{array}\right). \tag{4.23}$$

Eq. 4.23 will be conveniently denoted by

$$x = \mathbf{H}u. \tag{4.24}$$

It can easily be seen that $\mathbf{H}$ is no longer the parity check matrix of a MDS code, since its minimum distance is strictly less than the Singleton bound. This is proved by considering $\mathbf{H}$ as a generator matrix; thus the codewords generated by $\mathbf{H}$ are precisely the concatenation of codewords generated by $\mathbf{H}_{j_1}, \ldots, \mathbf{H}_{j_\mu}$. Therefore the codewords generated by $\mathbf{H}$ must have minimum distance

$$d_{min} = \min\{d_{min,j_1}, \ldots, d_{min,j_\mu}\} \tag{4.25}$$

where d_{min,j_i} is the minimum distance of the code corresponding to generator matrix $\mathbf{H}_{j_i}$. Therefore the code generated by $\mathbf{H}$ is not MDS. Now since a code is MDS if and only if its dual is MDS, the code whose parity check matrix is $\mathbf{H}$ is also not MDS.

Therefore $\mathbf{H}$ is not secure given the eavesdropper has side-information.

However, when the eavesdropper does not have side-information, we show that $\mathbf{H}$ is secure. Now *if* there exists a $1 \times (n_{j_1} + \cdots + n_{j_\mu})$ row vector b_i such that

$$b_i x = b_i \mathbf{H} u = I_i^{\mu k} u \tag{4.26}$$

where now $I_i^{\mu k}$ is a $1 \times \mu k$ row vector with 1 in position i and 0 elsewhere, then the eavesdropper can solve for the i^{th} symbol in u. Eq. 4.26 is equivalent to

$$I_i^{\mu k} \in \text{rowspace}(\mathbf{H}).$$

Thus if we show that $I_i^{\mu k} \notin \text{rowspace}(\mathbf{H})$ for all $i = 1, \ldots, \mu k$, then the eavesdropper cannot solve for any symbols in u. First we show that the rows of $\mathbf{H}$ are independent. This can be seen since the rows of each $\mathbf{H}_{j_1}, \ldots, \mathbf{H}_{j_\mu}$ are independent. Since these $\mathbf{H}_{j_1}, \ldots, \mathbf{H}_{j_\mu}$ are stacked in the form of Eq. 4.23, the rows of $\mathbf{H}$ are independent. Now suppose for some arbitrary $I_i^{\mu k}$, column i runs through $\mathbf{H}_r$ in $\mathbf{H}$. Therefore $I_i^{\mu k}$ is not in the rowspace consisting of all rows in $\mathbf{H}$ with matrices $\mathbf{H}_l$, $l \neq r$, since the i^{th} element in each of these $\mathbf{H}_l$ is 0, while it is 1 in $I_i^{\mu k}$.

Thus we only have to check that $I_i^{\mu k}$ is not in the rowspace consisting of the rows in $\mathbf{H}$ with matrix $\mathbf{H}_r$, i.e.

$$I_i^{\mu k} \notin \text{rowspace} \left(\begin{array}{c|c|c|c|c} \mathbf{0} & \cdots & \mathbf{0} & \mathbf{H}_r & \mathbf{0} \end{array} \right). \tag{4.27}$$

If we truncate the matrix above (right hand side of Eq. 4.27) by eliminating the $\mathbf{0}$ matrices, and truncate the corresponding symbols in $I_i^{\mu k}$, then the matrix reduces to $\mathbf{H}_r$, while the vector $I_i^{\mu k}$ reduces to some $1 \times k$ row vector I_l, $l \in \{1, \ldots, k\}$. But since $\mathbf{H}_r$ is secure (since it is MDS by the proof of Algorithm 1), $I_l \notin \text{rowspace}(\mathbf{H}_r)$, and thus Eq. 4.27 is also true.

There is one final technical point that we must prove. We have been assuming

that all u realizations in Eq. 4.24 are equally likely. This is true so long as $\mu < m$ (where m is the total number of users). If $\mu = m$, i.e. if the eavesdropper has access to *all* encoded messages, then by the correlation model (see Eq. 4.1), some u realizations (in Eq. 4.24) are impossible, because these u violate Eq. 4.1. On the other hand if $\mu = m - 1$, then there is no constraint on $\{u^k_{j_1}, \ldots, u^k_{j_\mu}\}$; only the m^{th} $u_{j_{\mu+1}}$ would have to be chosen so that all m messages satisfy Eq. 4.1. Thus as long as the eavesdropper has fewer than m encoded messages, the *corresponding* original messages are all equally likely, and thus u (in Eq. 4.24) are all equally likely.

D. Summary of Results

In this chapter we studied practical coding schemes based on DISCUS for the theoretical problem in Chapter III. First we defined a practical measure of secrecy that extends beyond the equivocation measure. This measure protects *each* symbol in the message, rather than the message as a whole. We showed that the MDS property is a necessary requirement on the subcodes of DISCUS. We then derived a coding scheme based on DISCUS where the challenge lies in satisfying this subcode requirement while satisfying the DISCUS supercode requirement at the same time. We showed that if the eavesdropper only possesses *one* encoded message and "a few" uncoded symbols from the message, then the other symbols in the message cannot be revealed with certainty. However if the eavesdropper possesses more than one encoded message, then the eavesdropper must not be permitted to possess any uncoded symbols.

Algorithm 1 Finding Secure Parity Check Matrices

Require: $\mathbf{H}_i$ for all $i = 1, \ldots, m$.

Ensure:

(i) $U_{1,j}, \ldots, U_{m,j} \in GF(k+1)$ uniformly distributed where $k+1$ is a power of a prime number and $k \geq 2(s+t)$;

(ii) Eq. 4.1 is satisfied;

(iii) ξ is a primitive element in $GF(k+1)$ and

$$\mathbf{A} = \begin{pmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{(k-1)} \\ 1 & \xi^2 & \xi^4 & \cdots & \xi^{2(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{2s} & \xi^{4s} & \cdots & \xi^{2s(k-1)} \end{pmatrix}$$

1: Partition the matrix $\mathbf{A} = \left(\begin{array}{c} \mathbf{A}_1 \\ \hline \vdots \\ \hline \mathbf{A}_m \end{array}\right)$ such that the $\mathbf{A}_i$s are $a_i \times k$ matrices, and

$$R_i \triangleq \frac{k - a_i}{k} \log_2(k+1) \tag{4.28}$$

for all $i = 1, \ldots, m$ satisfy

$$\sum_{i \in \mathcal{S}} R_i \geq H\left((U_j)_{j \in \mathcal{S}} \,|\, (U_j)_{j \in \{1,\ldots,m\} - \mathcal{S}} \right) \tag{4.29}$$

for all $\mathcal{S} \subseteq \{1, \ldots, m\}$. If this is not possible, then these rates cannot be used.

2: Select $\mathbf{H}_i$s such that $\mathbf{A}_i \mathbf{H}_i^{\mathrm{T}} = \mathbf{0}$ for all $i = 1, \ldots, m$.

Algorithm 2 Decoding

Require: $\hat{u}_i^k = u_i^k$ for all $i = 1, \ldots, m$.

Ensure: $x_i^{n_i} = \mathbf{H}_i u_i^k$ for all $i = 1, \ldots, m$ where $\mathbf{H}_i$ generated as in Algorithm 1.

1: Compute $\tilde{w}_i^{n_i} = \mathbf{E}_i x_i^{n_i}$ where $\mathbf{E}_i$ for all $i = 1, \ldots, m$ are elementary matrices such that

$$\mathbf{E}_i \mathbf{H}_i = \left(\begin{array}{c|c} \mathbf{I} & \tilde{\mathbf{H}}_i \end{array} \right) \triangleq \bar{\mathbf{H}}_i \tag{4.30}$$

where $\mathbf{I}$ is the identity matrix.

2: Compute the $r^k = \begin{pmatrix} \tilde{w}_1^{n_1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} \tilde{w}_m^{n_m} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, where the zero-padding makes each vector in the sum $k \times 1$.

3: Use a Reed-Solomon decoder (e.g. Berlekamp-Massey algorithm) to decode the received word r^k based on the RS code whose generator matrix is $\mathbf{A}$ from Algorithm 1. The output of the decoder is the codeword c^k.

4: Let $\mathbf{G}_i$ be the systematic generator matrix corresponding to parity check matrix $\bar{\mathbf{H}}_i$ (see Eq. 4.30) such that

$$\mathbf{G}_i = \left(\begin{array}{c|c} \tilde{\mathbf{G}}_i & \mathbf{I} \end{array} \right).$$

5: Solve for column vectors v_i, $i = 1, \ldots, m$ in

$$c^k = \left(\begin{array}{c|c|c} \mathbf{G}_1^T & \cdots & \mathbf{G}_m^T \end{array} \right) \left(\begin{array}{c|c|c} v_1^T & \cdots & v_m^T \end{array} \right)^T$$

6: Compute

$$\hat{u}_i^k \;=\; \mathbf{G}_i^{\mathrm{T}} v_i + \left(\begin{array}{cccc} (\tilde{w}_i^{n_i})^T & 0 & \cdots & 0 \end{array} \right)^T \tag{4.31}$$

for all $i = 1, \ldots, m$.

CHAPTER V

CHANNEL CODING AND DISTRIBUTED SECRECY*

In this chapter we study the interaction between channel coding and secrecy in the context of the general discrete memoryless interference channel. We derive inner and outer regions of the secrecy capacity region, which is the set of all channel coding rates such that unconditional secrecy is achieved. Surprisingly, the secrecy capacity region may not be empty, thus in contrast with the first part of our research, interference permits unconditional secrecy. The proof utilizes the random coding technique of Wyner's wiretap channel [10] and its generalization [11].

The system model studied in this chapter is motivated by the usage of mobile relay nodes. First the data gathering nodes are to encode their data without communicating with one another, and without the use of any cryptographic keys as motivated in Chapter I. The nodes' encoded data are then transmitted to nearby mobile relay nodes where their signals interfere with one another. We assume that a subset of these mobile relay nodes may be eavesdropped upon as motivated in Chapter II. These mobile nodes then travel until they are close to the base station where their payload is finally relayed to the base station without interference, but experience independent noise.

A. System Model

In Chapter III, the channels are noiseless, which means that the encoded messages never *mix* as they are transmitted to the base station. In contrast, the problem

*Part of the material in this chapter is reprinted with permission from W. Luh and D. Kundur, "Distributed Secret Sharing for Discrete Memoryless Networks," *IEEE Trans. on Information Forensics and Security*, 2008, to appear.

formulated here allows the encoded messages to *mix* via interference. Fig. 8 sum-

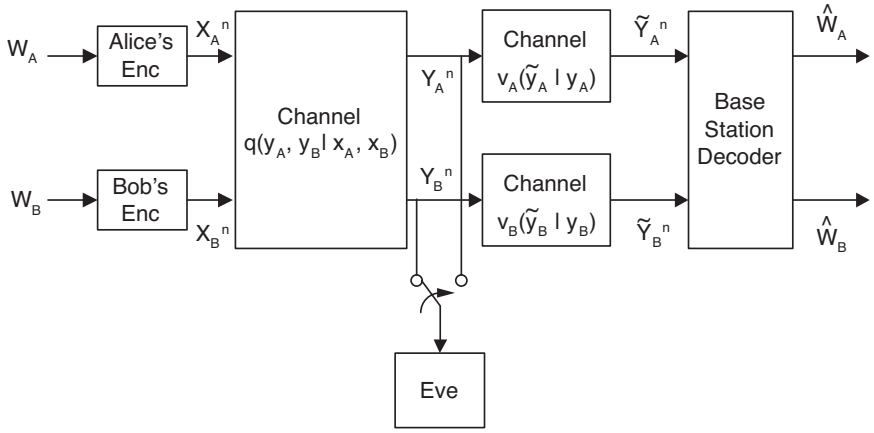

Fig. 8. Discrete Memoryless Sensor Network with Interference Model

marizes a sensor network secrecy model, which includes interference and additional noise for the BS decoder. Alice and Bob each process independent and uniformly distributed messages $W_A \in \mathcal{W}_A$ and $W_B \in \mathcal{W}_B$, respectively such that $\mathcal{W}_A, \mathcal{W}_B$ are finite sets. These messages may actually be generated from the encoder in Chapter III if the original data is correlated. Let the triple (f_A, f_B, φ) denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the BS's decoder. Note that in the previous chapters the superscript k was used to indicate that the source messages consisted of blocks of k letters; here the source messages are indices, thus there are no superscripts. Also, the base station had two decoders in Chapter III due to the need for different distortion criteria; here there are no distortion criteria, thus only one decoder suffices. Thus in this case $f_A : \mathcal{W}_A \to \mathcal{X}_A^n$, $f_B : \mathcal{W}_B \to \mathcal{X}_B^n$, $\varphi : \tilde{\mathcal{Y}}_A^n \times \tilde{\mathcal{Y}}_B^n \to \hat{\mathcal{W}}_A \times \hat{\mathcal{W}}_B$.

The discrete memoryless interference channel is characterized by the conditional probability $q(y_A, y_B | x_A, x_B)$. The BS receives encoded messages that are addition-

ally corrupted by the two independent discrete memoryless channels $v_A(\tilde{y}_A|y_A)$ and $v_B(\tilde{y}_B|y_B)$. This is a more realistic model than most wiretap channels since the BS is further from Alice and Bob than Eve, thus realistically the BS should receive noisier encoded messages, which is accounted for by $v_A(\cdot|\cdot), v_B(\cdot|\cdot)$.

The channel coding rates are defined by

$$R_1 \triangleq \frac{\log_2 |\mathcal{W}_A|}{n} \tag{5.1}$$

$$R_2 \triangleq \frac{\log_2 |\mathcal{W}_B|}{n} \tag{5.2}$$

corresponding to the encoders f_A, f_B. We use the subscripts 1 and 2 to distinguish the channel coding rates from the source coding rates in Eqs. 3.7 and 3.8. For this problem we are only interested in rates that achieve unconditional secrecy (maximum equivocation) since as we shall see, this is possible![1]

Definition 3 *A pair (r_1, r_2) corresponding to (R_1, R_2) is achievable if there exist encoders and decoder (f_A, f_B, φ) such that as $n \to \infty$*

$$R_1 > r_1 - \epsilon \tag{5.3}$$

$$R_2 > r_2 - \epsilon \tag{5.4}$$

$$\frac{H(W_A, W_B|Y_i^n)}{n} > R_1 + R_2 - \epsilon \tag{5.5}$$

$$P_e^{(n)} < \epsilon \tag{5.6}$$

for $i = A, B$ and $\epsilon > 0$ arbitrarily small where

$$P_e^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \sum_{\substack{(w_1,w_2)\in \\ \mathcal{W}_1\times\mathcal{W}_2}} Pr\{(\hat{W}_1, \hat{W}_2) \neq (w_1, w_2)|(w_1, w_2) \text{ sent}\}. \tag{5.7}$$

[1]Unconditional or perfect secrecy was originally defined by $I(W_A, W_B; Y_i^n) = 0$ or $H(W_A, W_B|Y_i^n) = H(W_A, W_B)$ for $i = A, B$. In this dissertation we use the weaker definition established in [10], i.e. Eq. 5.5, but still refer to this as unconditional secrecy.

In addition, all parties, Alice, Bob, and Eve have complete knowledge of f_A, f_B (except for any locally generated randomness) and any cryptographic keys used.

B. Secrecy Capacity Region

We derive sufficiency and necessity theorems. The outer region is now denoted $\mathcal{C}_{out}$ while the inner region is denoted by $\mathcal{C}_{in}$.

Theorem 6 (Outer Region) *Let $\mathcal{C}_{out}$ be the set of (r_1, r_2) that satisfy*

$$r_1 + r_2 \leq \min \left\{ \begin{array}{l} \max\ I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J) - I(V_A, V_B; \tilde{Y}_A|J), \\ \max\ I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J) - I(V_A, V_B; \tilde{Y}_B|J), \\ \max\ I(V_A, V_B; Y_A, Y_B|J) - I(V_A, V_B; Y_A|J), \\ \max\ I(V_A, V_B; Y_A, Y_B|J) - I(V_A, V_B; Y_B|J) \end{array} \right\}, \tag{5.8}$$

where the maxima are over $J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B) \leftrightarrow (\tilde{Y}_A, \tilde{Y}_B)$, $J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B) \leftrightarrow (\tilde{Y}_A, \tilde{Y}_B)$, $J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B)$, $J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B)$, respectively, and the distribution factors as

$$P_{J,V_A,V_B,X_A,X_B,Y_A,Y_B,\tilde{Y}_A,\tilde{Y}_B} = P_J P_{V_A|J} P_{V_B|J} P_{X_A|V_A} P_{X_B|V_B} P_{Y_A,Y_B|X_A,X_B} P_{\tilde{Y}_A|Y_A} P_{\tilde{Y}_B|Y_B} \tag{5.9}$$

Then $\mathcal{C}_{out}$ is an outer region.

Theorem 6 is proved in Section V-C-1.

Theorem 7 (Inner Region) *For each P_{J,V_A,V_B,X_A,X_B} factored as*

$$P_{J,V_A,V_B,X_A,X_B} = P_J P_{V_A|J} P_{V_B|J} P_{X_A|V_A} P_{X_B|V_B} \tag{5.10}$$

$\mathcal{C}_{inner}$ is defined as the set of all (r_1, r_2) such that

$$\begin{aligned} r_1 &= \left|\bar{R}_1 - U_1\right|^+ && (5.11)\\ r_2 &= \left|\bar{R}_2 - U_2\right|^+ && (5.12)\\ r_1 + r_2 &< I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J) - I(V_A, V_B; Y_i|J) && (5.13) \end{aligned}$$

and

$$\begin{aligned} 0 < \quad U_1 \quad &< I(V_A; Y_i|V_B, J) && (5.14)\\ 0 < \quad U_2 \quad &< I(V_B; Y_i|V_A, J) && (5.15)\\ I(V_A, V_B; Y_i|J) - \epsilon < \quad U_1 + U_2 \quad &< I(V_A, V_B; Y_i|J) && (5.16)\\ 0 < \quad \bar{R}_1 \quad &< I(V_A; Y_A, Y_B|V_B, J) && (5.17)\\ 0 < \quad \bar{R}_2 \quad &< I(V_B; Y_A, Y_B|V_A, J) && (5.18)\\ 0 < \quad \bar{R}_1 + \bar{R}_2 \quad &< I(V_A, V_B; Y_A, Y_B|J) && (5.19) \end{aligned}$$

for $i = A, B$. Then

$$\mathcal{C}_{in} \triangleq \bigcup_{P_{J,V_A,V_B,X_A,X_B}} \mathcal{C}_{inner} \qquad (5.20)$$

where the distributions factor as in Eq. 5.10 is an inner region.

Theorem 7 is proved in Section V-C-2.

1. Discussion

Theorem 6 suggests the possible existence of rates (since the result is an outer region) that achieve unconditional secrecy. From Theorem 7 it is difficult to see by visual inspection if there are actual rates that do achieve unconditional secrecy. We will give an example for the discrete memoryless case derived in Theorem 7.

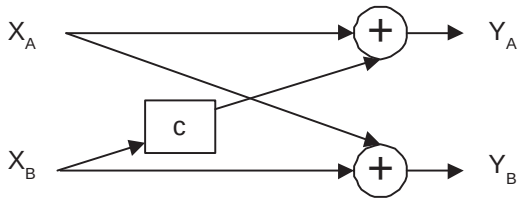

Fig. 9. Binary Erasure Sensor Network

The proof of Theorem 7 (see Section V-C-2) is based on the observation that the base station sees a multiple access channel (MAC) with *two* outputs, whereas Eve sees a MAC with only *one* output, depending on which noisy encoded messages she intercepts. In order for Eve to have no incentive to choose one noisy encoded message over the other, both MACs that Eve sees must be statistically identical. Mathematically this is seen in Eq. 5.16, since $U_1 + U_2$ essentially must equal the same value for both Y_A^n and Y_B^n (the outputs of each of the MACs that Eve would see depending on which one she intercepts). This restricts the number of discrete memoryless sensor networks (DMSNs) that could provide secrecy to a very small class.

We demonstrate an example using the binary erasure sensor network (BESN). Let the channel input alphabet be $\mathcal{X} = \{0, 1\}$ for both users, and the channel output alphabet be $\mathcal{Y} = \{0, 1, 2\}$. Let the overall channel be given by

$$Y_A = X_A + \overline{X_B} \tag{5.21}$$

$$Y_B = X_A + X_B, \tag{5.22}$$

where $\overline{X_B}$ is the binary complement of X_B and addition is the real addition, not the binary field addition. Fig. 9 depicts the BESN, where the "c" box denotes

Table III. Input-Output Table for the Binary Erasure Sensor Network

X_A	X_B	Y_A	Y_B
0	0	1	0
0	1	0	1
1	0	2	1
1	1	1	2

the complement.[2] For simplicity, we do not include the additional noisy channels $v_A(\cdot|\cdot), v_B(\cdot|\cdot)$. Table III shows the input-output relationship of this BESN. Clearly the base station is able to decode any messages without error since all pairs of (Y_A, Y_B) in Table III are unique; the capacity region for this two-output MAC is described using $\bar{R}_1$ for Alice's rate and $\bar{R}_2$ for Bob's rate. Next, Eve sees either the MAC of Eq. 5.21 or Eq. 5.22. Both these MACs are statistically identical if we choose $Pr\{X_A = 0\} = Pr\{X_B = 0\} = \frac{1}{2}$. The capacity region for these one-output MACs is described using U_1 for Alice's rate and U_2 for Bob's rate. Setting the random variable J constant, and using the deterministic channels $P_{X_A|V_A}$, $P_{X_B|V_B}$, the capacity regions for the two-output and one-input MACs can be derived and found to be:

$$\begin{aligned} \bar{R}_1 &\leq 1 & U_1 &\leq 1 \\ \bar{R}_2 &\leq 1 & U_2 &\leq 1 \\ \bar{R}_1 + \bar{R}_2 &\leq 2 & U_1 + U_2 &\leq \frac{3}{2}. \end{aligned}$$

Furthermore, by Eq. 5.16 we choose $U_1 + U_2 = \frac{3}{2}$, then the corresponding inner region

[2]Without complementation, the two outputs would be identical and thus one copy would be useless for decoding. This is only the case because the channel is deterministic, which is used in this example for simplicity.

(rates that achieve unconditional secrecy) can be derived using Theorem 7 and found to be

$$\left\{(r_1, r_2) : r_1 \geq 0, r_2 \geq 0, r_1 + r_2 \leq \frac{1}{2}\right\}.$$

For example, to achieve $(r_1, r_2) = (0.5, 0)$, choose $\bar{R}_1 = \bar{R}_2 = 1$ and $U_1 = 0.5, U_2 = 1$

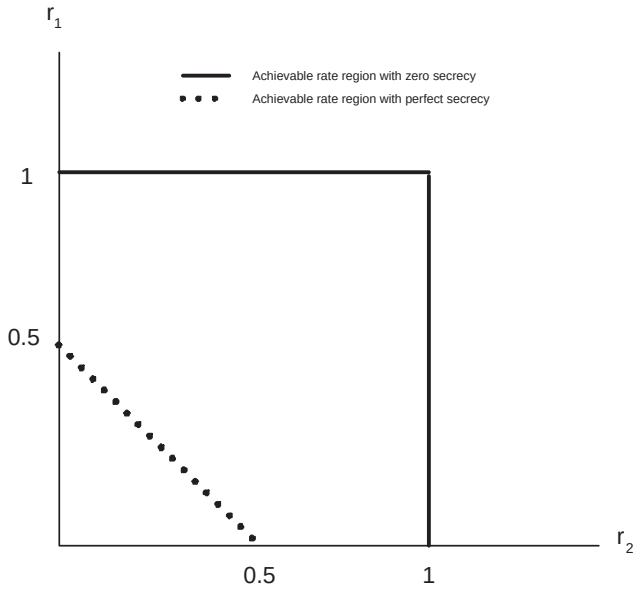

Fig. 10. Comparison of Achievable Rate Regions

(which satisfies $U_1 + U_2 = 1.5$), thus $r_1 = \bar{R}_1 - U_1 = 0.5$ and $\bar{r}_2 = R_2 - U_2 = 0$ according to Theorem 7. To achieve $(r_1, r_2) = (0.25, 0.25)$ (the middle point on the diagonal of the triangle, see Fig. 10) choose $\bar{R}_1 = \bar{R}_2 = 1$ and $U_1 = U_2 = 0.75$ (which satisfies $U_1 + U_2 = 1.5$), thus $r_1 = \bar{R}_1 - U_1 = 0.25$ and $\bar{r}_2 = R_2 - U_2 = 0.25$ according to Theorem 7. To conclude this example we contrast the achievable rate regions for the BESN for no secrecy and perfect secrecy in Fig. 10. Not surprisingly, the achievable rate region for the perfect secrecy case is a sub-region of that without secrecy. Note that Fig. 10 is not to be compared with Fig. 6 as the axes are different.

C. Proofs and Ancillary Results

1. Proof of Theorem 6

The proof makes use of the following lemma.

Lemma 6 (Lemma 4.1 **[9])** *For arbitrary random variables U, V and sequences of random variables Y^n, Z^n the following is true*

$$\begin{aligned} I(U;Y^n|V) - I(U;Z^n|V) &= \sum_{i=1}^{n} \Big(I(U;Y_i|Y^{i-1}, Z_{i+1}, \ldots, Z_n, V) \\ &\qquad - I(U;Z_i|Y^{i-1}, Z_{i+1}, \ldots, Z_n, V) \Big) \end{aligned} \tag{5.23}$$

where $Y^{i-1} = (Y_1, \ldots, Y_{i-1})$.

There are a total of four bounds for the sum of the rates. We prove the first of the two pairs in Theorem 6.

$$\begin{aligned} & n(R_1 + R_2) = H(W_A, W_B) = H(W_A, W_B|\tilde{Y}_A^n, \tilde{Y}_B^n) + I(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n) \\ \overset{(a)}{\leq} \; & n\epsilon_n + I(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n) \\ \overset{(b)}{=} \; & I(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n) - I(W_A, W_B; \tilde{Y}_A^n) + I(W_A, W_B; \tilde{Y}_A^n) + n\epsilon_n \\ \overset{(c)}{\leq} \; & I(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n) - I(W_A, W_B; \tilde{Y}_A^n) + I(W_A, W_B; Y_A^n) + n\epsilon_n \\ \overset{(d)}{\leq} \; & I(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n) - I(W_A, W_B; \tilde{Y}_A^n) + n\epsilon + n\epsilon_n \\ \overset{(e)}{=} \; & \sum_{i=1}^{n} \Big(I(W_A, W_B; \tilde{Y}_{A,i}, \tilde{Y}_{B,i}|\tilde{Y}_A^{i-1}, \tilde{Y}_B^{i-1}, \tilde{Y}_{A,i+1}, \ldots, \tilde{Y}_{A,n}) \\ & \quad - I(W_A, W_B; \tilde{Y}_{A,i}|\tilde{Y}_A^{i-1}, \tilde{Y}_B^{i-1}, \tilde{Y}_{A,i+1}, \ldots, \tilde{Y}_{A,n}) \Big) + n(\epsilon + \epsilon_n) \\ \overset{(f)}{=} \; & n \sum_{i=1}^{n} Pr\{\Theta = i\} \Big(I(W_A, W_B; \tilde{Y}_{A,i}, \tilde{Y}_{B,i}|K_i, \Theta = i) \\ & - I(W_A, W_B; \tilde{Y}_{A,i}|K_i, \Theta = i) \Big) + n(\epsilon + \epsilon_n) \end{aligned}$$

$$
\begin{aligned}
&= n\sum_{i=1}^{n} Pr\{\Theta=i\}\Big(I(W_A,W_B;\tilde{Y}_{A,\Theta},\tilde{Y}_{B,\Theta}|K_\Theta,\Theta=i) \\
&\quad -I(W_A,W_B;\tilde{Y}_{A,\Theta}|K_\Theta,\Theta=i)\Big)+n(\epsilon+\epsilon_n) \\
&\overset{(g)}{=} n\Big(I(W_A,W_B;\tilde{Y}_{A,\Theta},\tilde{Y}_{B,\Theta}|K_\Theta,\Theta)-I(S_A,S_B;\tilde{Y}_{A,\Theta}|K_\Theta,\Theta)\Big)+n(\epsilon+\epsilon_n) \\
&\overset{(h)}{=} n\Big(I(V_A,V_B;\tilde{Y}_A,\tilde{Y}_B|J)-I(V_A,V_B;\tilde{Y}_A|J)\Big)+n(\epsilon+\epsilon_n) \qquad (5.24)
\end{aligned}
$$

The explanations are as follows: (a) Fano's inequality from Eq. 5.6; (c) data processing inequality on the Markov chain $(W_A,W_B)\leftrightarrow Y_A^n\leftrightarrow\tilde{Y}_A^n$; (d) unconditional secrecy requirement if Eve intercepts Y_A^n (see Eq. 5.5); (e) use of Lemma 6; (f) by defining

$$K_i\triangleq(\tilde{Y}_A^{i-1},\tilde{Y}_B^{i-1},\tilde{Y}_{A,i+1},\ldots,\tilde{Y}_{A,n}) \qquad (5.25)$$

and also defining a uniform RV $\Theta=1,\ldots,n$ that is independent of all other RVs; (g) definition of conditioning; (h) by defining

$$\tilde{Y}_A\triangleq\tilde{Y}_{A,\Theta},\quad \tilde{Y}_B\triangleq\tilde{Y}_{B,\Theta},\quad J\triangleq(K_\Theta,\Theta),\quad V_A\triangleq(W_A,J),\quad V_B\triangleq(W_B,J). \qquad (5.26)$$

Finally, it is easily seen that

$$J\leftrightarrow(V_A,V_B)\leftrightarrow(X_A,X_B)\leftrightarrow(\tilde{Y}_A,\tilde{Y}_B)\quad\text{and}\quad V_A\leftrightarrow J\leftrightarrow V_B \qquad (5.27)$$

form Markov chains where the last chain follows since W_A,W_B are independent.

On the other hand, adding and subtracting $I(W_A,W_B;\tilde{Y}_B)$ in (b) instead of $I(W_A,W_B;\tilde{Y}_A)$ yields a different bound

$$R_1+R_2\leq\Big(I(V_A,V_B;\tilde{Y}_A,\tilde{Y}_B|J)-I(V_A,V_B;\tilde{Y}_B|J)\Big)+\epsilon+\epsilon_n \qquad (5.28)$$

with the same Markov chains (Eq. 5.27) and the same distribution factorization.

The other pair in Theorem 6 are derived in a similar manner with slight differences outlined below.

$$\begin{aligned} n(R_1+R_2) &= H(W_A,W_B) = H(W_A,W_B|Y_A^n,Y_B^n) + I(W_A,W_B;Y_A^n,Y_B^n) \\ &\overset{(a)}{\leq} H(W_A,W_B|\tilde{Y}_A^n,\tilde{Y}_B^n) + I(W_A,W_B;Y_A^n,Y_B^n) \\ &\overset{(b)}{\leq} n\epsilon_n + I(W_A,W_B;Y_A^n,Y_B^n) \\ &\overset{(c)}{=} I(W_A,W_B;Y_A^n,Y_B^n) - I(W_A,W_B;Y_A^n) + I(W_A,W_B;Y_A^n) + n\epsilon_n \\ &\overset{(d)}{\leq} I(W_A,W_B;Y_A^n,Y_B^n) - I(W_A,W_B;Y_A^n) + n\epsilon + n\epsilon_n \\ &\overset{(e)}{=} n\Big(I(V_A,V_B;Y_A,Y_B|J) - I(V_A,V_B;Y_A|J)\Big) + n(\epsilon+\epsilon_n) \end{aligned} \tag{5.29}$$

The explanations are as follows: (a) the data processing inequality on the Markov chain $(W_A,W_B) \leftrightarrow (Y_A^n,Y_B^n) \leftrightarrow (\tilde{Y}_A^n,\tilde{Y}_B^n)$ (b) Fano's inequality; (d) unconditional secrecy requirement if Eve intercepts Y_A^n; (e) same approach as in deriving Eq. 5.24, but now with the following Markov chain

$$J \leftrightarrow (V_A,V_B) \leftrightarrow (X_A,X_B) \leftrightarrow (Y_A,Y_B) \tag{5.30}$$

in place of the first Markov chain in Eq. 5.27.

On the other hand, adding and subtracting $I(W_A,W_B;Y_B^n)$ in (c) instead of $I(W_A,W_B;Y_A^n)$ gives the final bound

$$R_1+R_2 \leq \Big(I(V_A,V_B;Y_A,Y_B|J) - I(V_A,V_B;Y_B|J)\Big) + \epsilon + \epsilon_n \tag{5.31}$$

with the Markov chain in Eq. 5.30 and the same distribution factorization.

2. Proof of Theorem 7

a. Random Codebook Generation

Randomly generate a typical sequence j^n using the distribution $\prod_{i=1}^{n} P_J(j_i)$ and make this publically known to all parties including the BS and Eve. Generate $2^{n(\bar{R}_1-\delta)}$ sequences v_A^n using the distribution $\prod_{i=1}^{n} P_{V_A|J}(v_{A,i}|j_i)$ and $2^{n(\bar{R}_2-\delta)}$ sequences v_B^n using the distribution $\prod_{i=1}^{n} P_{V_B|J}(v_{B,i}|j_i)$ such that Eqs. 5.17 to 5.19 are satisfied.

Alice's codebook is then the arrangement of the v_A^ns in a $2^{\lfloor nr_1 \rfloor} \times 2^{n(U_1-\delta)}$ table, while Bob's codebook is the arrangement of the v_B^ns in a $2^{\lfloor nr_2 \rfloor} \times 2^{n(U_2-\delta)}$ table such that Eqs. 5.11 to 5.16 are satisfied (if possible). Suppose Alice's message w_A is indexed such that $w_A \in \{1, \ldots, 2^{\lfloor nr_1 \rfloor}\}$ and similarly Bob's message is $w_B \in \{1, \ldots, 2^{\lfloor nr_2 \rfloor}\}$. Thus each entry in Alice and Bob's codebooks can be indexed as $v_A^n(w_A, u_1)$ and $v_B^n(w_B, u_2)$, respectively. In addition as $n \to \infty$, the actual rates R_1, R_2 will satisfy the definitions in Eqs. 5.3 and 5.4.

b. Encoding

Alice encodes her w_A by randomly choosing a codeword v_A^n from row w_A of her tabular codebook, i.e. randomly (uniformly) selecting a column index u_1 resulting in $v_A^n(w_A, u_1)$. She then randomly generates x_A^n (to be sent over the channels) using the distribution $\prod_{i=1}^{n} P_{X_A|V_A}(x_{A,i}|v_{A,i})$. Similarly Bob encodes his w_B by randomly choosing a codeword v_B^n from row w_B of his tabular codebook, i.e. randomly selecting a column index u_2 resulting in $v_B^n(w_B, u_2)$. He then randomly generates x_B^n (to be sent over the channels) using the distribution $\prod_{i=1}^{n} P_{X_B|V_B}(x_{B,i}|v_{B,i})$. Thus the encoders are both stochastic.

c. Decoding

Let $A_\epsilon^{(n)}(J, V_A, V_B, \tilde{Y}_A, \tilde{Y}_B)$ be the set of jointly typical sequences $(J^n, V_A^n, V_B^n, \tilde{Y}_A^n, \tilde{Y}_B^n)$ [100]. Upon receiving $(\tilde{y}_A^n, \tilde{y}_B^n)$ the base station decoder declares the messages $(\hat{w}_A, \hat{w}_B)$ as having been sent if

$$(j^n, v_A^n(\hat{w}_A, u_1)), v_B^n(\hat{w}_B, u_2), \tilde{y}_A^n, \tilde{y}_B^n) \in A_\epsilon^{(n)}(J, V_A, V_B, \tilde{Y}_A, \tilde{Y}_B)$$

for any (u_1, u_2) if such a $(\hat{w}_A, \hat{w}_B)$ exists and is unique.

d. Probability of Error Analysis

Define the event

$$E_{a,b} \triangleq \{(j^n, v_A^n(a, u_1)), v_B^n(b, u_2), \tilde{y}_A^n, \tilde{y}_B^n) \in A_\epsilon^{(n)}(J, V_A, V_B, \tilde{Y}_A, \tilde{Y}_B)\}. \tag{5.32}$$

By the symmetry of the codebook construction we can assume without loss of generality that the messages $(w_A, w_B) = (1, 1)$ were sent. Thus

$$\begin{aligned}
P_e^{(n)} &= Pr\{ \text{ error } |(w_A, w_B) = (1, 1)\} \\
&= Pr\left\{ E_{1,1}^c \cup \bigcup_{a\neq 1, u_1} E_{a,1} \cup \bigcup_{b\neq 1, u_2} E_{1,b} \cup \bigcup_{\substack{a\neq 1, b\neq 1 \\ u_1, u_2}} E_{a,b} \right\} \\
&\leq Pr\{E_{1,1}^c|(w_A, w_B) = (1, 1)\} + \sum_{a\neq 1} \sum_{u_1} Pr\{E_{a,1}|(w_A, w_B) = (1, 1)\} \\
&\quad + \sum_{b\neq 1} \sum_{u_2} Pr\{E_{1,b}|(w_A, w_B) = (1, 1)\} \\
&\quad + \sum_{a\neq 1} \sum_{b\neq 1} \sum_{u_1} \sum_{u_2} Pr\{E_{a,b}|(w_A, w_B) = (1, 1)\}
\end{aligned} \tag{5.33}$$

by the union bound. The first term tends to 0 as $n \to \infty$ by the asymptotic equipartition theorem (AEP) [100].

$$\begin{aligned}
& Pr\{E_{a\neq 1,1}|(w_A, w_B) = (1,1)\} \\
= & \sum_{\substack{(j^n, v_A^n, v_B^n, \tilde{y}_A^n, \tilde{y}_B^n) \\ \in A_\epsilon^{(n)}(J, V_A, V_B, \tilde{Y}_A, \tilde{Y}_B)}} P_J^n(j^n) P_{V_A|J}(v_A^n|j^n) P^n_{V_B, \tilde{Y}_A, \tilde{Y}_B|J}(v_B^n, \tilde{y}_A^n, \tilde{y}_B^n|j^n) \\
\leq & \left| A_\epsilon^{(n)}(J, V_A, V_B, \tilde{Y}_A, \tilde{Y}_B) \right| 2^{-n(H(J)-\delta)} 2^{-n(H(V_A|J)-\delta)} 2^{-n(H(V_B, \tilde{Y}_A, \tilde{Y}_B|J)-\delta)} \\
\leq & 2^{-n(I(V_A; \tilde{Y}_A|V_B, J)-\delta')} \qquad (5.34)
\end{aligned}$$

Using the AEP, the other probabilities are

$$Pr\{E_{1,b\neq 1}|(w_A, w_B) = (1,1)\} \leq 2^{-n(I(V_B; \tilde{Y}_B|V_A, J)-\delta')} \qquad (5.35)$$

$$Pr\{E_{a\neq 1,b\neq 1}|(w_A, w_B) = (1,1)\} \leq 2^{-n(I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J)-\delta')} \qquad (5.36)$$

thus recalling the size and dimensions of the codebooks yields

$$\begin{aligned}
P_e^{(n)} \leq & \ \delta + 2^{n(\bar{R}_1-\delta)} 2^{-n(I(V_A; \tilde{Y}_A|V_B, J)-\delta')} + 2^{n(\bar{R}_2-\delta)} 2^{-n(I(V_B; \tilde{Y}_B|V_A, J)-\delta')} \\
& + 2^{n(\bar{R}_1+\bar{R}_2-\delta)} 2^{-n(I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J)-\delta')}. \qquad (5.37)
\end{aligned}$$

Therefore if Eqs. 5.17 to 5.19 are satisfied then the bound in Eq. 5.37 approaches 0 as $n \to \infty$.

e. Secrecy Analysis

$$
\begin{aligned}
& H(W_A, W_B|Y_i^n) \geq H(W_A, W_B|Y_i^n, J^n) = H(W_A, W_B, Y_i^n|J^n) - H(Y_i^n|J^n) \\
= \;& H(W_A, W_B, V_A^n, V_B^n, Y_i^n|J^n) - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) - H(Y_i^n|J^n) \\
= \;& H(W_A, W_B, V_A^n, V_B^n|J^n) + H(Y_i^n|W_A, W_B, V_A^n, V_B^n, J^n) \\
& \qquad - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) - H(Y_i^n|J^n) \\
\overset{(a)}{\geq} \;& H(V_A^n, V_B^n|J^n) + H(Y_i^n|V_A^n, V_B^n, J^n) - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) - H(Y_i^n|J^n) \\
\overset{(b)}{=} \;& H(V_A^n|J^n) + H(V_B^n|J^n) - I(Y_i^n; V_A^n, V_B^n|J^n) - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) \\
\overset{(c)}{=} \;& n(\bar{R}_1 + \bar{R}_2 - 2\delta) - I(Y_i^n; V_A^n, V_B^n|J^n) - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) \\
\overset{(d)}{\geq} \;& n(r_1 + r_2 - 2\delta - \epsilon) - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) \\
\overset{(e)}{\geq} \;& n(R_1 + R_2 - \epsilon') - H(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n) \\
\overset{(f)}{\geq} \;& n(R_1 + R_2 - \epsilon') - n\epsilon_n
\end{aligned}
\tag{5.38}
$$

where (a) the first term results from $H(W_A, W_B, V_A^n, V_B^n|J^n) \geq H(V_A^n, V_B^n|J^n)$ (property of entropy) and the second term from the encoding process, i.e. knowledge of V_A^n implies knowledge of W_A, and similarly knowledge of V_B^n implies knowledge of W_B; (b) since $H(V_A^n, V_B^n|J^n) = H(V_A^n|J^n) + H(V_B^n|V_A^n, J^n)$ and $V_A^n \leftrightarrow J^n \leftrightarrow V_B^n$ forms a Markov chain from the codebook generation; (c) from the codebook generation; (d) since $U_1 + U_2 \geq I(V_A, V_B; Y_i^n|J^n)$ is true from Eq. 5.16, and using the definitions of r_1 and r_2 from Eqs. 5.11 and 5.12 yields $\bar{R}_1 - r_1 + \bar{R}_2 - r_2 \geq I(V_A, V_B; Y_i^n|J^n) - \epsilon$; (e) from the floor operation in the codebook generation; (f) when Eve is given W_A and W_B, she has knowledge of the rows of the codebooks in which the codewords V_A^n and V_B^n were randomly chosen in the encoding processing. This reduces the codebooks in which she must search (using joint typical decoding with her eavesdropped Y_i^n) from the two codebooks in its entirety to just one row of each codebook. Using the same

technique as in Section V-C-2-d, it can be shown that Eve's average probability of error (which we denote by $P_e^{(n)'}$) is also bounded by quantities that vanish to 0 as $n \to \infty$ based on the random codebook generation *if* the upper bounds in Eqs. 5.14 to 5.16 are satisfied. Therefore by Fano's inequality

$$H(V_A^n, V_B^n | W_A, W_B, Y_i^n, J^n) \leq 1 + P_e^{(n)'} \log_2(|\mathcal{W}_A||\mathcal{W}_B|) \triangleq n\epsilon_n. \tag{5.39}$$

D. Summary of Results

In this chapter we studied the channel coding and secrecy tradeoffs for the sensor network model of Fig. 8. This model differs from those in the previous chapters in that intermediate mobile relay nodes are assumed to be situated near the data gathering nodes such that these mobile nodes receive interfering signals. Surprisingly, we showed that with the aid of interference, unconditional secrecy is now possible for certain cases. Specifically, we derived inner and outer regions for the capacity region. Our inner region is for the specific case when all of the eavesdropper's channels are "statistically similar;" hence intuitively the eavesdropper has no incentive in choosing one channel over the other. For the general discrete memoryless channel, pre-coding is required to maximize the users' rates. We demonstrated an example of a binary erasure sensor network showing that our results are not simply mathematical tricks.

CHAPTER VI

GAUSSIAN INTERFERENCE CHANNEL WITH SLOW AND FLAT RAYLEIGH FADING AND DISTRIBUTED SECRECY

This chapter is an extension of Chapter V from the discrete memoryless channels to channels suitable for wireless communications. In particular we assume that the interference channel has additive white Gaussian noise, and later augment this model with the additional challenge of slow and flat Rayleigh fading. Again we derive inner and outer regions of the secrecy capacity region for the non-fading case. Significantly we show that the special inner region can be simplified to such an extent that its description is merely a *single* region based on an optimal power allocation scheme without the need for pre-coding (as was the case in Chapter V). This is in contrast to various mutli-user wiretap channel capacity regions, which are usually constructed through a convex hull of an infinite union of regions. Next, our extension of the interference channel to slow and flat Rayleigh fading demonstrates that interference and random fading are not only friends rather than foes, but are in fact necessary enablers of unconditional secrecy.

A. System Model

For simplicity we formulate the problem for two nodes. Fig. 11 illustrates the wireless channel with interference. The noise vectors Z_1^n, Z_2^n are independent, and each component in the vector is an independent and identically distributed (i.i.d.) Gaussian random variable (RV), i.e. $Z_i^n = (Z_{i,1}, Z_{i,2}, \ldots, Z_{i,n})$ with each $Z_{i,j}$ independent and

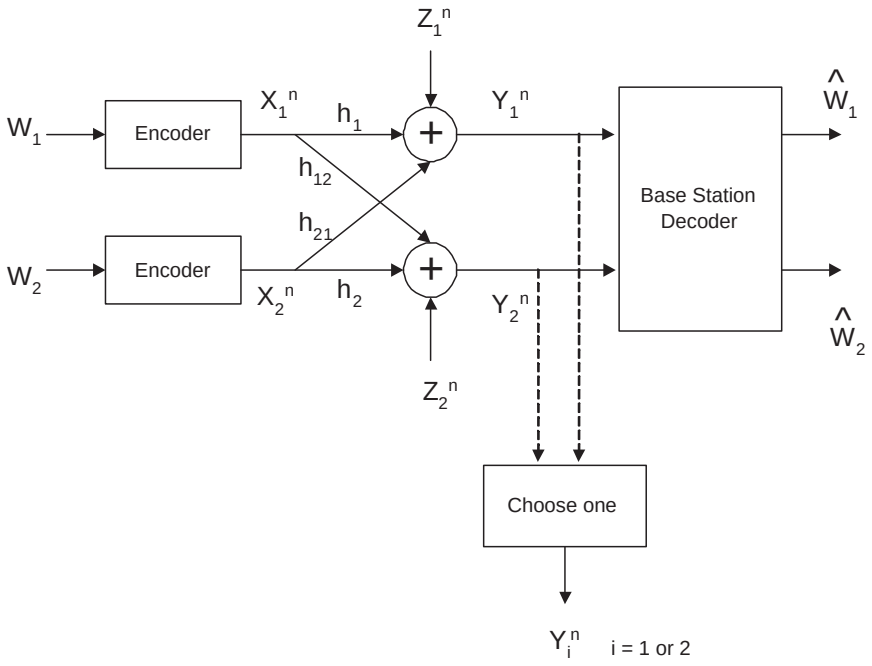

Fig. 11. Two-User Wireless Sensor Network with Eavesdropper

normally distributed, $\mathcal{N}(0, \sigma_i^2)$, for $i = 1, 2$. The outputs of the channel are given by

$$Y_1^n = h_1 X_1^n + h_{21} X_2^n + Z_1^n \tag{6.1}$$

$$Y_2^n = h_{12} X_1^n + h_2 X_2^n + Z_2^n. \tag{6.2}$$

The multiplicative terms h_1, h_2, h_{12}, h_{21} model the gains on the channels. For the first part of our results, we will assume that these are constants, and for the second part we derive a random fading model. More details on this second part will be provided in the subsequent treatment. The channels corresponding to h_{12}, h_{21} model the interference and we also call these *cross-links*. Thus the channel transition probability is factored as $p(y_1, y_2|x_1, x_2) = p(y_1|x_1, x_2)p(y_2|x_1, x_2)$. Furthermore we impose a power

constraint on the transmitters

$$\frac{1}{n}\mathbb{E}\|X_i^n\|^2 \leq P_i^{\max} \tag{6.3}$$

for $i = 1, 2$, where each transmitter has its own maximum allowable power given by $P_1^{\max}, P_2^{\max}$.

Note that our overall setup is different from [40], [39] in that: (1) there are no fixed wiretap channels, i.e. the eavesdropper can choose either Y_1^n or Y_2^n (but not both), where Y_1^n and Y_2^n are outputs of legitimate channels, and (2) the decoder (base station) receives and uses *both* Y_1^n and Y_2^n for decoding.

Definition 4 *A* $(2^{nR_1}, 2^{nR_2}, n)$ *code for the wireless sensor network depicted in Fig. 11 consists of two message sets* $\mathcal{W}_i = \{1, \ldots, 2^{nR_i}\}$ *for* $i = 1, 2$ *such that* W_i *is uniformly selected from the set* $\mathcal{W}_i$*, two (stochastic) encoding functions* $f_i : \mathcal{W}_i \to \mathcal{X}_i^n$ *for* $i = 1, 2$*, and one decoding function* $g : \mathcal{Y}_1^n \times \mathcal{Y}_2^n \to \mathcal{W}_1 \times \mathcal{W}_2$*. Thus the encoding distribution is factored as* $p(x_1, x_2|w_1, w_2) = p(x_1|w_1)p(x_2|w_2)$.

Let the average probability of error for the $(2^{nR_1}, 2^{nR_2}, n)$ be defined by

$$P_e^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \cdot \sum_{\substack{(w_1,w_2)\in \\ \mathcal{W}_1\times\mathcal{W}_2}} Pr\{(\hat{W}_1, \hat{W}_2) \neq (w_1, w_2)|(w_1, w_2) \text{ sent}\}. \tag{6.4}$$

Let secrecy (or confidentiality) be measured by Shannon equivocation or equivalently mutual information, e.g. $H(W_1, W_2|Y_i^n)$ or $I(W_1, W_2; Y_i^n)$ for either $i = 1$ or $i = 2$ depending on which Y_i^n the eavesdropper selects. Note that the eavesdropper is only permitted to select *one* out of the two channel outputs.

Definition 5 *A rate pair* (R_1, R_2) *is* achievable with unconditional secrecy *for the wireless sensor network if there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *codes such that for*

all $\epsilon > 0$

$$\begin{aligned} P_e^{(n)} &< \epsilon && (6.5) \\ \frac{1}{n} I(W_1, W_2; Y_i^n) &< \epsilon \\ \frac{1}{n} I(W_1; Y_i^n) &< \epsilon \\ \frac{1}{n} I(W_2; Y_i^n) &< \epsilon && (6.6) \end{aligned}$$

for $i = 1, 2$*, for* n *sufficiently large.*

The secrecy capacity region is defined as the closure of the set of all (R_1, R_2) achievable with unconditional secrecy, denoted by $\mathcal{C}$. We will derive outer and inner regions, $\mathcal{C}^{\text{outer}}$ and $\mathcal{C}^{\text{inner}}$, respectively, such that

$$\mathcal{C}^{\text{inner}} \subseteq \mathcal{C} \subseteq \mathcal{C}^{\text{outer}}.$$

B. Main Results

1. General Outer Region

We now state the general outer region result. Let $C(x) = \frac{1}{2}\log_2(1+x)$.

Theorem 8 (Outer Region) *Let* $\mathcal{C}^{outer}(P_1, P_2)$ *be the set of* (R_1, R_2) *such that*

$$R_1 + R_2 \leq \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - \max\left\{C(SNR_1), C(SNR_2)\right\} \tag{6.7}$$

where

$$K_{12} = \det\begin{pmatrix} h_1^2P_1 + h_{21}^2P_2 + \sigma_1^2 & h_1h_{12}P_1 + h_2h_{21}P_2 \\ h_1h_{12}P_1 + h_2h_{21}P_2 & h_{12}^2P_1 + h_2^2P_2 + \sigma_2^2 \end{pmatrix} \tag{6.8}$$

$$\begin{aligned} SNR_1 &= \frac{h_1^2P_1 + h_{21}^2P_2}{\sigma_1^2} && (6.9) \\ SNR_2 &= \frac{h_{12}^2P_1 + h_2^2P_2}{\sigma_2^2}. && (6.10) \end{aligned}$$

Then

$$\mathcal{C}^{outer} = \mathcal{C}^{outer}(P_1^{\max}, P_2^{\max})$$

is an outer region.

2. Equal SNR Inner Region

In this section we derive an inner region that is based on Gaussian codebooks and the equal SNR property:

$$SNR_1 = SNR_2 \triangleq SNR_{Eq}. \tag{6.11}$$

This equal SNR property restricts the users' powers to lie on a line segment determined by the channel parameters , i.e.

$$\alpha = \frac{h_2^2\sigma_1^2 - h_{21}^2\sigma_2^2}{h_1^2\sigma_2^2 - h_{12}^2\sigma_1^2} \tag{6.12}$$

$$\gamma_1 = \begin{cases} \frac{\sigma_2^2 h_{21}^2}{h_1^2 h_2^2} - \frac{\sigma_1^2}{h_1^2} & \text{if } \frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}, \\ \frac{\sigma_1^2 h_2^2}{h_{12}^2 h_{21}^2} - \frac{\sigma_2^2}{h_{12}^2} & \text{if } \frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2}, \\ \infty & \text{otherwise.} \end{cases} \tag{6.13}$$

$$\gamma_2 = \begin{cases} \frac{\sigma_1^2 h_{12}^2}{h_1^2 h_2^2} - \frac{\sigma_2^2}{h_2^2} & \text{if } \frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}, \\ \frac{\sigma_2^2 h_1^2}{h_{12}^2 h_{21}^2} - \frac{\sigma_1^2}{h_{21}^2} & \text{if } \frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2}, \\ \infty & \text{otherwise.} \end{cases} \tag{6.14}$$

$$\mathcal{A} = \{(P_1, P_2) : \gamma_1 \le P_1 \le P_1^{\max}, \gamma_2 \le P_2 \le P_2^{\max}, \quad P_1 = \alpha P_2, \alpha > 0\}, \tag{6.15}$$

where $\mathcal{A}$ is the set of admissible users' powers. In particular, we will show that if the power assignments in Table IV are in $\mathcal{A}$, then they are optimal, otherwise no admissible power assignments exist.

Table IV. Optimal Power Allocation

$\mathbf{P_2^{max}} > \mathbf{P_1^{max}}$	$0 < \alpha < 1$	$\alpha > 1$
$\alpha P_2^{\max} > P_1^{\max}$	$P_1 = P_1^{\max}$ $P_2 = P_1^{\max}/\alpha$	$P_1 = P_1^{\max}$ $P_2 = P_1^{\max}/\alpha$
$\alpha P_2^{\max} < P_1^{\max}$	$P_1 = \alpha P_2^{\max}$ $P_2 = P_2^{\max}$	
$\mathbf{P_2^{max}} < \mathbf{P_1^{max}}$	$0 < \alpha < 1$	$\alpha > 1$
$\alpha P_2^{\max} > P_1^{\max}$	$P_1 = \alpha P_2^{\max}$ $P_2 = P_2^{\max}$	$P_1 = P_1^{\max}$ $P_2 = P_1^{\max}/\alpha$
$\alpha P_2^{\max} < P_1^{\max}$		$P_1 = \alpha P_2^{\max}$ $P_2 = P_2^{\max}$

The inner region is based on two linear programs (LPs). Towards this end, define

$$b(P_1, P_2) = \begin{pmatrix} \min\left\{C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right), C\left(\frac{h_{12}^2 P_1}{\sigma_2^2}\right)\right\} \\ \min\left\{C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right), C\left(\frac{h_{21}^2 P_2}{\sigma_1^2}\right)\right\} \\ C\left(\frac{h_{12}^2 P_1}{\sigma_2^2} + \frac{h_1^2 P_1}{\sigma_1^2}\right) \\ C\left(\frac{h_{21}^2 P_2}{\sigma_1^2} + \frac{h_2^2 P_2}{\sigma_2^2}\right) \\ \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2}\right) \\ 0 \end{pmatrix} \tag{6.16}$$

where $(P_1, P_2) \in \mathcal{A}$. The inequality symbol $\preceq$ below applies the inequality $\leq$ between corresponding components of the vectors.

a. Linear Program 1

$$\begin{aligned} \text{minimize} \quad & \begin{pmatrix} 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} U_1^{(1)} & U_2^{(1)} & \bar{R}_1^{(1)} & \bar{R}_2^{(1)} \end{pmatrix}^T \\ \text{subject to} \quad & \\ & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} U_1^{(1)} \\ U_2^{(1)} \\ \bar{R}_1^{(1)} \\ \bar{R}_2^{(1)} \end{pmatrix} \preceq b \qquad (6.17) \\ & \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} U_1^{(1)} & U_2^{(1)} & \bar{R}_1^{(1)} & \bar{R}_2^{(1)} \end{pmatrix}^T = C\left(SNR_{Eq}\right) \qquad (6.18) \end{aligned}$$

b. Linear Program 2

$$\begin{aligned} \text{minimize} \quad & \begin{pmatrix} 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} U_1^{(2)} & U_2^{(2)} & \bar{R}_1^{(2)} & \bar{R}_2^{(2)} \end{pmatrix}^T \\ \text{subject to} \quad & \\ & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} U_1^{(2)} \\ U_2^{(2)} \\ \bar{R}_1^{(2)} \\ \bar{R}_2^{(2)} \end{pmatrix} \preceq b \qquad (6.19) \\ & \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} U_1^{(2)} & U_2^{(2)} & \bar{R}_1^{(2)} & \bar{R}_2^{(2)} \end{pmatrix}^T = C\left(SNR_{Eq}\right) \qquad (6.20) \end{aligned}$$

If $\mathcal{A} \neq \emptyset$, then let $\mathcal{C}^{\text{inner}}(P_1, P_2)$ for $(P_1, P_2) \in \mathcal{A}$ be the set of rate pairs (R_1, R_2)

defined by the convex hull of the following points

$$\left\{(0,0),(0,R_2^{(2)*}),(R_1^{(1)*},0),(R_1^{(1)*},R_2'),(R_1',R_2^{(2)*})\right\}.$$

such that $(U_1^{(1)*},U_2^{(1)*},\bar{R}_1^{(1)*},\bar{R}_2^{(1)*})$ and $(U_1^{(2)*},U_2^{(2)*},\bar{R}_1^{(2)*},\bar{R}_2^{(2)*})$ are optimal points for LPs 1 and 2 with $b=b(P_1,P_2)$, respectively, i.e. points that achieve the optimal values for the LPs with $(P_1,P_2)\in\mathcal{A}$, and

$$\begin{aligned} R_2' &= \min\left\{\frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right)-\bar{R}_1^{(1)*},C\left(\frac{h_{21}^2P_2}{\sigma_1^2}+\frac{h_2^2P_2}{\sigma_2^2}\right)\right\}-U_2^{(1)*} \\ R_1' &= \min\left\{\frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right)-\bar{R}_2^{(2)*},C\left(\frac{h_{21}^2P_2}{\sigma_1^2}+\frac{h_2^2P_2}{\sigma_2^2}\right)\right\}-U_1^{(2)*}. \end{aligned}$$

We will show in the proof of the upcoming theorem that when $\mathcal{A}\neq\emptyset$, the LPs are always feasible.

Theorem 9 *$\mathcal{C}^{inner}(P_1,P_2)\subseteq\mathcal{C}$, for all $(P_1,P_2)\in\mathcal{A}\neq\emptyset$, i.e. any rate pair $(R_1,R_2)\in\mathcal{C}^{inner}(P_1,P_2)$ is achievable. If (P_1,P_2) is obtained from the power allocation in Table IV, then $C^{inner}(P_1,P_2)$ is the largest inner region that contains all other inner regions.*

Note that if $\mathcal{A}=\emptyset$, then our convention is to let $\mathcal{C}^{\text{inner}}(P_1,P_2)=\emptyset$, and thus $\emptyset\subseteq\mathcal{C}$ is still true. An important result from Theorem 9 is that the largest inner region is described simply as the convex hull of a few points, rather than the convex hull of an (infinite) union of sets.

We now list an important tightness property that is immediate from the derivation of the inner region.

Corollary 1 (Tightness)

$$R_1^{(1)*} + R_2' = \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - C\left(SNR_{Eq}\right) \tag{6.21}$$

$$R_1' + R_2^{(2)*} = \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - C\left(SNR_{Eq}\right) \tag{6.22}$$

Corollary 1 along with Theorem 9 shows that the largest inner region partially coincides with the outer region (see Theorem 8) when $(P_1^{\max}, P_2^{\max}) \in \mathcal{A}$. This result states that under the equal SNR regime when the power constraint is admissible , the outer region is partially tight, and so Gaussian codebooks may be close to optimal for this inner region. This point will be illustrated in an example in Section VI-C-1. We will see in that example that finding the inner region does not require the use of linear programming. However the linear programming formulation gives us some convenience in notation, and also we shall see it used informally to give insights on one of the proofs.

3. Slow and Flat Rayleigh Fading

In this section we model the random fading as in [45], [82], [47], [48]. We consider the complex discrete-time base-band channel model, i.e. we assume that X_1, X_2 are complex-valued, that the additive noise variables are zero-mean circularly symmetric Gaussian, and the presence of a slowly and flat fading channel such that $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_{12}, \mathbf{h}_{21}$ (where now bold font signifies that the variables are *random*, not vectors) are independent circularly symmetric Gaussian random variables. Their realizations are constant for an entire codeword block (slow fading) and known by all parties (coherent).[1] Then $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ are exponentially-distributed with means $\beta_1, \beta_2, \beta_{12}, \beta_{21}$, re-

[1]The capacity will be doubled to account for the real and imaginary parts as in [45], [82], [47], [48].

spectively. We denote the powers of the noise for the two users by N_1 and N_2. In the works of [45], [82], [47], [48], the outage probability, defined as the probability that a target rate is unachievable, is of interest. In our work, we are interested in a simpler problem: the probability that it is impossible to achieve any non-zero rate given some power constraint. This is the same as $Pr\{\mathcal{A} = \emptyset\}$. We will derive this probability, and plot it for varying parameters.

Define the following variables:

$$\begin{aligned} SNR_{11} &\triangleq \frac{\beta_1 P_1^{\max}}{N_1}, \quad SNR_{22} \triangleq \frac{\beta_2 P_2^{\max}}{N_2}, \\ SNR_{12} &\triangleq \frac{\beta_{12} P_1^{\max}}{N_2}, \quad SNR_{21} \triangleq \frac{\beta_{21} P_2^{\max}}{N_1}, \end{aligned} \tag{6.23}$$

which can be interpreted as the single-user expected signal-to-noise (SNR) ratio, and

$$DCR \triangleq \frac{\beta_1 \beta_2}{\beta_{12}\beta_{21}}, \quad CDR \triangleq \frac{\beta_{12}\beta_{21}}{\beta_1 \beta_2}, \tag{6.24}$$

which we define as the direct-to-cross-expected-fading-ratio (DCR) and the cross-to-direct-expected-fading-ratio (CDR), respectively; essentially these two ratios measure how different the expected fading is on the direct links and on the cross-links. Finally define

$$\xi = \frac{(\beta_{12}N_1 + \beta_1 N_2)(\beta_2 N_1 + \beta_{21} N_2)}{\beta_1 \beta_2 \beta_{12} \beta_{21} N_1 N_2}, \tag{6.25}$$

as a constant independent of $P_1^{\max}, P_2^{\max}$. Equipped with these definitions, the prob-

ability of not achieving a non-zero rate is given by

$$\begin{aligned} Pr\{\mathcal{A}=\emptyset\} &= 1 - Pr\{\mathcal{A}\neq\emptyset\} \\ &= 1 - \frac{(\beta_1\beta_2+\beta_{12}\beta_{21})N_1N_2}{(\beta_{12}N_1+\beta_1N_2)(\beta_2N_1+\beta_{21}N_2)} \\ &+ DCR\cdot SNR_{11}^{-1}\cdot E(\xi\cdot SNR_{11}^{-1}) \\ &+ DCR\cdot SNR_{22}^{-1}\cdot E(\xi\cdot SNR_{22}^{-1}) \\ &+ CDR\cdot SNR_{12}^{-1}\cdot E(\xi\cdot SNR_{12}^{-1}) \\ &+ CDR\cdot SNR_{21}^{-1}\cdot E(\xi\cdot SNR_{21}^{-1}) \\ &- \frac{DCR}{SNR_{11}+SNR_{22}}\cdot E\left(\xi\frac{\beta_1\beta_2}{SNR_{11}+SNR_{22}}\right) \\ &- \frac{CDR}{SNR_{12}+SNR_{21}}\cdot E\left(\xi\frac{\beta_{12}\beta_{21}}{SNR_{12}+SNR_{21}}\right), \end{aligned} \tag{6.26}$$

where

$$E(x)=\exp(x)E_1(x), \quad E_1(x)=\int_x^\infty \frac{1}{t}\exp(-t)dt \tag{6.27}$$

and $E_1(x)$ is known as the exponential integral, which is common in the secrecy capacity of fading channels [47].

C. Interpretation, Numerical Example, and Discussion

Another way to view our problem is to consider $p(y|x)$ with $y=(y_1,y_2)$, $x=(x_1,x_2)$ as the main (legitimate) "single-user" channel to the base station. The wiretap channel can be viewed as $p'(\tilde{y}|y)$, where $\tilde{y}$ is either y_1 or y_2. In this way, the wiretap channel is degraded, and by the Gaussian wiretap channel theorem [21], the secrecy

capacity for this "single-user" channel is given by

$$\begin{aligned} C_S &= C_M - C_{MW} \\ &= I(X;Y) - I(X;\tilde{Y}) \\ &= I(X_1, X_2; Y_1, Y_2) - I(X_1, X_2, Y_i),\ i = 1 \text{ or } 2 \end{aligned}$$

which is precisely the upper bound in Theorem 8 for the Gaussian codebook. When applied to two users, it turns out that the users can time-share this C_S but cannot get a better rate than time-sharing C_S. Thus this interpretation gives insight into the outer bound.

Next we point out what it means to achieve one of the corner points, i.e. $(R_1, R_2) = (R_1, 0)$ and $(R_1, R_2) = (0, R_2)$. When one user has rate 0, that user is effectively jamming the eavesdropper's channel to the benefit of the legitimate sensor network, which has been studied in [40] under a different wiretap channel model.

1. Numerical Example for Inner Region

Next we give a numerical example that does not require linear programming. Recall that we introduced linear programming to aid many of the proofs and insights in this chapter. Once the theorems have been established, the derivation of the inner region does not require linear programming as we now show. Let $h_1^2 = 1, h_{12}^2 = 1/0.91, h_{21}^2 = 0.6, h_2^2 = 1,\ \sigma_1^2 = 0.9, \sigma_2^2 = 1,\ P_1^{\max} = 13.65, P_2^{\max} = 0.5$ for our example. We have chosen the maximum powers such that they already satisfy $P_1^{\max} = \alpha P_2^{\max}$ (where α is given by Eq. 6.12), and so we may allocate the maximum powers and not worry about using Table IV. In Fig. 12 we have the $\bar{\mathcal{R}}$ region bounded by the blue lines, and the $\mathcal{U}$ region given by the thicker red line (see Eqs. 6.45 and 6.46 for definition). The reader may verify that $R_1^{(1)*}$ (i.e. the maximum rate for User 1) can be acquired

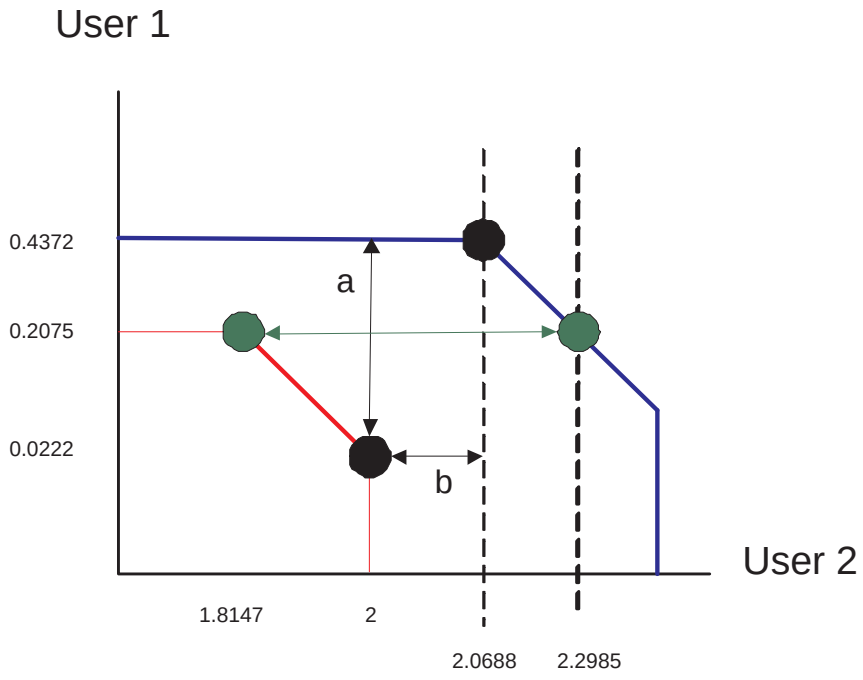

Fig. 12. Example Illustrating Inner Region Calculations without Linear Programming

by choosing the two black circles on the $\bar{\mathcal{R}}$ and $\mathcal{U}$ regions, and that $R_1^{(1)*}$ is then given by the distance marked a in Fig. 12; the R_2' corresponding to $R_1^{(1)*}$ is then the distance marked b in Fig. 12. Thus $(R_1^{(1)*}, R_2') = (0.415, 0.0688)$. Next the reader may verify that $R_2^{(2)*}$ (i.e. the maximum rate for User 2) can be acquired by choosing the two green circles on the $\bar{\mathcal{R}}$ and $\mathcal{U}$ regions, and that $R_2^{(2)*}$ is then given by the green distance in Fig. 12; the reader may also verify that there is no way to choose two green circles to yield a maximum rate for User 2, while still having a non-zero rate for User 1. Therefore the corresponding $R_1' = 0$. Thus $(R_1', R_2^{(2)*}) = (0, 0.4838)$. Note that both rate pairs sum to 0.4838, which is also the boundary of the outer region.

Given the points derived above, the inner region is then given in Fig. 13 as the shaded gray region. The thicker red diagonal line denotes the boundary of the outer region. It can be seen that the inner region for the equal SNR assumption is partially

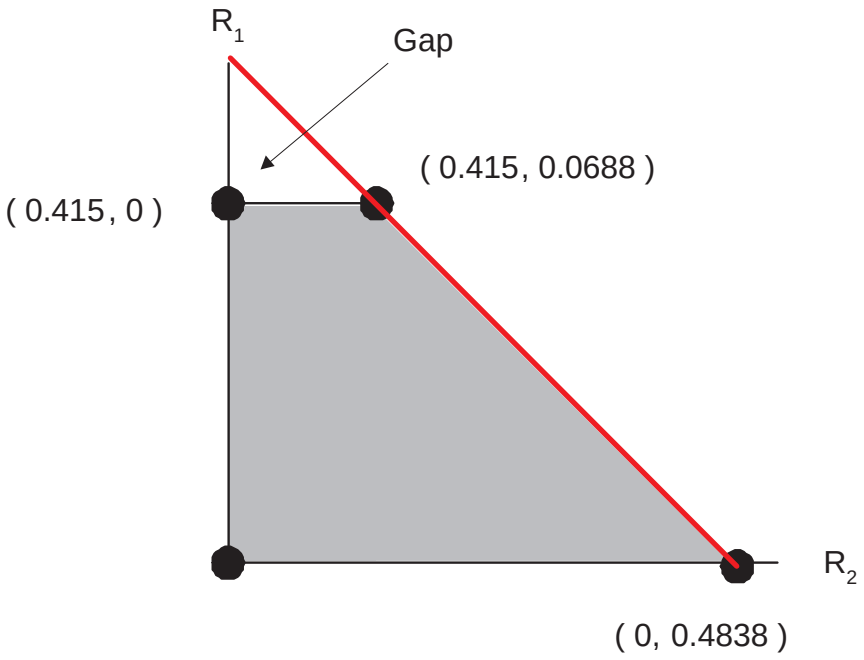

Fig. 13. Inner Region of Example

tight to the outer region. There is however a gap at the top.

In this example we chose parameters that satisfied the equal SNR assumption. It is easy to choose parameters that do not satisfy the equal SNR assumption. This observation motivates the next part, which deals with random fading.

2. Discussion on Random Fading

We pointed out that some parameters may not satisfy the equal SNR assumption, and thus coding using the equal SNR assumption cannot be used. If these parameters are fixed, then there is nothing we can do, i.e. the users cannot send messages in secrecy. However, this motivates the idea of random fading, which opens up the possibility that some realizations are amenable to the equal SNR assumption. Thus random fading is a friend rather than a foe as we further detail.

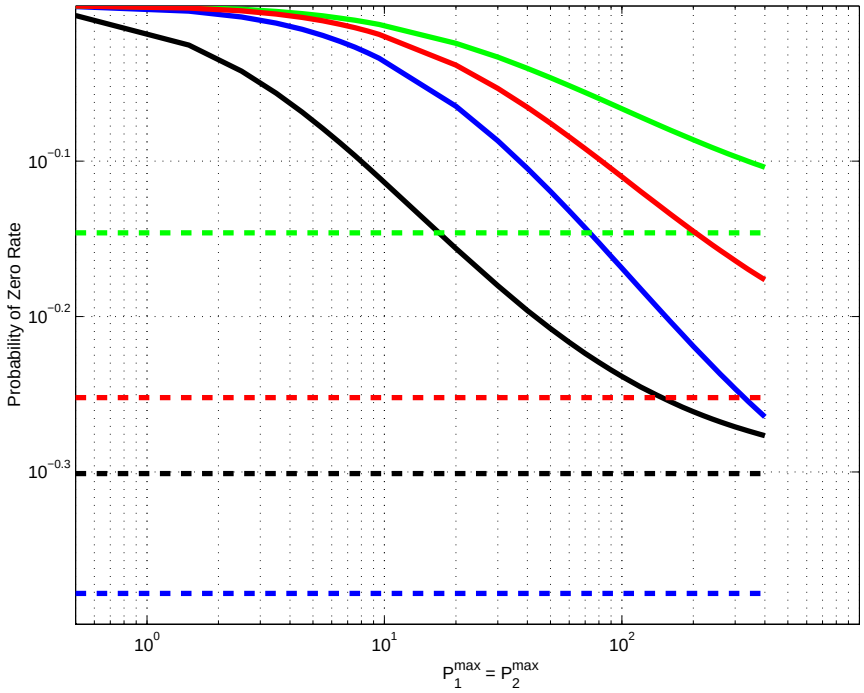

Fig. 14. Solid Lines: Probability That Users Cannot Achieve a Non-Zero Rate Given Maximal Power Constraints; Dotted Lines: When $P_1^{\max}, P_2^{\max} \to \infty$ (**Black:** $\beta_1 = \beta_2 = \beta_{12} = \beta_{21} = N_1 = N_2 = 1$, **Blue:** $\beta_1 = 1, \beta_2 = 0.5, \beta_{12} = 0.9, \beta_{21} = 0.1, N_1 = 1, N_2 = 2$, **Green:** $\beta_1 = 1, \beta_2 = 0.5, \beta_{12} = 0.2, \beta_{21} = 0.8, N_1 = 1, N_2 = 2$, **Red:** $\beta_1 = 1, \beta_2 = 0.3, \beta_{12} = 0.7, \beta_{21} = 0.1, N_1 = 2, N_2 = 1$)

Fig. 14 plots the derived $Pr\{\mathcal{A} = \emptyset\}$ for different channel parameters. There are three regions of interest that we will study: (1) $P_1^{\max}, P_2^{\max} \to 0$; (2) $P_1^{\max}, P_2^{\max} \to \infty$; (3) powers in between (1) and (2). The first two regions of interest are obvious and can be deduced simply from Eq. 6.59: when $P_1^{\max} = P_2^{\max} = 0$, the events never occur, and thus $Pr\{\mathcal{A} = \emptyset\} = 1 - Pr\{\mathcal{A} \neq \emptyset\} = 1$ as verified in Fig. 14; on the other hand when $P_1^{\max}, P_2^{\max} \to \infty$, it is easy to see that the only random event left would

be $\{\alpha > 0\}$, which is independent of $P_1^{\max}, P_2^{\max}$, and thus

$$Pr\{\mathcal{A} = \emptyset\} \to 1 - \frac{(\beta_1\beta_2 + \beta_{12}\beta_{21})N_1N_2}{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}. \tag{6.28}$$

With sufficiently large maximum allowable power, the probability of not achieving a non-zero rate is bounded by Eq. 6.28, which is depicted by the dotted lines in Fig. 14.

The third case is the most interesting case. From Fig. 14 we see that when $P_1^{\max}, P_2^{\max}$ is finite, the solid black curve performs better than the solid blue curve. However, in the infinite power region, the reverse is true: the dotted blue line performs better than the dotted black curve. In fact from Fig. 14, one can see the solid blue and black curves may intercept and cross over at some point. Eq. 6.26 is used informally for our interpretation of this third case. First, it is desirable to decrease the positive terms in Eq. 6.26. The positive terms may be decreased by increasing SNR_{ij}, since $\frac{1}{x}E(x)$ is a decreasing function. For example, in the term

$$DCR \cdot SNR_{11}^{-1} \cdot E(\xi \cdot SNR_{11}^{-1})$$

if SNR_{11} is increased, this term decreases. If the maximum powers $P_1^{\max}, P_2^{\max}$, are held constant, SNR_{11} may be increased by increasing β_1. The entire term may be further decreased if the denominator of DCR, $\beta_{12}\beta_{21}$, is increased. Thus we see that both β_1 (direct link) and $\beta_{12}\beta_{21}$ (cross-links) are increased together to decrease the above term. Similarly this argument can be applied to the other three positive terms in Eq. 6.26. This informally suggests that the expected fadings should approximately be equal to one another. Indeed, the black curve in Fig. 14 has the best performance in the finite power regime and it corresponds to the case when all parameters are equal.

D. Proofs and Ancillary Results

1. Proof of Theorem 8: Outer Region

We shall prove that with a *fixed* transmit power of (P_1, P_2), the rate pair $(R_1, R_2) \in \mathcal{C}^{\text{outer}}(P_1, P_2)$ is necessary. The derivation for the sum rate bound follows.

$$\begin{aligned} n(R_1+R_2) = H(W_1,W_2) &= H(W_1,W_2|Y_1^n,Y_2^n) + I(W_1,W_2;Y_1^n,Y_2^n) \\ &\overset{(a)}{\leq} n\epsilon_n + I(W_1,W_2;Y_1^n,Y_2^n) \\ &\overset{(b)}{=} I(W_1,W_2;Y_2^n) + I(W_1,W_2;Y_1^n|Y_2^n) + n\epsilon_n \\ &\overset{(c)}{\leq} n\epsilon + I(W_1,W_2;Y_1^n|Y_2^n) + n\epsilon_n \\ &\overset{(d)}{\leq} H(Y_1^n|Y_2^n) - H(Y_1^n|Y_2^n,W_1,W_2,X_1^n,X_2^n) + 2n\epsilon_n \\ &\overset{(e)}{\leq} H(Y_1^n|Y_2^n) - H(Y_1^n|Y_2^n,X_1^n,X_2^n) + 2n\epsilon_n \\ &= I(X_1^n,X_2^n;Y_1^n|Y_2^n) + 2n\epsilon_n \end{aligned} \tag{6.29}$$

The explanations are: (a) Fano's inequality; (c) the unconditional secrecy requirement of Eq. 6.6; (d) conditioning reduces entropy; (e) the data processing inequality on the Markov chain $(W_1, W_2) \leftrightarrow (X_1^n, X_2^n) \leftrightarrow (Y_1^n, Y_2^n)$. On the other hand, using the chain rule in (b) another way, gives another bound

$$n(R_1+R_2) \leq I(W_1,W_2;Y_1^n) + I(W_1,W_2;Y_2^n|Y_1^n) + n\epsilon_n$$

and using Eq. 6.6, and then $(c)-(e)$ again gives the other bound

$$n(R_1+R_2) \leq I(X_1^n,X_2^n;Y_2^n|Y_1^n) + 2n\epsilon_n. \tag{6.30}$$

To satisfy both bounds, we take the minimum of the two. Now we shall work with Eq. 6.29, and the same approach follows for Eq. 6.30. For now let X_1^n, X_2^n be Gaussian vectors such that their components are i.i.d., and let entropy and mutual information

be differential. Fixing a pair of transmit powers (P_1, P_2) we have

$$\begin{aligned} I(X_1^n, X_2^n; Y_1^n | Y_2^n) &= I(X_1^n, X_2^n; Y_1^n, Y_2^n) - I(X_1^n, X_2^n; Y_2^n) \\ &= \frac{n}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right) - nC(SNR_2) \end{aligned} \tag{6.31}$$

as the reader may verify. Next we bound the individual rates.

$$\begin{aligned} nR_1 &= H(W_1) = H(W_1|Y_1^n Y_2^n) + I(W_1; Y_1^n, Y_2^n) \\ &\overset{(a)}{\leq} n\epsilon_n + I(W_1; Y_1^n, Y_2^n) \\ &\overset{(b)}{=} I(W_1; Y_2^n) + I(W_1; Y_1^n | Y_2^n) + n\epsilon_n \\ &\overset{(c)}{\leq} n\epsilon + I(W_1; Y_1^n | Y_2^n) + n\epsilon_n \\ &\overset{(d)}{\leq} H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, W_1, X_1^n, X_2^n) + 2n\epsilon_n \\ &\overset{(e)}{=} H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, X_1^n, X_2^n) + 2n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_1^n | Y_2^n) + 2n\epsilon_n \end{aligned} \tag{6.32}$$

The explanations are the same as before. The chain rule of (b) can also be written in another way. Thus the individual bounds are the same as the sum rate bound.

Finally we prove that X_1^n, X_2^n maximizes Eq. 6.31 when they are chosen as vectors of i.i.d. Gaussian RVs. The proof follows easily from the clever device used in [57], and we include it here for completeness.

$$\begin{aligned} I(X_1^n, X_2^n; Y_1^n | Y_2^n) &= H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, X_1^n, X_2^n) \\ &= H(Y_1^n | Y_2^n) - H(Z_1^n | Z_2^n) \end{aligned} \tag{6.33}$$

Thus maximizing $I(X_1^n, X_2^n; Y_1^n | Y_2^n)$ over X_1^n, X_2^n is equivalent to maximizing $H(Y_1^n | Y_2^n)$ over X_1^n, X_2^n, since Z_1^n, Z_2^n are independent of X_1^n, X_2^n. Let $\mathbf{L}$ be a matrix such that $\mathbf{L}Y_2^n$ yields a vector in which each component in this vector is the best linear minimum mean square error (LMMSE) estimate of the corresponding component in vector Y_1^n.

Formally, let

$$\mathbf{L} \triangleq \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \tag{6.34}$$

where L_i a row vectors, and $L_i Y_2^n$ is the best LMMSE of $Y_{1,i}$. Then let the matrix $\mathbf{M}$ be the diagonal matrix in which the diagonal entries are the corresponding mean square estimation error. The following are information theoretic bounds.

$$\begin{aligned} H(Y_1^n|Y_2^n) &\overset{(a)}{=} H(Y_1^n - \mathbf{L}Y_2^n|Y_2^n) \\ &\overset{(b)}{\leq} H(Y_1^n - \mathbf{L}Y_2^n) \\ &\overset{(c)}{\leq} \frac{1}{2}\log(2\pi e)^n \det \mathbf{M}. \end{aligned} \tag{6.35}$$

The explanations follow: (a) follows since conditioning on Y_2^n makes $\mathbf{L}Y_2^n$ a constant; (b) conditioning reduces entropy; (c) the maximum entropy of random vector $Y_1^n - \mathbf{L}Y_2^n$ given a covariance matrix $\det \mathbf{M}$ is given by the expression of (c) [100]. To show that X_1^n, X_2^n achieves the maximum of Eq. 6.35, we show that the inequalities (b) and (c) are tight when X_1^n, X_2^n are the said Gaussian vectors.

From the orthogonality principle for the best LMMSE [101], $\mathbb{E}\{[(Y_1^n - \mathbf{L}Y_2^n)]_i Y_{2,j}\} = 0$ for each component i, j of the vectors. If X_1^n, X_2^n are Gaussian then the individual errors $[(Y_1^n - \mathbf{L}Y_2^n)]_i$ are also independent of $Y_{2,i}$, thus proving $Y_1^n - \mathbf{L}Y_2^n$ is independent of Y_2. Finally (c) is also tight since $Y_1^n - \mathbf{L}Y_2^n$ is a Gaussian random vector when X_1^n, X_2^n are Gaussian, which maximizes entropy for a covariance constraint.

2. Proof of Theorem 9: Inner Region

The proof of Theorem 9 consists of four parts. The first part is an unsimplified inner region (stated in Lemma 7 below) whose proof is similar (but with some differences) to the DMIC proof in Chapter V, which involves the convex hull of an infinite union

of regions. For completeness, the proof of Lemma 7 is included in Appendix A. The other three parts of the proof of Theorem 9 are entirely new to this chapter. The second part is the characterization of Lemma 7 via linear programming, i.e. the two LPs given in Section VI-B-2. The third part is to prove that increasing power implies increasing the inner region such that for $P_1 \leq Q_1$, $P_2 \leq Q_2$, $(P_1, P_2) \in \mathcal{A}$, $(Q_1, Q_2) \in \mathcal{A}$ implies $C^{\text{inner}}(P_1, P_2) \subseteq C^{\text{inner}}(Q_1, Q_2)$. This means that if we utilize the maximum admissible power, the resulting inner region is the largest inner region that is also a superset of all other inner regions. Finally the fourth part is to prove that Table IV provides the maximum admissible power. Towards this end, we divide the proof of Theorem 9 into its corresponding four sections.

a. Part 1: Gaussian Codebook and Corollary 1

The first part of the proof follows. Let $|x|^+ = \max\{x, 0\}$. Let the notation $x \stackrel{\circ}{=} a$ denote $a - \epsilon \leq x \leq a$ for $\epsilon > 0$ arbitrarily small. Recall that we only consider constructing achievable codes for the equal SNR case, i.e. $SNR_1 = SNR_2$, under Gaussian codebooks.

Lemma 7 *Let $\mathcal{C}^{inner}(P_1, P_2)$ be the set of (R_1, R_2) such that*

$$SNR_1 = SNR_2 \triangleq SNR_{Eq} \tag{6.36}$$

$$R_1 = \left|\bar{R}_1 - U_1\right|^+ \tag{6.37}$$

$$R_2 = \left|\bar{R}_2 - U_2\right|^+ \tag{6.38}$$

where

$$\begin{aligned} U_1 &\leq \min\left\{C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right), C\left(\frac{h_{12}^2 P_1}{\sigma_2^2}\right)\right\} && (6.39)\\ U_2 &\leq \min\left\{C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right), C\left(\frac{h_{21}^2 P_2}{\sigma_1^2}\right)\right\} && (6.40)\\ U_1 + U_2 &\doteq C\left(SNR_{Eq}\right) && (6.41)\\ \bar{R}_1 &\leq C\left(\frac{h_{12}^2 P_1}{\sigma_2^2} + \frac{h_1^2 P_1}{\sigma_1^2}\right) && (6.42)\\ \bar{R}_2 &\leq C\left(\frac{h_{21}^2 P_2}{\sigma_1^2} + \frac{h_2^2 P_2}{\sigma_2^2}\right) && (6.43)\\ \bar{R}_1 + \bar{R}_2 &\leq \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right). && (6.44) \end{aligned}$$

Then $\mathcal{C}^{inner}$ is the closure of the convex hull of

$$\bigcup_{(P_1,P_2)\in\mathcal{A}} \mathcal{C}^{inner}(P_1, P_2)$$

where $\mathcal{A}$ is given by Eq. 6.15.

The proof of Lemma 7 is included in Appendix A for completeness, and follows the same idea as the DMIC proof in Chapter V.

Remark 1: Notice that when $SNR_1 = SNR_2$ the sum rate bounds for both inner and outer regions match. If R_1, R_2 are non-zero, then choosing $\bar{R}_1, \bar{R}_2$ to achieve the bound in Eq. 6.44 yields Corollary 1. This is readily verified by the summing $R_1 + R_2 = \bar{R}_1 + \bar{R}_2 - (U_1 + U_2)$.

b. Part 2: Linear Program Formulation

Assume $\mathcal{A} \neq \emptyset$ and let $(P_1, P_2) \in \mathcal{A}$ be fixed. First we setup linear programs for finding the maximum rates of R_1 and R_2 for $\mathcal{C}^{\text{inner}}(P_1, P_2)$ as defined in Lemma 7. Finding the maximum R_1, R_2 can be formulated as the two linear programs below,

which easily follows from Lemma 7.

Linear Program 1

$$\begin{aligned} \text{maximize} \quad & \bar{R}_1 - U_1 \\ \text{subject to} \quad & U_1 \leq \text{ RHS of Eq. 6.39} \\ & U_2 \leq \text{ RHS of Eq. 6.40} \\ & \bar{R}_1 \leq \text{ RHS of Eq. 6.42} \\ & \bar{R}_2 \leq \text{ RHS of Eq. 6.43} \\ & \bar{R}_1 + \bar{R}_2 \leq \text{ RHS of Eq. 6.44} \\ & \bar{R}_2 - U_2 \geq 0 \\ & U_1 + U_2 = C\left(SNR_{Eq}\right) \\ & \bar{R}_1, \bar{R}_2, U_1, U_2 \geq 0 \end{aligned}$$

Linear Program 2

$$\begin{aligned} \text{maximize} \quad & \bar{R}_2 - U_2 \\ \text{subject to} \quad & U_1 \leq \text{ RHS of Eq. 6.39} \\ & U_2 \leq \text{ RHS of Eq. 6.40} \\ & \bar{R}_1 \leq \text{ RHS of Eq. 6.42} \\ & \bar{R}_2 \leq \text{ RHS of Eq. 6.43} \\ & \bar{R}_1 + \bar{R}_2 \leq \text{ RHS of Eq. 6.44} \\ & \bar{R}_1 - U_1 \geq 0 \\ & U_1 + U_2 = C\left(SNR_{Eq}\right) \\ & \bar{R}_1, \bar{R}_2, U_1, U_2 \geq 0 \end{aligned}$$

Let R_1^*, R_2^* be the maxima of Programs 1 and 2 resp. and let U_2', U_1' be returned from Programs 1 and 2 resp. and $\bar{R}_1', \bar{R}_2'$ be returned from Programs 1 and 2 resp. Define:

$$\begin{aligned} R_2' &= \min\left\{\frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - \bar{R}_1', \text{RHS of Eq. 6.43}\right\} - U_2' \\ R_1' &= \min\left\{\frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - \bar{R}_2', \text{RHS of Eq. 6.42}\right\} - U_1' \end{aligned}$$

Then we have the following corollary of Lemma 7.

Corollary 2 *$\mathcal{C}^{inner}(P_1, P_2)$ is given by the convex hull of the points*

$$\{(0,0), (0, R_2^*), (R_1^*, 0), (R_1^*, R_2'), (R_1', R_2^*)\}.$$

Proof 1 *Assume that the LPs are feasible, i.e. $R_1^*, R_2^* \geq 0$, then the achievability of the above points is obvious, and the convex hull operation can be explained using a time sharing argument. In addition, the fact that R_1^*, R_2^* are maximal implies the convex hull of the above points is the entire $\mathcal{C}^{inner}(P_1, P_2)$.*

To prove $R_1^*, R_2^* \geq 0$ (which also proves that the LPs are feasible), let

$$\begin{aligned} \bar{\mathcal{R}} = \{(x,y) \quad : \quad & 0 \leq x \leq \textit{RHS of Eq. 6.42}, \\ & 0 \leq y \leq \textit{RHS of Eq. 6.43}, \\ & 0 \leq x + y \leq \textit{RHS of Eq. 6.44}\} \end{aligned} \tag{6.45}$$

and

$$\begin{aligned} \mathcal{U} = \{(x,y) \quad : \quad & 0 \leq x \leq \textit{RHS of Eq. 6.39}, \\ & 0 \leq y \leq \textit{RHS of Eq. 6.40}, \\ & x + y = C(SNR_{Eq})\}. \end{aligned} \tag{6.46}$$

It is easy to show $\bar{\mathcal{R}} \supseteq \mathcal{U}$, thus there will always exist a point in $\bar{\mathcal{R}}$ and another point in $\mathcal{U}$, such that their difference results in a point whose coordinates are both non-

negative. By definition of R_1^*, R_2^* (being maxima), R_1^*, R_2^* also must be non-negative.

The two regions we defined in the proof, $\bar{\mathcal{R}}$ and $\mathcal{U}$ will come up again in the third part of the proof.

c. Part 3: Increasing Supersets

To prove that for $P_1 \leq Q_1$, $P_2 \leq Q_2$, $(P_1, P_2) \in \mathcal{A}$, $(Q_1, Q_2) \in \mathcal{A}$ implies $C^{\text{inner}}(P_1, P_2) \subseteq C^{\text{inner}}(Q_1, Q_2)$, we use the previous characterization of an inner region as the convex hull of a finite number of points. Essentially we must show that when power is increased, each of these points must increase too.

We start by using Corollary 1. Corollary 1 implies that the points along the diagonal of Fig. 15 sum to

$$f(\mathbf{Q}) = \frac{1}{2}\log_2\left(\frac{\det(\mathbf{Z}+\mathbf{H}\mathbf{Q}\mathbf{H}^T)}{\det \mathbf{Z}}\right) - \frac{1}{2}\log_2\left(1+\frac{\mathbf{H}_i\mathbf{Q}\mathbf{H}_i^T}{\sigma_i^2}\right)$$

where

$$\mathbf{H} = \begin{pmatrix} h_1 & h_{21} \\ h_{12} & h_2 \end{pmatrix},\ \mathbf{Q} = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix},\ \mathbf{Z} = \begin{pmatrix} \sigma_1^2 & 0 \\ 0 & \sigma_2^2 \end{pmatrix} \tag{6.47}$$

and $\mathbf{H}_i$ is row i of matrix $\mathbf{H}$. $f(\mathbf{Q})$ is increasing in P_1, P_2 as it has the form of the secrecy capacity of a degraded wiretap channel. Thus from this expression we know that the diagonal will increase when the powers are increased.

We now have to show the horizontal and vertical segments of Fig. 15 (if they exist), also increase with power. More generally, this is equivalent to showing that $R_1^{(1)*}, R_2^{(2)*}$ increase with increasing power. Fig. 16 illustrates a scenario in which we are trying to disprove, i.e. prove is impossible. Notice that the diagonal line increases as we proved above, but the horizontal and vertical parts decrease in this impossible scenario we set out to prove. To show $R_i^{(i)*}$ increases with power, we must find the

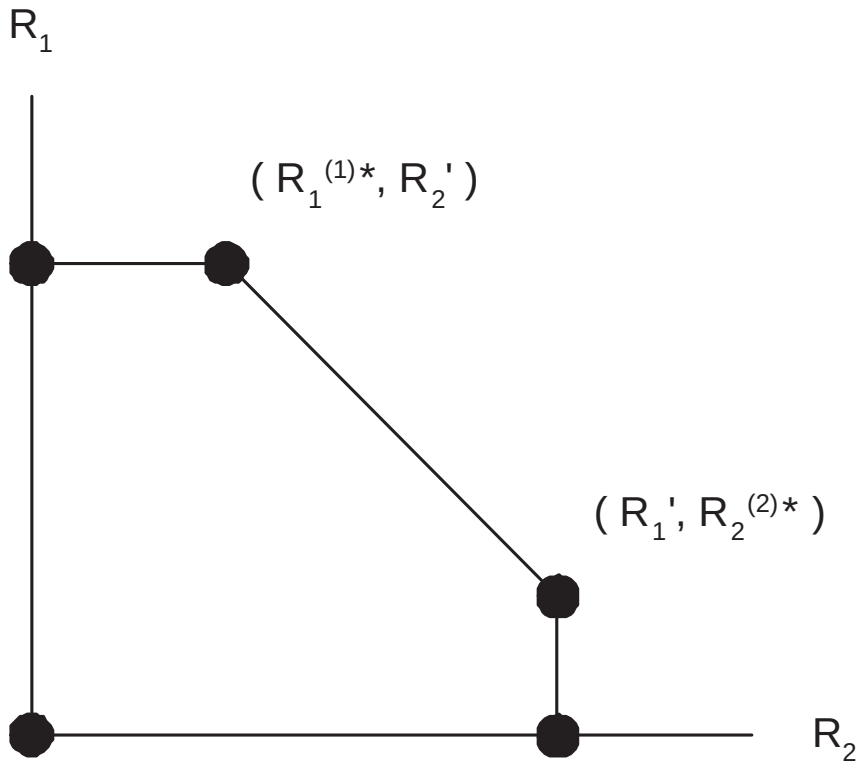

Fig. 15. General Inner Region

form(s) of $R_i^{(i)*}$. It turns out that $R_i^{(i)*}$ can take on two forms, i.e. either

$$\text{Form } A \;=\; \frac{1}{2}\log_2\left(\frac{K_{12}}{\sigma_1^2\sigma_2^2}\right) - C\left(SNR_{Eq}\right) \tag{6.48}$$

$$\text{Form } B \;=\; C_{\bar{R}_i}^{\max} + C_{U_j}^{\max} - C\left(SNR_{Eq}\right), \qquad i,j \in \{1,2\}, i \neq j \tag{6.49}$$

where $C_{\bar{R}_i}^{\max}$ is either the LHS of Eqs. 6.42 or 6.43 depending on i, and $C_{U_j}^{\max}$ is either the LHS of Eqs. 6.39 or 6.40 depending on j. Eqs. 6.48 and 6.49 can be observed from Appendix B. Also the derivation of these two forms via Appendix B can be further clarified by perusing the example in Section VI-C-1 first.

Eq. 6.48 is nothing more than $f(\mathbf{Q})$, which we have already shown increases with

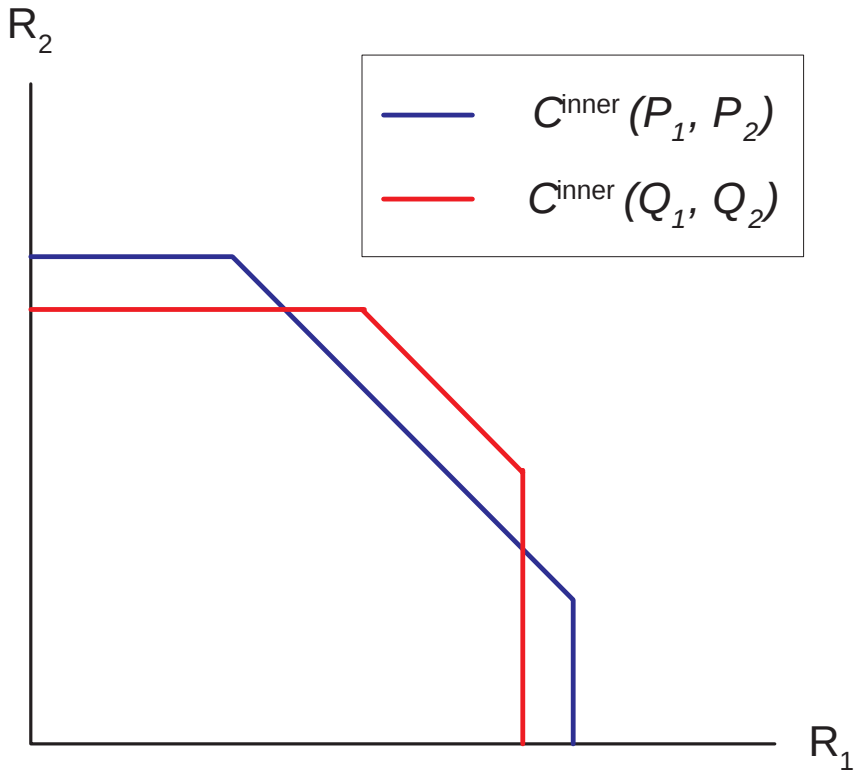

Fig. 16. Impossible Scenario When $(P_1, P_2) \preceq (Q_1, Q_2)$

power. Eq. 6.49 can also be written as

$$\begin{aligned}\text{Form } B &= \frac{1}{2}\log_2\left(1+\frac{h_1^2P_1+h_{21}^2P_2}{\sigma_1^2}+\frac{P_1P_2h_1^2h_{21}^2}{\sigma_1^2}+\frac{P_2h_2^2}{\sigma_2^2}+\frac{P_1P_2h_1^2h_2^2}{\sigma_1^2\sigma_2^2}\right)\\ &\quad -\frac{1}{2}\log_2\left(1+\frac{h_1^2P_1+h_{21}^2P_2}{\sigma_1^2}\right)\\ &= \frac{1}{2}\log_2\left(1+\underbrace{\frac{P_2(h_2^2\sigma_1^2+h_1^2P_1(h_2^2+h_{21}^2\sigma_2^2))}{\sigma_2^2(h_1^2P_1+h_{21}^2P_2+\sigma_1^2)}}_{\triangleq g(P_1,P_2)}\right). \qquad (6.50)\end{aligned}$$

Now it is straightforward to show $g(P_1, P_2)$ is increasing in (P_1, P_2) by verifying that $\frac{\partial g(P_1,P_2)}{\partial P_1} > 0$ and $\frac{\partial g(P_1,P_2)}{\partial P_2} > 0$, and so Eq. 6.49 also increases with power.

From this we have a partial conclusion. If $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate

of Form A, and if $(Q_1, Q_2) \in \mathcal{A}$ (where $(Q_1, Q_2) \succeq (P_1, P_2)$) also yields a maximum rate of Form A, then the maximum rate increases. Similarly if $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate of Form B, and if $(Q_1, Q_2) \in \mathcal{A}$ also yields a maximum rate of Form B, then the maximum rate increases.

For a complete conclusion we must also consider the scenario in which $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate of Form A, *but* $(Q_1, Q_2) \in \mathcal{A}$ yields a maximum rate of Form B, i.e. the forms change, and vice versa. Notice (observed from Appendix B) that Form B occurs when

$$C_{\bar{R}_i}^{\max} + C_{U_j}^{\max} \leq \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right), \quad i, j \in \{1, 2\}, i \neq j.$$

Thus when Form B occurs, Form A is larger than Form B. Therefore if we start with Form B, and applying (Q_1, Q_2) changes the maximum rate to Form A, then the maximum rate will have increased. Alternatively, consider starting with Form A, in which case we have

$$C_{\bar{R}_i}^{\max} + C_{U_j}^{\max} > \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right), \quad i, j \in \{1, 2\}, i \neq j.$$

Thus when Form A occurs, Form B is larger than Form A. Therefore if we start from Form A, and applying (Q_1, Q_2) changes the maximum rate to Form B, then the maximum rate will have increased. This proves that increasing power always results in an inner region that is a superset.

As a concluding remark, we point out that Form B corresponds to the inner region having a horizontal or vertical part, while Form A corresponds to not having a horizontal or vertical part.

d. Part 4: Maximum Power Allocation

First we prove that the power assignments must be from $\mathcal{A}$ (Eq. 6.15) under the equal SNR assumption. The fact that (P_1, P_2) must lie on the line $P_1 = \alpha P_2$ (where α is from Eq. 6.12) easily follows from solving the equation $SNR_1 = SNR_2$ as the reader may verify. The lower bounds γ_1, γ_2 (Eqs. 6.13 and 6.14) are not as straightforward to see. First note that α must be positive, otherwise P_1 would be negative, which is impossible. α is positive under the following conditions:

$$\frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \quad \text{and} \quad \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2} \quad \text{or} \tag{6.51}$$

$$\frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \quad \text{and} \quad \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}. \tag{6.52}$$

Next note that the $\mathcal{U}$ region is not a multiple access channel (MAC) region even if the almost-equality in Eq. 6.41 is changed to an equality $\leq$. This is because U_1, U_2 in Eqs. 6.39 and 6.40 are bounded by the minima of capacities of different channels. Thus we must manually enforce the following, (which is always guaranteed for a MAC):

$$C_{U_1}^{\max} + C_{U_2}^{\max} \geq C\left(SNR_{Eq}\right), \tag{6.53}$$

where $C_{U_1}^{\max}$ and $C_{U_2}^{\max}$ are the left hand sides of Eqs. 6.39 and 6.40, respectively. This is required since if Eq. 6.53 is *not* satisfied, then the almost-equality in Eq. 6.41 cannot be satisfied either, and the coding scheme of Lemma 7 cannot be used. From Eqs. 6.51 and 6.52, we can make Eq. 6.53 explicit.

When Eq. 6.52 is true, the reader can verify that

$$C_{U_1}^{\max} = C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right), \quad C_{U_2}^{\max} = C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right), \tag{6.54}$$

which implies

$$P_1 \geq \frac{\sigma_2^2 h_{21}^2}{h_1^2 h_2^2} - \frac{\sigma_1^2}{h_1^2}, \quad P_2 \geq \frac{\sigma_1^2 h_{12}^2}{h_1^2 h_2^2} - \frac{\sigma_2^2}{h_2^2}, \tag{6.55}$$

matching the corresponding cases in γ_1 and γ_2 (Eqs. 6.13 and 6.14), respectively. When Eq. 6.51 is true, the same technique may be applied. Thus this establishes the admissible power set $\mathcal{A}$.

From the Part 3 of this proof we know that allocating the maximum power is optimal. We now prove that Table IV assigns the maximum power. Let us assume for now that $\gamma_1 = \gamma_2 = 0$, so that only $P_1^{\max}$ and $P_2^{\max}$ are important.

Consider the case when $P_2^{\max} > P_1^{\max}$ and $0 < \alpha < 1$. We would like to choose $P_1^{\max}$ or $P_2^{\max}$ whichever is possible. If $\alpha P_2^{\max} > P_1^{\max}$, and we choose $P_1 = P_1^{\max}$, then $P_2 = P_1^{\max}/\alpha < P_2^{\max}$, thus User 2's power constraint is not violated. If $\alpha P_2^{\max} \leq P_1^{\max}$, and we choose $P_2 = P_2^{\max}$, then $P_1 = \alpha P_2^{\max} \leq P_1^{\max}$, thus User 1's power constraint is not violated.

Consider the case when $P_2^{\max} > P_1^{\max}$ and $\alpha > 1$. We would like to choose $P_1^{\max}$ or $P_2^{\max}$ whichever is possible. If $\alpha P_2^{\max} > P_1^{\max}$, and we choose $P_1 = P_1^{\max}$, then $P_2 = P_1^{\max}/\alpha P_2^{\max}$, thus User 2's power constraint is not violated. Finally, under this scenario it is impossible to have $\alpha P_2^{\max} \leq P_1^{\max}$, since $\alpha > 1$ and $P_2^{\max} > P_1^{\max}$.

Consider the case when $P_2^{\max} < P_1^{\max}$ and $0 < \alpha < 1$, which implies $P_2 > P_1$. We would like to choose $P_1^{\max}$ or $P_2^{\max}$ whichever is possible. If $\alpha P_2^{\max} \leq P_1^{\max}$, and we choose $P_2 = P_2^{\max}$ then User 1's power constraint is not violated since $P_1 = \alpha P_2^{\max}$. Finally, under this scenario it is impossible to have $\alpha P_2^{\max} > P_1^{\max}$, since $0 < \alpha < 1$, and $P_2^{\max} < P_1^{\max}$, thus the optimal power allocation for this scenario is always $P_1 = \alpha P_2^{\max}$ and $P_2 = P_2^{\max}$.

Consider the case when $P_2^{\max} < P_1^{\max}$ and $\alpha > 1$, which implies $P_2 < P_1$. We would like to choose $P_1^{\max}$ or $P_2^{\max}$ whichever is possible. If $\alpha P_2^{\max} > P_1^{\max}$, then $P_2 =$

$P_1^{\max}/\alpha < P_2^{\max}$, thus User 2's power constraint is not violated. If $\alpha P_2^{\max} \leq P_1^{\max}$, and we choose $P_2 = P_2^{\max}$, then User 1's power constraint is not violated as before.

Finally we deal with the case when $\gamma_1, \gamma_2 \neq 0$. In all cases in Table IV, the maximum power possible is allocated. Thus if this maximum power does not meet either $P_1 \geq \gamma_1$ or $P_2 \geq \gamma_2$, then no power allocation exists, and rates of zero are necessary for both users under our equal SNR assumption coding technique.

3. Informal Sensitivity Analysis Interpretation

Part 3 of the proof of Theorem 9 is quite tedious and does not provide clear insights. In this section we give a brief informal insight into why the maximum rates increase as the powers are increased using ideas from sensitivity analysis.

As always for the proofs assume $\mathcal{A} \neq \emptyset$. We will work with Linear Program 2 (LP 2), and note that the same ideas can be applied to Linear Program 1. LP 2 can be put into standard form, that is, the constraints are all equality constraints. Next, the dual function for LP 2 in standard form can be derived as

$$g(\nu) = \begin{cases} -d^T\nu & \text{if } \nu_1, \ldots, \nu_6 \geq 0, \\ & \nu_1 + \nu_6 + \nu_7 \geq 0, \\ & \nu_2 + \nu_7 \geq 1, \\ & \nu_4 + \nu_5 \geq -1, \\ -\infty & \text{otherwise.} \end{cases} \tag{6.56}$$

where

$$d = \begin{pmatrix} b \\ C\left(SNR_{Eq}\right) \end{pmatrix} \tag{6.57}$$

with b from Eq. 6.16. Therefore the primal program equality constraint has the

following form: $\mathbf{G}x - d = 0$ where d is the vector given in Eq. 6.57. Notice that when P_1, P_2 are increased, the components in the vector d increase; let $v \succeq 0$ be the vector of these increases. Thus when the powers are increased, d is perturbed and becomes $d + v$.

Let $p^*(v)$ be the optimal value of LP 2 as a function of v. We will not prove that $p^*(v)$ is differentiable at $v = 0$ as this discussion is informal, so towards this end let us assume that this is the case. Then since strong duality holds for LP 2 (since it is feasible), the optimal dual variables ν^* (cf. ν in Eq. 6.56) is related by

$$\nu_i^* = -\frac{\partial p^*(0)}{\partial v_i}, \tag{6.58}$$

and thus $\partial p^*(0) = -\nu_i^* \partial v_i$. Since $v \succeq 0$ this implies $\partial v_i \geq 0$. Next, from Eq. 6.56, we see that almost all $\nu_i \geq 0$, thus together with $\partial v_i \geq 0$, most $\partial p^*(0) \leq 0$. This means that increasing the power is likely to decrease the optimal value of LP 2, or in other words increase User 2's rate.

4. Derivation of Random Fading Result

It is easier to derive the complement probability $Pr\{\mathcal{A} \neq \emptyset\}$, and we do so towards this end. There are three main events that must occur: $\{\alpha > 0\}$, and $\{P_1^{\max} > \gamma_1\}, \{P_2^{\max} > \gamma_2\}$, of which $\alpha, \gamma_1, \gamma_2$ are functions of the random variables $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ described above. We simplify the derivation by separating the $\{\alpha > 0\}$ event into two disjoint events given by Eqs. 6.51 and 6.52, respectively. Since these two events are disjoint, the complement probability is the sum of two

probabilities.

$$\begin{aligned} Pr\{\mathcal{A} \neq \emptyset\} &= Pr\left\{ \frac{|\mathbf{h}_{21}|^2}{|\mathbf{h}_2|^2} > \frac{N_1}{N_2} \text{ and } \frac{|\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2} > \frac{N_2}{N_1} \right. \\ &\qquad \left. \text{and } P_1^{\max} \geq \frac{N_2|\mathbf{h}_{21}|^2}{|\mathbf{h}_1|^2|\mathbf{h}_2|^2} - \frac{N_1}{|\mathbf{h}_1|^2} \text{ and } P_2^{\max} \geq \frac{N_1|\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2|\mathbf{h}_2|^2} - \frac{N_2}{|\mathbf{h}_2|^2} \right\} \\ &+ Pr\left\{ \frac{|\mathbf{h}_{21}|^2}{|\mathbf{h}_2|^2} < \frac{N_1}{N_2} \text{ and } \frac{|\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2} < \frac{N_2}{N_1} \right. \\ &\qquad \left. \text{and } P_1^{\max} \geq \frac{N_1|\mathbf{h}_2|^2}{|\mathbf{h}_{12}|^2|\mathbf{h}_{21}|^2} - \frac{N_2}{|\mathbf{h}_{12}|^2} \text{ and } P_2^{\max} \geq \frac{N_2|\mathbf{h}_1|^2}{|\mathbf{h}_{12}|^2|\mathbf{h}_{21}|^2} - \frac{N_1}{|\mathbf{h}_{21}|^2} \right\} \end{aligned} \tag{6.59}$$

The above expression is still far too complex to obtain a closed form expression, thus we apply a few standard devices. The reader may verify that the above expression may be simplified to the following by combing conditions, using the total probability theorem, and noting that $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ are independent:

$$\begin{aligned} & Pr\{\mathcal{A} \neq \emptyset\} \\ = & \int_0^\infty \int_0^\infty Pr\left\{ |\mathbf{h}_2|^2 \frac{N_1}{N_2} < |\mathbf{h}_{21}|^2 \leq \frac{|\mathbf{h}_2|^2}{N_2}(P_1^{\max}|\mathbf{h}_1|^2 + N_1) \;\middle|\; |\mathbf{h}_1|^2 = s, |\mathbf{h}_2|^2 = t \right\} \\ & Pr\left\{ |\mathbf{h}_1|^2 \frac{N_2}{N_1} < |\mathbf{h}_{12}|^2 \leq \frac{|\mathbf{h}_1|^2}{N_1}(P_2^{\max}|\mathbf{h}_2|^2 + N_2) \;\middle|\; |\mathbf{h}_1|^2 = s, |\mathbf{h}_2|^2 = t \right\} \\ & Pr\{|\mathbf{h}_1|^2 = s\} Pr\{|\mathbf{h}_2|^2 = t\} \; ds \; dt \\ + & \int_0^\infty \int_0^\infty Pr\left\{ |\mathbf{h}_{21}|^2 \frac{N_2}{N_1} < |\mathbf{h}_2|^2 \leq \frac{|\mathbf{h}_{21}|^2}{N_1}(|\mathbf{h}_{12}|^2 P_1^{\max} + N_2) \;\middle|\; \right. \\ & \qquad \left. |\mathbf{h}_{12}|^2 = u, |\mathbf{h}_{21}|^2 = v \right\} \\ & Pr\left\{ |\mathbf{h}_{12}|^2 \frac{N_1}{N_2} < |\mathbf{h}_1|^2 \leq \frac{|\mathbf{h}_{12}|^2}{N_2}(|\mathbf{h}_{21}|^2 P_2^{\max} + N_1) \;\middle|\; |\mathbf{h}_{12}|^2 = u, |\mathbf{h}_{21}|^2 = v \right\} \\ & Pr\{|\mathbf{h}_{12}|^2 = u\} Pr\{|\mathbf{h}_{21}|^2 = v\} \; du \; dv. \end{aligned} \tag{6.60}$$

The simplified expression above allows us to use the cumulative distribution function (cdf) of the exponential distribution inside the integrals. Taking the integral then

yields

$$
\begin{aligned}
& Pr\{\mathcal{A} \neq \emptyset\} \\
= \; & \frac{(\beta_1\beta_2 + \beta_{12}\beta_{21})N_1N_2}{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)} \\
+ \; & \frac{\beta_1\beta_2N_1N_2}{\beta_{12}\beta_{21}(\beta_1N_2P_1^{\max} + \beta_2N_1P_2^{\max})} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_{12}\beta_{21}(\beta_1N_2P_1^{\max} + \beta_2N_1P_2^{\max})}\right) \\
+ \; & \frac{\beta_{12}\beta_{21}N_1N_2}{\beta_1\beta_2(\beta_{12}N_1P_1^{\max} + \beta_{21}N_2P_2^{\max})} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2(\beta_{12}N_1P_1^{\max} + \beta_{21}N_2P_2^{\max})}\right) \\
- \; & \frac{\beta_{21}N_2}{\beta_1\beta_2P_1^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2\beta_{12}N_1P_1^{\max}}\right) \\
- \; & \frac{\beta_1N_2}{\beta_{12}\beta_{21}P_2^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_2\beta_{12}\beta_{21}N_1P_2^{\max}}\right) \\
- \; & \frac{\beta_2N_1}{\beta_{12}\beta_{21}P_1^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_{12}\beta_{21}N_2P_1^{\max}}\right) \\
- \; & \frac{\beta_{12}N_1}{\beta_1\beta_2P_2^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2\beta_{21}N_2P_2^{\max}}\right). \qquad (6.61)
\end{aligned}
$$

Then applying the definitions in Eqs. 6.23, 6.24, 6.25 to Eq. 6.61 yields Eq. 6.26.

5. Inner Region for the Z-Channel

The inner region for the Z-channel is a straightforward application of [102]. In [102], a terminal wishes to send a secret message to a base station. A wiretapper nearby can also listen to the transmissions of the terminal. A second base station nearby produces artificial noise with the goal of jamming the wiretapper. This artificial noise also affects the first base station, however the first base station has a copy of this artificial noise, and hence can subtract it prior to decoding. The system model can be described by

$$Y_B^n = h_{TB}X_T^n + Z_B \qquad (6.62)$$

$$Y_W^n = h_{TW}X_T^n + h_{BW}X_B^n + Z_W \qquad (6.63)$$

where Y_B^n is the vector received at the first base station after subtracting the artificial noise, h_{TB} is the channel gain from the sending terminal to the first base station, X_T^n is the codeword sent by the terminal, $Z_B^n \sim \mathcal{N}(0, \sigma_B^2 I_n)$ is noise experienced on the channel from the terminal to the base station, Y_E^n is the vector received by the wiretapper, h_{TW} is the channel gain from the sending terminal to the wiretapper, h_{BW} is the channel gain from the second base station (the jammer) to the wiretapper, X_B^n is the artificial noise sent by the second base station, and $Z_W^n \sim \mathcal{N}(0, \sigma_W^2 I_n)$ accounts for the AWGN experienced by the wiretapper. For simplicity, we have subtracted X_B^n from the first base station, which is why it is absent in Eq. 6.62, although in practice the first base station would perform this in its decoder. This simplified system model is illustrated in Fig. 17. Let R_T be the rate of the sending terminal, and R_B be the

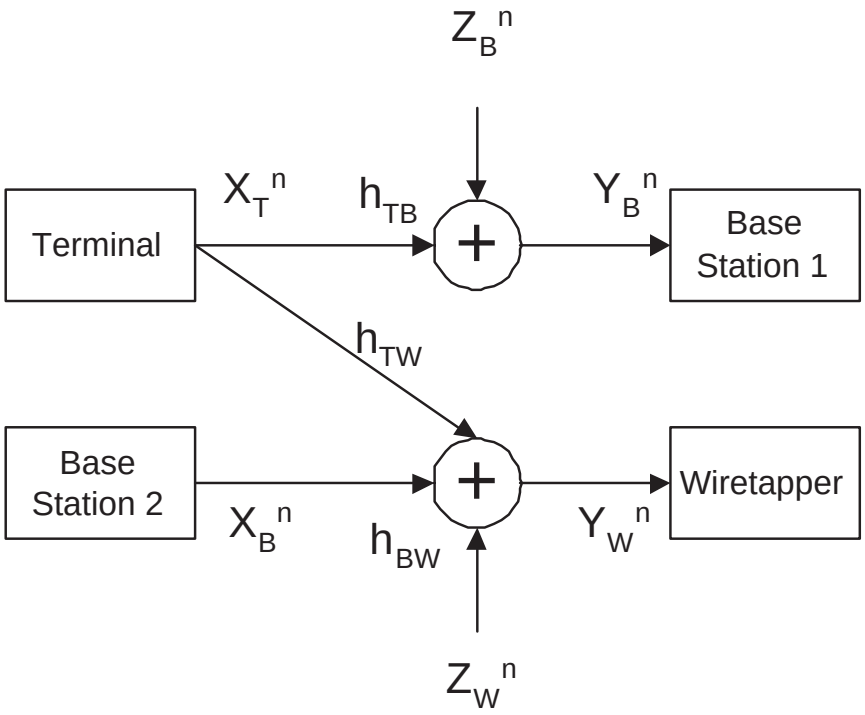

Fig. 17. Secure Communications via Cooperating Base Stations

rate of the second base station (the jammer). Let P_T be the power at the sending terminal, and P_B be the power at the second base station. In [102] the following rate R_T as a function of R_B is shown to be achievable with unconditional secrecy:

$$R_T(R_B) = \begin{cases} R_T^{(l)} & \text{if } R_B < C\left(\frac{h_{BW}^2 P_B}{\sigma_W^2 + h_{TW}^2 P_T}\right), \\ R_T^{(m)} & \text{if } C\left(\frac{h_{BW}^2 P_B}{\sigma_W^2 + h_{TW}^2 P_T}\right) < R_B \leq C\left(\frac{h_{BW}^2 P_B}{\sigma_W^2}\right), \\ R_T^{(u)} & \text{if } R_B > C\left(\frac{h_{BW}^2 P_B}{\sigma_W^2}\right). \end{cases} \tag{6.64}$$

where

$$R_T^{(l)} = \left| C\left(\frac{h_{TB}^2 P_T}{\sigma_B^2}\right) - C\left(\frac{h_{TW}^2 P_T}{\sigma_W^2}\right) \right|^+ \tag{6.65}$$

$$R_T^{(m)} = \left| C\left(\frac{h_{TB}^2 P_T}{\sigma_B^2}\right) - C\left(\frac{h_{TW}^2 P_T}{\sigma_W^2} + \frac{h_{BW}^2 P_B}{\sigma_W^2}\right) + R_B \right|^+ \tag{6.66}$$

$$R_T^{(u)} = \left| C\left(\frac{h_{TB}^2 P_T}{\sigma_B^2}\right) - C\left(\frac{h_{TW}^2 P_T}{\sigma_W^2 + h_{BW}^2 P_B}\right) \right|^+ . \tag{6.67}$$

Although this does not appear to be related to our problem, since the wiretapper has his own channel, our Z-channel is in fact a special case of this problem. Consider our Z-channel in which $h_{12} = 0$ in Fig. 11. In this case User 2 clearly cannot achieve unconditional secrecy. Thus User 2 must play the role of the jammer to protect User 1's message from a wiretapper who intercepts Y_1^n in Fig. 11. Note that since the wiretapper can only choose either Y_1^n and Y_2^n, the wiretapper should always choose Y_1^n, which is the only one containing the secret message; Y_2^n only contains noise and User 2's jamming signal. On the other hand since the base station receives both Y_1^n and Y_2^n, the base station can subtract X_2^n from Y_1^n if and only if User 2's rate is less than or equal to its channel capacity $C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right)$. Since User 2 should maximize its rate in order to jam the wiretapper as much as possible, we set $R_2 = C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right)$.

If we let $h_{TB} = h_{TW} = h_1$, $Z_B^n = Z_W^n = Z_1^n$, $h_{BW} = h_{21}$, $Y_W^n = Y_1^n$, and Y_B^n is equal to Y_1^n minus User 2's jamming signal (available to the base station through Y_2^n),

then the relationship between our Z-channel and Fig. 17 is apparent. Then setting $P_1 = P_T$, $P_2 = P_B$, $R_1 = R_T$, $R_2 = R_B = C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right)$ and then applying Eq. 6.64 yields the inner region for our Z-channel:

$$R_1 = \begin{cases} 0 & \text{if } \frac{h_2^2}{\sigma_2^2} < \frac{h_{21}^2}{\sigma_1^2 + h_1^2 P_1}, \\ \left| C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right) + C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right) - C\left(SNR_1\right) \right|^+ & \text{if } \frac{h_{21}^2}{\sigma_1^2 + h_1^2 P_1} < \frac{h_2^2}{\sigma_2^2} \leq \frac{h_{21}^2}{\sigma_1^2}, \\ C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right) - C\left(\frac{h_1^2 P_1}{\sigma_1^2 + h_{21}^2 P_2}\right) & \text{if } \frac{h_2^2}{\sigma_2^2} > \frac{h_{21}^2}{\sigma_1^2}. \end{cases} \tag{6.68}$$

where SNR_1, SNR_2 given in Eqs. 6.9 and 6.10, respectively. Interestingly, $R_1 \in \mathcal{C}^{inner}(P_1, P_2)$ where $\mathcal{C}^{inner}(P_1, P_2)$ is the equal SNR inner region in Section VI-B-2 for h_{12} chosen appropriately such that $SNR_1 = SNR_2$. The implication of this result is that adding the cross-link h_{12} does not lower the rate of User 1, but in fact usually increases the rate of User 1. The intuition is that adding the cross-link h_{12} gives the base station more information about User 1's secret message. Of course at the same time the wiretapper may now try to access User 1's secret message through the second channel, which in the Z-channel setup carried only User 2's jamming signal. However our equal SNR coding technique compensates for this, and usually out performs the Z-channel coding technique of [102] in terms of User 1's rate while still ensuring both channels are unconditionally secure.

E. Summary of Results

In this chapter we extended Chapter V to the Gaussian interference channel. Under this scenario, we showed many interesting and important properties. The "statistical similarity" property from Chapter V naturally translates to the equal SNR property. With a given power constraint, we found the set of admissible power schemes that ensures equal SNR. An important technical property we derived is the fact that the

inner region can be expressed as a single region (instead of an infinite union of regions as is the case in Chapter V), and that this region results from using the maximum power scheme from the set of admissible power schemes. When the power constraint lies in the admissible power set, the inner region and outer region partially coincide on the diagonal, which suggests that using Gaussian codebooks without pre-coding may be close to optimal. To further demonstrate that our inner region is significant, we showed the inner region of a related Z-channel problem is a subset of our inner region. Lastly, we derived a kind of "outage" probability under the slow and flat Rayleigh fading scenario, which shows that if we are willing to pay a price in power, then the channel has a non-zero probability of being favorable for unconditional secret communications under the equal SNR regime.

CHAPTER VII

SUMMARY, FUTURE WORK AND CONCLUSIONS

A. Summary

The core results in this dissertation establish the interaction between source coding and secrecy, and channel coding and secrecy. The main theoretical conclusion that this dissertation offers is that given our keyless, inter-node communicationless, and "secret sharing" eavesdropping model, noise/distortion alone is not enough to provide unconditional secrecy. Surprisingly, a necessity of unconditional secrecy is the existence of random interference and fading, which are usually seen as a hindrance to communications systems.

For the first part of our dissertation we analyze the interaction between source coding and secrecy using multiterminal source coding theorems [5]–[7]. We derive inner and outer regions for the set of all source coding and equivocation (measure of secrecy) rates (which we call the capacity region) for user-defined distortion criteria. We show that unconditional secrecy is only achievable if the distortion is maximal, which means no information is sent. We then show that feedback from the base station to the legitimate users does not improve equivocation. We do this by deriving an upper bound on the secret key rate that can be achieved *without* feedback, and comparing this to an upper bound on the secret key rate using feedback [8], [9].

In the second part of our research, we extend the existing distributed source coding using syndromes (DISCUS) Slepian-Wolf coding scheme. DISCUS is the practical implementation of the multitermianl source coding problem without distortion. We show that using equivocation as the measure of secrecy leaks too much information to the eavesdropper. This can be understood from our first result where unconditional

secrecy is unachievable and thus equivocation is not maximal. Thus this motivates the definition of a set of additional secrecy requirements. We show how these additional requirements can be implemented by modifying DISCUS. One of the main results is that the subcodes in DISCUS should be maximum distance separable, and furthermore we show how to partition a Reed-Solomon code to meet the subcode and supercode requirements of DISCUS.

In the third part of our research we study the interaction between channel coding and secrecy in the context of the general discrete memoryless interference channel. We derive inner and outer regions of the secrecy capacity region, which is the set of all channel coding rates such that unconditional secrecy is achieved. Surprisingly, the secrecy capacity region is not empty, thus in contrast with the first part of our research, interference permits unconditional secrecy. The proof utilizes the random coding technique of Wyner's wiretap channel [10] and its generalization [11].

In the final part of our research, we study the interference problem under wireless settings by assuming that the interference channel has additive white Gaussian noise, and later augmenting this model with the additional challenge of slow Rayleigh fading. Again we derive inner and outer regions of the secrecy capacity region for this special case. Significantly we show that the inner region can be simplified to such an extent that its description is merely a *single* region based on an optimal power allocation scheme without the need for pre-coding (as is the case with the DMIC). This is in contrast to various mutli-user information theory capacity regions, which are usually constructed viz. a convex hull of an infinite union of regions. Thus our simplified region not only contributes to information theorists' common goal of simplicity, but also allows future designers to work with a simpler region. Next, our extension of the interference channel to slow Rayleigh fading demonstrates that interference and random fading are not only friends rather than foes, but are in fact necessary enablers

of unconditional secrecy.

B. Future Work

The obvious need to implement solutions based on the theoretical foundations we have laid in this dissertation drives future work. We have provided a pioneering coding scheme (in Chapter IV) for the distributed source coding and secrecy problem based on DISCUS. We expect that as research in practical multiterminal source coding continues, newer codes that combine lossy compression and distributed secrecy will arise thus better serving multimedia communication needs.

Practical (Wyner) wiretap channel codes (excluding type II wiretap channel codes) for the channel coding and secrecy problem are still emerging. We expect that research in coding pertaining to variations of the wiretap channel will flourish once the solution for the original wiretap channel is solidified. Thus we expect that practical codes for our channel coding models of Chapters V and VI will be explored in the near future (since these models may be considered variations of the original wiretap channel).

C. General Conclusions

This dissertation explores the first information theoretic model of sensor network security/confidentiality. We identify some important differences between the nascent field of sensor networks and the classical computer and cellular networks that naturally require a shift to a keyless, inter-node communicationless, and "secret sharing" eavesdropping paradigm. A necessary first step of any bold paradigm shift is to discover the possible and impossible, the examination of which is central to this dissertation.

It is hoped that the solid foundations in this work will offer guidance for the design

of optimal or near-optimal solutions, the discovery of which would otherwise prove challenging if not impossible. More recent history has shown that when foundations in modern research are not first laid, the resulting solutions are ad hoc, and usually far from optimal. Of course there are exceptions to this observation, however more often than not, theoretical foundations drive optimal solutions. For example, modern coding schemes for communication systems are in part driven by the goal of reaching the Shannon limit in communications, and some even emulate the ideas of theoretical proofs: LDPC and turbo codes attempt to emulate the random coding idea, while DISCUS emulates the Slepian-Wolf binning idea. Thus it is hoped that information theorists and the practical sensor network community will both find this dissertation informative.

REFERENCES

[1] C.-Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, August 2003.

[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, June 2004.

[3] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. ACM/IEEE International Conference on Mobile Computing and Networking*, Seattle, WA, August 1999, pp. 263–270.

[4] I. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 921–60, March 2007.

[5] S.-Y. Tung, "Multiterminal source coding," Ph.D. dissertation, Cornell University, Ithaca, NY, 1978.

[6] K. B. Housewright, "Source coding studies for multiterminal systems," Ph.D. dissertation, University of California at Los Angeles, Los Angeles, CA, 1977.

[7] J. Barros and S. D. Servetto, "On the rate-distortion region for separate encoding of correlated sources," in *IEEE International Symposium on Information Theory*, Yokohama, Japan, June 29 - July 4 2003, pp. 171–176.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Trans. on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[10] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[11] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[12] W. Luh, D. Kundur, and T. Zourntos, "A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems," *EURASIP Journal on Applied Signal Processing*, pp. 218 – 234, January 2007.

[13] W. Luh and D. Kundur, "Distributed privacy for visual sensor networks via Markov shares," in *IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Columbia, MD, April 2006, pp. 11–20.

[14] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. on Information Theory*, vol. 29, no. 1, pp. 35–41, January 1983.

[15] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[16] U. M. Maurer, "The role of information theory in cryptography," in *Fourth IMA Conference on Cryptography and Coding*, Cirencester, UK, December 13–15 1993, pp. 49–71.

[17] A. B. Carleial and M. E. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. on Information Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[18] S. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Trans. on Information Theory*, vol. 23, no. 5, pp. 625–627, September 1977.

[19] J. L. Massey, "A simplified treatment of Wyner's wire-tap channel," in *Proc. 21st Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 5–7 1983, pp. 268–276.

[20] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 43, no. 2, pp. 712–714, March 1997.

[21] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[22] W. Stallings, *Network Security Essentials: Applications and Standards*. Upper Saddle River, NJ: Prentice-Hall, Inc., 1999.

[23] O. Goldreich, *Foundations of Cryptography: Basic Tools*. New York: Cambridge University Press, 2001, vol. I.

[24] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*. Upper Saddle River, NJ: Prentice-Hall, Inc., 2002.

[25] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL: CRC Press, 2005.

[26] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications (Special Issue on Security in Wireless Ad Hoc Networks)*, vol. 24, no. 2, pp. 247–260, February 2006.

[27] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairnes, Australia, September 2001, pp. 87–89.

[28] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. on Information Theory*, 2006, submitted.

[29] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. on Information Theory*, 2007, submitted.

[30] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," in *Proc. of IEEE Information Theory Workshop*, Lake Tahoe, CA, September 2 – 6 2007, pp. 595 – 600.

[31] I. Deslauriers, "Distributed encryption and the Slepian-Wolf theorem," in *Canadian Conference on Electrical and Computer Engineering*, Saskatoon, Sask., Canada, May 2005, pp. 93–97.

[32] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006, pp. 957 – 961.

[33] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 54, no. 3, pp. 976–1002, March 2008.

[34] ——, "Secrecy capacity region of binary and Gaussian multiple access channels," in *Proc. Allerton Conference on Communication, Control, and Computing*, Urbana, IL, Sept. 26–29 2006, pp. 1098–1106.

[35] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton*

Conference on Communication, Control, and Computing, Urbana, IL, Sept. 26–29 2006, pp. 305–313.

[36] ——, "Multi-terminal communications with confidential messages," in *Proc. Workshop on Information Theory and Applications*, La Jolla, CA, Jan. 29 – Feb. 2 2007, pp. 370 – 377.

[37] ——, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2493 – 2507, June 2008.

[38] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Asilomar Conf. on Signals, Systems and Computers*, Pacific Grove, CA, October 28 – November 1 2005, pp. 1747–1751.

[39] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *IEEE International Symposium on Information Theory*, Seattle, WA, July 9–14 2006, pp. 1164 – 1168.

[40] ——, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Information Theory and Applications Workshop*, San Deigo, CA, February 2007, pp. 404 – 413.

[41] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. of IEEE Information Theory Workshop*, Porto, Portugal, May 5–9 2008, pp. 405–409.

[42] ——, "The Gaussian wiretap channel with a helping interferer," in *Proc. of IEEE International Symposium on Information Theory*, Toronto, Ontario, Canada, July 6–11 2008, p. to appear.

[43] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. on Information Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[44] Y. Liang, H. V. Poor, and S. S. (Shitz), "Secrecy capacity region of parallel broadcast channels," in *Information Theory and Applications Workshop*, San Diego, CA, February 2007, pp. 245 – 250.

[45] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Internationl Symposium on Information Theory*, Seattle, WA, July 2006, pp. 356–360.

[46] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. Allerton Conference on Communication, Control, and Computing*, Urbana, IL, Sept. 26–29 2006, pp. 831–840.

[47] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Information Theory*, 2006, submitted.

[48] Y. Liang, H. V. Poor, and S. S. (Shitz), "Secure communication over fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2470 – 2492, June 2008.

[49] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2453 – 2469, June 2008.

[50] Y. Liang, H. V. Poor, and S. S. (Shitz), "Secrecy capacity region of fading broadcast channels," in *IEEE International Symposium on Information Theory*, Nice, France, June 24–29 2007, pp. 1010–1014.

[51] A. O. Hero, "Secure space-time communication," *IEEE Trans. on Information Theory*, vol. 49, no. 12, pp. 3235–3249, December 2003.

[52] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 4–9 2005, pp. 2152–2155.

[53] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 3, Dallas, TX, September 25–28 2005, pp. 1906–1910.

[54] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *IEEE Military Communications Conference*, vol. 3, Atlantic City, NJ, October 17–20 2005, pp. 1501–1506.

[55] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Information Sciences and Systems*, Baltimore, MD, March 14–16 2007, pp. 905–910.

[56] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1130–1134.

[57] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. on Information Theory*, 2007, submitted.

[58] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. on Information Theory*, 2007, submitted.

[59] A. Khisti and G. Wornell, "The MIMOME channel," in *Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, September 2007, pp. 625–632.

[60] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. on Information Theory*, 2007, submitted.

[61] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," California Institute of Technology, Pasadena, CA, Tech. Rep., October 2007. [Online]. Available: arxiv.org/abs/0710.1920

[62] T. Liu and S. S. (Shitz), "A channel-enhancement approach to the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. on Information Theory*, 2007, submitted.

[63] R. Liu and H. V. Poor, "Multiple antenna secure broadcast over wireless networks," in *Proc. of the International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 18–20 2007, pp. 203–216.

[64] ——, "Multi-antenna Gaussian broadcast channels with confidential messages," in *Proc. of the IEEE International Symposium on Information Theory*, Toronto, Ontario, Canada, July 6–11 2008, p. to appear.

[65] S. K. Leung-Yan-Cheong, "Multi-user and wire-tap channels including feedback," Ph.D. dissertation, Stanford University, Stanford, CA, 1976.

[66] R. M. Kahn, "Privacy in multi-user information theory," Ph.D. dissertation, Stanford University, Stanford, CA, 1979.

[67] E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *IEEE International Symposium on Information Theory*, Nice, France, June 24–29 2007, pp. 1150–1154.

[68] L. Lai, H. E. Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. on Information Theory*, 2007, submitted.

[69] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. of IEEE Information Theory Workshop*, Lake Tahoe, CA, September 2 –6 2007, pp. 608 – 613.

[70] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. on Information Theory*, vol. 32, no. 3, pp. 387–393, May 1986.

[71] ——, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. on Information Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[72] ——, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. on Information Theory*, vol. 37, no. 3, pp. 634 – 638, May 1991.

[73] D. Stinson and R. Wei, "Bibliography on secret sharing schemes," 1998, http://www.cacr.math.uwaterloo.ca/~dstinson/ssbib.html.

[74] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT & T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[75] C. Mitrpant, Y. Luo, and A. J. H. Vinck, "On the wire-tap channel of type II with side information," in *IEEE International Symposium on Information Theory (ISIT)*, Yokohama, Japan, June 29 - July 4 2003, pp. 307–307.

[76] Y. Luo, C. Mitrpant, and A. J. H. Vinck, "Some new characters on the wire-tap channel of type II," *IEEE Trans. on Information Theory*, vol. 51, no. 3, pp. 1222–1229, March 2005.

[77] V. K. Wei, "Generalized hamming weights for linear codes," *IEEE Trans. on Information Theory*, vol. 37, no. 5, pp. 1412–1418, Septmeber 1991.

[78] C. H. Bennett, G. Brassard, and J.-M. Roberts, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, April 1988.

[79] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography: Two Sides of One Tapestry*, R. E. B. et al., Ed. Norwell, MA: Kluwer, 1994, ch. 26, pp. 271–285.

[80] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. on Information Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[81] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *EUROCRYPT*, Bruges, Belgium, May 14–18 2000, pp. 351–368.

[82] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2515 – 2534, June 2008.

[83] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. of IEEE Information Theory Workshop*, Lake Tahoe, CA, September 2–6 2007, pp. 442 – 447.

[84] W. Luh and D. Kundur, "Distributed keyless security for correlated data with applications in visual sensor networks," in *ACM Multimedia and Security Workshop*, Dallas, TX, September 20–21 2007, pp. 75–86.

[85] 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, November 1983.

[86] ——, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. on Information Theory*, vol. 34, no. 4, pp. 835–842, July 1988.

[87] ——, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[88] D. Gunduz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proceedings of the 2008 IEEE Information Theory Workshop*, Porto, Portugal, May 5–9 2008, pp. 410–414.

[89] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[90] E. Verriest and M. E. Hellman, "Convolutional encoding for Wyner's wiretap channel," *IEEE Trans. on Information Theory*, vol. 25, no. 2, pp. 234–236, March 1979.

[91] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proc. IEEE International Symposium on Information Theory*, Adelaide, Australia, Septebmer 2005, pp. 2133 – 2137.

[92] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Information Theory Workshop on Frontiers in Coding Theory*, Lake Tahoe, CA, September 2–6 2007, pp. 337 – 342.

[93] V. Stanković, A. Liveris, Z. Xiong, and C. Georghiades, "Design of slepian-wolf codes by channel code partitioning," in *Proc. Data Compression Conference*, Snowbird, UT, March 2004, pp. 302–311.

[94] B. Furht, D. Socek, and A. M. Eskicioglu, *Multimedia Security Handbook*. Boca Raton, FL: CRC Press, 2005, ch. 3, pp. 95–132.

[95] S. Pradhan and K. Ramchandran, "Distributed source coding: Symmetric rates and applications to sensor networks," in *Proc. DCC'00*, Snowbird, UT, March 2000, pp. 363–372.

[96] W. Luh and D. Kundur, "Separate enciphering of correlated messages for confidentiality in distributed networks," in *IEEE Globecom*, Washington, DC, November 25–30 2007, pp. 1637 – 1641.

[97] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Birmingham, AL: Akademiai Kiado, 1997.

[98] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Workshop on Network Coding, Theory, and Applications (NETCOD)*, Riva Del Garda, Italy, April 2005, pp. 63–68.

[99] T. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources," *IEEE Trans. on Information Theory*, vol. 21, pp. 226–228, March 1975.

[100] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY: John Wiley & Sons, Inc., 2006.

[101] E. R. Dougherty, *Random Processes for Image and Signal Processing.* New York, NY: SPIE Optical Engeering Press, 1999.

[102] O. Simeone and P. Popovski, "Secure communications via cooperative base stations," *IEEE Communications Letters*, vol. 12, no. 3, pp. 188–190, March 2008.

APPENDIX A

PROOF OF LEMMA 7

Codebook generation

Randomly generate two tables. The first table will have $2^{n(\bar{R}_1-\epsilon)}$ vectors (codewords) whose components are randomly drawn from the normal distribution $\mathcal{N}(0, P_1^{\max}-\epsilon)$. Similarly, the second table will have $2^{n(\bar{R}_2-\epsilon)}$ vectors whose components are randomly drawn from the normal distribution $\mathcal{N}(0, P_2^{\max}-\epsilon)$. The first table has 2^{nR_1} rows and $2^{n(U_1-\epsilon')}$ columns, while the second table has 2^{nR_2} and $2^{n(U_2-\epsilon')}$ columns. The rates $\bar{R}_1, \bar{R}_2, U_1, U_2$ are chosen to satisfy Eqs. 6.39 to 6.44.

Encoding

If User 1 wishes to send index $i \in \{1, \ldots, 2^{nR_1}\}$, randomly (uniformly) select a codeword from row i of the first table; call this X_1^n. If User 2 wishes to send index $j \in \{1, \ldots, 2^{nR_2}\}$, randomly (uniformly) select a codeword from row j of the second table; call this X_2^n.

Decoding

Notice that the overall channel as seen by the base station is a MAC with independent inputs X_1^n and X_2^n, and output (Y_1^n, Y_2^n). It is known that the average probability of error tends to 0 as $n \to \infty$ if

$$\bar{R}_1 < I(X_1; Y_1, Y_2|X_2)$$

$$\bar{R}_2 < I(X_2; Y_1, Y_2|X_1)$$

$$\bar{R}_1 + \bar{R}_2 < I(X_1, X_2; Y_1, Y_2)$$

for some codebook generated randomly as above, which is precisely Eqs. 6.42 to 6.44 for the Gaussian MAC. Thus by the Gaussian MAC theorem, X_1^n and X_2^n are decodable by the base station given (Y_1^n, Y_2^n). In addition (X_1^n, X_2^n) are unique in the two tables resp. and thus the base station can uniquely identify the rows $(\hat{i}, \hat{j})$.

Secrecy Analysis

To show the above construction achieves unconditional secrecy, we write

$$\begin{aligned}
H(W_1, W_2|Y_i^n) &= H(W_1, W_2) - I(W_1, W_2; Y_i^n) \\
&= H(W_1, W_2) - H(Y_i^n) + H(Y_i^n|W_1, W_2) \\
&\overset{(a)}{=} H(W_1, W_2) - H(Y_i^n) + H(Y_i^n|X_1^n, X_2^n) \\
&\quad + H(Y_i^n|W_1, W_2) - H(Y_i^n|X_1^n, X_2^n, W_1, W_2) \\
&= H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) \\
&\quad + I(Y_i^n; X_1^n, X_2^n|W_1, W_2) \\
&= H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) \\
&\quad + H(X_1^n, X_2^n|W_1, W_2) - H(X_1^n, X_2^n|Y_i^n, W_1, W_2) \\
&\overset{(b)}{=} H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) + H(X_1^n|W_1) \\
&\quad + H(X_2^n|W_2) - H(X_1^n, X_2^n|Y_i^n, W_1, W_2) \\
&\overset{(c)}{=} H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) + n(U_1 - \epsilon') \\
&\quad + n(U_2 - \epsilon') - H(X_1^n, X_2^n|Y_i^n, W_1, W_2) \\
&\overset{(d)}{=} H(W_1, W_2) - 2n\epsilon'' - H(X_1^n, X_2^n|Y_i^n, W_1, W_2). \qquad \text{(A.1)}
\end{aligned}$$

The explanations are: (a) $(W_1, W_2) \leftrightarrow (X_1^n, X_2^n) \leftrightarrow Y_i^n$ forms a Markov chain; (b) from the factorization of the encoding distribution (cf. Definition 4); (c) from the codebook generation and encoding; (d) from Eq. 6.41. Finally note that the eaves-

dropper also sees a MAC, either $(X_1^n, X_2^n) \to Y_1^n$ if he intercepts Y_1^n or $(X_1^n, X_2^n) \to Y_2^n$ if he intercepts Y_2^n. When the eavesdropper is given the rows W_1, W_2 of the two tables, the eavesdropper is looking at a MAC code with $2^{n(U_1-\epsilon')}$, $2^{n(U_2-\epsilon')}$ codewords, which satisfy the MAC theorem (cf. Eqs. 6.39 to 6.41), and thus he is able to decode X_1^n, X_2^n by the MAC theorem whether he wishes to or not! Thus the last term in Eq. A.1 is bounded by Fano's inequality resulting in

$$H(W_1, W_2|Y_i^n) \geq H(W_1, W_2) - n\epsilon. \tag{A.2}$$

To complete the secrecy proof for each individual message, we write

$$\begin{aligned} H(W_1) + H(W_2|Y_i^n) &\geq H(W_1|Y_i^n) + H(W_2|W_1, Y_i^n) \\ &= H(W_1, W_2|Y_i^n) \\ &\geq H(W_1, W_2) - n\epsilon \\ &= H(W_1) + H(W_2) - n\epsilon \end{aligned} \tag{A.3}$$

where the last equality follows since W_1, W_2 are independent. This proves

$$H(W_2|Y_i^n) \geq H(W_2) - n\epsilon \tag{A.4}$$

and the secrecy for the other message can be proved in the same way.

Notice that in Eq. A.1(d), we used the equal SNR assumption of Eqs. 6.36 and 6.41 to ensure unconditional secrecy is achieved whether the eavesdropper intercepts Y_1^n or Y_2^n.

APPENDIX B

ENUMERATION OF $\bar{\mathcal{R}}, \mathcal{U}$ REGIONS

Recall in the proof of Corollary 2 the subtraction of points in the $\bar{\mathcal{R}}$ and $\mathcal{U}$ regions yield points in the inner region when the difference is positive. The $\mathcal{U}$ region is the (thicker) red diagonal lines in each of the plots in Fig. 18. The $\bar{\mathcal{R}}$ region consists of all points enclosed and including the blue lines in Fig. 18. Without loss of generality we have only plotted the interactions between these two regions along the vertical axes. Thus the maximum veritical distance between a blue line and the thick red line yields the maximum rate (either $R_1^{(1)*}$ or $R_2^{(2)*}$). The reader can verify that this maximum vertical distance only takes on two forms, A and B as given by Eqs. 6.48 and 6.49. It is perhaps easiest to see this by first perusing the example in Section VI-C-1.

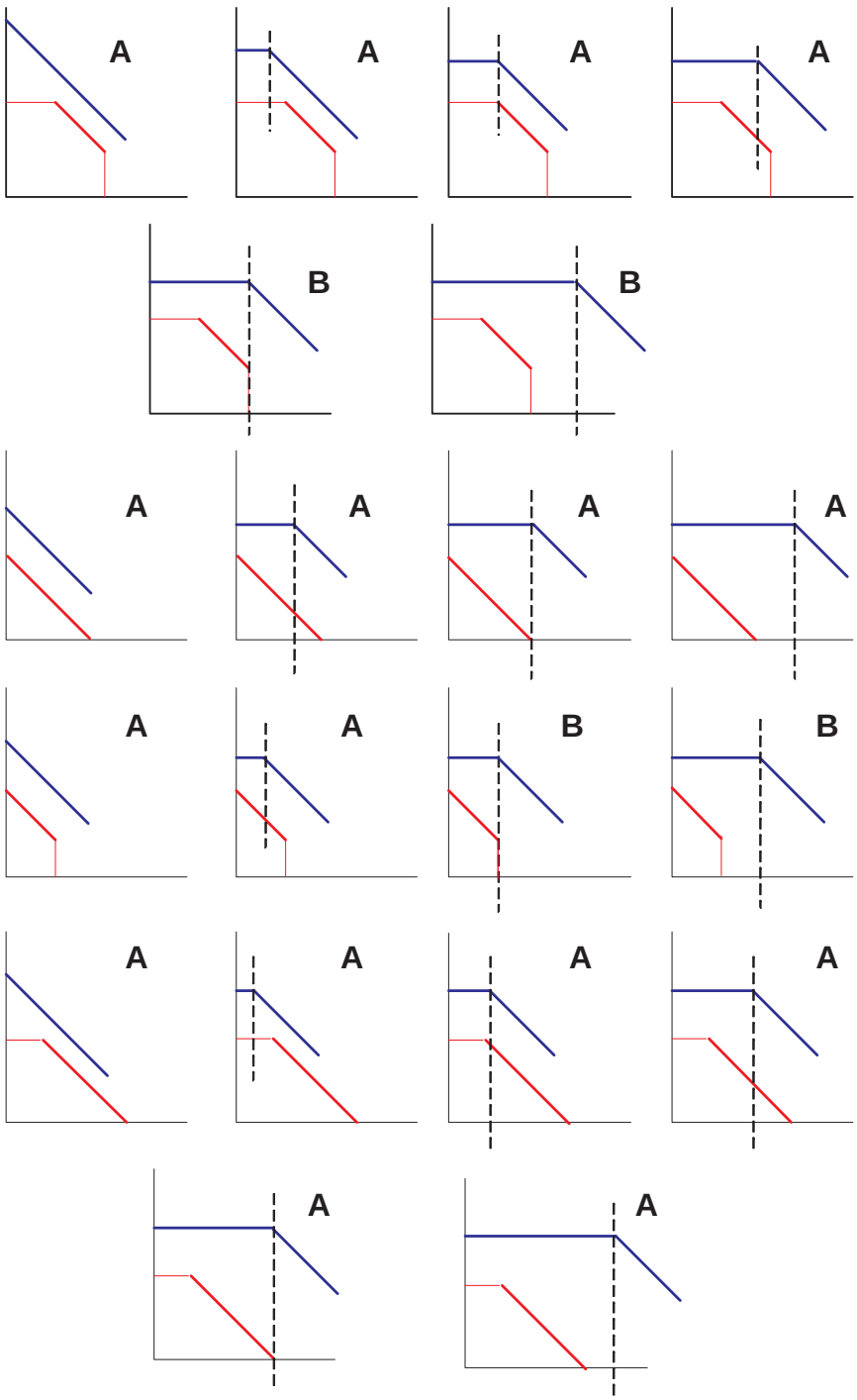

Fig. 18. $\bar{\mathcal{R}}, \mathcal{U}$ Region Interactions for Vertical Axes

VITA

William Luh received his B.A.Sc. with Honours in computer engineering from the University of Toronto in 2002, and his M.S. in electrical engineering from Texas A&M University in 2004. Since 2003 he has been a research assistant, and also delivered weekly recitations for ECEN 314 Systems and Signals. His research interests include multimedia security, such as digital watermarking and fingerpring, and recently information-theoretic secrecy. He can be reached at 4538 Mayflower Drive, Mississauga, Ontario, L5R 1S3, Canada. E-mail: william.luh@utoronto.ca.

The typist for this dissertation was William Luh.