Network Coding, Wireless Physical-layer Secret-key Generation (WPSG), and Their Relationships: From Unequal Erasure Protection (UEP) to Unequal Security Protection (USP)

by

Apirath Limmanee

PhD Thesis

Under the supervision of

Prof. Dr.-Ing. Werner Henkel

September 2011

submitted as a PhD thesis to

School of Engineering and Science

Abstract

The theme of this thesis is the relationships between two seemingly unrelated topics, which are network coding and wireless physical-layer secret-key generation (WPSG). As build-ups to such relationships, some specific aspects of each topic are discussed in detail at first. First of all, network coding issues of unequal erasure protection (UEP) and degree distribution distortion of LT-coded symbols are presented. After that, the analysis regarding key length and security enhancement in WPSG is given. Towards the end, relationships between network coding and WPSG are revealed in two aspects, which are security protocols using network coding and scalable security based on the weakly secure network coding concept.

Declaration of originality

I hereby declare that the research recorded in this proposal was composed and originated entirely by myself in cooperation with my advisor in the School of Engineering and Science, International University bremen, Germany.

Apirath Limmanee

Contents

List of Figures

Part I

Motivation, Overview, and Introduction

Chapter 1

Motivation and Overview

This thesis consists of a series of topics which are divided into three parts. The author decides to do so with the aim that each part will be self-contained, i.e., the reader may choose to read or skip one part without any serious damage. For example, those who have sound knowledge in communication systems and networks as well as network coding may skip Part I, those who are interested solely in network coding may read only Part II, and those who only wish to know the relationship between network coding and WPSG may read only the last part.

This first part is the introductory part consisting of three chapters. Chapter 2 discusses the basic knowledge of digital communication systems and networks. Chapter 3 discusses some aspects of graph theory related to network coding, as well as network coding itself, which is the major focus of this thesis, and rateless codes.

At the beginning of the millennium, Ahlswede et al. made a breakthrough in information theory by inventing network coding, which significantly increased network throughput by means of coding. The idea related information theory to graph theory, providing a means to reach the graph-theoretic max-flow limit in data networks. It states that when many sources transmit different data to many sinks, or when one source transmits the same data to many sinks (multicast), the maximum amount of data flow (max-flow) cannot be achieved by means of routing alone. Network coding is needed to achieve the max-flow.

Many developments follow. In 2003, Li et al. showed that a simple class of network coding, called linear network coding, sufficed to achieve the maximum flow. In the same year, Koetter and Médard proposed a greedy algorithm to find linear network coding solutions to the multicast problem. However, Koetter and Médard's algorithm is based on the idealized assumption that the given network has no delay, loses no packet, and has centralized knowledge of its topology, which is not the case in practice. Later, some more practical algorithms are proposed.

In 2003, Chou, Wu, and Jain simulated a distributed network coding scheme using the network topologies of several internet service providers, which resulted in almost optimal throughput. Moreover, several pioneering works from 2004 to 2007 [65–70] introduced network coding to wireless communications. Even cryptography became one of network coding applications with the introduction of secure network coding in 2002 [42, 60] as well as a subsequent work in [43].

The author, however, has maintained critical stance on network coding. While network coding brings several research opportunities to the field of digital communication, several issues must be dealt with as one looks closely. The author focuses on the issue of erasures in the network, which will be examined in Part II, consisting of Chapter 4 and 5. The author does not merely raise the issue, but also suggests the solutions.

Chapter 4 discusses unequal erasure protection (UEP) of network codes, suggesting that a network code assignment has a strong impact on the quality of the received scalable data for each receiver. Therefore, an assigment scheme based on the concept of equity among sink nodes is proposed, as well as a capitalist concept used to assign network codes by means of auction such that richer nodes get better data quality. After that, Chapter 5 investigates the problem of degree distribution distortion of LT-coded symbols when network coding is used and suggests a solution.

In Part III, the author turns his attention to a cryptographic technique called wireless physical-layer secret-key generation (WPSG). In Chapter 6, he investigates the extension of the technique from a direct communication to a relay one as well as a wireless network in general. In the latter case, the security of the technique relies on the network protocol used for transmitting pilot symbols. It is shown that network coding can enhance the protocol security.

In Chapter 7, it is shown that the security of this technique can be enhanced by means of key encoding, using the same concept of secret sharing as that in secure network coding. In addition, the concept of scalable security or unequal security protection (USP) is formally introduced and analyzed in the context of both secure network coding and WPSG.

Finally, Chapter 8 gives the conclusion and discusses future research topics.

Chapter 2

Introduction to Digital Communication Systems and Networks

Although the object of our investigation is communication networks in general, we would like, at first, to introduce the elements of point-to-point digital communication in Section 2.1, as well as the mathematical models of communication channels in 2.2. After that,

2.1 Basic Elements of A Secure Digital Communication System

In this section, we discuss those basic elements which constitutes a digital communication system. When talking about any communication system in general, three basic elements must certainly be there. They are the transmitter, the channel, and the receiver. However, when discussing a digital communication system in particular, we need to be specific about what constitutes the transmitter and the receiver. According to Proakis, a basic digital communication system can be shown in a block diagram in Fig. 1.1. [10]

To make the system secure, however, we need to insert two more blocks, which are

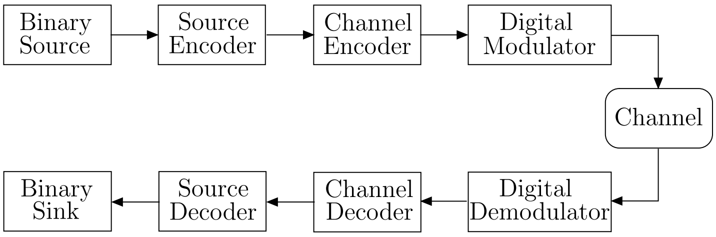

Figure 2.1: A basic digital communication system

encryptor and decryptor, as shown in Fig. 1.2.

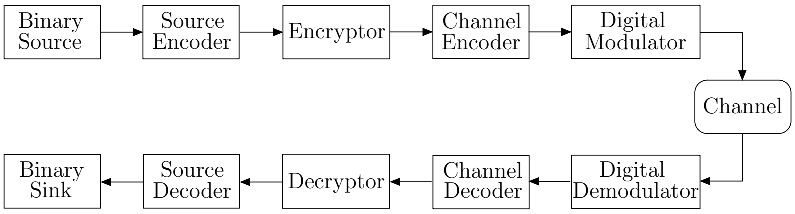

Figure 2.2: A secure digital communication system

A digital transmitter consists of four basic elements, which are a binary source, a source encoder, a channel encoder, and a digital modulator, whereas a digital receiver is composed of a digital demodulator, a channel decoder, a source decoder, and a binary sink.

A binary source in the transmitter generates information to be transmitted, be it audio, speech, or video data, in a binary representation. Usually, this representation is not the most economical one possible, i.e., it is possible to squeeze it into a shorter string of 0s and 1s without reducing the amount of information, or reducing only some insignificant amount of it. The source encoder is made for this task. It transform the data into another binary representation with less redundancy. These two blocks, however, are not the focus of this thesis.

Our concern in the thesis ranges from the third block, the encryptor, to the ninth block, the decryptor. Although the encryptor in Fig. 1.2 locates right after the source encoder, it is not necessarily the case when we consider some new cryptographic technologies, for example, physical-layer security and physical-layer secret-key generation, which will be discussed in detail in part III.

An encryptor provides security to the transmitted data. In cryptology, there are two types of security, which are theoretical security and practical security. They are based on different philosophies. Theoretical security, on the one hand, is based on theoretical impossibility of ciphers being broken, necessitating the mutual knowledge of the secret key between the transmitter and the receiver. Practical security, on the other hand, is based on practical difficulty of ciphers being broken, i.e., it takes too much time and labor to break them. The questions regarding how these two types of security are implemented will be dealt with in part III.

A channel encoder introduces some redundancy to the input data so that the output is immuned against deteriorating effects, such as errors and erasures, from the channel. There are numerous channel codes and several ways to classify them. They can be divided into block codes and convolutional codes, fixed-rate and rateless codes, or linear and non-linear codes. The datails will be explained in 2.3.

The purpose of a digital modulator is to map the binary representation after channel encoding into electromagnetic waves that can be transmitted along the channel. The simplest digital modulation is called binary modulation, which maps the binary digit 0 into a waveform $s_o(t)$ and the binary digit 1 into $s_1(t)$. This means each bit is transmitted in a separated waveform. In M-ary modulation ($M > 2$), however, $M = 2^b$ waveforms $s_i(t), i = 0, 1, ..., M - 1$ are used to represented b bits.

The communication channel is the physical medium used for transmission, e.g., the free space is the channel of wireless communication. In the design and analysis of digital communication systems, communication channels are represented by channel models, which are mathematical abstractions of these physical entities. We will discuss some channel models in the next section.

A digital demodulator, a channel decoder, a decryptor, and a source decoder perform reversed operations of a digital modulator, a channel encoder, an encryptor, and a source encoder, respectively. Their overall purpose is to give the binary sink the data which is as close as possible to that generated by the binary source. Two of them, which are the channel decoder and the decryptor, are relevant to this thesis. A special case of the former, the decoder of rateless codes, will be discussed in Section 2.4. The latter will be mentioned in Part III.

2.2 Channel Models

Since channel models are mathematical abstractions of physical channels, they can be divided into several categories based on two factors, which are the nature of physical channels and the levels of abstraction used. We will discuss four frequently used channel models which suit the purpose of this thesis.

2.2.1 Binary Erasure Channel (BEC)

Despite being proposed in 1955 by Elias, binary erasure channels are only widely employed after the emergence of the Internet. The model offers no possibility of transmission errors. It assumes that the data is either received correctly or not received at all. This assumption can only hold on network level of abstraction, where errors are assumed to be corrected by the data link layer. In reality, erasures may be caused by buffer overflows at intermediate routers, mismatching of packets' internal check-sum, or packets losing their ways.

The model can be illustrated by Fig. 2.3, in which X is the transmitted symbol and Y is the received one. If the erasure probability is p_e, the capacity C of the channel is given by

$$C = 1 - p_e. \tag{2.1}$$

2.2.2 Binary Symmetric Channel (BSC)

This model only allows transmitted symbols to be erred, but not erased. However, the physical reasons behind the transmission error are not included in the model. Therefore, this model is suitable for the data link level of abstraction. It can be illustrated by Fig. 2.4, in which X is the transmitted symbol and Y is the received one. If the error probability is p_s, the capacity C of the channel is given by

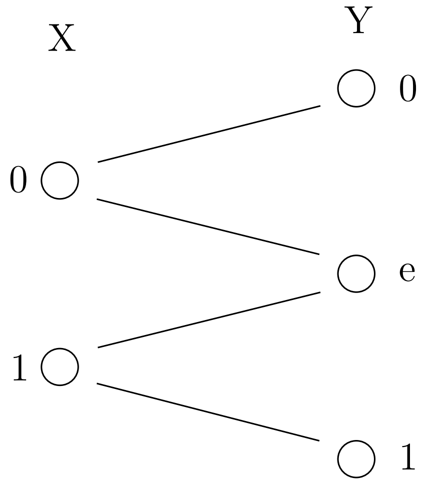

Figure 2.3: Binary Erasure Channel

$$C = 1 - H(p_s), \tag{2.2}$$

where

$$H(p_s) = p_s \log_2 \frac{1}{p_s} + (1 - p_s) \log_2 \frac{1}{1 - p_s}, \tag{2.3}$$

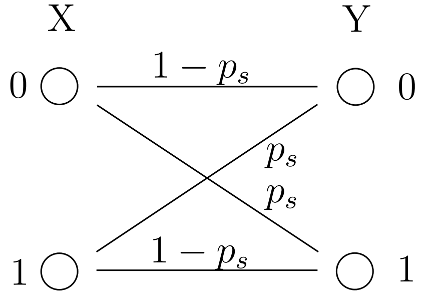

Figure 2.4: Binary Symmetric Channel

2.2.3 Additive White Gaussian Noise (AWGN) Channel

This channel model, belonging to the physical level of abstraction, explains the transmitted signal distortion as the addition effect of some noise $n(t)$, as follows.

$$r(t) = s(t) + n(t), \tag{2.4}$$

where $r(t)$ is the received signal at time t, $s(t)$ is the transmitted signal, and $n(t)$ is the noise which obeys the following Gaussian distribution.

$$p_n(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp -(x - m_x)^2/2\sigma^2, \tag{2.5}$$

where m_x is the mean of the distribution, which is zero in this case, and σ^2 is the noise variance.

The assumption of Gaussian distribution is supported by natural phenomenon of thermal agitation of the charge carriers inside an electrical conductor, of which amplitude is almost Gaussian distributed, and of which frequency spectrum is almost white, thus the name additive white gaussian noise (AWGN).

2.2.4 Rayleigh Fading Channel

The Rayleigh fading channel model is a physical abstraction of wireless channels, where signal rays from the transmitter is scattered by obstacles in the environment, forming a number of transmission paths to the receiver, who receives the summation of signal from these paths. Therefore, the received band-pass signal may be expressed as follows.

$$r(t) = \sum_n \alpha_n(t) s[t - \tau_n(t)], \tag{2.6}$$

where $\alpha_n(t)$ is the attenuation factor for the signal received on the n^{th} path and $\tau_n(t)$ is the propagation delay of the n^{th} path. Now, if the transmitted signal $s(t)$ is expressed as

$$s(t) = \Re[s_l(t) e^{j2\pi f_c t}], \tag{2.7}$$

where $s_l(t)$ is the low-pass transmitted signal in base-band and f_c is the carrier frequency, the received low-pass signal in base-band can be written as

$$r_l(t) = \sum_n \alpha_n(t) e^{-j2\pi f_c \tau_n(t)} s_l[t - \tau_n(t)]. \tag{2.8}$$

According to (2.8), the equivalent low-pass channel in base-band can be described by the following time-variant channel impulse response

$$c(\tau;t) = \sum_n \alpha_n(t) e^{-j2\pi f_c \tau_n(t)} \delta[t - \tau_n(t)]. \tag{2.9}$$

When the number of paths is large enough, the central limit theorem holds that the channel impulse response behaves according to a zero-mean, complex-valued, Gaussian distribution. If we denote the random variables of the real part, the imaginary part, and the envelope of the impulse response by C_R, C_I, and C_E, respectively, it follows that

$$C_E = \sqrt{C_R^2 + C_I^2}. \tag{2.10}$$

If C_R and C_I are independent Gaussian-distributed random variables with variance σ^2, the probability density function of C_E can be expressed as

$$p_{C_E}(r) = \frac{r}{\sigma^2} \exp -r^2/2\sigma^2. \tag{2.11}$$

This distribution is called Rayleigh, giving rise to the name Rayleigh fading channel. Note that when there are fixed scatterers or lines of sight in the channel, the zero-mean assumption does not hold and the distribution is therefore not Rayleigh-distributed but Ricean distributed. We, however, will not discuss Ricean distribution in detail.

2.3 Elements in Communication Networks: Routers and Relays

In more complicated networks such as the Internet, there are more channels and other elements involved in transmission. These elements are situated between the transmitter and the receiver and are usually called intermediate nodes. Traditionally, there are three important functions that these nodes may choose to perform to help packets reach the destination. These are store-and-forward, amplify-and-forward, and decode-and-forward.

After the emergence of network coding, the last two functions can be modified into amplify-and-forward with network coding and decode-and-forward with network coding, respectively.

No matter how sophisticated the signal processing techniques are at the intermediate nodes before packets are forwarded, the most important thing is that packets must be forwarded in the right direction. Otherwise, they will not reach the destination or might take a decade to reach it. Therefore, before discussing amplify-and-forward and three other methods, we will start from the most basic operation, store-and-forward, which is usually called routing. The nodes performing this function are called routers.

2.3.1 Routing Protocols and Algorithms

A routing protocol specifies rules for communications among routers. A routing algorithm is a part of the protocol that deals with route selection. Let us consider the Internet as an example. The Internet can be seen as a collection of sub-networks, each of which having its own specific protocol, connecting together. Since each sub-network is independent of all others, it is often called an autonomous system (AS). A routing algorithm within an AS is called an interior gateway protocol, whereas a routing algorithm used for routing between ASes is called an exterior gateway protocol.

The assembly of sub-networks in the Internet is made possible by a mutually agreed protocol, which is called the Internet Protocol (IP). As a network-layer protocol, IP provides best-effort (not guaranteed) services to the transport layer, i.e., transporting datagrams from source to destination, regardless of whether they are in the same network or not. At present, IP version 4 (IPv4) is the dominant protocol, but IP version 6 (IPv6) is also emerging.

Since the Internet is too big a scope to deal with in this thesis, we will now turn our attention to routing inside a network, not between networks. There are two types of routing algorithms, which are static algorithms and dynamic ones. Static algorithms, as the name implies, do not base their routing decisions on measurements or estimates of the current traffic and topology. One example of such algorithms is Dijkstra's shortest-path routing, which routes packets along the shortest path between the transmitter and receiver. Another example is flooding, in which every incoming packet is sent out to every line except the one via which it is received.

Despite the simplicity of static algorithms, modern computer networks generally use dynamic algorithms which can adapt the routing decisions to current network topology and load. Two of the most popular dynamic algorithms are distance vector routing and link state routing.

In distance vector routing, each router maintains a routing table containing one entry for each of the other routers. The entry contains two parts, the preferred outgoing line used for sending data to the router of that entry and the time or distance needed. The metric used to select the outgoing line may take number of hops, time delay, or number of packets queued along the path into account. Then, each router periodically transmits the time or distance needed to reach other routers to its neighbors, who update their tables accordingly.

The pitfalls of distance vector routing are that it does not take line bandwidth into account and takes a long time to converge. Therefore, it is used in the ARPANET only until 1979 before being replaced by link state routing. Unlike distance vector routing, in which each router informs only its neighbors about the cost or delay to all other routers, in link state routing, each router informs all others only about the delay or cost to its neighbors. Then, every router can compute the path that minimizes the cost.

Now, we would like to specifically introduce routing algorithms whose functions fit the purpose of this thesis, broadcast and multicast routing in wireline networks, as well as routing in mobile ad hoc networks (MANETs). The former relates primarily to network coding in part II, whereas the latter concerns physical-layer secret-key generation in part III.

2.3.2 Broadcast and Multicast Routing in Wireline Networks

Broadcast Routing in Wireline Networks

There are four major algorithms used for broadcasting a packet to all routers.

1. Flooding

Flooding means that every incoming packet is sent out to every outgoing line except the one on which it arrives. This generates vast numbers of duplicate packets. Three measures can be taken to reduce such numbers. One of them is to keep a hop counter in the packet header such that the packet is discarded when the number of hops reaches the tolerable maximum. Another technique is to make sure that the same packet is not transmitted twice by the same router. The last one is called selective flooding, meaning that routers only send the packets only along the lines going approximately to the right direction.

2. Multidestination Routing

3. Spanning Tree

4. Reverse Path Forwarding

2.3.3 Routing in Ad Hoc Networks

The discussion regarding routing in mobile ad-hoc networks (MANETs) in this section is related to wireless physical-layer secret-key generation in part III. By mobile ad-hoc networks (MANETs) we mean the networks in which routers are mobile, resulting in inconsistent topologies to which routing protocols must adapt.

2.3.4 Relaying in Wireless Networks: Amplify-and-forward and Decode-and-forward

If the intermediate elements do not merely store the received signal and forward it to the right direction, but also amplify it or decode and re-encode it before forwarding, they are usually called relays instead of routers.

2.3.5 Amplify-and-forward and Decode-and-forward with Network Coding

Chapter 3

Introduction to Graphs and Network Coding

Since network coding relates graph theory to communication theory, an introduction to the concept of graph is important for a complete understanding of network coding. In this chapter, after the introduction to graphs in Section 3.1, we present the min-cut max-flow theorem in 3.2. Network coding is primarily the solution to the max-flow problem in multicast application and will be introduced in

3.1 Graphs and Some Basic Definitions

A graph is a mathematical abstraction and simplification of many physical phenomena, thus enabling us to solve real-world problems under the branch of mathematics called graph theory. Graph theory is employed to tackle problems in such fields as communication engineering, computer science, physics, chemistry, biology, and sociology. Examples of graph-theoretical problems which find many applications are the shortest-path problem, the spanning tree problem, the max-flow problem, and the min-cost flow problem.

In general, a graph consists of only two essential sets of elements, which are the set V of nodes and the set E of edges. Therefore, a graph G is usually represented by the pair of those two sets such that $G = (V, E)$. Here, we give the following definitions of three types of graphs relevant to our topic, which are simple graphs, multigraphs, and directed graphs.

Definition 1 *A simple graph G consists of a node set $V(G)$ and an edge set $E(G)$, where each edge is a pair (u,v) of vertices $u,v \in V(G)$. Each pair of nodes u and v in G is joined by at most one edge*

Definition 2 *A multigraph G consists of a node set $V(G)$ and an edge set $E(G)$, where each pair of nodes u and v in G may be joined by more than one edge. Thus, each edge joining a pair of vertices $u,v \in V(G)$ is represented by $(u,v)_i$, where i is the index ensuring that the representation of each edge is distinct.*

Definition 3 *A directed graph G_D consists of a vertex set $V(G)$ and an edge set $E(G)$, where each edge is an ordered pair (u,v), that must be distinguished from (v,u), of vertices $u,v \in V(G)$.*

Figures 3.1 and 3.2 give examples of a simple directed graph and a multigraph, respectively. Note that Fig. 3.1 is also a multigraph since, according to our definitions, every simple graph is a multigraph, whereas Fig. 3.2 is neither a simple graph nor a directed graph since three edges connect F and G and no direction is associated with each edge.

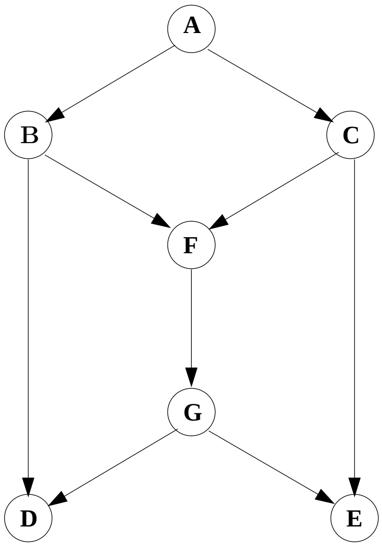

Figure 3.1: An example of a simple directed graph

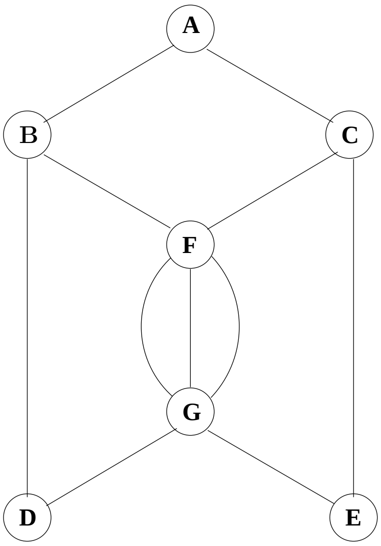

Figure 3.2: An example of a multigraph

When a directed graph is used in practice, it is useful to introduce a variable that measures the quantity flowing in each edge, such as the electric current in a circuit, or, in our case, the data rate in a network. We simply call this quantity "flow." The flow of (u, v) is denoted by x_{uv} such that $x_{uv} \leq c_{uv}$, where c_{uv} is the capacity of (u, v). Although some books suggest that a flow can be any real number, we will only allow it to be a non-negative integer in our application of digital communication systems. The reason for our choice is clear: Since the information is digitized, its amount can be represented by an integer. And since the network is represented by a directed graph, the flow direction is obvious and therefore a negative flow makes no sense.

3.2 The Min-cut Max-flow Theorem

Now we would like to introduce the max-flow problem in a digital communication network. In this problem, we have a graph with two special nodes, the source s and the sink t. This is an optimization problem of which objective is to maximize the amount of information flowing from s to t. We can give the mathematical formulation as follows.

Then, in order to analyze flows in a network, some more definitions are given.

Definition 4 *Max-flow Problem:*

maximize x_0

subject to

$$\sum_{\{j|(i,j)\in E(G)\}} x_{ij} - \sum_{\{j|(j,i)\in E(G)\}} x_{ji} = 0, \forall \tag{3.1}$$

We denote the set of all pairs of a set V by $\begin{pmatrix} V \\ 2 \end{pmatrix}$. Therefore, $E(G) \subseteq \begin{pmatrix} V(G) \\ 2 \end{pmatrix}$

3.3 Introduction to Network Coding

3.4 Theory of Network Coding

3.4.1 Linear Network Codes

3.4.2 Classification of Linear Network Codes

3.4.3 Generic Linear Network Codes

3.5 Rateless Codes

3.5.1 LT Codes

3.5.2 Raptor Codes

Part II

Network Coding Issues: Unequal Erasure Protection and Degree Distribution Distortion in LT-Coded Symbols

The emergence of scalable video coding standard means that some parts of transmitted data should be better protected than others. This concept is called unequal error/erasure protection (UEP). We will show in Chapter 4 that network coding inherently supports this concept. However, this will inevitably leads to conflicts among receiving nodes in a multicast session. We provide an economic analysis of the conflicts as well as an auction algorithm to resolve them.

Rateless codes, such as LT-codes and Rapter codes, are originally designed to guarantee that erasures in the network do not affect data recovery. This seems, at first thought, to imply that they do not support UEP, since the recovery of every data priority seems to be guaranteed. However, a subsequent work by Rahnavard, vellambi, and Fekri, shows that UEP can still be implemented using a similar concept of unequal recovery time (URT) [52]. Their technique ensures that, for an unlimited time, data of all priorities is recovered, but for a specific time range, higher-priority data will be recovered before the lower-priority one. This allows the receiving nodes to decide how long they want to spend time receiving data, according to the number of priorities that they need.

However, when rateless codes are used in a network with network coding, another problem arises. We call it the degree distribution distortion problem. This will make the recovery time of every data priority longer than the normal case without network coding. In chapter 5, we investigate this problem in LT-codes with the simplest case of a butterfly network and gives a solution.

Chapter 4

Unequal Erasure Protection (UEP) in Network Coding

4.1 Introduction to Erasures and Unequal Erasure Protection (UEP) in Network Coding

Recent works on network coding consider errors and erasures in networks [6, 18–20], whereas earlier ones model networks as graphs in which each edge represents an erasure-free channel with a unit capacity [13, 14, 49]. In this chapter, we consider each edge to represent the data transmission rate of one symbol per unit time in a binary erasure channel (BEC), i.e., the edge capacity is reduced from 1 to $1 - p$, if p denotes the erasure probability. We discuss this in the context of a generalized network in the next section.

When data is of different importance, it is natural that one prefers to better protect the high-priority data than the low-priority one against errors and erasures. This concept is called unequal error/erasure protection (UEP).

Scalable video and image data, such as Scalable Video Coding (SVC) standardized by JVT as an extension of H.264/AVC, consists of several layers of data [51]. Upper layers represent fine details added to lower ones. As shown in Fig., when the third layer data is missing, the receiver can only recover the first two layers since the recovery of the last two layers depends on successful recovery of the third. Scalable data therefore asks for unequal erasure protection (UEP), sometimes mentioned as unequal loss protection (ULP), such that the parts of data with higher priority are better protected against erasures.

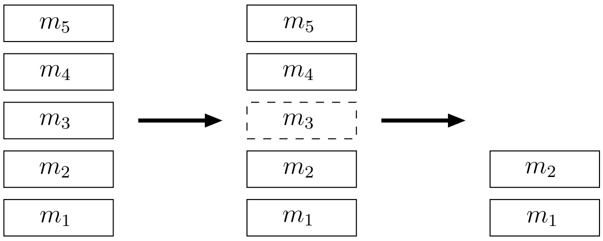

Figure 4.1: Network coding in a butterfly network

UEP has been implemented in several components of digital communication systems. UEP bit-loading for multi-carrier modulation is studied in , UEP coded modulation in , UEP bit-loading for MIMO-OFDM (Multiple-Input Multiple-Output- Orthogonal Frequency Division Multiplexing in , UEP Turbo codes based on puncturing and pruning in , and UEP LDPC Codes based on irregular variable and/or check nodes degrees in .

Unequal-erasure-protected network coding is proposed for the first time by the author and his supervisor. They analyze the effect of erasures on the recovery of scalable data when linear network coding is applied. They find that global encoding kernels (GEKs) describing linear network codes have different levels of built-in unequal-erasure-protecting (UEP) capability, allowing better protection of high-priority data when GEKs are wisely assigned. They also propose a sub-optimal assignment strategy based on the concept of equity. Later, several works related to UEP network coding are proposed.

We define some related terms and concepts of scalable data in section 4.3, which allows us to give a mathematical expression of the expected quality of the recovered scalable data in the presence of erasures. In section 4.4, we show that linear network codes have built-in UEP mechanisms affecting the quality of the recovered scalable data. Section 4.5 gives an example of a UEP network codes assignment problem, which can be solved by the strategy suggested in Section 4.6. The last section discusses the result and concludes.

4.2 The Edge-Disjoint Path Model with Binary Erasure Channels for Network Coding

Figure 1 shows network coding in a network that is usually called the butterfly network, where A aims to multicast two binary symbols b_1 and b_2 to D and E. We can see that the node F encodes b_1 and b_2 together to achieve the multicast rate of 2 bits per unit time, if each edge represents the capacity of one bit per unit time, D receives b_1 from the path ABD and can recover b_2 from the symbol $b_1 \oplus b_2$ from $ACFGD$, whereas E receives b_2 from the path ACE and recovers b_1 from the symbol $b_1 \oplus b_2$ from $ABFGD$. Had network coding not been there, only either b_1 or b_2 would have been able to pass the bottleneck FG in one unit time, i.e., one receiver would have been unable to use one of its possible transmission paths.

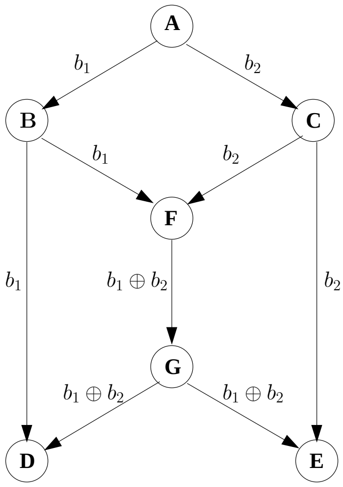

Figure 4.2: Network coding in a butterfly network

By means of network coding, all receivers can use all of their possible paths at the same time. In general cases, the multicast rate of ω suggests the existence of ω non-intersecting paths from the source to each sink, which are called edge-disjoint paths by Jaggi et al. [13], although the paths destined to different receivers may share some edges.

If each edge is modeled as a binary erasure channel (BEC), the erasure probability of an edge-disjoint path can be computed from erasure probabilities of all the edges from the source to the sink. The loss of a symbol in each edge-disjoint path does not affect the recovery in another. For example, the loss of b_1 at the edge BF does not affect the recovery of b_2 at D via $ACFGD$.

Let $p_{i,j,k}$ represents the erasure probability of the k^{th} edge belonging to the j^{th} path of the i^{th} sink. The overall erasure probability of data symbols from the j^{th} path belonging to the i^{th} sink, denoted by $P_{e,ij}$, becomes

$$P_{e,ij} = 1 - \prod_{k=1}^{|E(i,j)|} \left(1 - p_{i,j,k}\right), \tag{4.1}$$

where $|E(i,j)|$ denotes the number of edges in the j^{th} path of the i^{th} sink.

4.3 UEP Issues in Network Coding

Let us consider Fig. 2 again and see what will happen if one symbol is received at each sink whereas another one is erased. At D, if $b_1 \oplus b_2$ is erased, D still obtains b_1. But if b_1 is erased, D obtains neither b_1 nor b_2. This means, for D, b_1 is better protected than b_2. On the other hand, for E, b_2 is better protected. In case b_1 and b_2 are equally important, the network coding is fair. However, if b_1 is more important than b_2 and the erasure probability of each symbol is the same, D is in favor because its more-important symbol is better protected. Thus, to achieve fairness and optimality, the network encoding function of each edge-disjoint path should be carefully chosen.

The preferred choice of network codes for each receiver may vary depending on the situation. Although, in normal situation, D prefers the network coding pattern shown in Fig. 2 to that in Fig. 3, it will change preferrence if suddenly the link BD is broken. Thus, clever choice of network codes can also provide insurance.

Since the problem of insurance and fairness in the distribution of wealth is an economic problem, so is our problem. Therefore, in the next section, we will formulate it using such economic terms as utility, marginal value, and anticipation.

4.4 The Utility of Scalable Data

The "utility" is a numerical value representing the amount of satisfaction that a user receives from an object. In our case, a "user" simply refers to a receiver, whereas the term "object" deserves a careful consideration. If we define an object by a layer of scalable data, it might appear at first that we now have several types of objects, since each layer of data has different properties. However, for the sake of simplicity and orderliness, we will treat all the layers as the same type of objects which are arranged in order of importance. Moreover, each layer corresponds to an inseparable object, i.e., half a layer is considered meaningless. Thus, the word "layer" to be considered here needs not be the same as the one defined in any particular technical standards. It simply denotes an inseparable unit of data symbols. In this way, our formulation will correspond to the following law of diminishing marginal utility in economics.

Law 4.1 : Law of Diminishing Marginal Utility
1. The utility that each receiver gains from receiving scalable data depends on the number of received data layers.
2. The extra utility that a receiver gains from an increase in the number of received layers, which is called a marginal utility, is less if the previously received number of layers is greater.

According to Law 1, if any two receivers have exactly the same capability to extract utility from the same amount of received data, it can be concluded that an unequal amount of received layers between them will make the marginal utility of the one with privilege less than the other. Conversely, if a given receiver have more capability to extract utility, an equal distribution results in the larger marginal utility for that receiver.

The following definitions formally express the utility concept in scalable data. We formulate, in Definition 4.1, the mapping of scalable data into a scalable message in which each successive layer adds more details to the data. Therefore, each element in the scalable message corresponds to the "object" of our interest. After explaining the term "dependency level" in Definition 4.2, we define the "cumulative utility vector" and "marginal utility vector" corresponding to the law of diminishing marginal utility in Definition 4.3 and 4.4, respectively. Then, we define an "ordered set of scalable data" that can be mapped into an "ordered scalable message" in Definition 4.5, which possesses an interesting practical property: The incremental quality obtained by each recovered layer in the message is in a decreasing order. The ordered scalable message thus always prefers more erasure protection in the preceding symbol than the subsequent one.

Definition 4.1 *For any $\mathcal{S} = \{s_1, s_2, ..., s_\omega\}$, representing a set of scalable data with progressively increasing quality from s_1 to s_ω, the i^{th} element s_i can be mapped into a prefix vector $\mathbf{P_i}$= $[m_1, m_2, ..., m_i]$ of a scalable message $\mathbf{M}$= $[m_1, m_2, ..., m_\omega]$, which is an ω-dimensional row vector of a finite field $\mathbb{F}$.*

$$s_i \longmapsto [m_1, m_2, ..., m_i] \tag{4.2}$$

Definition 4.2 *A symbol m_k belonging to the scalable message $\mathbf{M} = [m_1, m_2, ..., m_\omega]$ has a dependency level of $\lambda(m_k) = j$ if its significance depends on the successful recovery of the symbols having the dependency level of $j - 1$ but not on those with larger dependency level. A symbol of which significance does not depend on any symbol has the dependency level of 1.*

Definition 4.3 *A functional vector $\mathbf{U_k}(\mathcal{S}) = [u_k(s_1), u_k(s_2),\ ..., u_k(s_\omega)]$, $k = 1, 2, ..., N$, where N is the number of sink nodes in the network-coded multicast, is called the cumulative utility vector assigned by the sink node k to the set of scalable data $\mathcal{S}$ described in Definition 1 if each element $u_k(s_i)$, $1 \leq i \leq \omega$, is a non-negative real number representing the private utility that the sink node k assigns to the scalable data s_i.*

Definition 4.4 *A functional vector $\Delta\mathbf{U_k}(\mathcal{S})$ is called the marginal utility vector assigned* *by the sink node k to the set of scalable data $\mathcal{S}$ described in Definition 1 if*

$$\begin{aligned}
\Delta\mathbf{U_k}(\mathcal{S}) &= [\Delta_1, \Delta_2, ..., \Delta_\omega] &(4.3)\\
&= [u_k(s_1) - u_k(s_0), u_k(s_2) - u_k(s_1), ...\\
&\quad ..., u_k(s_\omega) - u_k(s_{\omega-1})], &(4.4)
\end{aligned}$$

where $u_k(s_0) = 0$ and $u_k(s_i)$, $1 \leq i \leq \omega$, represents the element in the cumulative value vector $\mathbf{U_k}(\mathcal{S})$ defined in Definition 3.

Definition 4.5 *The set of scalable data $\mathcal{S}$ is said to be ordered if and only if the two following conditions are fulfilled.*

$$\begin{aligned}
\lambda(m_u) &\geq \lambda(m_v), 1 \leq v < u \leq \omega &(4.5)\\
\Delta_{i-1} &\geq \Delta_i, 1 < i \leq \omega &(4.6)
\end{aligned}$$

where $\lambda(m_j)$ and Δ_i denote the dependency level of the symbol m_j and the i^{th} element in the marginal utility vector of $\mathcal{S}$, respectively. A message $\mathbf{M}$ corresponding to an ordered set $\mathcal{S}$ of scalable data is called an ordered scalable message.

4.5 Utility of Scalable Data as Probabilistic Objects

Since data transmission is a random process subjected to probabilistic errors and erasures, we need to add probabilistic aspects into our concepts of "object" according to the following laws.

Law 4.2 : Laws of a Probabilistic Object

1. The concept of "object" is extended to include combination of objects with stated probabilities. For example, if A and B are objects, a 30-70 chance of A or B is also an object.

2. If the object A is preferred to the object B, and B to the object C, there will be some probability combination of A and C such that the individual is indifferent between it and B.

These probabilistic aspects are in accordance with Friedman and Savage's "The Utility Analysis of Choices Involving Risk," since erasures and errors in our data transmission can be considered as risks.

From Definition 4.4, if the prefix $\mathbf{P_{j-1}}$ in the ordered scalable message M has already been successfully recovered, the recovery of the symbol m_j will increase the utility by Δ_j. Now, since the transmission channels are assumed to be binary erasure channels, the object obtained at each receiver is a probabilistic object in Law 4.2. This means, according to the paragraph 1, that there are chances of receiving A, B, C, etc., which are data with different qualities and probabilities. However, all of these can be considered as one object with its own utility. Generalizing the law in the paragraph 2 with a linearity assumption, we can derive the utility of such an object by the following expected value.

$$\begin{aligned} E[U_i] &= \sum_{j=1}^{\omega} \left[\prod_{l=1}^{j} \varrho_{i,l} \right] \cdot \Delta_j & (4.7) \\ &= \sum_{j=1}^{\omega} \rho_{i,j} \cdot \Delta_j, & (4.8) \end{aligned}$$

where ϱ_{il} and $\rho_{i,j}$ represent the probabilities that the symbol m_l and the prefix $\mathbf{P_j}$ are recovered at the sink i, respectively. From (4.8), the quality improves if the term $\rho_{i,j}$, becomes larger, especially for a small j implying a large Δ_j. This reaffirms the essence of UEP, which is to better protect the high-priority preamble. $\rho_{i,j}$ depends on the transmission channels and our network codes, which will be investigated in the next section.

4.6 Utility of Global Encoding Kernels (GEKs) for Linear Network Codes

In the previous section, we consider scalable data as probabilistic objects and derive its utility. In this section, after having a quick review of the meaning of global encoding kernels (GEKs), we will see that the assignment of GEKs to the edges in the network is analogous to assigning received symbols to the sinks in an erasure-free network. In case there are erasures, we can identify the utility of GEKs based on erasure probabilities of transmission channels just as we can identify the utility of scalable data.

Let us now revisit the global encoding kernel (GEK) defined in Chapter 3. For a network that employs linear network coding, each of its edges in the graphical model, such as Fig. 1, is used to transmit the linear combination of the source symbols. This linear combination can either be represented locally as a linear function of symbols from adjacent edges, which is called "the local encoding mapping", or globally as a linear function of source symbols, which is called "the global encoding mapping" [49]. The global encoding mapping is described by a vector called "the global encoding kernel (GEK)," which is introduced here again in Definition 4.6.

Definition 4.6 *Let $\mathbb{F}$ be a finite field, ω a positive integer, and the ω-dimensional, $\mathbb{F}$-valued vector $\mathbf{M}$ the message generated by the source node $\mathcal{S}$. A function $f_e(\mathbf{M})$ of the edge e is said to be a linear global encoding mapping if there exists an ω-dimensional $\mathbb{F}$-valued column vector $\mathbf{f}_e$ such that*

$$f_e(\mathbf{M}) = \mathbf{M} \cdot \mathbf{f}_e. \tag{4.9}$$

$\mathbf{f}_e$ *is called the global encoding kernel [49].*

The assignment of the global encoding kernel $\mathbf{f}_e$ to the edge $e \in In(T)$, where $In(T)$ is the set of all incoming edges of the sink T, determines which linear combinations of symbols in the message $\mathbf{M}$ are received at T, when there is no erasure.

Since the symbols in the message have unequal utility, so do the combinations of them. It then follows logically that GEKs also have unequal utility. Before determining the utility of each GEK, we will classify the GEKs into levels based on the linear combination it yields. The levels of GEKs will be used to calculate their utility later.

We only consider the problem of assigning, given some local constraints, a suitable global encoding kernel for each edge according to the expected quality in (4.8), since the local encoding mapping can be easily derived thereafter.

To relate the $\rho_{i,j}$ to the network codes, we firstly define the UEP level of a global encoding mapping as follows.

Definition 4.7 *For a scalable message* $\mathbf{M}$*, which is an* ω*-dimensional row vector of a finite field* $\mathbb{F}$*, a global encoding mapping* $\gamma_i(\mathbf{M})$ *is of the* i^{th} *UEP level,* $0 < i \leq \omega$*, if there exists an* ω*-dimensional,* $\mathbb{F}$*-valued column vector* $\mathbf{C}_i = [c_1, c_2, ..., c_i, 0, 0, ..., 0]^T$*,* $c_i \neq 0$*, such that*

$$\gamma_i(\mathbf{M}) = \mathbf{M} \cdot \mathbf{C}_i = \sum_{j=1}^{i} c_j \cdot m_j. \tag{4.10}$$

$\mathbf{C}_i$ *is then called an* i^{th}*-UEP-level global encoding kernel.*

Now, let us consider an ordered scalable message $\mathbf{M} = [m_1, m_2, m_3]$, where m_1, m_2, and m_3 are binary symbols of the first, second, and third dependency level, respectively. According to Definition 4.7, there exist seven possible GEKs, one of the first UEP level, two of the second level, and four of the third level, as shown in Table 4.1.

Table 4.1: GEKs, their UEP levels, and the resulting network-coded symbols

UEP Levels	GEKs	Resulting Network-Coded Symbols
1	$[1\ 0\ 0]^T$	m_1
2	$[0\ 1\ 0]^T$	m_2
	$[1\ 1\ 0]^T$	$m_1 + m_2$
3	$[0\ 0\ 1]^T$	m_3
	$[1\ 0\ 1]^T$	$m_1 + m_3$
	$[0\ 1\ 1]^T$	$m_2 + m_3$
	$[1\ 1\ 1]^T$	$m_1 + m_2 + m_3$

From Table 4.1, the prefix $\mathbf{P}_2 = [m_1, m_2]$ can be recovered either from any two symbols from the levels 1 and 2 or from any three symbols from the level 3. For an arbitrary scalable message $\mathbf{M}= [m_1, m_2, ..., m_\omega]$, we can state as a general rule that, in order to recover the prefix $\mathbf{P}_i$, we need either i network coded-symbols belonging to i linearly independent GEKs of which UEP levels do not exceed i, or more than i symbols in case some UEP levels of GEKs exceed i.

The implication following from the analysis is that the GEKs in lower levels have more utility than those in higher levels since they contribute more to the recovery of high-priority bits. In order to determine the expected utility in the presence of erasures, we now have to consider the erasure probability in each edge-disjoint path discussed in 4.2.

Reconsidering eq. (4.8), assuming that the k^{th} edge-disjoint path of the sink i is used to transmit the k^{th} network-coded symbol to the sink i, the parameter $\rho_{i,j}$, which is the probability that the prefix $\mathbf{P}_j$ is recovered at the sink i, can be written as

$$\rho_{i,j} = \prod_{k=1}^{\omega} \mu_{j,k} \cdot [1 - P_{e,ik}] \,, \tag{4.11}$$

where $P_{e,ik}$ denotes the erasure probability of the path k used to transmit the k^{th} network-coded symbol to the sink i. $\mu_{j,k} = 1$ if the k^{th} network-coded symbol is needed to recover the prefix $\mathbf{P}_j$. Otherwise, $\mu_{j,k} = 0$.

Equations (4.8) and (4.11) show that, by changing the GEKs allocated to the edges, the expected utility of received data varies. Therefore, if the receiver i is allowed to assign a GEK to an edge or a set of edges, it can do so in such a way that its utility increases, sometimes at the expense of other receivers. The more GEKs a node i is allowed to choose, the better its satisfaction. This means there is a marginal utility associated with each increase in the number of such permissions, which is defined as follows.

Definition 4.8 *A functional vector $\mathbf{\Theta}_i$ is called the marginal utility vector assigned by* *the sink node i to the GEK allocation permissions if*

$$
\begin{aligned}
\mathbf{\Theta}_i &= [\theta_1, \theta_2, ..., \theta_\zeta] && (4.12)\\
&= [\mathcal{I}_{bi1} - \mathcal{I}_{wi1}, \mathcal{I}_{bi2} - \mathcal{I}_{wi2}, ... \\
&\quad ..., \mathcal{I}_{bi\zeta} - \mathcal{I}_{wi\zeta}], && (4.13)
\end{aligned}
$$

where ζ is the number of possible permissions. $\mathcal{I}_{bij}$ is the expected utility $E[U_i]$ in (4.8)when the sink i is allowed to allocate j GEKs, whereas $\mathcal{I}_{wij}$ is that when it is only allowed to allocate $j-1$ GEKs before one worst-case GEK is assigned to it in the j^{th} allocation. Thus, the difference between $\mathcal{I}_{bij}$ and $\mathcal{I}_{wij}$ reflects how important it is for i to receive the j^{th} allocation permission.

4.7 The Problem of GEK Assignment

According to (4.8) and (4.11), the best option for the sink i is to make $\rho_{i,j}$ large for small j to satisfy the UEP requirements and optimize the scalable data quality. To do so, it first sorts the erasure probability $P_{e,ik}$ such that $P_{e,ik} \leq P_{e,ir}$ for any $1 \leq k < r \leq \omega$, and, after that, allocates a q^{th} level GEK to the path with the index $k = q$ [6].

However, as earlier discussed in Section 3, this simple allocation scheme may not be possible due to conflicts among sink nodes as well as linear independence and dependence constraints of GEKs. Linear independence constraints ensure that the maximum information flow is achieved at each node, whereas linear dependence represents topological constrains, i.e., the GEK of any outgoing edge of the node i must be linearly dependent on the GEKs of incoming edges.

In order to make $\rho_{i,j}$ large for small j to satisfy the UEP requirements and optimize the scalable data quality, as mentioned in Section 4.3, we first sort the erasure probability $P_{e,ik}$ such that $P_{e,ik} \leq P_{e,ir}$ for any $1 \leq k < r \leq \omega$. Then we find that the ideal strategy is to allocate a first-UEP-level GEK to the path with the index $k = 1$, such that we only need the path with the lowest erasure probability to recover the most important prefix

$\mathbf{P}_1$. In this case, $\rho_{i,1} = 1 - P_{e,i1}$, which is the highest possible $\rho_{i,1}$. Next, we allocate a second-UEP level GEK to the path with next-to-the-lowest erasure probability, i.e., $k = 2$, such that $\rho_{i,2} = (1 - P_{e,i1})(1 - P_{e,i2})$, which is the highest possible $\rho_{i,2}$. We then keep allocating a q^{th} level GEK to the path with the index $k = q$ until reaching the last path.

In practical multicast, however, it may be impossible to apply the ideal strategy to all receivers due to conflicts among them and some side constraints. This poses an economic problem of optimal distribution of goods, which are discussed countlessly in economic literature. The proper solution depends on to which camp the decision maker belongs, i.e. whether he is a socialist, capitalist, or somewhere in between. Although we will not give arguments about economic philosophy in general, we propose two solutions to our GEK assignment problem according to different standards of evaluation. The first one is more socialist and the second more capitalist.

4.8 Maximin Assignment of Global Encoding Kernels (GEKs)

The assignment of global encoding kernels is a difficult problem involving some basics questions to be answered prior to any algorithm design. Since the quality of the received scalable data at each receiving node depends on the GEKs used as well as the erasure probability at each edge, any entity who is responsible for GEK assignment can only do so optimally if it knows all the erasure probabilitites involved. After having derived the utility of GEKs, we will now show

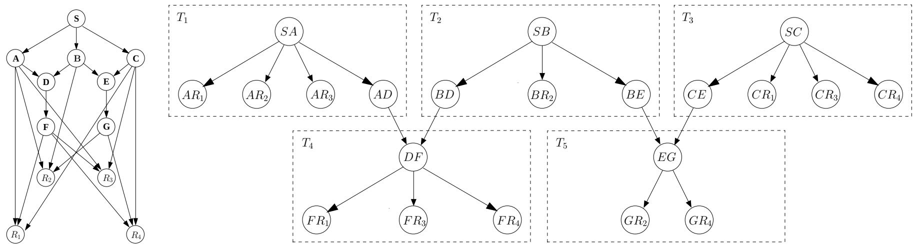

Figure 4.3: Derivation of a Minimum Subtree Graph

4.9 An Ascending-bid Auction Algorithm for GEK Allocation

We assume that the source node is the auctioneer and the sinks are participants who bid for the rights to choose the GEK allocation. Since we will not give a monopoly to any single sink node, the allocation problem is formulated as a multiple-item auction. For this kind of auction, the dynamic counterpart of Vickrey's effective static design [23] has recently been proposed by Ausubel [24], whose idea will be used in our auction as follows. The source node calls a price, bidders respond with quantities, and the process iterates with increasing price until demand is not greater than supply.

Although the supply is the total number of GEK allotments, it does not equal the total number of edges, because some edges are forced by the topology to have the same GEK. Thus, before the auction begins, the source node has to derive the minimum subtree graph of the network. An example is shown in Fig. 2, in which the network on the left is transformed into a line graph on the right such that each node in the right graph corresponds to an edge in the left one. Then, the nodes in the right graph can be grouped into five subtrees, each of which is surrounded by dashed lines, such that the members in each subtree are forced by the topology to have the same GEK. In this case, the problem of assigning GEKs to twenty-six edges is reduced to that of assigning them to six subtrees.

Let $\mathcal{T}$ represent the set of all subtrees. The source wishes to allocate $|\mathcal{T}|$ GEKs to $|\mathcal{T}|$ subtrees, not on its own but by means of a $|\mathcal{T}|$-item auction. The sink i who wins x_i items is allowed to choose the allocation of x_i GEKs to x_i subtrees in order to maximize its satisfaction. The source then distributes the data accordingly and informs the intermediate coding nodes about the local encoding functions they have to use.

According to Ausubel's idea, a bidder's payment is not the product of its final quantity and the final price. Rather, at the price ψ, the auctioneer sees if the aggregate demand x_{-i} of bidder i's competitiors is less than the supply $|\mathcal{T}|$. If so, $|\mathcal{T}|-x_{-i}$ items are clinched and awarded to i with the price ψ. Since the winner's payment depends on its competitors bids and not its own bids, every participant has incentive to reveal truthfully its value for the item. [24]

Our auction, however, requires some modification since each clinched item and the resulting GEK allocation of a winning sink affects the demand of others. This is best explained by an example.

Table 4.2: Preference order of GEK allocation

Sink	Preference Order		
R_1	T_4	T_3	T_1
R_2	T_2	T_1	T_5
R_3	T_1	T_4	T_3
R_4	T_5	T_4	T_3

Suppose that the source node $\mathcal{S}$ in Fig. 2 would like to multicast an ordered scalable message $\mathbf{M} = [m_1, m_2, m_3]$, of which each element m_i has a dependency level of i, to four sink nodes R_1, R_2, R_3, and R_4. We assume that Table 2 reflects the preference order of GEK allocation, e.g., if R_1 is allowed to allocate only one GEK, it will choose the best one and assign it to T_4. If two allotments are allowed, R_1 will assign two GEKs to T_4 and T_3. The preference order relates to the erasure probability of each edge-disjoint path discussed in earlier sections. Each sink's main preference is to allocate the GEKs with lower UEP levels to the paths with lower erasure probability. This means, according to Table 2, the path from the source that reaches R_1 via T_4 has lower erasure probability than those reaching R_1 via T_3 and T_1.

Let each receiver's estimate of its marginal values θ_1, θ_2, and θ_3, as defined in Definition 8 be shown below.

$\boldsymbol{\Theta}$	R_1	R_2	R_3	R_4
θ_1	123	75	85	45
θ_2	113	5	65	25
θ_3	40	3	7	5

Now, let the auction start with the initial price of 10. At this price, R_1 is happy to buy three allotments, while R_2 will buy only one, since the price exceeds the second marginal value. Accordingly, the response from each receiver is shown in the first row of Table 3. Since nobody cliches anything at this point, the source node raises the price. When the price reaches 25, R_4 has no profit to be gained from the second allotment, and therefore changes its response, as shown in the second row of Table 3.

Table 4.3: The Sinks' Responses to the Increasing Price

Sinks	R_1	R_2	R_3	R_4
Responses to 10	3	1	2	2
Responses to 25	3	1	2	1
Responses to 25+ϵ	3	1	1	1
Responses to 40	2	1	1	1

From R_1's perspective, the demands of all other bidders are four, while five allotments are available. If other sinks bid monotonically, R_1 is now guaranteed to win at least one allotment. Thus, according to our rule, R_1 clinches one allotment at the price of 25. It then chooses the first-level GEK to allocate to T_4. This allocation affects the marginal values of every sink except R_1. They are updated as follows.

$\boldsymbol{\Theta}$	R_1	R_2	R_3	R_4
θ_1	123	75	85	45
θ_2	113	4	6	3
θ_3	40	2	-	-

Due to the allocation of T_4, R_3 and R_4's last entries are removed since they now have only (T_1, T_3) and (T_5, T_3), respectively, to bid for. At the next announced price 25+ϵ, R_3's response changes, as shown in the third row of Table 3.

Since R_1 is now guaranteed to win two items, it is allowed to allocate one GEK to T_3.

After that, the marginal values are updated again, as follows.

$\boldsymbol{\Theta}$	R_1	R_2	R_3	R_4
θ_1	123	71	62	42
θ_2	113	3	-	-
θ_3	40	1	-	-

At a price of 40, the demand equals the supply, as shown in the fourth row of Table 3, and the market clears. Each of R_2, R_3, and R_4 clinches one object at this price and assigns a GEK to T_2, T_1, and T_5, respectively.

The algorithm implementing the auction at the source node is shown as follows.

Algorithm 1 *Problem: Allocate a GEK $\mathbf{f}_t \in \mathbb{F}^\omega$ to each $t \in \mathcal{T}$ such that the sets of linear independence and dependence constraints are satisfied.*

1. Initialize the number of available items $N_T = |\mathcal{T}|$, the cumulative clinches $C = 0$, the cumulative quantity $X = 0$, the individual current clinches $\gamma_i = 0$ and individual cumulative clinches $\Gamma_i = 0$ for the node i, $i = 1, 2, ..., n$. Set the current price ψ as the initial price ψ_0. Broadcast linear dependence and independence constraints to all sink nodes.

2. At an appropriate time $t + \Delta t_i$, where Δt_i is the time offset calculated from the distance between the source and the sink i, send the current price ψ to the sink i and wait for response.

3. Upon receiving the quantity x_i from every sink i, update X, Γ_i, and γ_i as follows.

$$X = \sum_{i=1}^{n} x_i \tag{4.14}$$

$$x_{-i} = X - x_i \tag{4.15}$$

$$Y_i = \Gamma_i \tag{4.16}$$

$$Z = C \tag{4.17}$$

$$\Gamma_i = \begin{cases} |\mathcal{T}| - x_{-i} & \textit{if } |\mathcal{T}| > x_{-i} \\ 0 & \textit{otherwise} \end{cases} \tag{4.18}$$

$$\gamma_i = \Gamma_i - Y_i \tag{4.19}$$

$$C = \sum_{i=1}^{n} \Gamma_i \tag{4.20}$$

4. From 3, if $C - Z > 0$, go to 5. Otherwise, go to 10.

5. Find the index $j \in \mathcal{K}$, $\mathcal{K} = \{\forall k | \gamma_k \neq 0\}$ such that $x_j \geq x_i$, for every $i \neq j$, $i \in \mathcal{K}$. If more than one x_j are found, randomly select one of them.

6. Inform the sink node j about the individual current clinches γ_j. Wait for response.

7. If the response is negative, let $x_j = x_j - 1$ and go back to 3. In case the affirmative response, together with the GEK $\mathbf{f}_r$ that j chooses to allocate to the subtree $r \in \mathcal{T}$, is received, check if the allocation violates the linear dependence or independence constraints. If so, randomly allocate a GEK satisfying the constraints to r. If not, allocate $\mathbf{f}_r$ to r.

8. Broadcast the index of the allocated subtree in 7 and its GEK to all nodes.

9. Let $Z = Z + 1$, $\mathcal{K} = \mathcal{K} - \{j\}$, and $N_T = N_T - 1$. If $N_T > 0$, go back to 4. Otherwise, the algorithm ends.

10. Update the price such that $\psi = \psi + \Delta\psi$. Go back to 2.

In Step 3, the cumulative clinches Γ_i for the sink i is computed as the difference between the supply $|\mathcal{T}|$ and the aggregate demand x_{-i} of its opponents. Y_i is simply a variable used to store the previous Γ_i such that, after Γ_i is updated in (16), the individual clinches γ_i at the current price can be computed from (17). In a similar manner, the variable Z in (15) is used to count the previous cumulative clinches C, which will be updated in (18).

In Step 4, if the updated cumulative clinches C is greater than the previous clinches Z, we continue with Steps 5 to 8, which allow one GEK to be allocated. According to Steps 5 and 6, when more than one sink node clinches some objects at a specific price, the nodes which bid for higher quantity are allowed to choose the allocation prior to those bidding for lower quantity.

Step 9 increases Z by 1 and checks whether there are still some items available. If there is, we return to Step 4 to compare the increased Z with C. If C is still greater than Z, we repeat Steps 5 to 9. Otherwise, no more item is clinched at this price and the price is raised in Step 10.

4.10 Conclusion

Chapter 5

Network Coding with LT Codes as Erasure Codes

This chapter shows that LT-encoding at the source node and network coding at intermediate nodes cannot be applied together sequentially in binary erasure channels (BECs) without significant receiver performance degradation due to the distortion of the degree distribution in received LT-coded symbols. Two countermeasures are discussed. The first one is wise assignment of network codes, which totally eradicates the distortion in some specific, but not all, cases. The second one, being more universal, is a cooperation between the source and the relay nodes. The source introduces buffers for temporarily storing LT-coded output prior to transmission. Each buffer is a first-in-first-out (FIFO) queue associated with one outgoing edge of the source node. It is shown that under some conditions related to the degree of a particular LT-coded symbol, it is better to put that symbol into one buffer instead of another in order to keep the degree distribution distortion low. In addition, we paradoxically discover that the relay node, instead of always performing network coding, can improve the receiver performance by discarding some LT-coded symbols with a certain probability, since this will reduce the degree distribution distortion.

5.1 Introduction and The System Model of Relay Network Multicast with LT and Network Codes

LT codes or other rateless codes as a forward error correction (FEC) scheme are arguably most useful in multicast applications in which its one-to-many nature makes the acknowledgement scheme very unpleasant. LT codes can potentially generate an infinite stream of coded output symbols such that, even when some symbols are erased, the receiver can recover k original symbols using any K received coded symbols when K is only slightly larger than k.

Like LT codes, network codes find their first and simplest application in multicast. However, both types of codes have opposite aims. While LT codes increase redundancy in the networks to compensate for erasures, network codes decrease it by means of coding at the bottlenecks.

According to Fig. 5.1, where A aims to multicast two binary symbols b_1 and b_2 to D and E, we can see that the node F encodes b_1 and b_2 together to achieve the multicast rate of 2 bits per unit time, if each edge represents the capacity of one bit per unit time. D receives b_1 from the path ABD and can recover b_2 from the symbol $b_1 \oplus b_2$ from $ACFGD$, whereas E receives b_2 from the path ACE and recovers b_1 from the symbol $b_1 \oplus b_2$ from $ABFGD$. Had network coding not been there, only either b_1 or b_2 would have been able to pass the bottleneck FG in one unit time, i.e., one receiver would have been unable to use one of its possible transmission paths.

In this paper, we assume that the source node generates LT-coded symbols which are subsequently network coded by intermediate nodes along their ways to the receivers. To make things more concrete, Fig. 5.2 displays a block diagram showing all encoding and decoding processes as well as the buffer structure from the source to the destinations in accordance with the network in Fig. 5.1.

One can observe a switch placed after the LT-Encoder block and prior to two buffers. While traditional network coding only requires that the switch turns to each buffer half

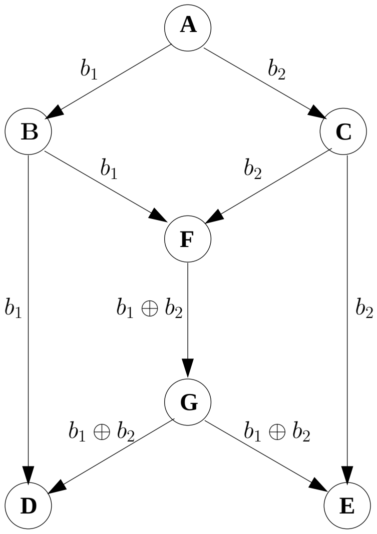

Figure 5.1: Network coding in a butterfly network

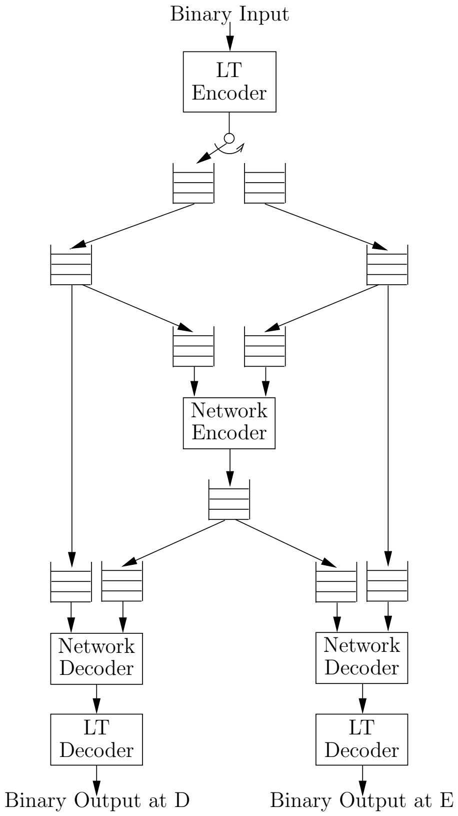

Figure 5.2: Detailed system model including encoding and decoding blocks as well as the buffer structure

of the time, it is not the case in this paper, in which the switching decision depends on the degree of the current LT-encoding output. This is one major discovery in this work.

Despite having our own system shown in Fig. 5.2, we are aware of previous works dealing with similar problems. Therefore, we present a short review of their works in the next section.

After that, Section 5.3 elaborates on important parts in our system, such as LT encoder and decoder. The most crucial function influencing the LT-decoder performance is the degree distribution which must be carefully chosen by the encoder. Section 5.4, however, shows that the well-designed degree distribution can easily be distorted by network coding in binary erasure channels (BECs), leading to a significant degradation in receiver performance.

Section 5.5 provides a solution to the problem for some special cases by means of wise assignment of network codes. In other cases, however, we need a cooperative scheme proposed in Section 5.6 to improve the receiver performance, as shown in Section 5.7.

5.2 Related Literature

Although many recent works regarding network coding focus on two-way wireless relay networks rather than relay network multicasts [65, 69, 71], it is suggested in [69] that the problem of two-way relay networks, and of information exchange in general, can be transformed into a multicast problem via some graph transformations. Thus, the study of information multicast in this work might lead to further discoveries in more generalized cases.

In addition, main components used in those systems are identical or similar to ours. The decode-and-forward (DF) scheme used in [71] employs a channel encoder at each transmitter and a network encoder at the relay, which is structurally identical to our system. However, we use LT codes instead of turbo codes and therefore need no decoder at the relay. This is similar to distributed LT codes proposed in [64], but the receiver in that system receives information only from the relay, whereas our sink receives it via the direct path as well. Since LT codes are erasure correcting codes, binary erasure channels (BECs) are used in our model instead of Gaussian channels.

Like in our system, the buffering scheme is considered important and given careful attention in [69, 72].

5.3 LT and Network Encoding and Decoding

Three steps are needed to generate an LT-coded symbol. Firstly, a degree d is selected from a degree distribution, which is a discrete probability density function mapping a degree to the probability that the degree is selected. Secondly, d original symbols are chosen uniformly at random. Finally, an output symbol is derived by XORing all chosen symbols from the previous step [36].

In this paper, we use a robust soliton distribution, which is constructed such that the failure probability of the message-passing decoder is δ for a given number $K = k + O(\sqrt{k} \cdot \ln^2(k/\delta))$ of received symbols [36].

Definition 1 *The robust soliton distribution (RSD) $\mu(i)$ is derived from the normalization of two functions $\rho(i)$ and $\tau(i)$ as*

$$\mu(i) = \frac{\rho(i) + \tau(i)}{\beta}, \ 1 \leq i \leq k, \tag{5.1}$$

where

$$\rho(i) = \begin{cases} 1/k, & i = 1 \\ 1/(i(i-1)), & 2 \leq i \leq k, \end{cases} \tag{5.2}$$

$$\tau(i) = \begin{cases} R/(i \cdot k), & 1 \leq i \leq (round(k/R)) - 1, \\ (R\ln(R/\delta))/k, & i = k/R, \\ 0, & otherwise, \end{cases} \tag{5.3}$$

$$R = c \cdot \sqrt{k} \cdot \ln(k/\delta), \tag{5.4}$$

$$\beta = \sum_{i=1}^{k} (\rho(i) + \tau(i)). \tag{5.5}$$

The paramater c in (6.9) is a suitable non-negative constant used in the design, whereas δ is the failure probability mentioned earlier [36].

The robust soliton distribution with parameters $k = 1000$, $c = 0.1$, and $\delta = 0.5$ is shown in Fig. 3. The most important observation regarding the plot is that it has two peaks at 2 and 42.

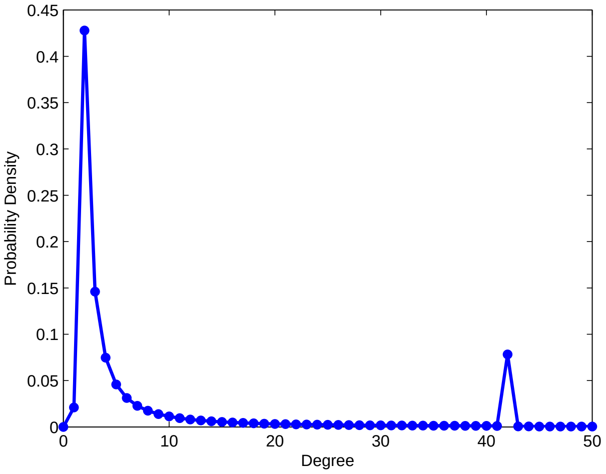

Figure 5.3: Robust soliton distribution with $k = 1000$, $c = 0.1$, and $\delta = 0.5$

Now, let us consider the network in Fig. 1. Assume that node A would like to multicast LT-coded outputs b_1 and b_2 with the robust soliton distribution shown in Fig. 3 to D and E. After the node D receives b_1 and $b_1 + b_2$, it first deducts b_1 from $b_1 + b_2$ to obtain b_2.

We call this deduction "network decoding". After that, both b_1 and b_2 are LT-decoded by the message-passing algorithm, as described in [?], to obtain the original message.

Unfortunately, when network coding is used in severe erasure channels, the well-designed degree distribution can be distorted before LT-coded symbols reach the destination. The next section addresses this issue as well as the resulting receiver performance deterioration.

5.4 Degree Distribution Distortion and Receiver Performance Deterioration in Binary Erasure Channels

Suppose that the edge BD is a binary erasure channel having an erasure probability of 0.1 whereas other edges are erasure-free. Thus, on average, once every ten times the receiver D does not have b_1 to deduct from $b_1 + b_2$ to complete the network decoding process. Instead, $b_1 + b_2$ enters directly into the LT decoding process. Therefore, on average, for every ten symbols of b_1 and ten of b_2 transmitted, D receives nine b_1, nine b_2 (after network decoding), and one $b_1 + b_2$. If b_1 and b_2 follow the robust soliton distribution $\mu(i)$, the overall degree distribution becomes

$$\psi(i) = \frac{18}{19}\mu(i) + \frac{1}{19}\varphi(i), \tag{5.6}$$

where $\varphi(i)$ is the degree distribution of $b_1 + b_2$.

It is precisely the $\varphi(i)$ that alters the overall degree distribution of D's received symbols from the robust soliton case. Since, in practice, the number k of LT input symbols is large, we can assume that the LT-encoded symbols b_1 and b_2 are not made up of some common original symbols. This allows us to approximate the overall degree distribution at D after network decoding as

$$\psi(i) \approx \begin{cases} \frac{18}{19}\mu(i), \ i = 1 \\ \frac{18}{19}\mu(i) + \frac{1}{19}\sum_{j=1}^{i-1}\mu(j)\mu(i-j), \ \text{otherwise.} \end{cases} \tag{5.7}$$

Figures 4 and 5 compare the plot of the robust soliton distribution $\mu(i)$ in the erasure-free case with the distorted distribution due to erasures at BD obtained by the analytical approximation $\psi(i)$ in (6.15) and that obtained from simulation by counting the degree of 10^7 symbols received at D around the two peaks at 2 and 42, respectively. We can see that the steepness of the peaks are lessened in the distorted case. Moreover, an unwanted peak is formed at 44.

Although the distortion of the degree distribution is small, its effect on the performance is clearly visible. Fig. 6 shows the histogram of the number of LT-coded symbols needed to be transmitted until the original symbols can be recovered by D. Fig. 7 makes a comparison between the number of symbols needed to be transmitted when the erasure probability of BD is 0.1 in the network in Fig. 1 and that when the erasure probability is 0.05 in normal point-to-point communication. Although the average erasure probabilities in both cases are the same, the network coding case requires more symbols due to the distortion of the degree distribution.

5.5 The First Solution: Wise Assignment of Network Codes

In case erasures occur only along the edge BD with the erasure probability of 0.1, the solution to the degree distribution distortion problem is very simple. We change our network codes from those in Fig. 1 into those in Figure 8. Since we now transmit $b_1 + b_2$ instead of b_1 along BD, when $b_1 + b_2$ is erased, D only receives b_1, yielding no distortion, when $b_1 + b_2$ is not erased, D can network-decode and receive both b_1 and b_2, yielding no distortion either.

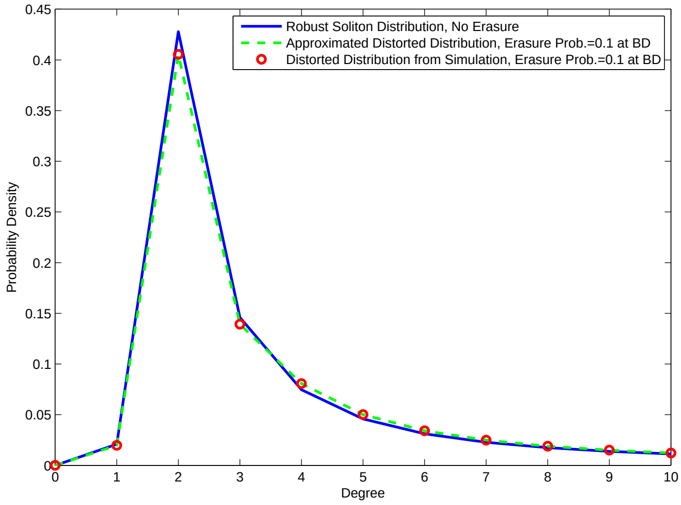

Figure 5.4: Robust soliton distribution around the first peak in comparison with distorted distribution caused by erasures at the edge BD

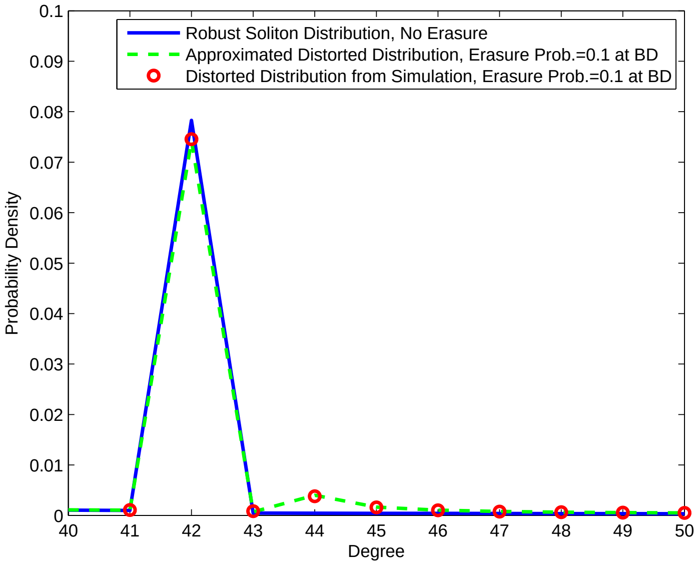

Figure 5.5: Robust soliton distribution around the second peak in comparison with distorted distribution caused by erasures at the edge BD

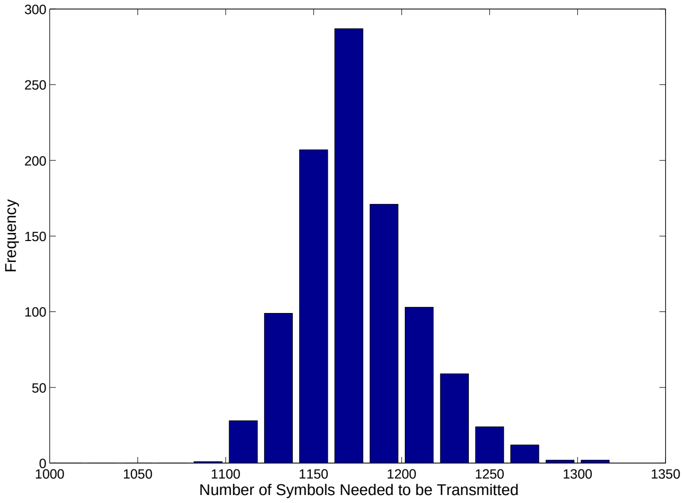

Figure 5.6: Histogram of the number of LT-encoded symbols needed to be transmitted such that all original symbols are recovered

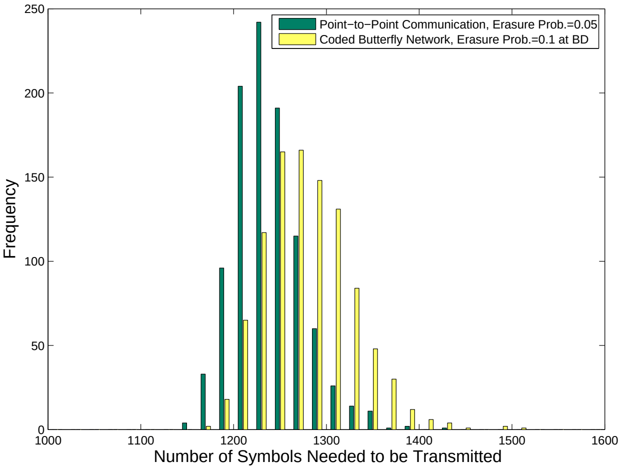

Figure 5.7: Comparison of histograms of the number of LT-encoded symbols needed to be transmitted such that all original symbols are recovered in two cases, point-to-point communication with the erasure probability of 0.05 and coded butterfly network with the erasure probability of 0.1 at BD

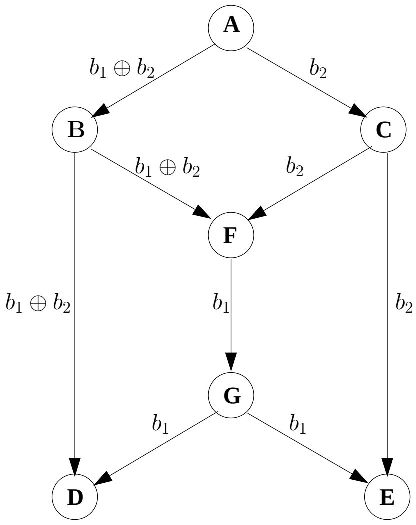

Figure 5.8: Network coding in a butterfly network when only BD is erasure-prone

This solution can be performed by the source alone. When the source A is informed by B that there are severe erasures at BD, it simply transmits $b_1 + b_2$ instead of b_1 to B while other nodes just work as usual. In general, this solution is applicable when erasures occur along a single edge, with the transmission pattern depending on which edge is erasure-prone, as shown in Table 1.

Table 5.1: Recommended Transmission When An Edge is Erasure-prone

Erasure-prone Edge	Choices of Recommended Transmission to (AB, AC)
AB or BF or GE	(b_1, b_2), (b_2, b_1), $(b_1 + b_2, b_1)$, $(b_1 + b_2, b_2)$
AC or CF or GD	(b_1, b_2), (b_2, b_1), $(b_1, b_1 + b_2)$, $(b_2, b_1 + b_2)$
BD	$(b_1 + b_2, b_1)$, $(b_1 + b_2, b_2)$
CE	$(b_1, b_1 + b_2)$, $(b_2, b_1 + b_2)$
FG	(b_1, b_2), (b_2, b_1)

The next section deals with a more general case in which more than one edge is erasure-prone.

5.6 The Cooperative Solution Performed by the Source and the Relay

As an example, consider the case when both the edges BD and CE are erasure-prone. In this case, we cannot find a solution from the previous section that satisfies both receivers. If A chooses to transmit $(b_1 + b_2, b_2)$ to (AB, AC), the receiver D is satisfied but E still suffers from the degree distribution distortion.

It can be imagined that the ideal solution can be found such that, instead of transmitting b_1 and b_2 with the robust soliton distribution, we use another degree distribution $\nu(i)$ which, after being distorted by erasures, becomes the robust soliton distribution. However, such a distribution is very difficult, if not impossible, to be found. Indeed, it is proven in a similar work [64] that one cannot find a degree distribution $\nu(i)$ for b_1 and b_2 such that $b_1 + b_2$ follows the robust soliton distribution.

Since we cannot achieve this ideal solution, we will offer a cooperative scheme performed by the source node A and the relay node F that corrects the degree distribution distortion only in the positions that most affect the performance. Those positions are at degrees 2, 4, 44, and 84.

The severe distortion at 4, 44, and 84 is due to the high probability that b_1 and b_2 have the degrees of 2 or 42, causing $b_1 + b_2$ to have the degree of 4, 44, or 84 with higher probability than what is required, whereas the distortion at 2 is due to the fact that $b_1 + b_2$ cannot have the degree 2 unless both b_1 and b_2 have the degree of 1, which is unlikely.

According to our cooperative scheme, the distortion at 44 and 84 is reduced by applying a buffering scheme at the source. The scheme arranges the LT-encoder output in such an order that b_1 and b_2 with degrees of 2 and 42, 42 and 2, or 42 and 42 are not allowed to be simultaneously transmitted and mixed at the relay thereafter, as implemented in Step 4) of Algorithm 1. In addition, the distortion at 2 and 4 is corrected by selectively discarding some symbols at the relay, i.e., when both b_1 and b_2 have the degree of 2, there is a probability p_c that the relay performs network coding and a probability $1 - p_c$ that either b_1 or b_2 is transmitted while the other is discarded. This will relieve the excess of symbols with degree 4 and the shortage of those with degree 2. The scheme is implemented in Algorithm 2.

Algorithm 1 *The buffering scheme performed by the source*

Let

- $S_l = \begin{cases} 1 \textit{ if the switch is pushed to the left buffer} \\ 0 \textit{ if the switch is pushed to the right buffer} \end{cases}$,
- λ_n *be the LT-encoder output at the discrete time* $n = 0, 1, 2, ..., N_{max}$*,*
- $d(\lambda_n)$ *be the degree of* λ_n*,*
- N_B *be the size of each buffer,*
- $B_l(m), m = 0, 1, 2, ..., N_B - 1$ *be the* m^{th} *element in the left buffer such that* $B_l(m)$ *precedes* $B_l(m+1)$*,*
- $B_r(q), q = 0, 1, 2, ..., N_B - 1$ *be the* q^{th} *element in the right buffer such that* $B_r(q)$ *precedes* $B_r(q+1)$*,*
- π_l*,* π_r *be the pointers of the left and the right buffer, respectively,*
- *and* b_1*,* b_2 *be the current symbol to be transmitted to the edges* AB *and* AC*, respectively,*

```
1) Initialize
    $n := 0$
    $S_l := 1$
    $B_l(0) := \lambda_0$
    $\pi_l := 1$
    $\pi_r := 0$
    $\{B_l(m) | m = 1, 2, ..., N_B - 1\} := \emptyset$
    $\{B_r(q) | q = 0, 1, 2, ..., N_B - 1\} := \emptyset$
2) $n := n + 1$
3) if $S_l = 0$ {
        $S_l := 1$
        *if* $\pi_l < N_B$ {
            $B_l(\pi_l) := \lambda_n$
            $\pi_l := \pi_l + 1$ }}
*4) while* $S_l = 1$ {
        *if* $(d(\lambda_n), d(B_l(\pi_r))) \notin \{(2, 42), (42, 2), (42, 42)\}$ {
            $S_l := 0$
            *if* $\pi_r < N_B$ {
                $B_r(\pi_r) := \lambda_n$
                $\pi_r := \pi_r + 1$ }}
        *else* {
            *if* $\pi_l < N_B$ {
                $B_l(\pi_l) := \lambda_n$
                $\pi_l := \pi_l + 1$ }}}
*5) if the channel access is allowed* {
        $b_1 := B_l(0)$
        $b_2 := B_r(0)$
        $B_l(m) := B_l(m + 1),\ m = 0, 1, 2, ..., N_B - 1$
        $B_r(q) := B_r(q + 1),\ q = 0, 1, 2, ..., N_B - 1$
        $\pi_l := \pi_l - 1$
        $\pi_r := \pi_r - 1$
        *Transmit* $b_1$ *and* $b_2$. }
*6) if* $n < N_{max} - 1$ {
        *Go back to 2).* }
    *else* {
        *Exit.* }
```

Algorithm 2 *The discarding scheme performed by the relay*

Let

- b_1, b_2 *be the current symbol received by* F *from the edges* BF *and* CF, *respectively,*

- *$d(b_n)$ be the degree of b_n, $n = 1, 2$*
- *and $p_c \in [0, 1]$ be a design parameter used as the probability that F performs network coding.*

```
1) if $(d(b_1), d(b_2)) \neq (2, 2)$ {
        Change the header and transmit $b_1 \oplus b_2$ }.
    else {
        Generate a uniformly random number $r_1$ in the range [0,1].
        if $r_1 < p_c$ {
            Change the header and transmit $b_1 \oplus b_2$ }.
        else {
            Generate a uniformly random number $r_2$ from the set $\{0, 1\}$.
            if $r_2 = 0$ {
                Transmit $b_1$ }
            else {
                Transmit $b_2$ }}}
2) Repeat 1) when new $b_1$ and $b_2$ arrive.
```

From Step 3) in Algorithm 1, we can see that when the previous switch position is at the right buffer ($S_l = 0$), it will always be turned to the left one ($S_l = 1$) as the current symbol arrives. On the other hand, in Step 4), the switch position will only change from left to right only if this does not create the degree distribution pair we aim to avoid.

Note that the information regarding the linear combination of original symbols for each LT-coded output is contained in the header. Therefore, in Algorithm 2, the header must be changed if we transmit $b_1 \oplus b_2$.

5.7 Results, Conclusions, and Future Works

Figure 9 compares the histograms of the number of symbols needed to be transmitted by the source such that all original symbols are recovered in two cases, without the proposed algorithm and with Algorithm 1. We can see that Algorithm 1 reduces the variance of the number of required symbols, thus making the histogram of the latter case more concentrated near the middle at 1270. When both algorithms are applied, as shown in Fig. 10, the histogram resembles a left-shifted version of that in Fig. 9 when only Algorithm 1 is applied. Instead of simple histograms, Figure 11 plots normalized cumulative histograms to clearly show that less symbols are needed to be transmitted when both algorithms are applied. We can conclude that our cooperative scheme improves the receiving performance, not only when the erasure probability at BD is 0.1, but also when it is 0.2 and 0.05. The larger the erasure probability, the greater the improvement.

In a more complicated network, a node can act as both a relay for upstream nodes and a source for downstream ones. Therefore, the subtree analysis as suggested in [14] is needed to identify whether a given node's buffering scheme should follow Algorithm 1, Algorithm 2, or a modified algorithm combining both of them. In addition, the relationship between erasure probabilities in all edges and the suitable parameter p_c used in Algorithm 2 should be studied further.

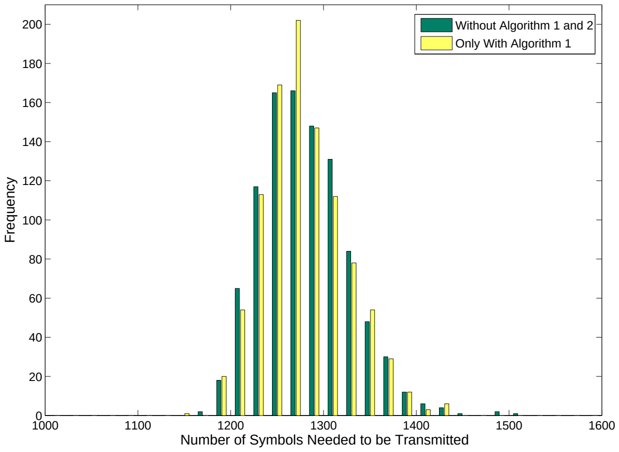

Figure 5.9: Comparison of histograms of the number of LT-encoded symbols needed to be transmitted in a coded butterfly network with the erasure probability of 0.1 at BD such that all original symbols are recovered in two cases, without using the proposed algorithm and with Algorithm 1

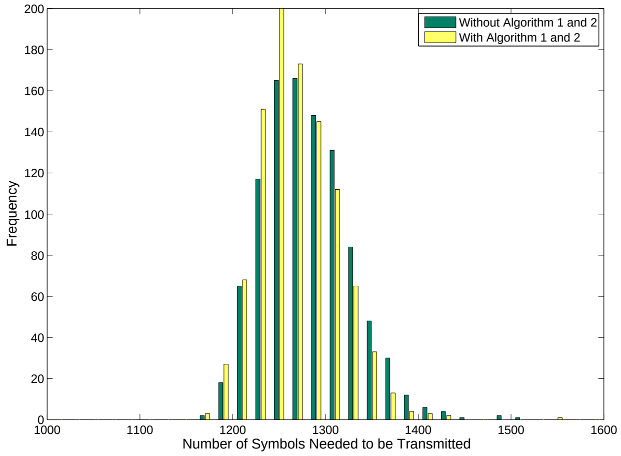

Figure 5.10: Comparison of histograms of the number of LT-encoded symbols needed to be transmitted in a coded butterfly network with the erasure probability of 0.1 at BD such that all original symbols are recovered in two cases, without using the proposed algorithm and with Algorithms 1 and 2

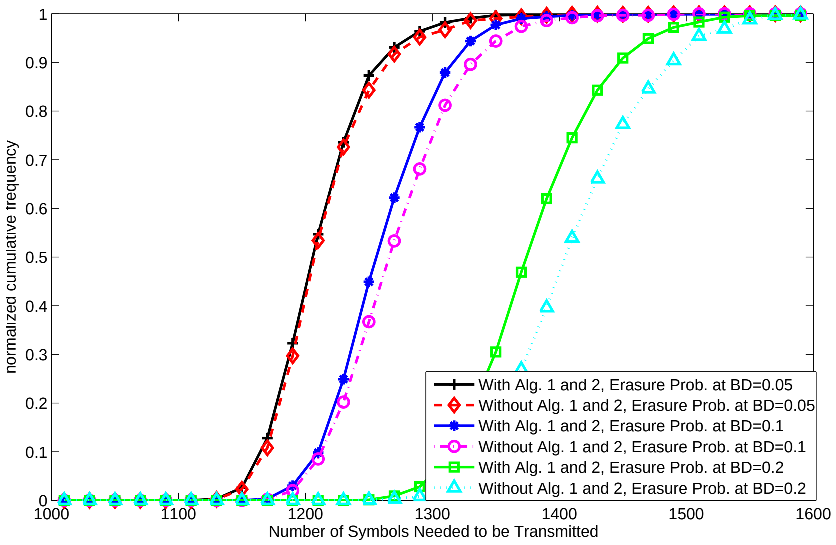

Figure 5.11: Comparison of normalized cumulative histograms of the number of LT-encoded symbols needed to be transmitted in a coded butterfly network with varying erasure probability at BD such that all original symbols are recovered in two cases, without using the proposed algorithm and with Algorithms 1 and 2

Part III

Wireless Physical-layer Secret-key Generation (WPSG) and Network Coding Techniques for Security Enhancement

Containing in this part are two network-coding-related ideas used for security enhancement of wireless physical-layer secret-key generation (WPSG). The first one employs network coding in the security protocol for pilot symbol transmission in WPSG. The second one adopts the secret sharing concept used in secure network coding as the basis of what we call "physical-layer key encoding." With this encoding, the eavesdropper may correctly estimate some key symbols, yet knows nothing about the secret message. These two points are discussed in Chapter 6 and 7, respectively.

Some other aspects of WPSG are also discussed. In Chapter 6, an information theoretic analysis of key generation, key extension in relay networks, and some other security protocols are presented. In Chapter 7, the scalable security concept is formally derived and applied to WPSG.

Chapter 8 summarizes all topics discussed so far and gives some ideas for further research.

Chapter 6

Wireless Physical-layer Secret-key Generation (WPSG) in Relay Networks: Key Generation Limits, Physical Key Encoding, and Security Protocol

A physical-layer security scheme based on mutual channel-state-information (CSI) [1], [58] is considered in this chapter. In undertaking to describe the recent development in our own research, we find ourselves obliged to begin with the basic components of cryptosystems in general. Section 6.1 discusses some general ideas and concepts in cryptology and introduces the cryptosystem model of wireless physical-layer secret-key generation (WPSG). Section 6.2 gives some information theoretic limits relevant to the key generation process in the case of direct communication without relays as well as some simulation results. After that, Section 6.3 extends our analysis regarding the amount of generated key further to the cases in which relay nodes are present between the transmitter and the receiver. Then, Section 6.4 investigates the rate of key generation.

It would be insufficient to talk only about how much or how long the key can be generated in a cryptosystem without considering the possibility that the enemy cryptanalyst has an access to the key.

All the sections mentioned so far focus on how much, or how long, the key can be generated, without considering the possibility that the enemy cryptanalyst can predict some parts of the key. In case there is such possibility, Section provides a countermeasure by means of what we call "physical key encoding."

6.1 Cryptosystem of Wireless Physical-layer Secret-key Generation (WPSG)

Massey [55] suggests a model of a secret-key cryptosystem as shown in Fig. 1. Its concept of security is based on Shannon's idea of perfect secrecy, which means that, for a plain text $\mathbf{X}$ and its cryptogram $\mathbf{Y}$, $P(\mathbf{X} = \mathbf{x}|\mathbf{Y} = \mathbf{y}) = P(\mathbf{X} = \mathbf{x})$ for all possible plain texts $\mathbf{x} = [x_1, x_2, ..., x_M]$ and cryptograms $\mathbf{y}$. In this case, neither the knowledge of the cryptogram $\mathbf{y}$ nor large computational power can help an enemy cryptanalyst to decrypt the message $\mathbf{x}$, unless he or she knows the secret key.

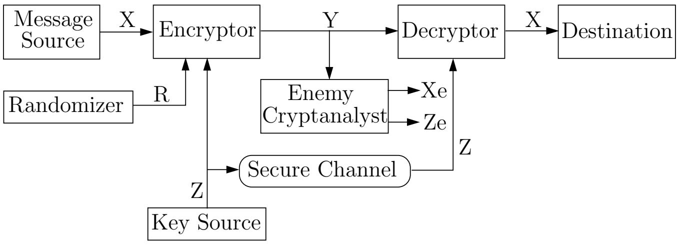

Figure 6.1: A secret-key cryptosystem

In Massey's generalized model, the encryptor mixes the plain text $\mathbf{X}$ with the random message $\mathbf{R}$ and the secret key $\mathbf{Z}$ to achieve perfect secrecy. However, some systems, such as the "one-time pad," which will be discussed later, do not require $\mathbf{R}$. In such cryptosystems, the major difficulty in the implementation lies in the secure distribution of the key.

The scope of this thesis is on the new idea of transforming wireless channel state information (CSI) into secret keys, which will be called wireless physical-layer secret-key generation (WPSG) from now on. It is widely known that wireless channel coefficients, characterized by their phases and amplitudes, depend heavily on the location, the environment, and the movement of the transmitter and the receiver to the extent that other terminals except the two can predict almost nothing about their channel parameters, and hence their secret key. The generation of the secret key consists of two steps, deriving the channel estimates before quantizing them into secure key symbols. It is important to distingish WPSG from the term ”physical layer security” used in [59], which requires that the legitimate users' channels have SNR advantage over those of eavesdroppers.

Channel estimates can be derived using a known pilot sequence, which is transmitted back and forth between the transmitter and the receiver such that they can learn about channel coefficients from the symbols distorted by the channel. The outcome of the channel estimation process is a set of complex channel coefficients which must be quantized into secret key symbols, as shown in Fig. 2. The process of key generation is discussed in detail in [56], [1]. The amount of generated key will determine whether our transmission is secure or not.

6.2 Information Theoretic Limits of the Key Generation

This section studies the amount of key expected to be generated from wireless channels. When there is only one antenna each for the transmitter and the receiver, the channel is described as single-input single-output (SISO) or a scalar channel. When each of the transmitter and the receiver have more than one antenna, secret key can be generated from more than one channel. These channels are said to be multiple-input multiple-output (MIMO) or vector channels. A scalar channel can be considered a special case of vector channels.

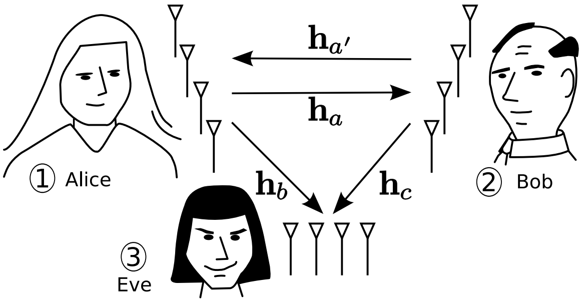

Figure 6.2: A generic communication system model

Now let us consider a communication system model in Fig. 6.2. In this case, there are three parties involved. Alice and Bob are a legitimate transmitter-receiver pair who generate secret key for their secure communication from reciprocal channel vectors $\mathbf{h}_a$ and $\mathbf{h}_{a'}$ where $\mathbf{h}_a = \mathbf{h}_{a'}$, whereas Eve is an eavesdropper who tries to predict the secret key generated by Alice and Bob by using information from channel vectors $\mathbf{h}_b$ and $\mathbf{h}_c$. When Eve is closely located to either Alice or Bob, there might be correlation between $\mathbf{h}_c$ and $\mathbf{h}_{a'}$ or between $\mathbf{h}_b$ and $\mathbf{h}_a$, respectively, enabling her to estimate some key. According to [56, 57], when there are many scatterers, e.g. if the number of wireless multi-paths between each transmit-receive antenna pair is more than 10, the referred correlation is negligible when the distance between Eve and Alice or Bob is larger than one wavelength. However, when there is only one or two multi-paths, the correlation is significantly high.

In [56], two rigorous metrics have been developed for quantifying the information theoretic limits of key generation in the scenario depicted in Fig. 6.2, where Alice and Bob are legitimate users and Eve is a potential eavesdropper. Generalized complex vector channels are considered, where a reciprocal channel $h_a = h_{a'}$ links Alice and Bob, and h_b and h_c are estimated by and convey information to Eve. Given the users have noisy estimates of the channels (denoted $\hat{h}_a$, $\hat{h}_{a'}$, $\hat{h}_b$, and $\hat{h}_c$), we refer to available key bits I_K as the maximum number of independent key bits that can be generated per channel observation, given by $I_K = I(h_a; h_{a'})$, where $I(\cdot;\cdot)$ denotes mutual information. Likewise, the maximum number of independent key bits that can be generated and are secure from an eavesdropper are the secure key bits $I_{SK} = I(\hat{h}_a, \hat{h}_{a'}|\hat{h}_b, \hat{h}_c)$. In [**?**], closed-form expressions for I_K and I_{SK} are derived for correlated complex Gaussian vector channels.

To illustrate key generation in Fig. 6.2, consider a simple scenario with scalar channels. Alice sends a pilot signal x to Bob, who derives the channel estimate $\hat{h}_a$ of the channel h_a from the received signal $y_b = h_a x + n_b$, where n_b denotes complex Gaussian noise at Bob. After that, Bob sends x to Alice, who derives the estimate $\hat{h}_{a'}$ of $h_{a'}$ in a similar manner. The number of available key bits I_K per channel observation that can be generated by Alice and Bob is given by $I_K = I(\hat{h}_a; \hat{h}_{a'})$. If the time between Alice's transmission and Bob's is short, we can assume reciprocity or $h_a = h_{a'}$. Assuming further that h_a is Rayleigh-distributed with a standard deviation of 0.5, we obtain a simulation result in Fig. **??** showing the relationship between I_K and the signal-to-noise ratio, which is the ratio of the power of x to the Gaussian noise power at Bob and Alice. We also derive the results when the key is derived from the envelope of channel parameters only, such that $I_K = I(|\hat{h}_a|; |\hat{h}_{a'}|)$.

6.3 Possible Key Extensions

In a generalized wireless network, the length of the key can be extended by having it generated from several transmission paths instead of only one. Although it is obvious that the total key length is the summation of the length from all paths, the key length from each path is not easily derived when there are relays in between. For instance, if there is one relay in the path, as illustrated in Fig. 6.3, the channel parameter h_a between the transmitter and the receiver becomes $h_{aT} = h_{a1} \cdot h_{a2}$, which is the product of two complex Gaussian random variables. If we let the real part of h_{aT}, h_{a1}, and h_{a2} be h_{aTr}, h_{a1r}, and h_{a2r}, respectively, and the imaginary part be h_{aTi}, h_{a1i}, and h_{a2i}, respectively, we have

$$h_{aTi} = h_{a1i} h_{a2r} + h_{a1r} h_{a2i}. \tag{6.1}$$

If we denote the random variables representing the random processes that generate h_{aTi}, $h_{a1i} h_{a2r}$, and $h_{a1r} h_{a2i}$ by Z, X, and Y respectively, the probability density function

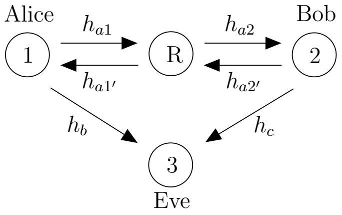

Figure 6.3: A communication system model with one relay

$f_Z(z)$ will be the convolution of $f_X(x)$ and $f_Y(y)$.

$$f_Z(z) = \int_{-\infty}^{\infty} f_X(z-y) f_Y(y) dy \ . \tag{6.2}$$

In our case, X and Y have the same probability density function

$$f_X(x) = f_Y(x) = 4\frac{K_0(4x)}{\pi} \ , \tag{6.3}$$

where $K_0(x) = \int_0^\infty \frac{\cos(xt)}{\sqrt{t^2+1}} dt$ is a modified Bessel function of the second kind. From eqs. (6.2) and (6.3), we can derive the distribution of the imaginary part, which is the same as that of the real one, of channel parameters in the one-relay case. Our simulation result in Fig. 6.4 shows that, due to the altered distribution of channel parameters, the number of possible key bits in the one-relay case is less than the direct communication case. Note that this is just the comparison between two exemplary cases. The consideration regarding the mobility effect on the key generation rate is taken into account in the next subsection.

6.4 Investigation of Key Generation Rate

In a direct communication, if the transmitter and the receiver have not moved, no new key can be generated since the channel is static. Therefore, the key generation rate depends heavily on the movements of transmitter and receiver. Assuming that channel parameters are sampled once every sampling time t_s, the average key generation rate becomes

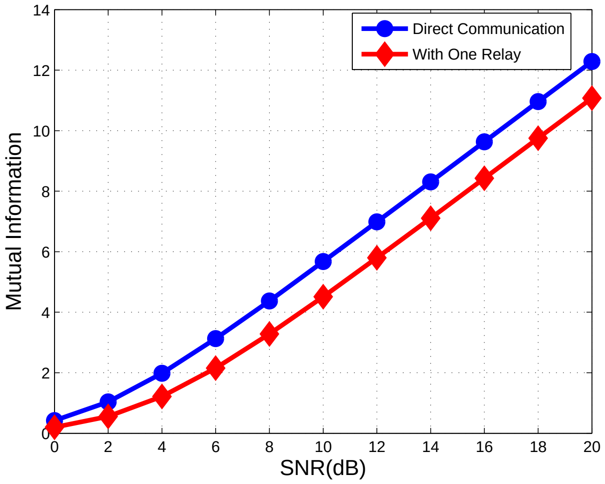

Figure 6.4: A simulation result showing mutual information between the channel estimates of Alice and Bob in two cases, direct communication and communication with one relay

$$R_k = \lim_{n\to\infty} \frac{\sum_{i=0}^{n-1} I_k(it_s)}{nt_s} , \tag{6.4}$$

where

$$I_k(it_s) = I\left(\hat{h}_a(it_s); \hat{h}_{a'}(it_s) \;\middle|\; \hat{h}_a((i-1)t_s), \hat{h}_{a'}((i-1)t_s), ..., \hat{h}_a(0)), \hat{h}_{a'}(0)\right). \tag{6.5}$$

The mutual information in (6.5) depends on how far the transmitter and the receiver can travel within t_s. It is therefore related to the velocity and the mobility model if the value is to be obtained by simulation.

6.5 Secure Key Symbols and Vulnerable Key Symbols

We can imagine that when an eavesdropper is located very close to either the transmitter or the receiver, our scheme is not totally secure since there may be correlation between.... This is illustrated in Fig.

6.6 Introduction

Massey [55] suggests a model of a secret-key cryptosystem as shown in Fig. 1. Its concept of security is based on Shannon's idea of perfect secrecy, which means that, for a plain text $\mathbf{X}$ and its cryptogram $\mathbf{Y}$, $P(\mathbf{X} = \mathbf{x}|\mathbf{Y} = \mathbf{y}) = P(\mathbf{X} = \mathbf{x})$ for all possible plain texts $\mathbf{x} = [x_1, x_2, ..., x_M]$ and cryptograms $\mathbf{y}$. In this case, neither the knowledge of the cryptogram $\mathbf{y}$ nor large computational power can help an enemy cryptanalyst to decrypt the message $\mathbf{x}$, unless he or she knows the secret key.

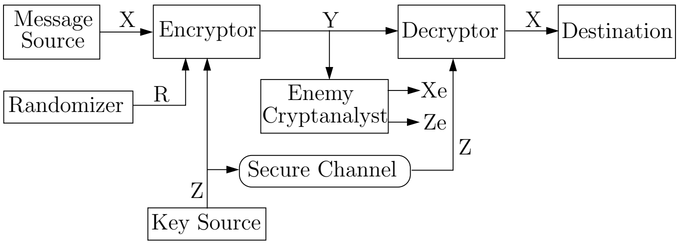

Figure 6.5: A secret-key cryptosystem

In Massey's generalized model, the encryptor mixes the plain text $\mathbf{X}$ with the random message $\mathbf{R}$ and the secret key $\mathbf{Z}$ to achieve perfect secrecy. However, some systems, such as the "one-time pad," which will be discussed later, do not require $\mathbf{R}$. The major difficulty in the implementation of such cryptosystems lies in the secure distribution of the key. There is recently a new idea of transforming wireless channel state information (CSI) into secret keys. It is widely known that wireless channel coefficients, characterized by their phases and amplitudes, depend heavily on the location, the environment, and the movement of the transmitter and the receiver to the extent that other terminals except the two can predict almost nothing about their channel parameters, and hence their secret key. The generation of the secret key consists of two steps, deriving the channel estimates before quantizing them into secure key symbols. We refer to this technique as "wireless physical-layer secret-key generation." This must be distingished from the term "physical layer security" used in [59], which requires that the legitimate users' channels have SNR advantage over those of eavesdroppers.

Channel estimates can be derived using a known pilot sequence, which is transmitted back and forth between the transmitter and the receiver such that they can learn about channel coefficients from the symbols distorted by the channel. The outcome of the channel estimation process is a set of complex channel coefficients which must be quantized into secret key symbols, as shown in Fig. 2. The process of key generation is discussed in detail in [56], [1].

Since, in a generalized wireless network, there can be several channels that the pilot sequence can take to travel from one node to another, the technique implicitly assumes a bi-lateral agreement between the two nodes regarding the channel to be used for key generation. Earlier works did not tell how to form such an agreement in a secure manner, we will do it in the next section.

Although the enemy cryptanalyst is not located at the same place as the receiver during transmission, he or she may have been there before and it is possible that channel coefficients (especially the amplitudes) do not change much. Therefore, it is wise to assume that he or she can correctly predict some key symbols and we should try to find some countermeasures. To do so, we use a similar concept to Shamir's secret sharing [4] and Cai and Yeung's secure network coding [60]. We call our scheme ”physical-layer key encoding,” which is designed such that, up to a certain threshold, partial knowledge of key symbols derived from the channel leaves the encoded key completely undetermined. This is performed at the transmitter prior to the one-time pad encryptor block in our wireless physical-layer secret-key cryptosystem shown in Fig. 2 and will be discussed in detail in Section III.

In Section IV, we suggest how to set the number of vulnerable bits based on an equivalent model of the eavesdropper. Section V then concludes the paper.

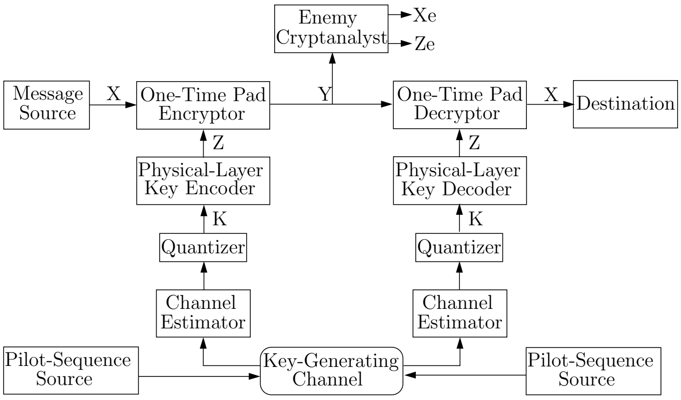

Figure 6.6: A modified secret-key cryptosystem based on mutual CSI with physical-key encoding and decoding

6.7 Physical-Layer Key Encoding for One-Time-Pad Encryptor

In this section, we shall present physical-layer key encoding which generates "the encoded key" $\mathbf{Z} = [Z_1, Z_2, ..., Z_J]$ as a codeword from "an original quantized key" $\mathbf{K} = [K_1, K_2, ..., K_{I_K}]$ and feeds it into the one-time pad encryptor. The encoder aims at protecting the secret key in case the enemy can correctly estimate some channel coefficients, and hence some original quantized key symbols. Three parameters, I_K, I_{SK}, and I_{VK} are of interest to the encoder. The first one, I_K, is the number of symbols that can be generated by the quantizer in Fig. 2. The second one, I_{SK}, is the number of secure key symbols that the enemy cannot correctly estimate, whereas the third, I_{VK}, is the number of vulnerable ones that he or she can correctly estimate, such that $I_K = I_{SK} + I_{VK}$.

The information-theoretic derivation of I_K, I_{SK}, and I_{VK} is discussed in [56] but not in this paper, where we are more interested in the following questions: Given I_K, I_{SK}, and I_{VK}, what is the important property of the physical-layer key encoding that ensures perfect secrecy as well as efficiency? How can we choose the code rate? And how can we derive the optimal code? Some questions will be answered by theorems 1-3 proposed in this section. Before going that far, we will first describe the one-time pad encryptor.

Consider a non-randomized cipher in which elements in the plaintext $\mathbf{X} = [X_1, X_2, ..., X_M]$, ciphertext $\mathbf{Y} = [Y_1, Y_2, ..., Y_N]$, and secret key $\mathbf{Z} = [Z_1, Z_2, ..., Z_J]$ all take values in the L-

ary alphabet and $J = N = M$. Suppose that the key is chosen to be completely random, i.e., $P(Z_i = z) = L^{-M}$, $i = 1, 2, ..., M$, for all possible values z of the secret key, and that the enciphering transformation is

$$Y_i = (X_i + Z_i) \bmod M, \; i = 1, 2, ..., M. \tag{6.6}$$

Since, for each possible choice x and y of X_i and Y_i, respectively, there is a unique z such that $Z_i = z$ satisfies (7.2), it follows that $P(Y_i = y|X_i = x) = L^{-M}$ for every particular y and x, no matter what the statistics of X_i may be. Thus, X_i and Y_i are statistically independent, and hence this system provides perfect secrecy [55]. The system is called a modulo-L Vernam system or one-time pad and is used in our model in Fig. 2 to combine the message and the encoded key together.

Since, out of the total I_K quantized key symbols, I_{VK} symbols are vulnerable symbols, we can see that, had a one-time pad encryptor been used without physical-key encoding, I_{VK} ciphertext symbols would have been decrypted by the eavesdropper. Thus, in order to construct a secure Y_1, we use the following linear combination for Z_1.

$$Z_1 = (K_1 + K_2 + ... + K_{I_{VK}+1}) \bmod M \tag{6.7}$$

After substituting (7.3) into (7.2) using $i = 1$, we can see that even if the set of all vulnerable key symbols is a subset of $\{K_1, K_2, ..., K_{I_{VK}+1}\}$, there is still one symbol that is unknown to the eavesdropper. If every key symbol is statistically independent of others, perfect secrecy of Y_1 is achieved.

Now, in order to construct Z_2, Z_3, and so on, we perform a linear combination of I_{VK} key symbols similar to (7.3). Therefore, our physical-layer key encoding can be defined by a linear block code C_p transforming an I_K-tuple $\mathbf{K}$ over $GF(q^{I_K})$ of key symbols obtained from the quantizer into an M-tuple codeword $\mathbf{Z}$ over $GF(q^M)$. We propose the following theorem providing two necessary and sufficient conditions for perfect secrecy.

Theorem 1 *If I_{VK} out of I_K physical-layer key symbols generated by the quantizer can be correctly estimated by the eavesdropper, the cryptosystem in Fig. 2 still maintains perfect secrecy if and only if each member in the I_K-dimensional vector $\mathbf{K}$ is independent of one another and the physical-layer code C_p has the following properties.*

1.1. Every codeword has a Hamming weight of at least $I_{VK} + 1$.

1.2. Every linear combination of any subset of codewords gives a Hamming weight of at least $I_{VK} + 1$.

Proof From earlier discussion it should be clear that the first condition is necessary. The necessity of the second condition can be proved by contradiction as follows. If the combination of ν codewords $\sum_{i=1}^{\nu} Z_i$ gives a Hamming weight of $I_{VK} + 1 - \delta$, where δ is a positive integer, the eavesdropper who calculates $\sum_{i=1}^{\nu} Y_i$ may know the exact value of $\sum_{i=1}^{\nu} Z_i$ since the Hamming weight of the combination does not exceed the number of vulnerable symbols. If $\sum_{i=1}^{\nu} Z_i$ is known, perfect secrecy is not achieved because these ν encoded key symbols are not independent.

As for the sufficiency, we can also prove it by contradiction. Now, we have to prove that if perfect secrecy is not achieved, either the condition 1.1 or 1.2 is not satisfied. By definition, perfect secrecy in a one-time-pad system is not achieved only if either 1) at least one Z_i, $i = 1, 2, ..., M$ is known or 2) any linear combination of some Z_i is known implying linear dependence among key symbols. Since 1) and 2) will not happen if the condition 1.1 and 1.2 are, respectively, satisfied, the two conditions are sufficient.

Now, we focus our attention on the special case when $\mathbf{K}$ and $\mathbf{Z}$ are vectors of binary data and present the second theorem.

Theorem 2 *If $\mathbf{K} \in GF(2^{I_K})$, in order to generate $\mathbf{Z} \in GF(2^n)$, which is a codeword of n encoded key bits providing perfect secrecy in our system, the following conditions on I_K are necessary and sufficient.*

2.1. If $I_{VK}+1$ is even,

$$I_K \geq \frac{(n+1)}{2}(I_{VK}+1) \tag{6.8}$$

2.2 If $I_{VK}+1$ is odd,

$$I_K \geq \frac{(n+1)}{2}(I_{VK}+1)+\frac{(n-1)}{2} \tag{6.9}$$

Proof We prove this theorem by mathematical induction. We first demonstrate that the theorem is valid for $n = 1$ and $n = 2$ before showing that if the theorem is valid for any n, it will hold true for $n+1$. The case of $n = 1$ can be easily validated by substituting it into (3) and (4) and observing that the resulting I_K corresponds to that in Theorem 1.

Given Z_1 in Eq. (7.3), when $I_{VK}+1$ is an even number. Let

$$Z_2 = K_{\frac{1}{2}(I_{VK}+3)} \oplus K_{\frac{1}{2}(I_{VK}+5)} \oplus ... \oplus K_{\frac{3}{2}(I_{VK}+1)}. \tag{6.10}$$

Now, the generator matrix generating Z_1 and Z_2 can be written as follows.

$$\mathbf{G_p} = \begin{bmatrix} \overbrace{1\,1\,...\,1\,1\,1\,...\,1}^{I_{VK}+1}\ \overbrace{0\,0\,...\,0\,0\,0\,...\,0}^{I_K-I_{VK}-1} \\ \underbrace{0\,0\,...\,0}_{\frac{1}{2}(I_{VK}+1)}\underbrace{1\,1\,...\,1\,1\,1\,...\,1}_{I_{VK}+1}\ 0\,0\,...\,0 \end{bmatrix}^T = [\mathbf{g}_1\ \mathbf{g}_2] \tag{6.11}$$

such that

$$\mathbf{Z} = [Z_1, Z_2] = \mathbf{K}\cdot\mathbf{G_p}, \tag{6.12}$$

where

$$\mathbf{K} = [K_1, K_2, ..., K_{I_K}]. \tag{6.13}$$

When $n = 2$, i.e., only two encoded key bits are to be constructed, we can see from (6.11) that $I_K = \frac{3}{2}(I_{VK}+1)$ original key bits from the quantizer are sufficient, i.e., the zero padding after the $\frac{3}{2}(I_{VK}+1)^{th}$ is trivial. This sufficient value of I_K holds for any given $\mathbf{g}_1$ with Hamming weight of $I_{VK}+1$ because, in order to choose $I_{VK}+1$ rows of $\mathbf{g}_2$ with 1-valued elements, we should have $\frac{I_{VK}+1}{2}$ rows where those elements of $\mathbf{g}_1$ in the same positions have the value 1. In other words, if we pile $\mathbf{g}_2$ up onto $\mathbf{g}_1$, at most $\frac{I_{VK}+1}{2}$

positions of 1-valued elements may overlap. If there are more overlapping positions, the second condition in Theorem 1 will be violated. If there are less overlapping positions, no condition is violated, but it is not an economical use of original quantized key bits because I_K must now be greater than $\frac{3}{2}(I_{VK}+1)$.

We can therefore conclude that with $n=2$ and an even $I_{VK}+1$, $I_K \geq \frac{(n+1)}{2}(I_{VK}+1)$ is a necessary and sufficient condition on I_K. If we follow the same line of reasoning with $n>2$, we see that when each $\mathbf{g}_{i+1}$ is piled up onto the heap of $\mathbf{g}_j$, $j=1,2,...,i$, the most economical way in terms of the number of original quantized key bits used is still to have $\frac{I_{VK}+1}{2}$ 1-valued elements in overlapped positions with any 1-valued elements in any of those $\mathbf{g}_j$, $j=1,2,...,i$. This means at least $\frac{I_{VK}+1}{2}$ more original quantized key bits are needed for each increment of n, thus completing the proof of 2.1.

A similar line of reasoning can be used to prove 2.2. With odd I_K+1, $\mathbf{G_p}$ in (6) becomes

$$\mathbf{G_p} = \begin{bmatrix} \overbrace{1\;1\;...\;1\;1\;1\;...\;1}^{I_{VK}+1}\;\overbrace{0\;0\;...\;0\;0\;0\;...\;0}^{I_K-I_{VK}-1} \\ \underbrace{0\;0\;...\;0}_{\frac{1}{2}(I_{VK}+2)}\underbrace{1\;1\;...\;1\;1\;1\;...\;1}_{I_{VK}+1}\;0\;0\;...\;0 \end{bmatrix}^T = [\mathbf{g}_1\;\mathbf{g}_2] \qquad (6.14)$$

With the overlapped positions reduced from $\frac{I_{VK}+1}{2}$ in the even case to $\frac{I_{VK}}{2}$ in the odd case, the value of necessary I_K for each n increases. One can verify Eq. (4) when $n=2$ by looking at the $\mathbf{G_p}$ in (9). With $n \geq 2$, at least $\frac{I_{VK}+2}{2}$ more original quantized key bits are needed for each increment of n, thus completing the proof of 2.2.

The next theorem concerns the asymptotic rate of the code.

Theorem 3 *The minimum asymptotic code rate of C_p as $n \to \infty$ is $\frac{I_{VK}+1}{2}$ if $I_{VK}+1$ is even. Otherwise, it is $\frac{I_{VK}+2}{2}$.*

Proof The code rate is the ratio between the number of originial bits to that of encoded ones. Therefore, the asymptotic code rate as $n \to \infty$ is derived by dividing (3) and (4) by n and finding the limit of the results as as $n \to \infty$.

From the proof of Theorem 2, we have derived our generator matrix prototype of a physical-layer key encoder for any value of I_{VK}, when $I_{VK}+1$ is even or odd in equations (10) or (11), respectively.

$$\mathbf{G_p} = \left[\begin{array}{c} \overbrace{1\,1 \ldots 1\,1 \ldots 1}^{I_{VK}+1}\ \overbrace{0 \ldots 0\,0 \ldots 0\,0\,0 \ldots 0}^{I_K-I_{VK}-1} \\ \underbrace{0\,0 \ldots 0}_{\frac{1}{2}(I_{VK}+1)}\underbrace{1 \ldots 1\,1 \ldots 1}_{I_{VK}+1}\ 0 \ldots 0\,0\,0 \ldots 0 \\ \vdots \\ \underbrace{0\,0 \ldots 0\,0 \ldots 0\,0 \ldots 0\,0 \ldots 0}_{I_K-I_{VK}-1}\underbrace{1\,1 \ldots 1}_{I_{VK}+1} \end{array} \right]^T \tag{6.15}$$

$$\mathbf{G_p} = \left[\begin{array}{c} \overbrace{1\,1 \ldots 1\,1 \ldots 1}^{I_{VK}+1}\ \overbrace{0 \ldots 0\,0 \ldots 0\,0\,0 \ldots 0}^{I_K-I_{VK}-1} \\ \underbrace{0\,0 \ldots 0}_{\frac{1}{2}(I_{VK}+2)}\underbrace{1 \ldots 1\,1 \ldots 1}_{I_{VK}+1}\ 0 \ldots 0\,0\,0 \ldots 0 \\ \vdots \\ \underbrace{0\,0 \ldots 0\,0 \ldots 0\,0 \ldots 0\,0 \ldots 0}_{I_K-I_{VK}-1}\underbrace{1\,1 \ldots 1}_{I_{VK}+1} \end{array} \right]^T \tag{6.16}$$

6.8 The Practical Number of Vulnerable Bits for the Design of Physical-Layer Key Encoding

The analysis given in the last section is based on the assumption that the encoder knows I_{VK}. However, it is still unclear how we can derive I_{VK} in practice. We therefore propose two models of the enemy cryptanalyst, on which our estimate of I_{VK} will be based.

According to Fig. 4 (a), the enemy is modeled to have almost the same structure as the legitimate transmitter and receiver. However, since it can only estimate channel coefficients from an imaginary channel which differs from the key-generating channel used by the legitimate terminals, we propose an equivalent model in Fig. 4 (b). In the equivalent model, the enemy does estimate the key-generating channel, but the quantized key $\mathbf{K}$ is distorted by a binary symmetric channel (BSC), erring each estimated key bit with a probability p. The relationship between p and the I_{VK} previously mentioned is shown in Theorem 4.

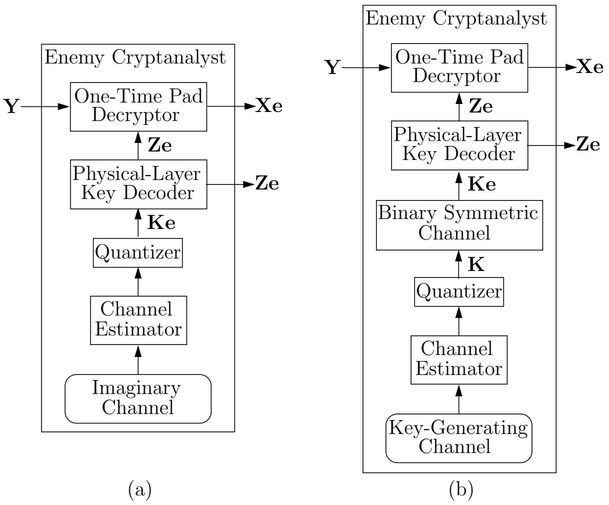

Figure 6.7: The model of an enemy cryptanalyst (a), and its equivalent (b)

Theorem 4 *If the enemy cryptanalyst behaves according to the model in Fig. 4 (b) having p as the error probability of the binary symmetric channel, and the generator matrix prototype in the form of equations (10) or (11) is used, when $I_{VK}+1$ is even or odd, respectively, the following conditions on I_{VK} are sufficient for perfect secrecy.*

4.1. If $I_{VK}+1$ is even,

$$I_{VK}+1 \geq \begin{cases} \lceil -\frac{2}{\log_2(1-p)} \rceil \ , & \textit{if } \lceil -\frac{2}{\log_2(1-p)} \rceil \textit{ is even} \\ \lceil -\frac{2}{\log_2(1-p)} \rceil + 1 \ , & \textit{if } \lceil -\frac{2}{\log_2(1-p)} \rceil \textit{ is odd.} \end{cases} \tag{6.17}$$

4.2. If $I_{VK}+1$ is odd,

$$I_{VK}+1 \geq \begin{cases} \lceil -\frac{2}{\log_2(1-p)} \rceil - 1 \ , & \textit{if } \lceil -\frac{2}{\log_2(1-p)} \rceil \textit{ is even} \\ \lceil -\frac{2}{\log_2(1-p)} \rceil \ , & \textit{if } \lceil -\frac{2}{\log_2(1-p)} \rceil \textit{ is odd,} \end{cases} \tag{6.18}$$

where $\lceil -\frac{2}{\log_2(1-p)} \rceil$ is the smallest integer that is larger than $-\frac{2}{\log_2(1-p)}$.

Proof For perfect secrecy, the probability that the enemy can successfully decrypt x bits in the plaintext is at most $(\frac{1}{2})^x$, which equals the success probability of clueless guess.

Therefore, according to equations (10) or (11), if $x = 1$,

$$\begin{aligned}(1-p)^{I_{VK}+1} &\leq \frac{1}{2} &(6.19)\\ I_{VK}+1 &\geq -\frac{1}{\log_2(1-p)} &(6.20)\end{aligned}$$

Now, if $x = n$, which is the number of bits in the generated codeword as well as the number of bits in the plaintext, and $I_{VK}+1$ is even,

$$(1-p)^{\frac{n+1}{2}(I_{VK}+1)} \leq (\frac{1}{2})^n \tag{6.21}$$

For very large n, (16) becomes

$$\begin{aligned}\lim_{n\to\infty}(1-p)^{\frac{n+1}{2}(I_{VK}+1)} &\leq \lim_{n\to\infty}(\frac{1}{2})^n &(6.22)\\ (1-p)^{\frac{n}{2}(I_{VK}+1)} &\leq (\frac{1}{2})^n &(6.23)\\ I_{VK}+1 &\geq -\frac{2}{\log_2(1-p)} &(6.24)\end{aligned}$$

We can see that, as n increases, the minimal value of $I_{VK}+1$ that should be set also increases. If we denote by $\lceil -\frac{2}{\log_2(1-p)} \rceil$ the smallest integer that is larger than $-\frac{2}{\log_2(1-p)}$, the direct consequence of (19), when $I_{VK}+1$ is constrained to be an even number, will be the condition 4.1.

In case $I_{VK}+1$ is odd, we use the prototype in Eq. (11) and follow the same reasoning.

$$\begin{aligned}(1-p)^{\frac{n+1}{2}(I_{VK}+1)+\frac{n-1}{2}} &\leq (\frac{1}{2})^n &(6.25)\\ \lim_{n\to\infty}(1-p)^{\frac{n+1}{2}(I_{VK}+1)+\frac{n-1}{2}} &\leq \lim_{n\to\infty}(\frac{1}{2})^n &(6.26)\\ (1-p)^{\frac{n}{2}(I_{VK}+2)} &\leq (\frac{1}{2})^n &(6.27)\\ I_{VK}+1 &\geq -\frac{2}{\log_2(1-p)}-1 &(6.28)\end{aligned}$$

This results in the condition 4.2. Therefore, with the same p, we can set $I_{VK}+1$ to be smaller by 1 bit if it is odd than if it is even.

6.9 Discussion and Conclusion

We have proposed a secure protocol to ensure that the legitimate transmitter and receiver generate their secret key from the same physical channel. We have also included physical-layer key encoding into the system to provide perfect secrecy even when some key symbols are correctly estimated by the eavesdropper who knows the code.

We have suggested two simple generating matrix prototypes for our physical-layer key encoding for two specific cases, when $I_{VK}+1$ is even and when it is odd, where I_{VK} is the number of vulnerable key bits. $I_{VK}+1$ is related to I_K, the number of original key bits needed from the quantizer, by Theorem 2. In case $I_{VK}+1$ is unknown, we may use Theorem 4 to derive it from the probability p that the eavesdropper incorrectly estimates a key bit. For example, $I_{VK}+1$ is at least 5 when p is 0.25, yielding an asymptotic code rate of 3, as predicted by Theorem 3.

Chapter 7

Physical-layer Key Encoding for Wireless Physical-layer Secret-key Generation (WPSG) with Unequal Security Protection (USP)

7.1 Scalable Security in Secure Network Coding

The scalable security concept has been earlier considered by several researchers [76–79]. Almost all of them, however, use the partial encryption technique such that only the important part of data is encrypted. Since our focus is on information-theoretic security, we like to point out that the problem is not really a matter of black or white. It is not that one only has two choices whether to encrypt or not. We can encrypt the most important part with the strictest form of security, which is Shannon security and the less important part with what is called "weak security."

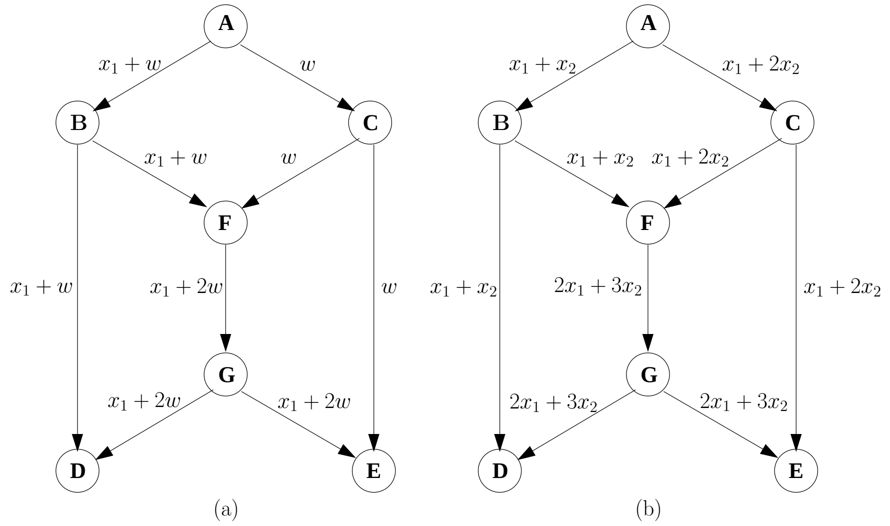

Figure 7.1: Secure network coding in a butterfly network

7.2 Meaningful Information, Shannon Security, Weak Security, and Scalable Security

Definition 7.1 *Consider a set of messages M. Let U and G be subsets of the set containing the multicast information symbols. We say that M has no information about U given G if $I(U; M|G) = 0$. We say that M has no meaningful information about U given G if $I(x_i(t); M|G) = 0$,*

$$s_i \longmapsto [m_1, m_2, ..., m_i] \tag{7.1}$$

7.3 Simplified Fork-rake Networks

In a generalized network having some routers between Alice and Bob, we need a secure protocol for the transmission of pilot symbols for the key generation. To differentiate secure protocols from insecure ones, let us consider a simplified fork-rake network in Fig. **??** as an example. Alice broadcasts a pilot packet x to all relays R_1 to R_n within her transmission range. Each relay R_i receives $h_{ai}x$, where h_{ai} is the channel gain between Alice and the relay and x is the pilot sequence. Using an amplify-and-forward scheme, each relay R_i chooses whether to forward $a_i h_{ai} x$, where a_i is the amplification gain to Bob, or not. Then, Bob receives $\sum_{i \in \mathcal{F}} a_i h_{ai} h_{ib} x$, where h_{ib} is the channel gain between the relay R_i and Bob, whereas $\mathcal{F}$ is the index set of relays that choose to forward the pilot packet. After that, Bob derives the key and transmits x back to every R_i that has previously forwarded the packet to Bob. Such a relay R_i, assuming that the channel gain has not changed yet, receives $h_{ib}x$ and forwards $a_i h_{ib} x$ to Alice, who derives the key from $\sum_{i\in\mathcal{F}} a_i h_{ai} h_{ib} x$.

7.4 Introduction to Wireless Physical-layer Secret-key Generation (WPSG)

Massey [55] suggests a model of a secret-key cryptosystem as shown in Fig. 1. Its concept of security is based on Shannon's idea of perfect secrecy, which means that, for a plain text $\mathbf{X}$ and its cryptogram $\mathbf{Y}$, $P(\mathbf{X} = \mathbf{x}|\mathbf{Y} = \mathbf{y}) = P(\mathbf{X} = \mathbf{x})$ for all possible plain texts $\mathbf{x} = [x_1, x_2, ..., x_M]$ and cryptograms $\mathbf{y}$. In this case, neither the knowledge of the cryptogram $\mathbf{y}$ nor large computational power can help an enemy cryptanalyst to decrypt the message $\mathbf{x}$, unless he or she knows the secret key.

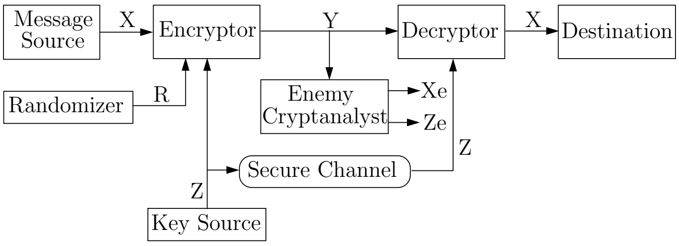

Figure 7.2: A secret-key cryptosystem

In Massey's generalized model, the encryptor mixes the plain text $\mathbf{X}$ with the random message $\mathbf{R}$ and the secret key $\mathbf{Z}$ to achieve perfect secrecy. However, some systems, such as the "one-time pad," which will be discussed later, do not require $\mathbf{R}$. The major difficulty in the implementation of such cryptosystems lies in the secure distribution of the key. There is recently a new idea of transforming wireless channel state information (CSI) into secret keys. It is widely known that wireless channel coefficients, characterized by their phases and amplitudes, depend heavily on the location, the environment, and the movement of the transmitter and the receiver to the extent that other terminals except the two can predict almost nothing about their channel parameters, and hence their secret key. The generation of the secret key consists of two steps, deriving the channel estimates before quantizing them into secure key symbols. We refer to this technique as ”wireless physical-layer secret-key generation.” This must be distingished from the term ”physical layer security” used in [59], which requires that the legitimate users' channels have SNR advantage over those of eavesdroppers.

Channel estimates can be derived using a known pilot sequence, which is transmitted back and forth between the transmitter and the receiver such that they can learn about channel coefficients from the symbols distorted by the channel. The outcome of the channel estimation process is a set of complex channel coefficients which must be quantized into secret key symbols, as shown in Fig. 2. The process of key generation is discussed in detail in [56], [1]. The amount of generated key will determine whether our transmission is secure or not.

7.5 Information Theoretic Limits of the Key Generation

This section studies the amount of key expected to be generated from wireless channels. When there is only one antenna each for the transmitter and the receiver, the channel is described as single-input single-output (SISO) or a scalar channel. When each of the transmitter and the receiver have more than one antenna, secret key can be generated from more than one channel. These channels are said to be multiple-input multiple-output (MIMO) or vector channels. In [?], two rigorous metrics have been developed for quantifying the information theoretic limits of key generation in the scenario depicted in Fig. 6.2, where Alice and Bob are legitimate users and Eve is a potential eavesdropper. Generalized complex vector channels are considered, where a reciprocal channel $h_a = h_{a'}$ links Alice and Bob, and h_b and h_c are estimated by and convey information to

Eve. Given the users have noisy estimates of the channels (denoted $\hat{h}_a$, $\hat{h}_{a'}$, $\hat{h}_b$, and $\hat{h}_c$), we refer to available key bits I_K as the maximum number of independent key bits that can be generated per channel observation, given by $I_K = I(h_a; h_{a'})$, where $I(\cdot;\cdot)$ denotes mutual information. Likewise, the maximum number of independent key bits that can be generated and are secure from an eavesdropper are the secure key bits $I_{SK} = I(\hat{h}_a, \hat{h}_{a'}|\hat{h}_b, \hat{h}_c)$. In [?], closed-form expressions for I_K and I_{SK} are derived for correlated complex Gaussian vector channels.

To illustrate key generation in Fig. 6.2, consider a simple scenario with scalar channels. Alice sends a pilot signal x to Bob, who derives the channel estimate $\hat{h}_a$ of the channel h_a from the received signal $y_b = h_a x + n_b$, where n_b denotes complex Gaussian noise at Bob. After that, Bob sends x to Alice, who derives the estimate $\hat{h}_{a'}$ of $h_{a'}$ in a similar manner. The number of available key bits I_K per channel observation that can be generated by Alice and Bob is given by $I_K = I(\hat{h}_a; \hat{h}_{a'})$. If the time between Alice's transmission and Bob's is short, we can assume reciprocity or $h_a = h_{a'}$. Assuming further that h_a is Rayleigh-distributed with a standard deviation of 0.5, we obtain a simulation result in Fig. **??** showing the relationship between I_K and the signal-to-noise ratio, which is the ratio of the power of x to the Gaussian noise power at Bob and Alice. We also derive the results when the key is derived from the envelope of channel parameters only, such that $I_K = I(|\hat{h}_a|; |\hat{h}_{a'}|)$.

7.6 Introduction

Massey [55] suggests a model of a secret-key cryptosystem as shown in Fig. 1. Its concept of security is based on Shannon's idea of perfect secrecy, which means that, for a plain text $\mathbf{X}$ and its cryptogram $\mathbf{Y}$, $P(\mathbf{X} = \mathbf{x}|\mathbf{Y} = \mathbf{y}) = P(\mathbf{X} = \mathbf{x})$ for all possible plain texts $\mathbf{x} = [x_1, x_2, ..., x_M]$ and cryptograms $\mathbf{y}$. In this case, neither the knowledge of the cryptogram $\mathbf{y}$ nor large computational power can help an enemy cryptanalyst to decrypt the message $\mathbf{x}$, unless he or she knows the secret key.

In Massey's generalized model, the encryptor mixes the plain text $\mathbf{X}$ with the random

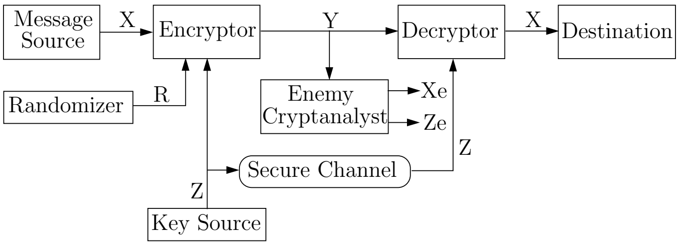

Figure 7.3: A secret-key cryptosystem

message **R** and the secret key **Z** to achieve perfect secrecy. However, some systems, such as the "one-time pad," which will be discussed later, do not require **R**. The major difficulty in the implementation of such cryptosystems lies in the secure distribution of the key. There is recently a new idea of transforming wireless channel state information (CSI) into secret keys. It is widely known that wireless channel coefficients, characterized by their phases and amplitudes, depend heavily on the location, the environment, and the movement of the transmitter and the receiver to the extent that other terminals except the two can predict almost nothing about their channel parameters, and hence their secret key. The generation of the secret key consists of two steps, deriving the channel estimates before quantizing them into secure key symbols. We refer to this technique as "wireless physical-layer secret-key generation." This must be distingished from the term "physical layer security" used in [59], which requires that the legitimate users' channels have SNR advantage over those of eavesdroppers.

Channel estimates can be derived using a known pilot sequence, which is transmitted back and forth between the transmitter and the receiver such that they can learn about channel coefficients from the symbols distorted by the channel. The outcome of the channel estimation process is a set of complex channel coefficients which must be quantized into secret key symbols, as shown in Fig. 2. The process of key generation is discussed in detail in [56], [1].

Since, in a generalized wireless network, there can be several channels that the pilot sequence can take to travel from one node to another, the technique implicitly assumes a bi-lateral agreement between the two nodes regarding the channel to be used for key generation. Earlier works did not tell how to form such an agreement in a secure manner, we will do it in the next section.

Although the enemy cryptanalyst is not located at the same place as the receiver during transmission, he or she may have been there before and it is possible that channel coefficients (especially the amplitudes) do not change much. Therefore, it is wise to assume that he or she can correctly predict some key symbols and we should try to find some countermeasures. To do so, we use a similar concept to Shamir's secret sharing [4] and Cai and Yeung's secure network coding [60]. We call our scheme "physical-layer key encoding," which is designed such that, up to a certain threshold, partial knowledge of key symbols derived from the channel leaves the encoded key completely undetermined. This is performed at the transmitter prior to the one-time pad encryptor block in our wireless physical-layer secret-key cryptosystem shown in Fig. 2 and will be discussed in detail in Section III.

In Section IV, we suggest how to set the number of vulnerable bits based on an equivalent model of the eavesdropper. Section V then concludes the paper.

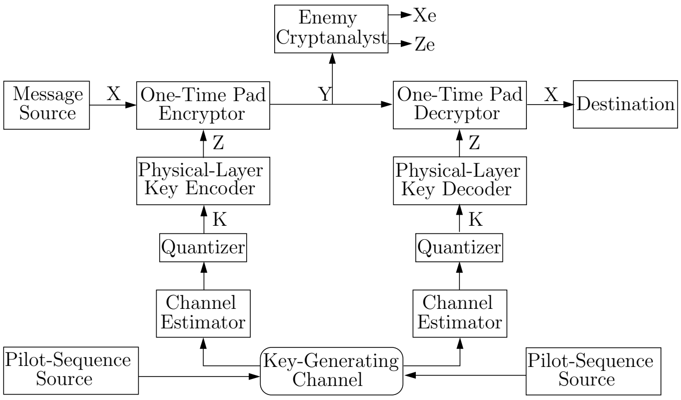

Figure 7.4: A modified secret-key cryptosystem based on mutual CSI with physical-key encoding and decoding

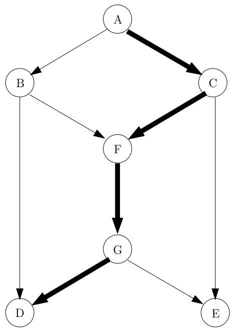

Figure 7.5: A butterfly network

7.7 Wireless Physical-Layer Secret-Key Generation Protocol

In this section, we propose a simple scheme to guarantee that the receiver derives the secret key from the same channel as the transmitter does. The advantage of this scheme is that it supports datagram networks in which the transmission route might not be known in advance by the transmitter and the receiver. The transmitter and the receiver always generate the secret key from the same channel without knowing from which channel they do. This lack of explicit routing information makes life very hard for the eavesdropper.

The scheme proceeds as follows. First, the transmitter passes a complete packet containing a pilot sequence to a next node on the way to the receiver and broadcasts a packet header to all other neighbors. That next node follows the same procedure regarding its following node and other neighbors. This repeats until the packet reaches the receiver, who uses it to estimate the channel parameters and derive the secret key. After that, a packet with the same pilot sequence is sent back along the same path. To do so, the receiver sends it to every neighbor, who, after reading the header, only sends the packet further upstream if it belongs to the forward path. Again, this repeats until the transmitter gets the packet back and derives the secret key accordingly.

To illustrate the scheme, let us consider the butterfly network in Fig. 3. If we consider $ACFGD$ as a forward path from A to D, the scheme proceeds as follows.

Forward:

1. A sends a packet to C and its header also to B.

2. C sends the packet to F and its header also to E.

3. F sends the packet to G and its header to B.

4. G sends the packet to D and its header also to E.

Reverse:

1. D sends the packet to B and G.

2. After reading the header, B discards the packet, whereas G sends it to F and E.

3. After reading the header, E discards the packet, whereas F sends it to B and C.

4. After reading the header, B discards the packet, whereas C sends it to A and E.

5. After reading the header, E discards the packet, whereas A successfully receives it, together with the correct channel information.

7.8 Physical-Layer Key Encoding for One-Time-Pad Encryptor

In this section, we shall present physical-layer key encoding which generates ”the encoded key” $\mathbf{Z} = [Z_1, Z_2, ..., Z_J]$ as a codeword from ”an original quantized key” $\mathbf{K} = [K_1, K_2, ..., K_{I_K}]$ and feeds it into the one-time pad encryptor. The encoder aims at protecting the secret key in case the enemy can correctly estimate some channel coefficients, and hence some original quantized key symbols. Three parameters, I_K, I_{SK}, and I_{VK} are of interest to the encoder. The first one, I_K, is the number of symbols that can be generated by the quantizer in Fig. 2. The second one, I_{SK}, is the number of secure key symbols that the enemy cannot correctly estimate, whereas the third, I_{VK}, is the number of vulnerable ones that he or she can correctly estimate, such that $I_K = I_{SK} + I_{VK}$.

The information-theoretic derivation of I_K, I_{SK}, and I_{VK} is discussed in [56] but not in this paper, where we are more interested in the following questions: Given I_K, I_{SK}, and I_{VK}, what is the important property of the physical-layer key encoding that ensures perfect secrecy as well as efficiency? How can we choose the code rate? And how can we derive the optimal code? Some questions will be answered by theorems 1-3 proposed in this section. Before going that far, we will first describe the one-time pad encryptor.

Consider a non-randomized cipher in which elements in the plaintext $\mathbf{X} = [X_1, X_2, ..., X_M]$, ciphertext $\mathbf{Y} = [Y_1, Y_2, ..., Y_N]$, and secret key $\mathbf{Z} = [Z_1, Z_2, ..., Z_J]$ all take values in the L-ary alphabet and $J = N = M$. Suppose that the key is chosen to be completely random, i.e., $P(Z_i = z) = L^{-M}$, $i = 1, 2, ..., M$, for all possible values z of the secret key, and that the enciphering transformation is

$$Y_i = (X_i + Z_i) \bmod M, \;\; i = 1, 2, ..., M. \tag{7.2}$$

Since, for each possible choice x and y of X_i and Y_i, respectively, there is a unique z such that $Z_i = z$ satisfies (7.2), it follows that $P(Y_i = y|X_i = x) = L^{-M}$ for every particular y and x, no matter what the statistics of X_i may be. Thus, X_i and Y_i are statistically independent, and hence this system provides perfect secrecy [55]. The system is called a modulo-L Vernam system or one-time pad and is used in our model in Fig. 2 to combine the message and the encoded key together.

Since, out of the total I_K quantized key symbols, I_{VK} symbols are vulnerable symbols, we can see that, had a one-time pad encryptor been used without physical-key encoding, I_{VK} ciphertext symbols would have been decrypted by the eavesdropper. Thus, in order to construct a secure Y_1, we use the following linear combination for Z_1.

$$Z_1 = (K_1 + K_2 + ... + K_{I_{VK}+1}) \bmod M \tag{7.3}$$

After substituting (7.3) into (7.2) using $i = 1$, we can see that even if the set of all vulnerable key symbols is a subset of $\{K_1, K_2, ..., K_{I_{VK}+1}\}$, there is still one symbol that is unknown to the eavesdropper. If every key symbol is statistically independent of others, perfect secrecy of Y_1 is achieved.

Now, in order to construct Z_2, Z_3, and so on, we perform a linear combination of I_{VK} key symbols similar to (7.3). Therefore, our physical-layer key encoding can be defined by a linear block code C_p transforming an I_K-tuple $\mathbf{K}$ over $GF(q^{I_K})$ of key symbols obtained from the quantizer into an M-tuple codeword $\mathbf{Z}$ over $GF(q^M)$. We propose the following theorem providing two necessary and sufficient conditions for perfect secrecy.

7.9 Discussion and Conclusion

We have proposed a secure protocol to ensure that the legitimate transmitter and receiver generate their secret key from the same physical channel. We have also included physical-layer key encoding into the system to provide perfect secrecy even when some key symbols are correctly estimated by the eavesdropper who knows the code.

We have suggested two simple generating matrix prototypes for our physical-layer key encoding for two specific cases, when $I_{VK}+1$ is even and when it is odd, where I_{VK} is the number of vulnerable key bits. $I_{VK}+1$ is related to I_K, the number of original key bits needed from the quantizer, by Theorem 2. In case $I_{VK}+1$ is unknown, we may use Theorem 4 to derive it from the probability p that the eavesdropper incorrectly estimates a key bit. For example, $I_{VK}+1$ is at least 5 when p is 0.25, yielding an asymptotic code rate of 3, as predicted by Theorem 3.

Chapter 8

Summary, Conclusion, and Future Works

8.1 Summary and Conclusion

Physical key encoding has been presented in Chapter 7 as a means to protect security in the presence of vulnerable key symbols. The encoded output key is shorter than the input, thus sacrificing some key length for the sake of security. The counterpart of physical key encoding is Slepian Wolf coding, which adds some redundancy to the quantized key such that legitimate receivers are protected against key mismatch due to channel estimation error.

The relationship between physical key encoding and Slepian Wolf coding in WPSG is similar to source coding and channel coding in a communication system in such a way that the latter expands what the former contracts. It is proved that optimality is achieved when the source coding and the channel coding in a communication perform their tasks separately. It is yet to be proved whether such optimality holds with the separation of physical key encoding and Slepian Wolf coding in WPSG.

Just as channel coding has an unequal-error-protection (UEP) capability, physical key encoding has an unequal-security-protection (USP) capability. The concept of USP or scalable security has been previously discussed [76–79], but it is more precisely defined in terms of generalized weak security in our work. Since weak security is also inherent in secure network coding, it follows that secure network coding possesses USP capability as well.

Secure network coding is a class of network coding used for cryptographic purposes. The earlier purpose of network coding is to facilitate multicast transmission. Although both deterministic and random network coding can improve the multicast rate, only deterministic network coding can guarantee max-flow transmission. Another advantage of deterministic network coding is that we are better in control of the unequal-erasure-protection (UEP) capability, as discussed in Chapter 4. This UEP property can lead to conflicts among the multicast receivers in terms of received data quality. When the conflicts are considered as economic problems of resource distribution, an auction algorithm can be used to resolve them, as proposed in Chapter 4. If they are considered as political problems, a voting algorithm could be an interesting solution.

In practice, network coding will probably be used in a system in which channel coding is present. A problem occurs when the channel coding performance depends on the degree distribution of the codes, which may be affected by network coding and erasures in the network. A particular problem in LT-codes is discussed in Chapter 5 and a cooperative buffering scheme is proposed as a solution.

In conclusion, this thesis highlights several interrelationships among several subjects in the fields of coding and cryptography. We pictorially summarize it in Fig. 8.1. Apart from this, network protocol aspects are also considered for WPSG in generalized networks in Chapter 6, showing that network coding can enhance the security of the WPSG protocol.

8.2 Future Works

In the following, we shortly address some possibilities for future research.

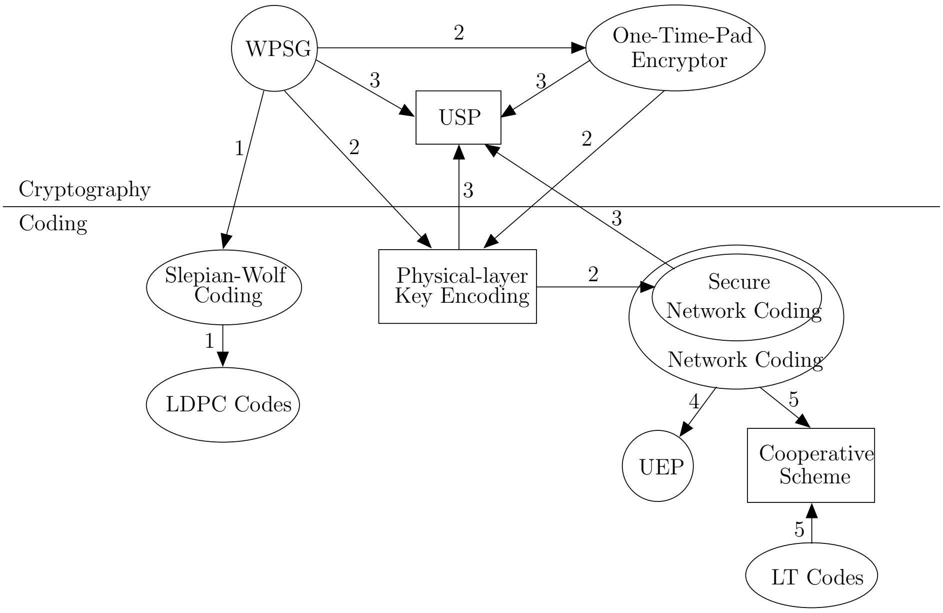

Figure 8.1: Interrelationships among mentioned subjects

8.2.1 Network Coding for WPSG

Apart from our research project, there exists an important contribution on one-relay WPSG made by Shimizu et al. They show that network coding helps make one-relay WPSG more secure [80]. Figure 8.2(b) gives an illustration of their scheme, which they call "multiple-access amplify-and-forward (MA-AF)," as compared with the normal amplify-and-forward scheme in Fig. 8.2(a). For simplicity, we do not consider the effect of noise here and assume that the amplification factor at the relay is 1. The effects of these two factors are discussed in detail in [80].

The normal amplify-and-forward scheme is the same as Protocol 1 in Section 2.2.10, which is the least secure. The relay, after receiving the pilot packet x multiplied by the channel gain from Alice in the first time slot, amplifies and forwards it to Bob in the second one. The process repeats itself in the third and fourth time slot with the roles of Alice and Bob interchanged.

In the first time-slot of the MA-AF scheme, Alice receives xh_{ar} whereas Bob receives xh_{rb}, where h_{ar} and h_{rb} are Alice-relay and relay-Bob channel gains, respectively. In the second time slot, the signal from Alice and Bob adds together such that the relay receives $x(h_{ar} + h_{rb})$. The relay then forwards this to Alice and Bob in the third time slot. Alice

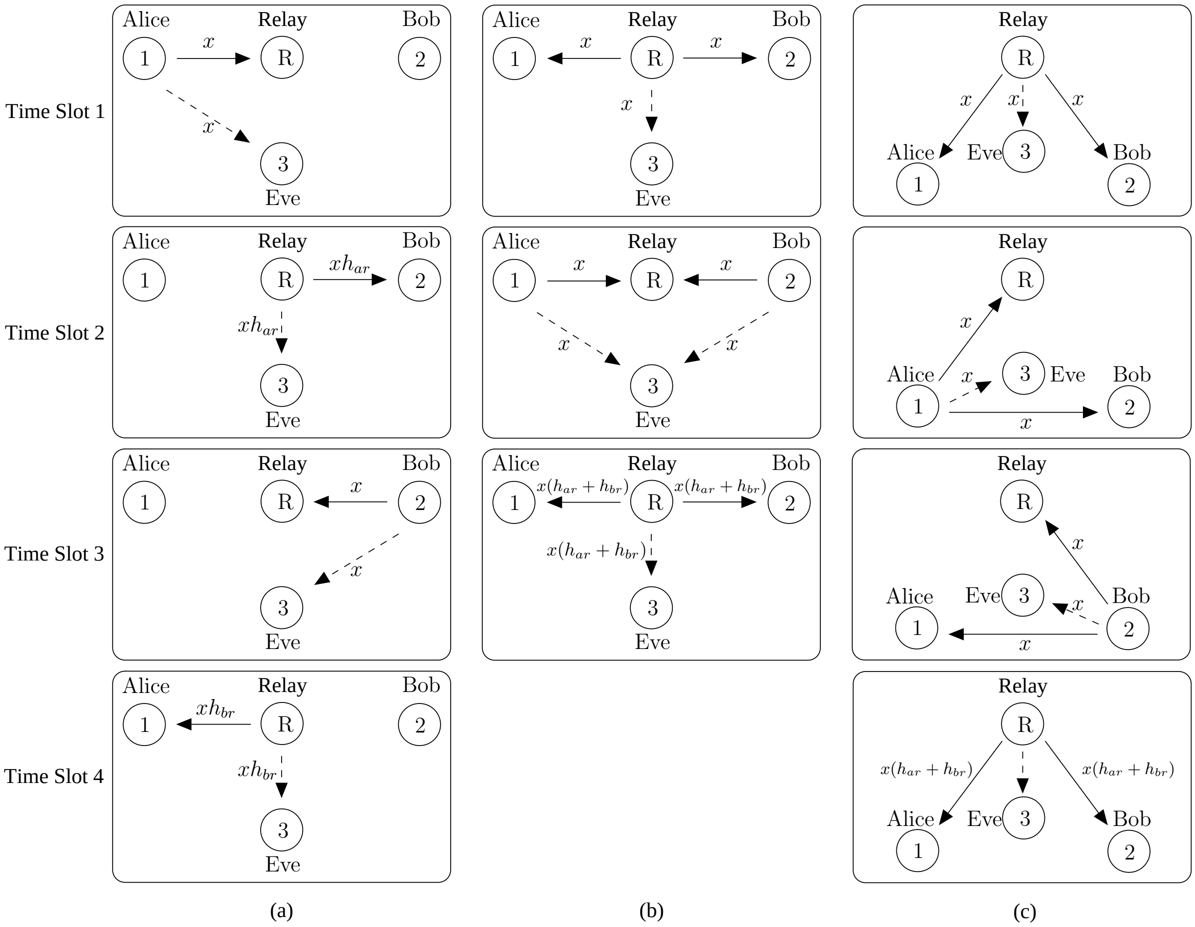

Figure 8.2: One-relay WPSG schemes, each arrow representing a transmitted signal: (a) amplify and forward, (b) MA-AF, (c) our proposed scheme

and Bob can then derive the overall channel gain $h_{ar}h_{rb}$ from the signal they receive in the first and the third time slots. Since the channel information sent out by the relay is neither h_{ar} nor h_{rb} but a network-coded combination, which is $h_{ar} + h_{rb}$, the enemy will find it more difficult to derive $h_{ar}h_{rb}$.

Investigation of Different Network Coding and Relaying Patterns

When Alice and Bob are within each other's transmission range, the efficiency of key generation can be enhanced as shown by our proposed scheme in Fig. 8.2(c). With an extension by one time slot, Alice and Bob can now generate a secret key from two paths, the direct one and the relayed one.

Apart from the triangular shape in Fig. 8.2(c), it is interesting to investigate the graphs with other shapes, such as a quadrilateral or a polygon in general, and compare the key generation efficiency. Also, one might design a scheme to generate secret keys not only for Alice and Bob, but also for the relays. One may further ask such graph-theoretic questions as how the convexity of the shape, or the completeness of the graph, affect key generation. (A shape is convex if all the points along the straight line connecting any two points within it lie inside. A graph is complete if every pair of nodes is connected by an edge.)

Generalizing the MA-AF Scheme

When the distance between Alice and Bob is larger, we need more than one relay and thus a generalized network coding scheme. The main question is whether a corresponding scheme can be derived by using Shimizu's procedure as a building block, and how.

Protocols for WPSG with Network Coding

If some local key is generated by the triangular geometry in Fig. 8.2(c), how can we make it compatible with the key generation schemes using different geometry and network coding patterns in other locations?

8.2.2 Effects of Mobility on Key Extension, Regeneration Rate, and Protocols

Key Extension and Regeneration Rate

Node mobility in a wireless network has profound effects on the key length and key regeneration rate due to two reasons. The obvious one is that the faster the nodes move, the faster the change in channel parameters and therefore the higher the key regeneration rate. The less obvious reason is that the mobility model affects the spatial node distribution. According to Bettstetter, Resta, and Santi, the node distribution $f_{\mathbf{X}}(\mathbf{x})$ of the random way point (RWP) mobility model, where $\mathbf{x} = (x, y)$ is a coordinate in two-dimensional space, consists of three components such that [81]

$$f_{\mathbf{X}}(\mathbf{x}) = f_s(\mathbf{x}) + f_p(\mathbf{x}) + f_m(\mathbf{x}) \ . \tag{8.1}$$

The nodes that remain static for the whole simulation time account for the static component $f_s(\mathbf{x})$. Those who are pausing between their moves make up the pause component $f_p(\mathbf{x})$, whereas those who are moving are responsible for the mobility component $f_m(\mathbf{x})$. In the RWP model, the distribution eventually reaches the steady state after some simulation time. The analytical expression of each component in the distribution is discussed in detail in [81]. Figure 8.3 shows the mobility component normalized such that the integral over the one-unit-squared region equals one.

We aim at deriving some empirical results from simulation regarding key regeneration rate as well as the optimal channel sampling rate as functions of the node mobility.

Protocols

As the nodes move and the topology changes, some wireless channels used for key generation are disconnected and other channels are added to replace them. We therefore need an adaptive protocol to determine the followings: 1) When will a channel be dropped from being used for key generation? 2) Which nodes are authorized to drop it? 3) How

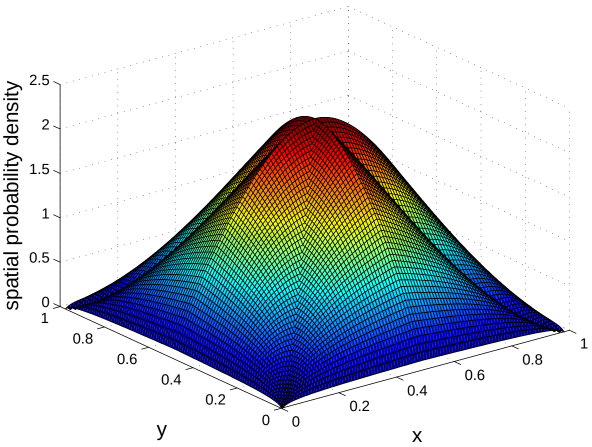

Figure 8.3: The normalized mobility component of the spatial node distribution in the RWP model

do other nodes know that the channel is dropped?

8.2.3 Economics of UEP Network Coding

The auction problem considered in our previous work [7] is only one specific economic problem among many. There are two more problems that we would like to investigate, the bargaining problem and the hierarchical network coding game.

The Bargaining Problem of UEP Network Coding

The bargaining problem is a non-zero-sum game which allows some cooperation among players. Let us consider network coding in a butterfly network in Fig. 8.4(a). Our knowledge about UEP network coding tells us that D obtains better data quality if b_1 is of higher priority than b_2 and every edge has the same erasure probability. Indeed, D may have won an auction over E to obtain this network coding pattern. However, D and E may reach an agreement that, when the edge AB alone is failing or having lots of erasures, the network coding pattern in Fig. 8.4(b) is used instead. This is beneficial for both D and E.

We aim at exploring the conditions under which bargaining is beneficial as well as the optimal bargain in numerical values for each receiver in a generalized network.

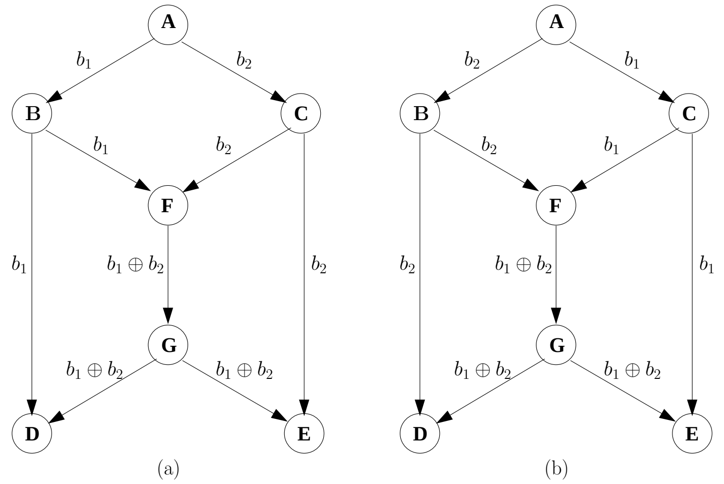

Figure 8.4: A double-butterfly network illustrating hierarchical network coding

The Hierarchical Network Coding Game

In more complicated networks, transmission paths from one source to certain sinks may need to pass some intermediate nodes which are also information sources themselves, as shown in Fig. 8.5. In such a case, network coding functions cannot be assigned by a single source. Instead, every source plays in a Stackelberg game based on von Stackelberg's "Marktform und Gleichgewicht [83]." According to Fig. 8.5, the source node A is considered the leader in the game since it has to make the first decision about global encoding kernels (GEKs) used for the edges AB and BC. After that, B and C can observe A's action and derive their optimal strategies.

Since more than one source node is considered, this game approach can be considered as a generalization of our previous analyses in [6, 7].

8.2.4 Joint LT-Network Coding

We would like to extend, generalize, and synthesize our previous works in UEP network coding [6, 7] and joint LT-network coding [8]. We aim at finding joint LT-network coding solutions in an arbitrary network instead of just a butterfly network, as well as introducing the UEP concept into joint LT-network coding.

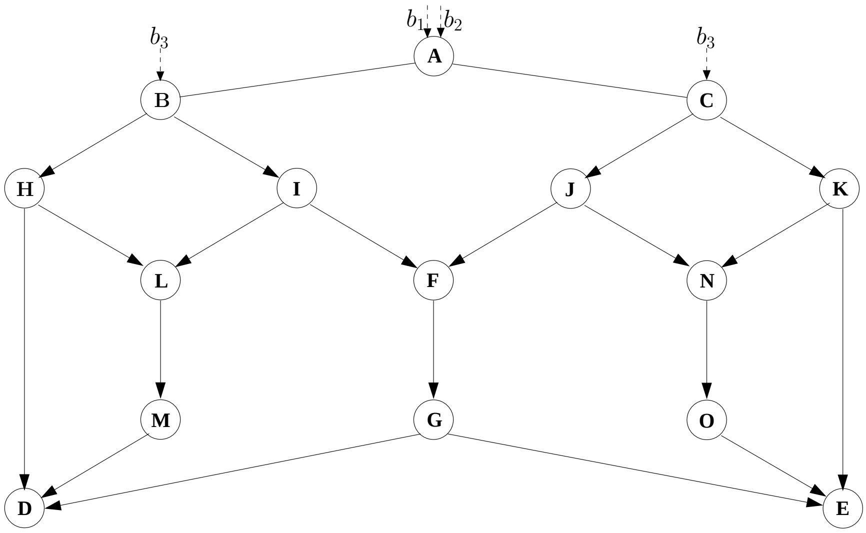

Figure 8.5: A double-butterfly network illustrating hierarchical network coding

Bibliography

[1] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys Through Multipath," *Proc. 2008 IEEE Int. Conf. Acoustics, Apeech, and Signal Processing*, Las Vegas, Mar.-Apr. 2008.

[2] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, "Network Information Flow," IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.

[3] A. Sayeed, A. Perrig, "Secure Wireless Communications: Secret Keys Through Multipath," *IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Mar.-Apr. 2008.

[4] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[5] S.-Y.R. Li, R.W. Yeung, and N. Cai, "Linear Network Coding," IEEE Trans. Inform. Theory, vol. 49, no. 2, pp. 371-381, Feb. 2003.

[6] A. Limmanee, W. Henkel, "UEP Network Coding for Scalable Data," 5^{th} Int. Symp. on Turbo Codes and Related Topics, Lausanne, Sep. 2008.

[7] A. Limmanee, W. Henkel, “Ascending-bid auction for unequal-erasure-protected network coding,” IEEE Information Theory Workshop, Taormina, Oct. 2009.

[8] A. Limmanee, W. Henkel, “A Cooperative Scheme for Shaping Degree Distribution of LT-Coded Symbols in Network Coding Multicast,” Int. ITG Conf. Source and Channel Coding, Siegen, Jan. 2010.

[9] 3GPP, "3GPP; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Protocol and Codecs," 26.346 v6.3.0 (2005-12).

[10] J.G. Proakis, "Digital Communications," McGraw-Hill, Boston, 2001.

[11] S.-K. Chang, K.-C. Yang, and J.-S. Wang "Unequal-Protected LT Code for Layered Video Streaming," IEEE Int. Conf. on Communications, May 2008.

[12] R.W. Yeung, S.-Y.R. Li, N. Cai, and Z. Zhang, "Network Coding Theory," Foundation and Trends in Communications and Information Theory, vol. 2, nos. 4 and 5, pp. 241-381, 2005.

[13] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial Time Algorithms for Multicast Network Code Construction," IEEE Trans. Inform. Theory, vol. 51, no. 6, pp. 1973-1982, Jun. 2005.

[14] C. Fragouli, E. Soljanin, and A. Shokrollahi, "Network Coding as a Coloring Problem," in Proc. Conf. Information Sciences and Systems, Princeton, NJ, Mar. 2004.

[15] M. Friedman and L.J. Savage, "The Utility Analysis of Choices Involving Risk," The Journal of Political Economy, vol. 56, no. 6, pp. 279-304, 1948.

[16] A. Shokrollahi, "Raptor Codes," IEEE Trans. Inform. Theory, vol. 52, no. 6, pp. 2551-2567.

[17] A. Shokrollahi, "Raptor Codes," Int. Symp. Inform. Theory (ISIT 2004), Chicago, Jun.-Jul. 2004.

[18] R.W. Yeung, and N. Cai, "Network Error Correction, Part I: Basic Concepts and Upper Bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19-36, 2006.

[19] R. Koetter, and F.R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579-3591, Aug. 2008.

[20] Y. Lin, B. Li, and B. Liang, "Differentiated Data Persistence with Priority Random Linear Codes," 27th *Int. Conf. on Distributed Computing Systems*, Jun. 2007.

[21] R.K. Ahuja, T.L. Magnanti, and J.B. Orlin, *Network Flows: Theory, Algorithms, and Applications*, Prentice-Hall, New Jersey, 1993.

[22] A.P. Lerner, *The Economics of Control*, Augustus M. Kelley Publishers, NY, 1970.

[23] W. Vickrey, "Counterspeculation, Auctions, and Competitive Sealed Tenders," *Journal of Finance*, vol. 16, no. 1, pp. 8-37, Mar. 1961.

[24] L.M. Ausubel, "An Efficient Ascending-bid Auction for Multiple Objects," *The American Economic Review*, vol. 94, no. 5, pp. 1452-1475, Dec. 2004.

[25] J.F. Nash, Jr., "The Bargaining Problem" *Econometrica*, vol. 18, no. 2, pp. 155-162.

[26] W. Henkel and N. von Deetzen, "Path Pruning for Unequal Error Protection Turbo Codes," 2006 International Zurich Seminar on Communications, Zurich, February 22-24, 2006.

[27] N. von Deetzen and S. Sandberg, "Design of Unequal Error Protection LDPC Codes for Higher Order Constellations," IEEE International Conference on Communications (ICC 2007), Glasgow, Scottland, UK, June 24-28, 2007.

[28] S. Sandberg and N. von Deetzen, "Design of Bandwidth-Efficient Unequal Error Protection LDPC Codes," accepted for publication in IEEE Transactions on Communications, January 2008.

[29] L. Sassatelli, W. Henkel, and D. Declercq, "Check-Irregular LDPC Codes for Unequal Error Protection under Iterative Decoding," 4th International Symposium on Turbo Codes & Related Topics in connection with the 6th International ITG-Conference on Source and Channel Coding, Munich, April 4-7, 2006.

[30] N. von Deetzen and W. Henkel, “On Code Design for Unequal Error Protection Multilevel Coding,” 7th ITG Conference on Source and Channel Coding 2008 (SCC’08), Ulm, Germany, January 14-16, 2008.

[31] N. von Deetzen and W. Henkel, “Unequal Error Protection Multilevel Codes and Hierarchical Modulation for Multimedia Transmission,” accepted at International Symposium on Information Theory 2008 (ISIT 2008), Toronto, Canada, July 6-11, 2008.

[32] W. Henkel and K. Hassan, “OFDM (DMT) Bit and Power Loading for Unequal Error Protection,” OFDM-Workshop 2006, Hamburg, Aug. 30 - 31, 2006.

[33] K. Hassan, W. Henkel, “UEP with Eigen Beamforming for Partial Channel Information MIMO-OFDM,” 2007 IEEE Sarnoff Symposium, Princeton, NJ, USA, Apr. 30 - May 2, 2007.

[34] K. Hassan and W. Henkel, “UEP MIMO-OFDM with Beamforming-Combining for Imperfect Channel Information,” OFDM-Workshop 2007, Hamburg, Aug. 27 - 28, 2006.

[35] W. Henkel, “SVD, a Spatial Code with RS Code Properties,” submitted to ICC 2008, Dresden.

[36] M. Luby, “LT codes,” in Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002.

[37] A. Shokrollahi, Raptor Codes, IEEE Transactions on Information Theory, no. 6, pp. 25512567, June 2006.

[38] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, L. Tolhuizen, Polynomial Time Algorithms for Multicast Network Code Construction, IEEE Trans. Inform. Theory, vol. 51, pp. 1973-1982, Jun. 2005.

[39] R.W. Yeung, and N. Cai, Network Error Correction, Part I: Basic Con- cepts and Upper Bounds Communications in Information and Systems, vol. 6, no 1, pp. 19-36, 2006.

[40] N. Cai, and R.W. Yeung, Network Error Correction, Part II: Lower Bounds Communications in Information and Systems, vol. 6, no 1, pp. 37-54, 2006.

[41] N. Cai, and R.W. Yeung, "Secure Network Coding," International Symposium on Information Theory, Lausanne, 2002.

[42] http://personal.ie.cuhk.edu.hk/ITIP/ISIT02/secure.ps

[43] J. Feldman, T. Malkin, R.A. Servedio, and C. Stein, "On the Capacity of Secure Network Coding," preprint.

[44] J.L. Massey, "An Introduction to Contemporary Cryptology," Proceedings of the IEEE, vol. 76, no. 5, May 1998.

[45] 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.

[46] S.-Y.R. Li, R.W. Yeung, and N. Cai, "Linear Network Coding," IEEE Trans. Inform. Theory, vol. 49, pp. 371-381, Feb. 2003.

[47] R. Koetter, and M. M*é*dard, "An Algebraic Approach to Network Coding," IEEE/ACM Trans. Networking, vol. 11, pp. 782-795, Oct. 2003.

[48] P.A. Chou, Y. Wu, and K. Jain, "Practical Network Coding," 51^{st} Allerton Conf. Communication, Control, and Computing, Oct. 2003.

[49] R.W. Yeung, S.-Y.R. Li, N. Cai, and Z. Zhang, "Network Coding Theory," Foundation and Trends in Communications and Information Theory, vol. 2, nos 4 and 5, pp. 241-381, 2005.

[50] L. Rizzo, "Effective Erasure Codes for Reliable Computer Communication Protocols," Computer Communication Review, Apr. 1997.

[51] S.-K. Chang, K.-C. Yang, and J.-S. Wang, ”Unequal-Protected LT Code for Layered Video Streaming,” International Conference on Communications, Beijing, May 2008.

[52] N. Rahnavard, B.N. Vellambi, and F. Fekri, ”Rateless Codes with Unequal Error Protection Property,” IEEE Trans. Inform. Theory, Vol. 53, no 4, pp. 1521 - 1532, Apr. 2007.

[53] H. Schwarz, D. Marpe, and T. Wiegand, ”Overview of the Scalable Video Coding Extension of the H.264/AVC Standard,” IEEE Trans. Circuits and Systems for Video Technology, Sep. 2007.

[54] I. A. Glover, and P. M. Grant, Digital Communications, Prentice Hall, 2004.

[55] J.L. Massey, ”An Introduction to Contemporary Cryptology,” Proc. IEEE, vol. 76, no. 5, pp. 533-549, May 1988.

[56] J. Wallace, ”Secure Physical Layer Key Generation Schemes: Performance amd Information Theoretic Limits,” *IEEE Int. Conf. Communications*, Dresden, Jun. 2009.

[57] J.W. Wallace and R.K. Sharma, “Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis,” *IEEE Tran. Information Forensics and Security*, vol. 5, no. 3, pp. 381-391, Sep. 2010.

[58] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, ”Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels,” *IEEE Trans. Antennas and Propagation*, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[59] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, ”Wireless Information-Theoretic Security,” *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[60] N. Cai, and R.W. Yeung, ”Secure Network Coding,” *IEEE Int. Symp. Information Theory*, Jun. 2002.

[61] X. Sun, X. Wu, C. Zhao, M. Jiang, and W. Xu, “Slepian-Wolf Coding for Reconciliation of Physical Layer Secret Keys,” *Proc. IEEE WCNC 2010*, Sydney, Apr. 2010.

[62] D. Slepian and J.K. Wolf, “Noiseless Coding of Correlated Information Sources,” *IEEE Trans. on Information Theory*, vol. 19, no. 4, pp. 471-480, Jul. 1973.

[63] F.A. Hayek, “Competition as A Discovery Procedure,” *Quarterly journal of Austrian economics*, vol. 5, iss. 3, pp. 9-24, Sep. 2002.

[64] S. Puducheri, J. Kliewer, and T.E. Fuja, “Distributed LT Codes,” *IEEE Int. Symp. Information Theory*, Jul. 2006.

[65] P. Popovski and H. Yomo, “Physical Network Coding in Two-way Wireless Relay Channels,” *IEEE Int. Conf. Communications*, Jun. 2007.

[66] P. Popovski and H. Yomo, “Wireless Network Coding by Amplify-and-forward for Bi-directional Traffic Flows,” *IEEE Communication Letter*, vol. 11, no. 1, pp. 16-18, Jan. 2007.

[67] S. Zhang, S.C. Liew, and P.P. Lam, “Hot Topic: Physical-layer Network Coding,” *Proc. MobiCom’06*, pp. 358-365, ACM, 2006.

[68] S. Katti, and D. Katabi, “Embracing Wireless Interference: Analog Network Coding,” *Proc. Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 397-408, 2007.

[69] Y. Wu, P.A. Chou, and S.-Y. Kung, “Information Exchange in Wireless Networks with Network Coding and Physical-layer Broadcast,” *2005 Conf. Information Sciences and Systems*, Mar. 2005.

[70] Y. Wu, P.A. Chou, and S.-Y. Kung, “Information Exchange in Wireless Networks with Network Coding and Physical-layer Broadcast,” *Technical Report MSR-TR-2004-78*, Aug. 2004.

[71] C. Hausl, and J. Hagenauer, “Iterative Network and Channel Decoding for The Two-way Relay Channel,” *IEEE Int. Conf. Communications*, Jun. 2006.

[72] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, “XORs in The Air: Practical Wireless Network Coding,” *IEEE/ACM Trans. Networking*, vol. 16, no. 3, pp. 497-510, Jun. 2008.

[73] C. Yao, J.K. Zao, C.-H Wang, S.-Y.R. Li, N.A. Claude, K.-K. Yen, “On Separation Vectors of Static Linear Network Codes with UEP Capability,” *submitted to Int. Symp. Network Coding*, Beijing, Jul. 2011.

[74] W. Cheng, L. Yu, F. Xiong, and W. Wang, “Trusted Network Coding in Wireless Ad Hoc Networks,” *IEEE Global Communications Conf. (GLOBECOM)*, Miami, Dec. 2010.

[75] S. Fu, T. Zhang, and M. Colef, “Secrecy in Two-way Relay Systems,” *IEEE Global Communications Conf. (GLOBECOM)*, Miami, Dec. 2010.

[76] T. Kunkelmann and R. Rainema, “A Scalable Security Architecture for multimedia communication standards,” *Int. Conf. Multimedia Computing and Systems*, Ottawa, Jun. 1997.

[77] J. Meyer and F. Gadegast, “Security Mechanisms for Multimedia Data with the Example MPEG-1 Video,” SECMPEG Project Report, 1995.

[78] T.B. Maples and G.A. Spanos, “Performance Study of a Selective Encryption Scheme for the Security of Networked Real-time Video,” *Int. Conf. Computer and Communications*, Las Vegas, 1995.

[79] I. Agi and L. Gong, “An Empirical Study of Secure MPEG Video Transmissions,” *ISOC Symp. Network and Distributed System Security*, San Diego, 1996.

[80] T. Shimizu, H. Iwai, H. Sasaoka, and A. Paulraj, “Secret Key Agreement Based on Radio Propagation Characteristics in Two-way Relaying Systems,” *IEEE Global Communications Conf. (GLOBECOM)*, Miami, Dec. 2010.

[81] C. Bettstetter, G. Resta, and P. Santi, “The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks,” *IEEE Trans. Mobile Computing*, vol. 2, no. 3, pp. 257-269, Jul.-Sep., 2003.

[82] E. van Damme and S. Hurkens, “Endogeneous Stackelberg Leadership,” *Games and Economic Behavior*, vol. 28, iss. 1, pp. 105-129, Jul. 1999.

[83] H. von Stackelberg, “Marktform und Gleichgewicht,” Springer-Verlag, Berlin, 1934.