Shanghai Jiao Tong University
University of Michigan - Shanghai Jiao Tong University Joint Institute

---

Channel-Width Adaptation and Physical-Layer Secrecy in Wireless Networks

by

Pengfei Huang

A thesis submitted in satisfaction of the
requirements for the degree of Master of Science in
Electrical and Computer Engineering at Shanghai Jiao Tong University

---

Committee in charge:
Prof. Xudong Wang, Chair
Prof. Mian Li
Prof. Xinen Zhu

Shanghai
March, 2013

Abstract

As wireless networks rapidly evolve into the next generation, many challenging issues need to be resolved. Among them, throughput and security are the most critical ones. With high throughput, a wireless network saves precious resource of spectrum and delivers quality of service for wireless applications. With sufficient security, a wireless network wins trust of customers. To this end, this thesis targets at novel mechanisms for enhancing throughput of wireless mesh networks and for ensuring security of wireless networks.

Throughput research in this thesis is focused on wireless mesh networks, which is an indispensable part of the next generation wireless networks. An orthogonal frequency division multiple access (OFDMA) based channel-width adaptation scheme is first proposed to improve the throughput of wireless mesh networks. This scheme is then analyzed under the framework of network optimization. Its computational complexity is proved to be NP-complete. Thus, a greedy algorithm is derived to obtain a suboptimal solution. Based on the greedy algorithm, a distributed medium access control (MAC) protocol is designed to achieve OFDMA-based channel-width adaptation in wireless mesh networks. Performance results show that the new protocol dramatically improves the throughput of wireless mesh networks.

Security research in this thesis is focused on physical layer secrecy, as it is the ultimate path to wireless network security. Two topics are studied in this thesis. In the first topic, a fast secret key generation scheme is developed for wireless networks with long coherence time. This scheme combats the shortage of time diversity via an innovative virtual channel approach. Opportunistic beamforming is adopted to increase the key generation rate, and frequency diversity is exploited to ensure that the key secrecy grows with the key size. This new secret key generation scheme can be easily adopted in both narrowband and wideband systems. In the second topic, impact of artificial noise to the secrecy of a large scale wireless network is analyzed based on the notion of secrecy transmission capacity. Analytical results reveal the relationship between the secrecy transmission capacity and system parameters, and also provide insights on how system parameters can be designed to improve secrecy transmission capacity of a wireless network.

This page is left blank for the Chinese title and Chinese abstract

上海交通大学

交大密西根学院

无线网络信道带宽调节和物理层安全的研究

黄鹏飞

上海交通大学密西根学院硕士学位论文

信息与通信工程专业

委员会成员：

王旭东 （主席）

李冕

朱欣恩

上海

2013 年 3 月

附件四

上海交通大学
学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：黄鹏飞

日期：2013 年 2 月 21 日

附件五

上海交通大学

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于

保密□，在___年解密后适用本授权书。

不保密☑。

（请在以上方框内打“√”）

学位论文作者签名：黄鹏飞　　指导教师签名：

日期：2013 年 2 月 21 日　　日期：2013年 3月14日

摘要

随着无线网络的飞速发展，有许多具有挑战性的问题需要解决。其中，吞吐量和安全性是最关键的两个问题。具有了高吞吐量，无线网络就能节省宝贵的频谱资源并能为无线应用提供高质量的服务。有了足够的安全性，无线网络就会赢得客户的信赖。为此，本论文旨在设计新的机制来提高无线网状网络的吞吐量和保证无线网络的安全性。

关于吞吐量的研究，本论文主要集中在无线网状网络，这种网络是下一代无线网络一个不可缺少的部分。我们首先提出了一种基于正交频分多址接入原理的信道带宽调节方法来提高无线网状网络的吞吐量。然后，在网络优化框架下分析了该方法，其计算复杂性被证明是 NP-完全的。因此，我们提出了一种贪心算法来获得次优解。基于贪心算法，我们设计了一种分布式介质访问控制协议以实现在无线网状网络中的信道带宽调节。性能测试结果表明，新提出的协议极大地提高了无线网状网络的吞吐量。

本论文中安全性的研究集中在物理层安全，因为物理层安全是通向无线网络安全的最终之路。关于物理层安全，本论文研究了两个课题。在第一个课题中，我们设计了在具有长相干时间的无线网络中快速生成密钥的方法。该方法通过虚拟信道的波动克服了时间分集的缺乏。在该方法中，机会波束成型用来增加密钥的生成速率，频率分集用来确保密钥的安全性随着密钥长度的增加而增强。这种新的密钥生成方法可以很容易地在窄带和宽带系统中实现。在第二个课题中，基于安全传输容量，我们分析了人工噪声对大规模无线网络安全性的影响。分析结果给出了安全传输容量和系统参数之间的关系。这为我们如何通过设计系统参数来提高无线网络的安全传输容量提供了帮助。

Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the rapid development of wireless communication technologies, wireless networks (e.g., WiFi, 3G cellular system, and ZigBee) have been widely accepted and have become an indispensable part of our daily life. On the one hand, the growing number of wireless users and the increasing demand for high-speed data applications (e.g., real-time games and high-definition video) require that wireless networks support high data rate services effectively and efficiently. To achieve this goal, communication system parameters, e.g., transmission power, modulation, channel coding, and the number of antennas, have been optimized to enhance the performance of wireless communications. In addition to these traditional system parameters, channel width has recently been considered as a new important parameter to further improve multiple performance metrics of a wireless communication link, including transmission rate, communication range, resilience to delay spread, and power consumption. On the other hand, with ubiquitous applications of wireless networks, security has become a critical issue when wireless networks are used to transmit confidential messages, e.g., on-line credit card transactions. Compared to traditional wired communications, wireless communications are easier to be eavesdropped due to the broadcast nature of wireless medium. Recently, physical-layer secrecy has been proposed to resolve this issue. From the perspective of information theory, perfect secrecy can be

achieved by physical-layer secrecy. Thus, it is envisaged as a promising approach to security of wireless networks.

In this thesis, we focus on two research problems of wireless networks. The first one is about throughput enhancement for wireless mesh networks, which is a critical part of the next generation wireless networks. The second one consists of two topics: 1) fast secret key generation in static wireless networks; 2) analysis of the impact of artificial noise to network secrecy capacity.

In the rest of this chapter, the background and the objective of the above research problems are introduced.

1.1 Channel-Width Adaptation

Channel-width adaptation can optimize a few performance metrics of a wireless communication link. For example, given a certain level of transmission power, reducing the channel width can reliably increase the communication range of a wireless link. If the channel width is further reduced, then the power consumption can also be decreased without compromising the communication range. Thus, channel-width adaptation can optimize both communication range and power consumption that are usually in conflict with each other in a wireless link with fixed channel width [Chandra et al. (2008)]. In another example, considering a vehicular network based on orthogonal frequency division multiplexing (OFDM), when a vehicle moves from a rural area to a suburban area, the delay spread of its communication link may increase to a level larger than the guard interval of OFDM symbols; reducing channel width is effective to fix this problem [Cheng et al. (2008)].

Because of the benefits of channel-width adaptation, supporting multiple options of channel width in a communication radio has become a common practice. For example, many IEEE 802.11 chipsets made by Atheros (now part of Qualcomm) support channel width of

5MHz, 10MHz, 20MHz, and 40MHz. Similarly, worldwide interoperability for microwave access (WiMAX) and long-term evolution (LTE) chipsets also support a set of different channel widths. However, how to utilize such communication radios to improve network performance is a nontrivial task, because a wireless network usually involves many communication links that all demand channel-width adaptation. In a point-to-multipoint (PMP) wireless network (like the IEEE 802.11 basic service set in infrastructure mode) or an extended PMP network (like the IEEE 802.11 extended service set), research work has been conducted to utilize channel-width adaptation. In [Chandra et al. (2008)], the advantages of channel-width adaptation are analyzed using commodity IEEE 802.11 radios. A simple channel-width adaptation algorithm is derived for the basic scenario of a single link with two communication nodes. In [Moscibroda et al. (2008)] [Bahl et al. (2012)], the channel widths of all APs in the distribution system of an IEEE 802.11 network are optimized according to different traffic load distribution in each basic service set. As a result, throughput and fairness of bandwidth distribution of the entire IEEE 802.11 network are greatly enhanced [Moscibroda et al. (2008)] [Bahl et al. (2012)]. A general case of adaptive channel-width allocation for base stations considering the demands of clients is analyzed in [Azar et al. (2011)], where throughput maximization is formulated as a maximum bipartite flow problem.

The channel-adaptation algorithms in [Chandra et al. (2008)] [Moscibroda et al. (2008)] [Bahl et al. (2012)] [Azar et al. (2011)] are not applicable to a multihop wireless network, because they all assume the network works in a single-hop infrastructure network. For a large scale multihop wireless network, there still lack channel-width adaptation algorithms. Various types of multihop wireless networks are characterized by different features, which leads to different requirements and challenges in channel-width adaptation. For example, in a mobile ad-hoc network, channel-width adaptation can be utilized to compensate delay-spread and increase link stability. However, since the network topology is highly variable due to mobility, allocating different channel widths to different links is an extremely challenging task. In a

wireless mesh network (WMN) [Akyildiz et al. (2005)], mobility is minimal. Particularly, in the infrastructure of a WMN, all communication links remain stationary [Akyildiz et al. (2005)]. As a result, some issues like communication range, delay-spread, and link stability are usually considered during the wireless network design and deployment phase. However, there exists one highly variable parameter that impacts the performance of WMNs, which is traffic load distribution on each link. To support variable traffic load in each link of a large scale WMN, resource allocation is needed for each link. However, given a fixed channel width, such resource allocation lacks flexibility and leads to low resource utilization and throughput. Thus, in this thesis, channel-width adaptation is adopted to support heterogeneous traffic demands on various links in WMNs.

1.2 Physical-Layer Secrecy

Traditional security mechanism in wired networks depends on shared secret keys to support a wide variety of security services. However, this approach is not suitable for wireless networks as they are vulnerable to eavesdropping due to the broadcast nature of wireless medium. Recently, the physical-layer secrecy has drawn a lot of attention, because it achieves perfect secrecy from a perspective of information theory. The research on physical-layer secrecy can be classified into two major areas: 1) wireless secret key generation; 2) analysis of information-theoretical secrecy capacity.

1.2.1 Wireless Secret Key Generation

Wireless secret key generation demands a scheme for a legitimate sender and a receiver to utilize their wireless channel as the common source to share their secret key. The basic idea is to take advantage of the reciprocal and location-specific properties of a wireless channel. Based on the reciprocity, the channel states estimated by the legitimate sender and the receiver are the same

within a short time. Therefore, these two legitimate communication nodes can extract a secret key from the variations of a wireless channel. Thanks to the location-specific property, the channel state observed at the third node, i.e., eavesdropper, is uncorrelated with that between the legitimate parties. Hence, the eavesdropper can not extract the same secret key from the channel state.

In general, two legitimate communication nodes can share the secret key through magnitude, phase, and Received Signal Strength Indication (RSSI) of their common wireless channel. Research work has been carried out on this emerging area. In [Mathur et al. (2008)], a system is developed on an FPGA board to measure the channel impulse response from the preamble of a packet, generating error-free secret bits at a speed about 1 bit/s in a real indoor wireless environment. In [Jana et al. (2009)], RSSI is collected from the off-the-shelf 802.11 board to extract the secret key in both static and mobile scenarios. Their results indicate that the mobility can increase the secret key generation rate. In [Zeng et al. (2010)], multiple antennas are utilized to increase the key generation rate within a coherence time. Since only spatial diversity is considered, improvement of key generation rate is limited by the number of antennas. In [Madiseh et al. (2008)] [Wilson et al. (2007)], a secret key is extracted from different paths of a single impulse of a UWB system. Apart from channel magnitude or RSSI based methods, the secret key generation in [Sayeed and Perrig (2008)] [Koorapaty et al. (2000)] is based on the phase reciprocity of each subchannel in a multi-carrier communication system. In [Wang et al. (2011)], a phase-based secret key generation scheme is proposed for narrowband systems, and the secret key generation rate is improved by randomly choosing the initial phases of pilot sequences. With existing secret key generation schemes, the secret key generation rate is low in static wireless networks, due to lack of channel variations. To solve this problem, a channel independent scheme is proposed in [Gollakota and Katabi (2011)]. However, this scheme is specifically designed for OFDM systems. Therefore, in this thesis, we develop a novel scheme that is applicable to different communication systems.

1.2.2 Information-Theoretical Secrecy Capacity

Research on information-theoretical secrecy capacity is focused on how to determine the maximum communication rate under the constraint of secrecy of a communication channel. It dates back to the Shannon's notion of perfect secrecy [Shannon (1949)]. In the pioneering work of Wyner [Wyner (1975)], the wiretap channel for point to point communication is introduced. The research results are then extended to the Gaussian wiretap channel in [Leung-Yan-Cheong and Hellman (1978)] and the broadcast channel in [Csiszár and Korner (1978)]. Perfect secrecy is shown to be achievable when the legitimate channel is better than the eavesdropping channel. From an information-theoretic view, for a system that consists of a legitimate sender Alice, a receiver Bob, and an eavesdropper Eve, the secrecy capacity can be characterized. For the general non-degraded Gaussian wiretap channel in [Csiszár and Korner (1978)], the secrecy capacity C_s is given by

$$C_s = max_{f_x \in F}[I(X;Y) - I(X;Z)]^+, \tag{1.1}$$

where X is the channel input at Alice, Y is the channel output at Bob, and Z is the channel output at Eve. F is the set of all probability density functions at the channel input under power constraint. Thus, if Eve has a better channel condition than Bob, the secrecy capacity C_s is zero. Since the mutual information terms $I(X;Y)$ and $I(X;Z)$ are concave in f_x, we can formulate a lower bound R_s for the secrecy capacity C_s

$$R_s = [max_{f_x \in F} I(X;Y) - max_{f_x \in F} I(X;Z)] \leq max_{f_x \in F}[I(X;Y) - I(X;Z)]^+ = C_s, \tag{1.2}$$

where the secrecy rate R_s is the difference between the legitimate channel capacity from Alice to Bob and the eavesdropping channel capacity from Alice to Eve. This lower bound R_s is often adopted for a simplified calculation of the achievable secrecy rate, because each mutual

information term can be determined individually. For some scenarios, it has been proven that the secrecy rate R_s can be equal to the secrecy capacity C_s, e.g., in a single-user system with single and multiple antennas.

Channel fading is lately considered helpful to secure communications when the eavesdropping channel is stronger than the legitimate channel [Bloch et al. (2008)] [Gopala et al. (2008)]. For the fading wiretap channel like

$$\begin{aligned} y &= hx + n, \\ z &= gx + n, \end{aligned} \tag{1.3}$$

where x is the transmitting signal from Alice with average power constraint P and $x \sim \mathcal{CN}(0, P)$, y is the received signal by Bob, z is the received signal by Eve, h is the channel fading gain between Alice and Bob, g is the channel fading gain between Alice and Eve, and n is the additive white Gaussian noise, i.e., $n \sim \mathcal{CN}(0, \sigma_n^2)$. The secrecy rate R_s can be calculated using the following equation

$$R_s = [log_2(1 + \frac{|h|^2 P}{\sigma_n^2}) - log_2(1 + \frac{|g|^2 P}{\sigma_n^2})]^+. \tag{1.4}$$

So far many research papers have been focused on advanced physical layer techniques to improve secrecy capacity. One important aspect is to adopt beamforming to substantiate the quality of the legitimate link in a multi-antenna system. In [Shafiee and Ulukus (2007)], beamforming is shown to be the optimal strategy for secrecy in MISO systems. Then, the robust designs of power allocation to maximize the secrecy rate are investigated in [Huang and Swindlehurst (2011)] and [Li and Ma (2011)]. To further enhance secrecy, besides transmitting data with beamforming, part of the total transmitting power is allocated to generate artificial noise in the null space of the legitimate channel to confuse eavesdroppers [Goel and Negi (2008)]. Based on [Goel and Negi (2008)], beamforming and artificial noise are shown to improve the

secrecy for the MIMO-OFDM system in [Romero-Zurita et al. (2011)]. In [Romero-Zurita et al. (2012)], an optimization problem, which aims to minimize the total power consumption on both data and artificial noise to satisfy both the minimum SNR at the legitimate receiver and a given average SNR at each eavesdropper, is formulated and solved. In [Zhou and McKay (2010)], a closed-form analytical result of the ergodic secrecy capacity for a legitimate communication link with some eavesdroppers is derived, and then the optimal power allocation between data and artificial noise is studied to maximize the ergodic secrecy capacity. In [Ghogho and Swami (2011)], a probabilistic framework is considered for physical layer secrecy in MIMO systems, where locations of eavesdroppers are modeled as a Poisson point process. However, existing analytical results are only applicable to the scenario with single communication link. In this thesis, we adopt stochastic geometry to analyze the secrecy capacity of a large scale wireless network that consists of multiple communication links.

1.3 Organization of the Thesis

The rest of this thesis is organized as follows.

In Chapter 2, we study the problem on how to leverage channel-width adaptation to improve the throughput of a wireless mesh network. A novel OFDMA-based channel-width adaptation scheme is designed. Based on this scheme, a MAC protocol is developed for wireless mesh networks.

In Chapter 3, fast secret key generation is investigated for static wireless networks. We propose a novel scheme that integrates opportunistic beamforming and frequency diversity to combat the shortage of time diversity. Our scheme can be used in both narrowband and wideband systems.

In Chapter 4, impact of artificial noise to the secrecy capacity of a large scale wireless network is studied. We adopt stochastic geometry to derive the secrecy transmission capacity.

Analytical results provide insights on how to design system parameters to improve the capacity of the entire network.

The thesis is concluded in Chapter 5.

Chapter 2

OFDMA-Based Channel-Width Adaptation in Wireless Mesh Networks

2.1 Motivation

It is rather common in a wireless mesh network (WMN) that some links experience heavy traffic load, while other links only need to support light traffic. Obviously, this problem cannot be properly solved if communication nodes are equipped with fixed channel width. An effective solution is to leverage channel-width adaptation in all links of WMNs. Thus, channel-width adaptation algorithms and protocols are studied in this chapter with an objective to satisfy heterogeneous traffic demands on various links.

Traditionally, channel width of a link can be adjusted by selecting different options (e.g., 5, 10, 20, and 40MHz) available in a radio. In this chapter, orthogonal frequency division multiple access (OFDMA) is adopted to provide a different approach. We consider a single radio WNN, where each radio adopts OFDMA. Then, channel width of each radio can be simply adjusted by selecting a different number of subchannels. Thus, the problem of adapting channel width to heterogeneous traffic demands in various links of a WMN is converted to another problem,

i.e., how to allocate subchannels to different links of a WMN such that the throughput of the entire network is maximized.

So far many research papers have addressed the channel allocation problem in WMNs. For papers on single-radio multi-channel operation [So and Vaidya (2004)] [Maheshwari et al. (2006)] [Aryafar et al. (2008)], their results are not applicable to the OFDMA-based channel-width adaptation, because fixed channel width is assumed. For papers on multi-radio multi-channel operation [Das et al. (2005)] [Subramanian et al. (2008)], their algorithms cannot be adopted either, because in the OFDMA-based channel-width adaptation, there exists a constraint that each node can either transmit or receive packets on subchannels at one time slot, whereas this constraint is not considered in the multi-radio multi-channel scenarios. In [Li et al. (2009)], different channel width is available through channel combining on a radio for the WMNs. However, the approach explained in [Li et al. (2009)] is different from our OFDMA-based scheme in a single radio WMN in two aspects: 1) in [Li et al. (2009)], one node can only maintain one communication link. However, in our scheme, one node can simultaneously support several communication links with different nodes; 2) in [Li et al. (2009)], a radio can only use continuous channels, but a radio in our scheme can transmit on any subchannels in the communication band. To date there also exist research results on subcarrier allocation for OFDMA WMNs. In [Lee and Leung (2006)], fair allocation of subcarrier and power is studied for a specific WMN with one mesh router and multiple mesh clients. Thus, their point to many points (PMP) structure is different from our ad hoc network model. In [Cheng and Zhuang (2009)], a joint power-subcarrier-time allocation algorithm is derived for one cluster of a WMN. In each cluster, the mesh router is responsible for resource assignment for its mesh clients. Thus, their network structure is also PMP. More recently, the resource allocation problem of multihop OFDMA WMNs are conducted in [Bayan and Wan (2010)] [Kim et al. (2008)] [Bai et al. (2011)] [Mai and Chen (2011)]. However, these papers are focused on a relay-based two-hop network model. Thus, their algorithms are not applicable to a generic WMN. Consequently, to solve the

subchannel allocation problem for channel-width adaptation in generic WMNs, new resource allocation algorithms need to be derived and an appropriate one must be identified to conduct channel-width adaptation in a distributed MAC protocol. To achieve this goal, we have made the following contributions in this chapter:

1. Channel-width adaptation is proposed to resolve the issue of mismatch between link capacity and traffic demands. Instead of a traditional adaptation mechanism by choosing different available spectrum (i.e., frequency center and frequency bandwidth), subchannel allocation in OFDMA is specified as a new channel-width adaptation mechanism. Based on this new mechanism, channel-width adaptation problem in WMNs is converted into a subchannel allocation problem.

2. An optimization problem is formulated to investigate the channel-width adaptation problem in WMNs. The corresponding decision problem of this optimization problem is proved to be NP-complete, which reveals the complexity of channel-width adaptation in WMNs. To reduce the complexity, a greedy algorithm is proposed to obtain the suboptimal solution. With the feasible solution from the greedy algorithm as the initial population, a genetic algorithm is derived to obtain a near-optimal solution. With the genetic algorithm as a reference, the greedy algorithm is shown to achieve comparable performance as that of the genetic algorithm.

3. It is shown that the greedy algorithm can be executed distributedly under some constraints. Thus, it is employed to develop a distributed MAC protocol for channel-width adaptation in OFDMA WMNs. The MAC protocol is highly adaptive to dynamic network conditions such as the traffic demand on each link. The throughput of the entire network can be greatly improved.

The remainder of this chapter is organized as follows. The basic mechanisms and benefits of channel-width adaptation based on OFDMA are explained in Section 2.2. The subchannel

allocation problem for channel-width adaptation is formulated in Section 2.3, where a greedy algorithm and a genetic algorithm are developed to obtain a near optimal solution to the resource allocation problem. Based on the greedy algorithm, a distributed MAC protocol is proposed in Section 2.4. Performance results are presented in Section 2.5, and the chapter is concluded in Section 2.6.

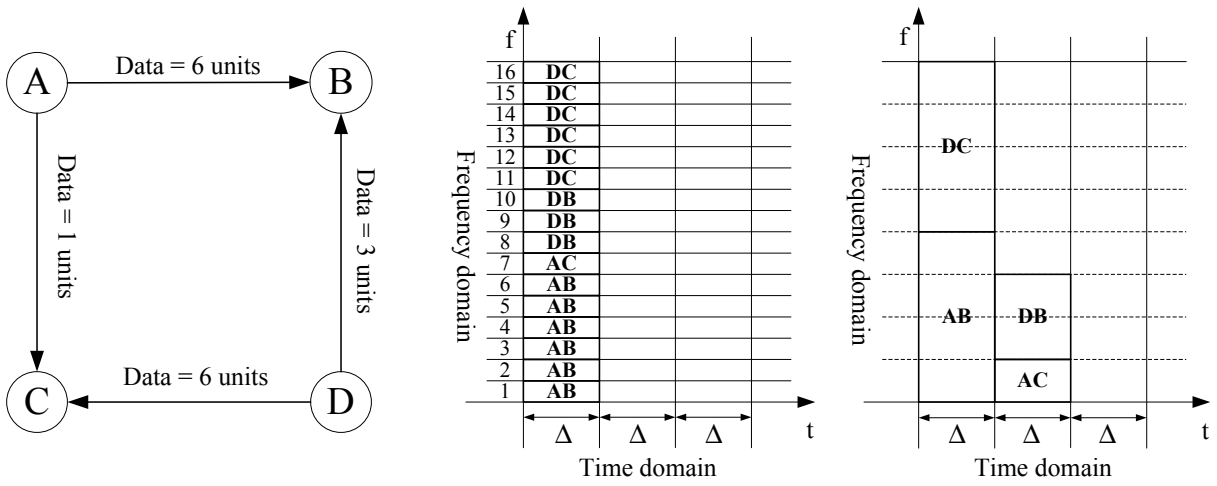
2.2 Channel-Width Adaptation Based on OFDMA: Mechanisms and Benefits

2.2.1 OFDMA-Based Channel-Width Adaptation Mechanisms

We consider a single radio WMN. Traditionally, the channel width of a link can be adjusted by selecting: 1) different options of channel width (e.g., 5, 10, 20, and 40MHz) available in a radio; 2) the center frequency of the operation channel spectrum.

However, its performance is impacted by several drawbacks. Firstly, the granularity of channel width adjustment is constrained and the step size of channel-width adjustment is also limited. For example, the minimum channel width in an IEEE 802.11 radio must be 5MHz and the step size is $5, 10$, or 20MHz. Secondly, the operation spectrum of a channel on a radio must be consecutive.

In this chapter, a different approach is proposed to adjust channel width. It is based on the capability of subchannels (i.e., a number of subcarriers) allocation of OFDMA. Compared to a radio with traditional channel-width adaptation scheme, an OFDMA-based radio brings several advantages: 1) it is flexible to adjust channel width to support traffic demand by selecting a different number of subchannels; 2) it does not require the spectrum of the chosen subchannels be consecutive, and the step size of channel-width adjustment can be as fine as one subchannel; 3) a single OFDMA radio node can support multiple communication links at the same time.



(a) Communication topology (b) OFDMA based scheme (c) Traditional scheme

Figure 2.1: The benefits of the OFDMA-based channel-width adaptation scheme

2.2.2 Benefits of the OFDMA-Based Channel-Width Adaptation

The benefits of the OFDMA-based channel-width adaptation are demonstrated in the following example.

The simple communication topology consists of four nodes A, B, C and D, as shown in Figure 2.1(a). Each node is equipped with one radio. The links are directional and the system follows TDMA. The whole spectrum is assumed to be 40MHz. For the OFDMA-based channel-width adaptation mechanism, the whole spectrum is assumed divided into 16 subchannels. While for the traditional channel-width adaptation scheme, it is assumed the channel width can be 5MHz, 10MHz, 20MHz or 40MHz and the center frequency of the channel can be arbitrarily adjusted. We also assume one subchannel per time slot Δ can convey 1 unit, and the traffic demands in a TDMA frame for links AB, AC, DB and DC are 6, 1, 3, and 6 units respectively.

Consider the OFDMA-based channel-width adaptation scheme. The subchannel and time slot allocation is shown in Figure 2.1(b). Thus, to support all traffic demands, the TDMA frame can be as short as Δ, and the throughput of the network is $(6 + 1 + 3 + 6)/1 = 16$ $(units/\Delta)$.

Consider the traditional channel-width adaptation scheme. The channel and time slot allocation is shown in Figure 2.1(c). To support all traffic demands, the TDMA frame needs to be 2Δ. Thus, the throughput of the network is $(6+1+3+6)/2 = 8$ $(units/\Delta)$.

This simple example demonstrates that the network throughput can be greatly improved by the OFDMA-based channel-width adaptation scheme for the following reasons: 1) an OFDMA radio can support several communication links simultaneously; 2) the granularity of channel-width adjustment of an OFDMA radio can be as small as a subchannel.

With OFDMA, the channel-width adaptation algorithm has to take the following two items into consideration: 1) subchannel allocation in frequency domain and time domain; 2) transmitting and receiving constraint, i.e., in a time slot, the subchannels allocated to a radio can only be used for either transmitting or receiving packets.

2.3 Channel-Width Adaptation Algorithms Based on OFDMA

In this section, the problem of resource allocation for channel-width adaptation is formulated first, and then the corresponding greedy and genetic algorithms are derived.

2.3.1 Problem Formulation

We consider a TDMA WMN consisting of N nodes and L directional links. Each node is equipped with an OFDMA radio. The transmission range of each node is R, and the interference range is $R^{'}$. The network can be modeled as a directional communication graph $G(V, A)$, where V is a set of nodes, and A is a set of directed edges. We have $|V| = N$, and $|A| = L$. For link $l(i, j) \in A$, node $i \in V$ is the transmitter node and node $j \in V$ is the receiver node, i.e., node i sends data to node j.

In our network model, the length of a time slot is fixed, but the TDMA frame length is

variable according to the fluctuating traffic demands of all links in the system. More specifically, when resource allocation is performed, the total number of time slots is determined such that traffic demands of all links are satisfied within a TDMA frame. This design eliminates the need of admission control, which is a preferred feature for data networks. To be consistent with this design, the traffic demand of a link is not specified as the actual traffic load. Instead, it is specified as the number of resource units per TDMA frame, and each unit represents the data transmitted in one subchannel per time slot, which is the same as the definition in Section 2.2. For easy specification of traffic demands, when a node needs to specify the traffic demand of a link, it selects a traffic demand level from the set of $\{1, 2, \ldots, M\}(units)$, and the selected level is proportional to its expected actual traffic load. The above design of the TDMA frame structure and the resource allocation mechanism achieves time slotted resource sharing among links of all nodes. It is well suited for data networks.

In our OFDMA-based channel-width adaptation mechanism, it is assumed that the whole spectrum is divided into W subchannels and one subchannel can carry one unit data per time slot. The OFDMA-based radio can transmit data on any combination of the subchannels.

We use the protocol model [Jain et al. (2005)] as the interference model. Under this model, a transmission from node i to node j is successful at a time slot if two conditions are satisfied: 1) $d_{ij} \leq R$; 2) any node k, which occupies at least one overlapping subchannel with link $l(i, j)$ and $d_{kj} \leq R^{'}$, is not transmitting, where d_{ij} is the distance between node i and node j.

Thanks to the OFDMA technique, the problem of channel-width adaptation can be converted into a resource allocation problem: Given different traffic demands on each link, how to assign time slot and subchannel under some constraints such that the total traffic demands can be satisfied with the least number of time slots, i.e., the network throughput is maximized. It can be formulated as follows.

First, our objective is to minimize the number of time slots (i.e., the length of one TDMA frame) that can support the given traffic demands. Total time slots consumption of the network

is denoted as T. Thus, the objective function is

$$\textit{Minimize } T. \tag{2.1}$$

We need to determine proper time slot and subchannel allocation for each directional link. For link $l(i,j)$, $X(i,j,t,s)$ denotes its allocation status at time slot t and subchannel s, so $X(i,j,t,s) \in \{0,1\}$. Thus, we have the following constraint:

$$\begin{aligned} &X(i,j,t,s) \in \{0,1\}, \\ &\forall l(i,j) \in A,\ \forall t = 1,2,\ldots,T,\ \forall s = 1,2,\ldots,W. \end{aligned} \tag{2.2}$$

However, (2.2) does not consider the potential interference between links. To capture this situation, we need a *link interference constraint* below:

$$\begin{aligned} &X(i,j,t,s) + X(p,q,t,s) \leq 1, \\ &\forall l(i,j) \in A,\ \forall t = 1,2,\ldots,T,\ \forall s = 1,2,\ldots,W,\ \forall l(p,q) \in I_{l(i,j)}, \end{aligned} \tag{2.3}$$

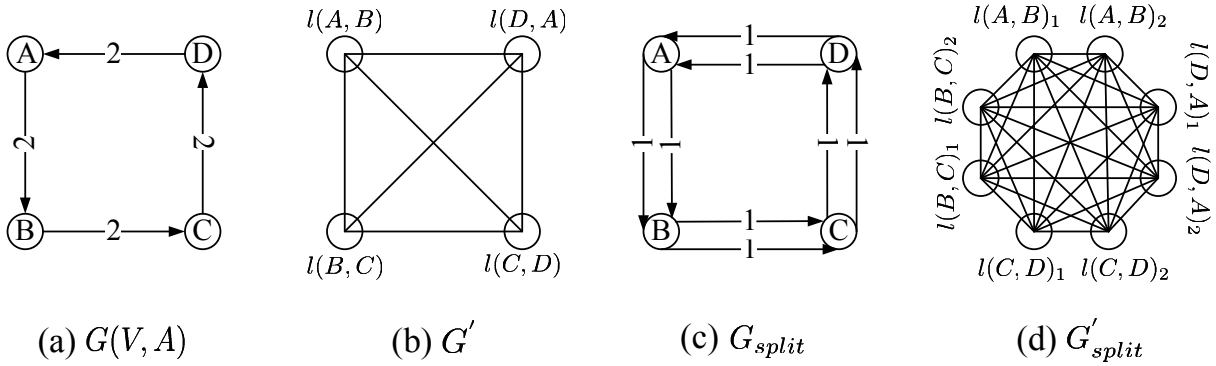
where $I_{l(i,j)}$ is the interference set of link $l(i,j)$.

Since the single radio OFDMA is adopted, every node in one time slot should either transmit or receive on all the occupied subchannels. Thus, for a certain link $l(i,j)$, we have the following *transmitting and receiving constraint* (*Tx/Rx constraint*) :

$$\begin{aligned} &X(i,j,t,s) \cdot \Big[X(i,j,t,s) + \sum_{f=1}^{W} \sum_{p \in In(i)} X(p,i,t,f) + \sum_{g=1}^{W} \sum_{q \in Out(j)} X(j,q,t,g)\Big] \leq 1, \\ &\forall l(i,j) \in A,\ \forall t = 1,2,\ldots,T,\ \forall s = 1,2,\ldots,W, \end{aligned} \tag{2.4}$$

where $In(i)$ is a set of nodes that have data to send to node i (i.e., link $l(p,i) \in A$ for any $p \in In(i)$), and similarly $Out(j)$ is the set of nodes which receive data from node j.

Finally, to satisfy the traffic demand of each link, for every link $l(i,j) \in A$, we need to



(a) $G(V, A)$ (b) G' (c) G_{split} (d) G'_{split}

Figure 2.2: (a) The communication graph, (b) the interference graph of the communication graph, (c) the split communication graph, and (d) the interference graph of the split communication graph

consider the *traffic demand constraint*:

$$\begin{aligned} &\sum_{t=1}^{T}\sum_{s=1}^{W} X(i,j,t,s) \geq D(i,j), \\ &D(i,j) \in \{1,2,\ldots,M\}, \end{aligned} \tag{2.5}$$

where $D(i,j)$ is the traffic demand on link $l(i,j)$. This constraint means that each link should be assigned with enough time slots and subchannels to support the traffic demands.

Consequently, we have formulated the optimization problem of time slot and subchannel two dimensional resource allocation for the OFDMA-based channel-width adaptation. We call this problem as single radio OFDMA-based resource allocation (SRORA) problem, i.e., to optimize objective (2.1), subject to constraints (2.2), (2.3), (2.4) and (2.5). We denote the minimum time slots consumption of the problem SRORA as $T_{optimal}$.

Theorem 2.1. *The decision problem of the optimization problem SRORA that whether K time slots is enough to satisfy the total network traffic demands is NP-complete.*

Proof: First, for any given solution, whether all the constraints are satisfied can be determined in polynomial time. Thus, it is NP. Then, we consider the special case of our problem by fixing $W = 1$ and $D(i,j) = 1$ for all links. Using the protocol interference model, we convert the directional link $l(i,j) \in A$ in the communication graph $G(V, A)$ into the vertex in the cor-

responding interference graph $G^{'}$, as shown in Figure 2.2(b). Based on the interference graph $G^{'}$, each link $l(i,j)$ in the communication graph $G(V,A)$ can construct an interference set $I_{l(i,j)}$. Since in this special case only one subchannel and one unit traffic demand for all links, every link only needs one time slot in a frame in order to satisfy *traffic demand constraint* (2.5). To satisfy *link interference constraint* (2.3), any link in $I_{l(i,j)}$ should be assigned a different time slot from that of link $l(i,j)$. In this special case, when *link interference constraint* (2.3) is satisfied, *Tx/Rx constraint* (2.4) is also automatically satisfied due to the two facts: 1) the links $l(p,i)$ where $p \in In(i)$ and links $l(j,q)$ where $q \in Out(j)$ are in set $I_{l(i,j)}$; 2) the link in $I_{l(i,j)}$ is assigned with different time slot from the link $l(i,j)$. Therefore, whether K time slots is enough for all links to support their traffic demands in the communication graph $G(V,A)$ is equivalent to the problem whether K colors is enough to color the vertices in the corresponding interference graph $G^{'}$. In other words, this special case problem can be polynomially transformed into the vertex coloring problem, which is NP-complete [Garey and Johnson (1979)]. Thus, our general decision problem is NP-complete.

2.3.2 A Greedy Algorithm

Since the problem SRORA is NP-complete, a low-complexity greedy algorithm is proposed for the single radio OFDMA-based resource allocation problem, and we call it GR-SRORA.

In our greedy algorithm, links are assigned with time slot and subchannel in a certain sequential order just like coloring the vertices in the corresponding interference graph. However, here we also need to consider *Tx/Rx constraint*.

The GR-SRORA is described in Algorithm 2.1. It works as follows. 1) Lines 2-15 are used to assign the time slot and subchannel to link $l(i,j)$ under *link interference constraint* and *Tx/Rx constraint*. First, the resource consumption status table of link $l(i,j)$ (i.e., $\Phi(i,j,t,s)$) captures *link interference constraint*. For any t and s, if $\Phi(i,j,t,s) = 1$, it means time slot t and subchannel s is occupied by a link in the interference set of link $l(i,j)$ (i.e., $I_{l(i,j)}$). Second, the

Algorithm 2.1 GR-SRORA

Input:

- Communication graph $G(V, A)$
- Resource consumption status table of link $l(i, j)$: $\Phi(i, j, t, s)$
- Single radio OFDMA constraint table of link $l(i, j)$: $\Psi(i, j, t)$
- Traffic demand on link $l(i, j)$: $D(i, j)$
- Number of total subchannels: W

Output:

- Network time slots consumption: T_{greedy}
- The maximum time slot assigned to link $l(i, j)$: $T_{l(i,j)}$
- Time slot and subchannel allocation result for link $l(i, j)$: $X(i, j, t, s)$

Initialization:

- $\Phi(i, j, t, s) = 0$
- $\Psi(i, j, t) = 0$
- $T_{greedy} = 0$
- $T_{l(i,j)} = 0$

for all $l(i, j) \in A$ **do**
  for $t = 1$ to $+\infty$ **do**
    if $D(i, j) == 0$ **then**
      Break
    end if
    if $\Psi(i, j, t)! = 1$ **then**
      for $s = 1$ to W **do**
        if $D(i, j) > 0$ && $\Phi(i, j, t, s) == 0$ **then**
          $X(i, j, t, s) = 1$
          $D(i, j) = D(i, j) - 1$
          $T_{l(i,j)} = t$
        end if
      end for
    end if
  end for
  for all $l(p, q) \in A$ **do**
    Update $\Phi(p, q, t, s)$
    Update $\Psi(p, q, t)$
  end for
end for
$T_{greedy} = \max_{l(i,j) \in A} T_{l(i,j)}$
Stop

single radio OFDMA constraint table of link $l(i,j)$ (i.e., $\Psi(i,j,t)$) captures *Tx/Rx constraint*. For any t, if $\Psi(i,j,t)=1$, it means link $l(i,j)$ can not transmit on any subchannel on time slot t. 2) Lines 16-19 are executed after a link assignment. Two tables $\big(\Phi(p,q,t,s)$ and $\Psi(p,q,t)\big)$ of each link are updated, and these two tables will be used for the next link assignment. 3) Line 21 is used to calculate the network time slots consumption T_{greedy}.

To understand the performance of the greedy algorithm GR-SRORA, in the following, we show the properties of the problem SRORA's optimal solution $T_{optimal}$ and the GR-SRORA's greedy solution T_{greedy}, with the help of the split communication graph G_{split} of the original communication graph $G(V,A)$ and the split interference graph G'_{split}, as shown in Figure 2.2.

Theorem 2.2. *For the optimal solution of problem SRORA $T_{optimal}$ and the greedy solution of GR-SRORA T_{greedy}, $\lceil \frac{\chi(G'_{split})}{W} \rceil \leq T_{optimal} \leq T_{greedy} \leq T_{max} = \delta(G'_{split}) + 1$, where $\lceil \cdot \rceil$ is the ceiling function, $\delta(\cdot)$ is the maximum degree of a graph, and $\chi(\cdot)$ is the chromatic number of a graph.*

Proof: The proof consists of two parts. First, we show the property of $T_{optimal}$. In communication graph $G(V,A)$, each directional link $l(i,j)$, whose traffic demand is $D(i,j)$, is split into $D(i,j)$ virtual directional links between node i and node j to construct the split communication graph G_{split}, as shown in Figure 2.2(c). Based on the protocol interference model, the split communication graph G_{split} is converted into corresponding interference graph G'_{split}, as shown in Figure 2.2(d), where each vertex is greedily colored, i.e., assigning different timeslot-subchannel pairs to interfering virtual links in the split communication graph G_{split}. After coloring, each link in communication graph $G(V,A)$ certainly satisfies *link interference constraint*. The minimum number of colors (i.e., timeslot-subchannel pairs) the interference graph G'_{split} consumes is the chromatic number $\chi(G'_{split})$ [Bondy and Murty (1976)]. Since W subchannels are available for each time slot, the total minimum number of time slot consumption is $\lceil \frac{\chi(G'_{split})}{W} \rceil$, if only considering *link interference constraint*. However, the problem SRORA also has *Tx/Rx constraint*. Thus, the optimal solution of SRORA must be larger than or equal

to $\lceil \frac{\chi(G'_{split})}{W} \rceil$, i.e., $\lceil \frac{\chi(G'_{split})}{W} \rceil \leq T_{optimal}$. Second, we show the property of T_{greedy}. We consider the worst case, where there exists only one subchannel (i.e., W=1). In this special case, for any link assignment order $\vec{\mathcal{L}}$ run by GR-SRORA, there exists a corresponding greedy coloring order in G'_{split}. Thus, the color number in G'_{split} is exactly the total time slot consumption $T^{worst}_{greedy}(\vec{\mathcal{L}})$. Since for any greedy coloring order in G'_{split}, the color number consumption is at most $\delta(G'_{split}) + 1$ [Johnson (1974)]. Thus, for any link assignment order $\vec{\mathcal{L}}$, the total network time slot consumption $T^{worst}_{greedy}(\vec{\mathcal{L}})$ is upper bounded by $T_{max} = \delta(G'_{split})+1$. In general cases, the number of subchannels W is usually a constant larger than 1. Thus, for any link assignment order $\vec{\mathcal{L}}$, the total time slot consumptions calculated by GR-SRORA $T_{greedy}(\vec{\mathcal{L}})$ is certainly equal or less than $T^{worst}_{greedy}(\vec{\mathcal{L}})$. Thus, $T_{greedy} \leq T_{max} = \delta(G'_{split}) + 1$. Therefore, combining the results from two parts, $\lceil \frac{\chi(G'_{split})}{W} \rceil \leq T_{optimal} \leq T_{greedy} \leq T_{max} = \delta(G'_{split}) + 1$, which means $T_{greedy} \leq (\delta(G'_{split}) + 1) \cdot T_{optimal} / (\lceil \frac{\chi(G'_{split})}{W} \rceil)$.

The complexity of the GR-SRORA is analyzed as follows. It is assumed that the number of links L is a variable, subchannel number W and traffic demand upper bound M for each link are constants. In Algorithm 2.1, Lines 2-15 are for assigning time slot and subchannel to link $l(i, j)$. Its complexity is $\mathcal{O}(T_{max})$, where T_{max} is the upper bound of T_{greedy}. As shown in *Theorem* 2.2, $T_{max} = \delta(G'_{split}) + 1$. Since $\delta(G'_{split}) + 1 \leq M \times L + 1$, $T_{max} \leq M \times L + 1$. Thus, the complexity is $\mathcal{O}(L)$. Lines 16-19 are for updating $\Phi(i, j, t, s)$ and $\Psi(i, j, t)$. Its complexity is $\mathcal{O}(L)$. In all, for Lines 1-22, the total complexity is $L \times (\mathcal{O}(L) + \mathcal{O}(L))$. Therefore, the total complexity is $\mathcal{O}(L^2)$.

2.3.3 A Genetic Algorithm

Since the greedy algorithm GR-SRORA usually can only obtain the suboptimal solution, we adopt a genetic algorithm (GA) to obtain a near optimal result as a theoretical reference for our greedy algorithm.

In order to apply the genetic algorithm, the number of decision variable $X(i, j, t, s)$ in

optimization problem SRORA needs to be constant. Since for a certain network, the number of links L and the number of subchannels W are constants, we also need to fix the total time slots for assignment so that the number of $X(i,j,t,s)$ will be fixed. From *Theorem* 2.2, $T_{optimal}$ is upper bounded by $T_{max} = \delta(G'_{split}) + 1$ for a given communication graph $G(V,A)$. Due to this bound, the problem SRORA can be paraphrased as a following formulation:

$$\textit{Minimize } T$$

s.t.

$$\begin{cases} X(i,j,t,s) + X(p,q,t,s) \leq 1, \\ \left[X(i,j,t,s) + \sum_{f=1}^{W} \sum_{p \in In(i)} X(p,i,t,f) + \sum_{g=1}^{W} \sum_{q \in Out(j)} X(j,q,t,g)\right] \cdot X(i,j,t,s) \leq 1, \\ \sum_{t=1}^{T_{max}} \sum_{s=1}^{W} X(i,j,t,s) \geq D(i,j), \\ X(i,j,t,s) \in \{0,1\}, \\ \forall l(i,j) \in A,\ \forall s = 1,2,\ldots,W,\ \forall l(p,q) \in I_{l(i,j)},\ \forall t = 1,2,\ldots,T_{max}. \end{cases}$$

The objective T is the maximum occupied time slot in the network and is calculated with decision variable $X(i,j,t,s)$ as:

$$T = \max_{t \in \{1,2,\ldots,T_{max}\}} t$$

$$\text{s.t.} \max_{l(i,j) \in A, s \in \{1,2,\ldots,W\}} X(i,j,t,s) \neq 0.$$

Based on this new formulation, a genetic algorithm is developed for single radio OFDMA-based resource allocation problem. We call it GA-SRORA. Different from classic optimization

methods like gradient based approaches, GA is suitable to deal with the integer programming problems. Although there is no absolute guarantee for the GA-SRORA to obtain an optimal solution, the algorithm can be executed for a long time. In this way, a near-optimal or optimal solution can be obtained.

GA evolves its generation into the next one via three essential steps: reproduction, crossover, and mutation. Thus, GA-SRORA is executed according to the following steps.

1. Initialize Population: The population of our algorithm GA-SRORA consists of chromosomes. Each chromosome is represented by $X(i,j,t,s)$ of all links.

2. Evaluation and Fitness Assignment: For every chromosome, its fitness needs to be minimized in GA-SRORA. The fitness should capture the objective function and the constraints in paraphrased SRORA problem. As a result, the fitness is described as:

$$
\begin{aligned}
&Fitness = T + P \cdot (C_1 + C_2 + C_3),\\
&C_1 = \sum_{l(i,j)\in A} \max[0, 1 - \sum_{t=1}^{T_{max}} \sum_{s=1}^{W} X(i,j,t,s)/D(i,j)],\\
&C_2 = \sum_{l(i,j)\in A} \sum_{l(p,q)\in I_{l(i,j)}} \sum_{t=1}^{T_{max}} \sum_{s=1}^{W} \max[0, X(i,j,t,s) + X(p,q,t,s) - 1],\\
&C_3 = \sum_{l(i,j)\in A} \sum_{t=1}^{T_{max}} \sum_{s=1}^{W} \max[0, \big(X(i,j,t,s) + \sum_{f=1}^{W} \sum_{p\in In(i)} X(p,i,t,f)\\
&\qquad + \sum_{g=1}^{W} \sum_{q\in Out(j)} X(j,q,t,g)\big) \cdot X(i,j,t,s) - 1],
\end{aligned}
$$

   where T is the maximum occupied time slot in the network and is obtained with $X(i,j,t,s)$, P is a penalty parameter, C_1, C_2 and C_3 are derived from *traffic demand constraint*, *link interference constraint*, and *Tx/Rx constraint*, respectively.

3. Reproduction: According to the fitness, better chromosomes are copied and worse ones are removed, while holding population size constant. A fair selection is applied to generate

"winners" and put them into the "mating pool".

4. Crossover: Parent chromosomes swap a subset of their strings, generating two new chromosomes called children.

5. Mutation: A new chromosome generated by changing values of some bits in its string. This step reduces the chance of falling into the local optimal point.

6. The steps 2-5 are repeated for U rounds to obtain a relatively stable solution.

The complexity of the GA-SRORA can be derived similarly to the Algorithm 2.1. For iteration rounds U, population size V, and link number L, the complexity of GA-SRORA is $\mathcal{O}(UVL^3)$.

2.4 Distributed MAC for OFDMA-Based Channel-Width Adaptation

In this section, a distributed MAC protocol is proposed for the OFDMA-based channel-width adaptation. It is developed based on the greedy algorithm.

2.4.1 Distributed Operation of the Greedy Algorithm

Every node i maintains four tables: 1) $Q_{in}(i,p,q)$, which indicates whether the time slot p and subchannel q is occupied by a link which is the receiving link (i.e., ingoing link) of a node in the interference range of node i; 2) $Q_{out}(i,p,q)$, which indicates whether the time slot p and subchannel q is occupied by a link which is the sending link (i.e., outgoing link) of a node in the interference range of node i; 3) $O_{in}(i,t)$, which indicates whether time slot t is occupied by any receiving link of node i; 4) $O_{out}(i,t)$, which indicates whether time slot t is occupied by

any sending link of node i. How such information is collected is explained in Sections 2.4.3 and 2.4.4.

For a given link $l(i,j)$, sending node i is responsible for assigning time slots and subchannels to support a given number of units (denoted as $D(i,j)$) in a TDMA frame. With the above variables, the resource assignment of link $l(i,j)$ can be executed as:

1. Information fusion: Based on the protocol interference model, any receiving link of a node which is located in the interference range of node i or any sending link of a node which is located in the interference range of node j will potentially interfere with link $l(i,j)$, so node i needs to communicate with node j to collect all the resource usage information by combining tables $Q_{in}(i,p,q)$ and $Q_{out}(j,p,q)$ before resource allocation is conducted. Due to the single radio OFDMA *Tx/Rx constraint*, the node i should also obtain table $O_{out}(j,t)$ from node j, and then determine which time slot is still available by checking $O_{in}(i,t)$ and $O_{out}(j,t)$.

2. Time slot and subchannel allocation: For the first time slot, node i assigns the unoccupied subchannels to link $l(i,j)$ to support the traffic demands. If the first time slot is not enough, it goes to the second time slot. It repeats this process until the sum of the assigned subchannels can support the traffic demand of link $l(i,j)$. During this period, any link $l(p,q) \in I_{l(i,j)}$ (i.e., $l(p,q)$ is any receiving link of a node which is located in the interference range of node i or any sending link of a node which is located in the interference range of node j) can not conduct assignment simultaneously.

3. Table update: After assignment of link $l(i,j)$, all the nodes in the interference range of node i and node j must update their tables immediately.

To support the above functions, the control messages need to be received within the interference range such that: 1) when a certain link $l(i,j)$ is in the assignment process, all its

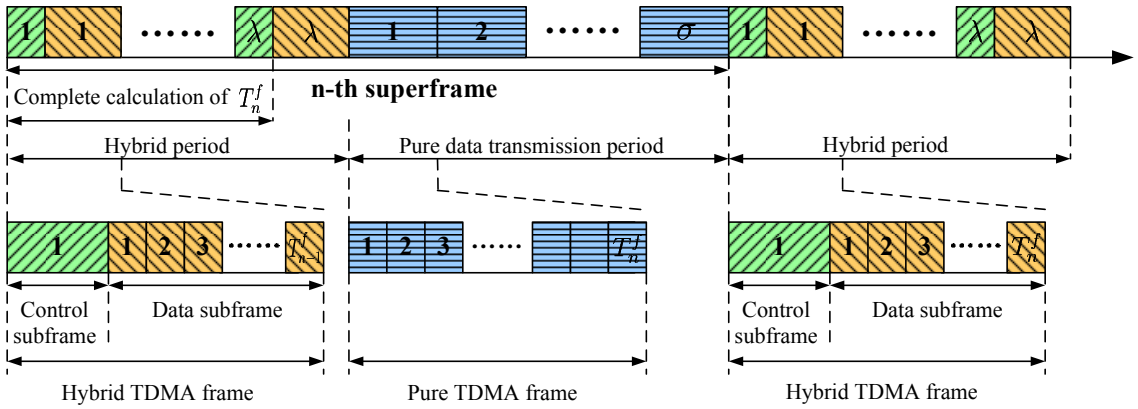


Figure 2.3: Frame structure

interference links will keep quiet; 2) after assignment of link $l(i, j)$, all the nodes in the interference range of node i and node j will update their tables.

In order for the control messages to cover the interference range, the lowest transmission rate is adopted to contend for assignment and broadcast assignment results. Every node contends to assign the resource to its outgoing links in a greedy way. Two nodes far away enough can conduct the assignment simultaneously. This above process is called distributed GR-SRORA (DGR-SRORA). Based on this process, a distributed multi-subchannel TDMA MAC protocol is developed in Sections 2.4.2-2.4.4.

2.4.2 Frame Structure

The TDMA MAC protocol works in a hybrid way, as shown in Figure 2.3. In each superframe, the system completes a new resource allocation in λ control subframes and data transmission on the assigned time slots and subchannels in the rest time.

A superframe includes two parts: hybrid period and pure data transmission period. The hybrid period consists of λ hybrid TDMA frames, where λ is a constant and must be set large enough for all the nodes to complete resource allocation. A hybrid TDMA frame is comprised of two subframes: control subframe and data subframe. Each consists of a number of time slots. The control subframe is used for resource allocation. The data subframe is used for data

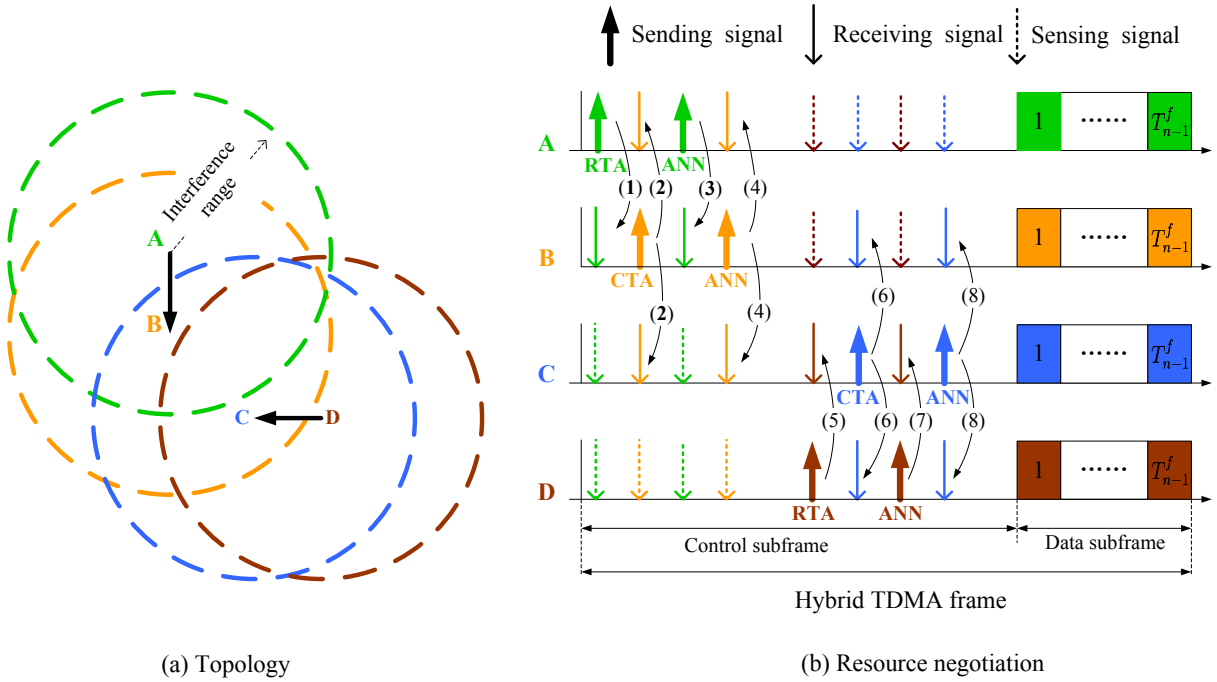


Figure 2.4: Operation of the MAC protocol

transmission. The pure data transmission period consists of σ pure TDMA frames, where σ is a constant. These TDMA frames are only used for data transmission.

As shown in Figure 2.3, in the n-th superframe, the length of the data subframe in the hybrid period is T^f_{n-1}, which is determined in the $(n-1)$-th superframe. In the hybrid period of the n-th superframe, the system completes the resource allocation and calculates T^f_n, which is the length of one pure TDMA frame in the pure data transmission period of n-th superframe and also is the length of the data subframe in the hybrid period of $(n+1)$-th superframe.

In the control subframe of the hybrid period, each node uses an RTS/CTS mechanism to contend for time slots and subchannels allocation. In all TDMA frames for data transmission, each node adopts CSMA/CA to access the assigned time slots and subchannels. This can prevent collisions due to allocation error or out of network interference. As a result, our MAC protocol is actually a TDMA MAC overlaying CSMA/CA.

2.4.3 Distributed Resource Allocation Procedure

The control subframe in Figure 2.3 is used for signaling of distributed resource allocation. Control messages are sent with the lowest transmission rate using all subchannels. For resource assignment of link $l(i, j)$, the negotiation between node i and node j follows the procedure below:

1. Node i sends an RTA (request-to-assign) packet to node j. All the nodes except node j in the sensing range of node i keep quiet.

2. Upon receiving the RTA packet, node j sends node i a CTA (clear-to-assign) packet, which contains $Q_{out}(j, p, q)$ and $O_{out}(j, t)$. All the nodes except node i in the sensing range of node j keep quiet.

3. Upon receiving the CTA packet, node i relies on tables: $Q_{in}(i, p, q)$, $Q_{out}(j, p, q)$, $O_{in}(i, t)$ and $O_{out}(j, t)$ to assign the time slot and subchannel to link $l(i, j)$. Then, node i broadcasts an ANN (announcement) packet, which contains the assignment result for link $l(i, j)$, to all nodes in its interference range.

4. Upon receiving the ANN packet, all the nodes in the interference range of node i update their tables. Then node j also broadcasts an ANN packet to all nodes in its interference range, and the receiving nodes update their tables.

An example of resource allocation procedure is explained below. The signaling messages are transmitted in the lowest rate to cover all the nodes in the interference range and the exchange procedure is shown in Figure 2.4.

1. Node A starts to assign time slots and subchannels for link $l(A, B)$. It broadcasts an RTA packet to node B. Node C and node D can sense the signaling, so they keep quiet.

2. Node B receives the RTA packet, and then broadcasts a CTA packet, which contains $Q_{out}(B, p, q)$ and $O_{out}(B, t)$, to node A. Node A and node C can receive this packet, but node D can only sense it.

3. Node A receives the CTA packet, and broadcasts an ANN packet, which contains the assignment result for the link $l(A, B)$. Node B receives this packet, but node C and node D can only sense it.

4. When node B receives the ANN packet, it updates its own tables and rebroadcasts the ANN packet. Node A and node C receive it and update their tables, but node D can only sense it.

5. Node D starts to assign time slots and subchannels for link $l(D, C)$. It broadcasts an RTA packet to node C. Node A and node B can sense the signaling, so they keep quiet.

6. Node C receives the RTA packet, and then broadcasts a CTA packet, which contains $Q_{out}(C, p, q)$ and $O_{out}(C, t)$, to node D. Node D and node B can receive this packet, but node A can only sense it.

7. Node D receives the CTA packet, and broadcasts an ANN packet, which contains the assignment result for the link $l(D, C)$. Node C receives this packet, but node A and node B can only sense it.

8. When node C receives the ANN packet, it updates its own tables and rebroadcasts the ANN packet. Node D and node B receive it and update their tables, but node A can only sense it.

In the distributed algorithm, every node determines its own time slot. Thus, the largest time slot in one node may be different from that of another node. In order to avoid inconsistent TDMA frame in different links, the largest time slot in the allocation must be known to all

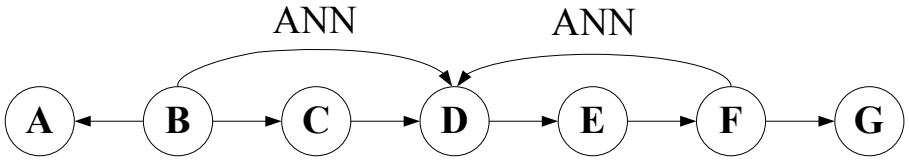


Figure 2.5: Announcement packet collision in the case of multiple interference domains

nodes. This can be done by the following simple procedure: when a node gets resource allocation information from another node, it compares its largest time slot with the one in the allocation information. If its own value is smaller, it needs to update its largest time slot number and broadcast the updated information to its neighbours. Otherwise, no action is needed.

2.4.4 Enhancement for the Case of Multiple Interference Domains

The above protocol is effective for the single interference-domain, because every time only one link is in the assignment process and other nodes can hear the signaling and keep quiet. However, in the case of multiple interference domains, there exist collisions in ANN packets. For example, in Figure 2.5, node B and node F successfully make reservation for the assignment for link $l(B, A)$ and link $l(F, G)$ by exchanging RTA and CTA packets. However, it is possible that the ANN packets broadcast by node B and node F simultaneously arrive at node D which lies in their interference range. Thus, node D can not receive the correct ANN packet, which leads to errors for the following link assignment. To reduce the probability of collisions in ANN packets, we propose a scheme as follows. For the assignment process of link $l(i, j)$, node i and node j exchange RTA and CTA packets as usual. The process of broadcasting ANN packets is modified to reduce the collision probability: 1) node i and node j broadcast ANN packets in turn for K_{ANN} rounds instead of only one round; 2) before broadcasting ANN packet, the sending node randomly chooses a waiting time in the backoff window W_{ANN} and delays the ANN packet transmission for the chosen waiting time.

Although this scheme cannot guarantee no collision, the collision probability drops dramatically with the increased K_{ANN} and W_{ANN}. It should be noted that how to design an effective

distributed MAC protocol in multiple interference domains is still an open problem.

2.5 Performance Results

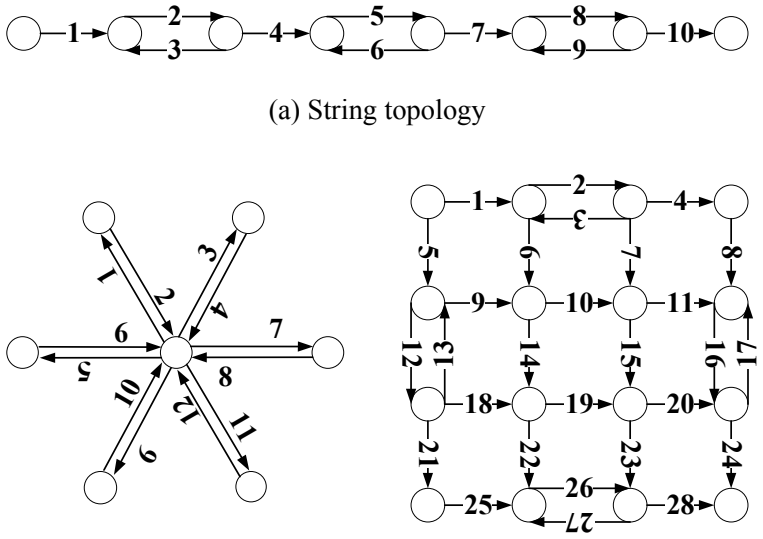
In this section, simulations are carried out to evaluate our algorithms and protocols for different topologies. In the simulation, each node is equipped with one radio. The available spectrum is as wide as 40MHz, and the corresponding rate using whole spectrum is 108Mbps. In our OFDMA-based channel-width adaptation scheme, the whole spectrum is divided into 64 subchannels and the length of one time slot is 5 ms. We assume one subchannel per time slot can transmit 1 unit data.

2.5.1 Simple Topologies

The greedy and genetic algorithms are evaluated under three simple topologies in Figure 2.6. In each topology, the link ID is marked in the figure, and all the links have the same length, which represents the communication range of each node. The interference range is set twice the communication range.

For each link, the traffic demand is uniformly distributed in $\{1, \ldots, 128\}$ (*units*). The network throughput is defined as the ratio of the total traffic demands of the network in a TDMA frame to the length of a TDMA frame.

For each topology, we take three tests to compare the network throughput achieved by our single radio OFDMA-based channel-width adaptation algorithms (i.e., GR-SRORA and GA-SRORA) with the one achieved by the single radio traditional channel-width adaptation (SRTCWA) scheme and the one achieved by the single radio fixed channel width (SRFCW) scheme. The SRTCWA and SRFCW are executed with the same procedure as GR-SRORA (i.e., greedily assign time slot and channel to all the links in the same order with GR-SRORA), but they consider different constraints. In SRTCWA, there are four options of channel width (i.e.,

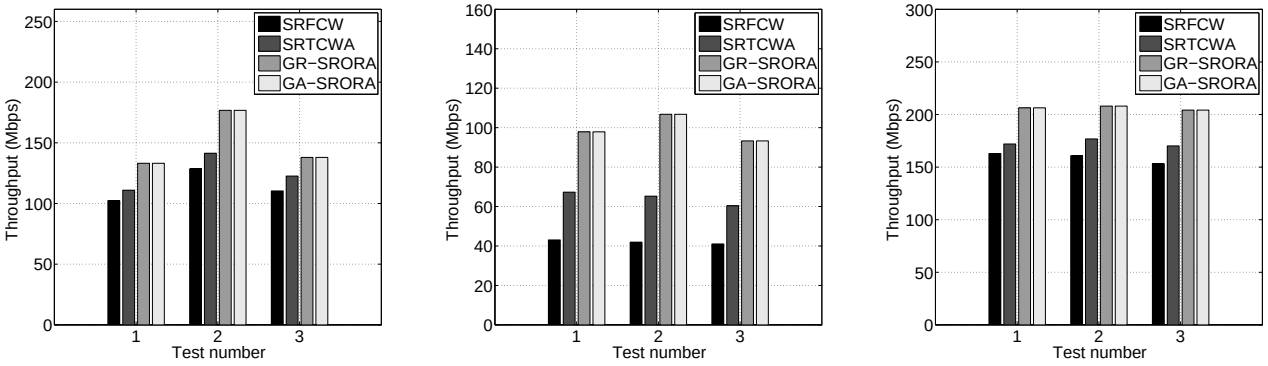


(a) String topology

(b) Star topology

(c) Grid topology

Figure 2.6: Simple topologies



(a) String topology (b) Star topology (c) Grid topology

Figure 2.7: Network throughput for simple topologies

5, 10, 20, and 40MHz), and the center frequency of each channel can be adjusted. Similarly, in SRFCW, there are two 20MHz orthogonal channels. In both SRTCWA and SRFCW, in one time slot, the number of channels assigned to a node should be less than one.

For string topology, as shown in Figure 2.7(a), on average the network throughput of GR-SRORA are 19.2% higher than the one achieved by the SRTCWA and 30.8% higher than the one achieved by the SRFCW. In this network structure, the improvement is not very evident due to lack of one point to multi-point structure in the string topology.

For star topology, as shown in Figure 2.7(b), on average the network throughput of GR-SRORA are 54.5% higher than the one achieved by the SRTCWA and 136.4% higher than the one achieved by the SRFCW. Such a significant improvement is due to the OFDMA mechanism, which ensures the central node supports several communication links simultaneously. Thus, our OFDMA-based channel-width adaptation scheme is very suitable for this star structure.

For grid topology, as shown in Figure 2.7(c), on average the network throughput of GR-SRORA are 19.3% higher than the one achieved by the SRTCWA and 29.8% higher than the one achieved by the SRFCW.

As shown in Figure 2.7, the greedy algorithm achieves nearly the same throughput as that of the GA based algorithm. This indicates that the greedy algorithm is effective to obtain near-optimal solution to the channel-width adaptation problem in WMNs.

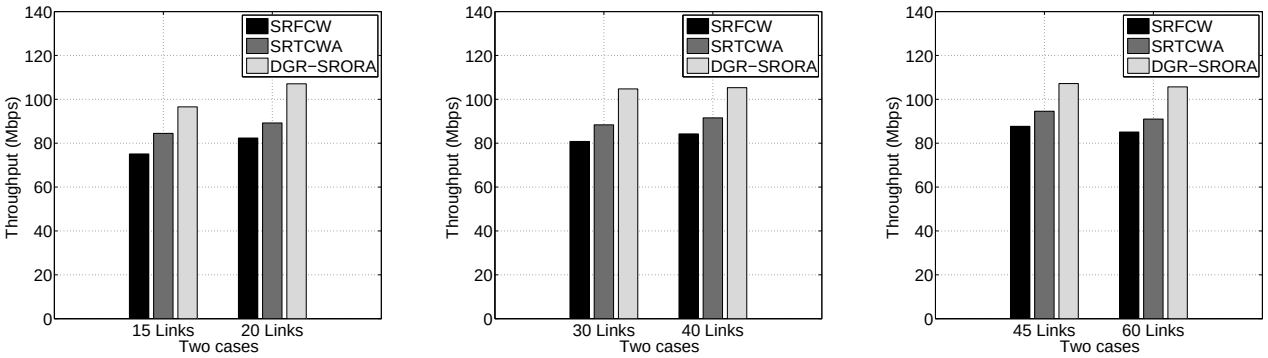
2.5.2 Randomized Topology

Our distributed MAC protocol is evaluated in the randomized topology. The communication range of each node is 100m, the interference range is 200m, and the sensing range is 300m.

The RTA and CTA packets are 120 bytes, and the ANN packet is 30 bytes. As explained in Section 2.4, the lowest transmission rate is adopted for sending these signaling packets and it is set 6 Mbps.

Single Interference-Domain Scenario

In this scenario, nodes are randomly distributed in a circle whose diameter is 200m. Since all nodes can hear each other, the ANN packet collision will not happen. The distributed MAC protocol (DGR-SRORA) in Section 2.4 is adopted. The ANN packets are broadcast only for one round. In the simulation, six cases of Node-Link pairs are considered: 10 nodes 15 links, 10 nodes 20 links, 20 nodes 30 links, 20 nodes 40 links, 30 nodes 45 links and 30 nodes 60 links. For each case, the nodes are randomly distributed and the links are randomly chosen. The



(a) 10 Nodes (b) 20 Nodes (c) 30 Nodes

Figure 2.8: Network throughput for single interference-domain scenario

Table 2.1: Total resource allocation time for single interference-domain scenario

Control Subframe	Data Subframe	Nodes: 10 Links: 15	Nodes: 10 Links: 20	Nodes: 20 Links: 30	Nodes: 20 Links: 40	Nodes: 30 Links: 45	Nodes: 30 Links: 60
20 ms	80 ms	9.2 ms	11.3 ms	18.4 ms	104.5 ms	112.1 ms	202.3 ms
15 ms	85 ms	9.2 ms	11.3 ms	103.9 ms	110.5 ms	202.4 ms	214.7 ms
10 ms	90 ms	9.2 ms	101.8 ms	200.5 ms	205.9 ms	305.7 ms	407.0 ms
5 ms	95 ms	104.0 ms	202.5 ms	304.7 ms	504.4 ms	801.5 ms	1100.5 ms

traffic demand for each link is uniformly distributed in $\{1, \ldots, 128\}$ ($units$).

1. Network Throughput

For each case of Node-Link pair, the distributed protocol DGR-SRORA is compared to the SRTCWA and SRFCW. The network throughput of each case is averaged over five tests and is shown in Figure 2.8. It indicates in each case our OFDMA-based channel-width adaptation scheme outperforms the SRTCWA and SRFCW. Compared to the SRTCWA, for all the cases, DGR-SRORA improves the network throughput by 14.3%, 20.0%, 18.5%, 15.0%, 13.3% and 16.1%, respectively. When compared to the SRFCW, for all the cases, DGR-SRORA enhances the network throughput by 28.6%, 30.0%, 29.6%, 25.0%, 22.2% and 24.2%, respectively.

2. Resource Allocation Delay

The total time required for the distributed resource allocation procedure is investigated. In our simulation, the sum of the control subframe and the data subframe is assumed to be 100 ms. For each case of Node-Link pair, we consider different lengths of control subframe and

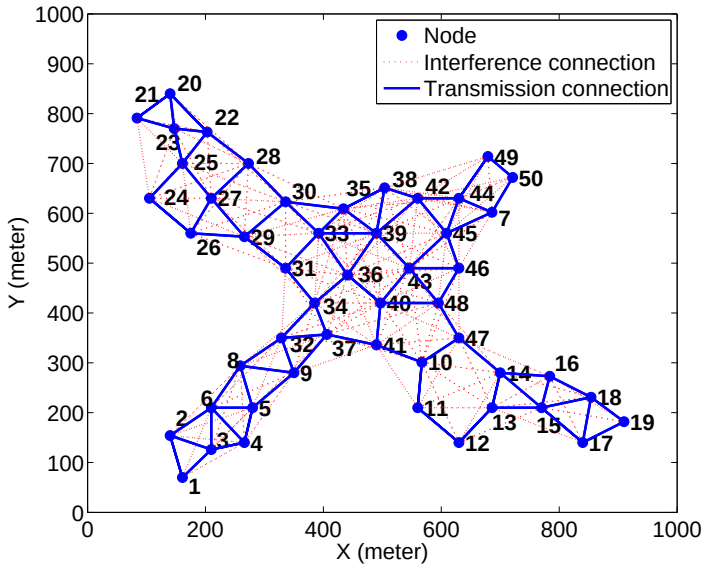


Figure 2.9: Network topology

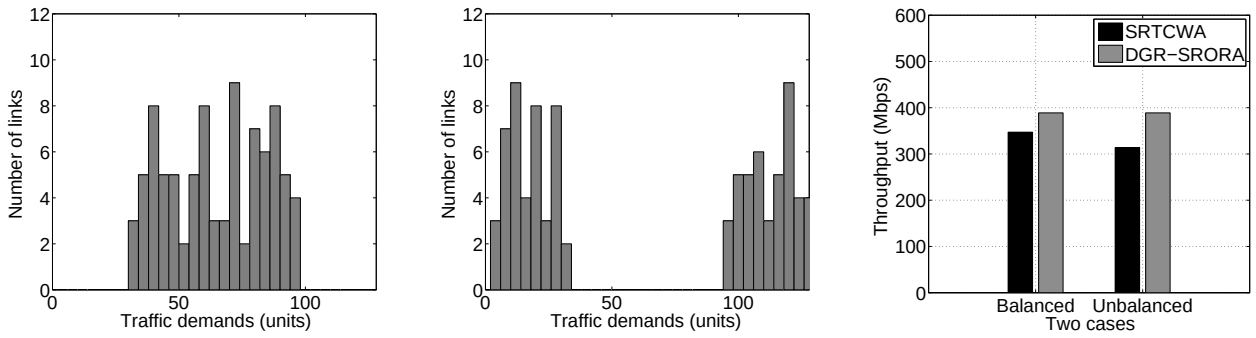
data subframe. The results are shown in Table 2.1. For each case of Node-Link pair, when the control subframe is longer, the allocation delay is smaller. Thus, if we need a faster allocation procedure, a larger control subframe is necessary, which leads to more overhead in signaling. However, even if the overhead is less than 10% for signaling, the allocation can be done within 1 second for Node-Link pairs: 10-15, 10-20, 20-30, 20-40, and 30-45. Such a fast allocation procedure means that our MAC protocol is highly adaptive to dynamic network conditions such as topology change or traffic variations.

Multi-Interference-Domain Scenario

In this scenario, 50 nodes are randomly distributed in a square whose side length is 1000 meter, as shown in Figure 2.9. The distributed MAC protocol with modified ANN packets transmission in Section 2.4 is adopted. In this protocol, the ANN packets are broadcast after a randomly chosen waiting time for several rounds.

1. Network Throughput

We investigate the impact the network traffic demand distribution brings to the network throughput in Figure 2.9. Since there exist multiple interference domains, the distributed



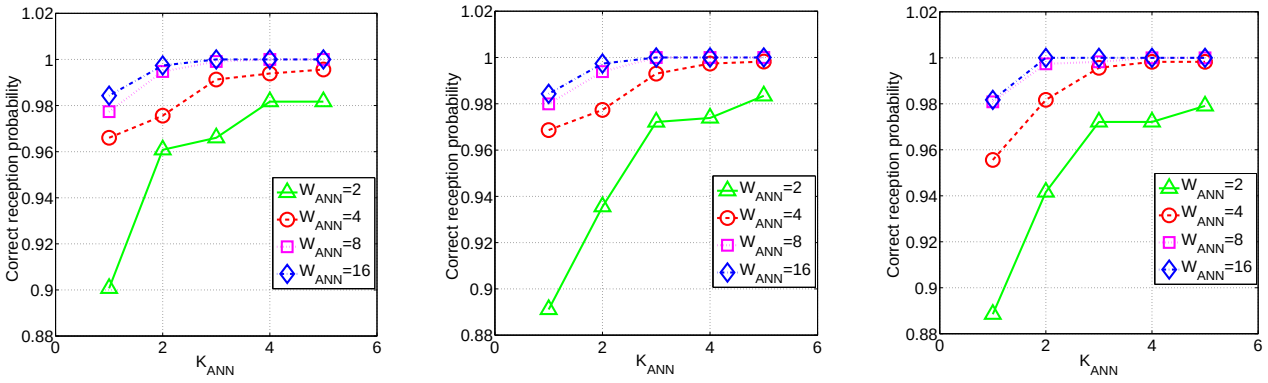
(a) Balanced traffic (b) Unbalanced traffic (c) Network throughput

Figure 2.10: Network throughput under different traffic distributions

protocol DGR-SRORA may have allocation error due to the ANN packet collision. Thus, we set broadcasting rounds and backoff window properly large to avoid the collision. We randomly choose 88 links in Figure 2.9 for the test. Two cases with different traffic distributions are considered. In the first case, the traffic demand of each link is balanced and is uniformly distributed in $\{32, \ldots, 96\}$, as shown in Figure 2.10(a). In the second case, the traffic demand of each link is unbalanced and is uniformly distributed in $\{1, 32\}$ or $\{96, 128\}$, as shown in Figure 2.10(b). The network throughput of these two cases are shown in Figure 2.10(c). As compared to the traditional channel-width adaptation scheme (i.e., SRTCWA), the MAC protocol with OFDMA-based channel-width adaptation improves the network throughput by 12% and 24% in case one and two, respectively. Our OFDMA-based channel-width adaptation scheme obtains higher throughput improvement in the case of unbalanced traffic distribution, because the OFDMA-based scheme makes it possible that each node can allocate resource more properly and support several communication links simultaneously.

2. Performance of Modified ANN Packets Broadcasting Mechanism

In Section 2.4.4, we propose that the ANN packets are broadcast after a randomly chosen waiting time for several rounds in order to reduce the collision probability. In this test, how well this mechanism works is investigated with different broadcasting rounds K_{ANN} and backoff window W_{ANN}. In Figure 2.9, we randomly choose 88 links for testing. Three cases with 10ms, 15ms and 20ms control subframes are considered. In each case, the broadcasting rounds K_{ANN}



(a) Control subframe: 10ms (b) Control subframe: 15ms (c) Control subframe: 20ms

Figure 2.11: ANN packet reception probability of the entire network for multi-interference-domain scenario

Table 2.2: Total resource allocation time for multi-interference-domain scenario

Rounds	$W_{ANN}(10ms)^a$				$W_{ANN}(15ms)^b$				$W_{ANN}(20ms)^c$			
	2	4	8	16	2	4	8	16	2	4	8	16
K_{ANN}=1	0.20s	0.31s	0.50s	1.01s	0.11s	0.20s	0.31s	0.51s	0.10s	0.11s	0.21s	0.41s
K_{ANN}=2	0.21s	0.40s	0.71s	1.21s	0.20s	0.21s	0.41s	0.81s	0.11s	0.20s	0.31s	0.52s
K_{ANN}=3	0.31s	0.50s	0.91s	1.70s	0.20s	0.30s	0.51s	1.11s	0.12s	0.21s	0.40s	0.71s
K_{ANN}=4	0.40s	0.60s	1.21s	2.70s	0.21s	0.40s	0.61s	1.51s	0.20s	0.30s	0.51s	0.90s
K_{ANN}=5	0.50s	0.70s	1.31s	3.30s	0.30s	0.41s	0.80s	1.70s	0.21s	0.31s	0.52s	1.10s

[a]The length of the control subframe is 10ms
[b]The length of the control subframe is 15ms
[c]The length of the control subframe is 20ms

varies from 1 to 5, and the broadcasting delay time is randomly chosen in backoff window W_{ANN}. The W_{ANN} is set 2, 4, 8 and 16 (The unit is the transmission time of an ANN packet), respectively. The total correct reception probability is defined as the ratio of the sum of the actual receiving ANN packets number of each node to the sum of the theoretical receiving ANN packets number of each node. From Figure 2.11, in each case, for the fixed K_{ANN}, the correct reception probability is higher with larger W_{ANN}. Similarly, for the fixed W_{ANN}, the correct reception probability is increased with increased K_{ANN}. For each case, when $K_{ANN} = 3$ and $W_{ANN} = 16$, or when $K_{ANN} = 4$ and $W_{ANN} = 8$, the correct reception probability can reach 1.

3. Resource Allocation Delay

The total time required for the distributed resource allocation procedure in Section 2.4.4 is

also investigated. In our simulation, the sum of the control subframe and the data subframe is assumed to be 100 ms. Three cases with 10ms, 15ms and 20ms control subframes are considered. The results are shown in Table 2.2. When the control subframe is longer, the allocation delay is smaller. Thus, if we need a faster allocation procedure, a larger control subframe is necessary, which leads to more overhead in signaling. In each case, for the fixed K_{ANN}, the allocation time is increased with the increased W_{ANN}. Similarly, for the fixed W_{ANN}, the allocation time is increased with the increased K_{ANN}. For $K_{ANN} = 3$ and $W_{ANN} = 16$, the maximum time consumption of three cases is 1.70s (the 10ms control subframe case). For $K_{ANN} = 4$ and $W_{ANN} = 8$, the maximum time consumption of three cases is 1.21s (the 10ms control subframe case). Therefore, with 10% signaling overhead, the correct reception probability can reach 1 with allocation time less than 2s.

2.6 Summary

In WMNs, there always exists a mismatch between the link capacity and the traffic demand. In this chapter, an OFDMA-based channel-width adaptation mechanism was proposed to eliminate such mismatch of each link in WMNs. It was formulated as a subchannel and time slot allocation problem and was proved to be NP-complete. Thus, a greedy algorithm and a genetic algorithm were developed to obtain the suboptimal solution. Based on the greedy algorithm, a distributed MAC protocol was designed to carry out channel-width adaptation for all links in the WMN. Simulation results showed that the new MAC protocol outperformed MAC protocols with traditional channel-width adaptation scheme.

Chapter 3

Fast Secret Key Generation in Static Wireless Networks

3.1 Motivation

Recently, there has been great interest in generating a shared secret key based on the physical (PHY)-layer security techniques [Ren et al. (2011)]. Different from the traditional secret key sharing procedure like Diffie-Hellman key exchange protocol, PHY-layer based secret key generation approach does not rely on computational hardness and can even achieve information-theoretical secrecy [Mathur et al. (2008)].

In wireless networks, the legitimate sender and the receiver utilize their two-way reciprocal wireless channel as the common source to share their secret key. So far many research papers have emerged in this area. The legitimate communication pair can share a secret key through the channel magnitude and RSSI [Mathur et al. (2008)] [Jana et al. (2009)] [Zeng et al. (2010)] [Madiseh et al. (2008)] [Wilson et al. (2007)], or through the channel phase [Sayeed and Perrig (2008)] [Koorapaty et al. (2000)] [Wang et al. (2011)].

However, the performances of the above schemes heavily depend on large channel variation.

In environments with long coherence time, the channel variation is limited, so the secret key generation rate is extremely low. This problem has been addressed in [Gollakota and Katabi (2011)], where a channel independent scheme is proposed. In this scheme, the transmitter sends the same key sample twice, and the receiver randomly jams one of the samples to confuse the eavesdropper. The secrecy depends on the statistical characteristics of transmitting data in an OFDM system. Thus, this scheme is only effective for an OFDM-based system.

In this chapter, we take a different approach to generate secret keys in a wireless environment with long coherence time. It combats shortage of time diversity by exploiting opportunistic beamforming and frequency diversity. Since the rate and range of channel fluctuations can be utilized to generate secret keys, we induce channel fluctuations with two antennas. This type of "virtual" channel variations are actually accomplished via opportunistic beamforming* [Viswanath et al. (2002)]. However, unlike the work in [Viswanath et al. (2002)] where parameters of multiple antennas are randomly selected to generate channel fluctuations for exploring opportunistic transmissions, our scheme deliberately controls these parameters to ensure the quality of key generation. Virtual channel variation dramatically increases the key generation rate. However, there exists correlation in channel fluctuations between the legitimate channel and the eavesdropping channel. As a result, the secrecy does not constantly improve as the key size increases. In order to ensure secrecy growth with the key size, frequency diversity is considered. More specifically, different portions of the same key are generated in different frequency channels. By integrating virtual channel variations and frequency diversity, a nearly perfect secret key can be generated at a rate of $2 \sim 20$Kb/s.

In this chapter, the secret key generation scheme is investigated in both narrowband systems (e.g., GSM) and wideband systems (e.g., WiFi). Both analysis and simulations are carried out to evaluate performance parameters including key generation rate, agreement, randomness, and secrecy.

*Opportunistic beamforming does not require specially designed antennas.

The remainder of this chapter is organized as follows. The system model and our design are given in Section 3.2. Key generation is designed and analyzed in Section 3.3. Application of our design to narrowband and wideband systems is investigated in Section 3.4. Performance results are presented in Section 3.5. Extensions of our scheme are discussed in Section 3.6, and the chapter is concluded in Section 3.7.

3.2 System Model and Design Principles

3.2.1 System Model

We consider a general secure wireless communication system, as shown in Figure 3.1. The legitimate transmitter Alice sends messages to the legitimate receiver Bob in the presence of the eavesdropper Eve. Similar to assumptions in other papers [Mathur et al. (2008)] [Wang et al. (2011)], we assume Eve knows the communication protocol between the legitimate transmitter and the receiver, and can perform channel estimation with received signals. Alice is equipped with two antennas, Bob with one antenna, and Eve with multiple antennas. For simplicity, the number of all antennas in the system is indexed from 1 to k, as shown in Figure 3.1. The system is assumed narrowband, and extension to wideband is considered in Section 3.4.2. The wireless channel is assumed to be reciprocal. h_{13} and h_{23} are the complex channel gains from antennas 1 and 2 on Alice to antenna 3 on Bob. Similarly, h_{1k} and h_{2k} are the complex channel gains from Alice to antenna k on Eve.

Considering the transmitter of Alice, if symbol $x[m]$ transmitted from Alice is multiplied by the complex number $\sqrt{\alpha}e^{j\theta_1}$ on antenna 1 and $\sqrt{1-\alpha}e^{j\theta_2}$ on antenna 2 (where $\alpha \in [0,1]$, $\theta_1 \in [0, 2\pi]$, and $\theta_2 \in [0, 2\pi]$), Bob receives the following signal:

$$y_{AB}[m] = d_{AB}^{-\frac{\gamma}{2}}(\sqrt{\alpha}e^{j\theta_1}h_{13} + \sqrt{1-\alpha}e^{j\theta_2}h_{23})x[m] + w_{AB}[m], \tag{3.1}$$

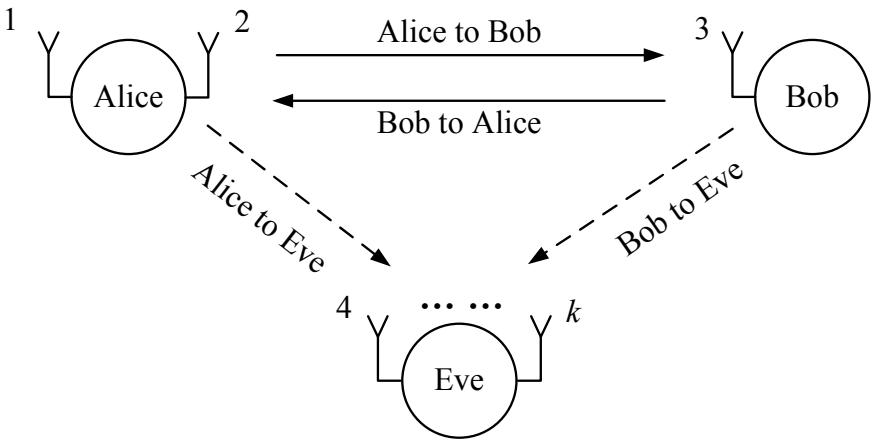


Figure 3.1: The secure communication model

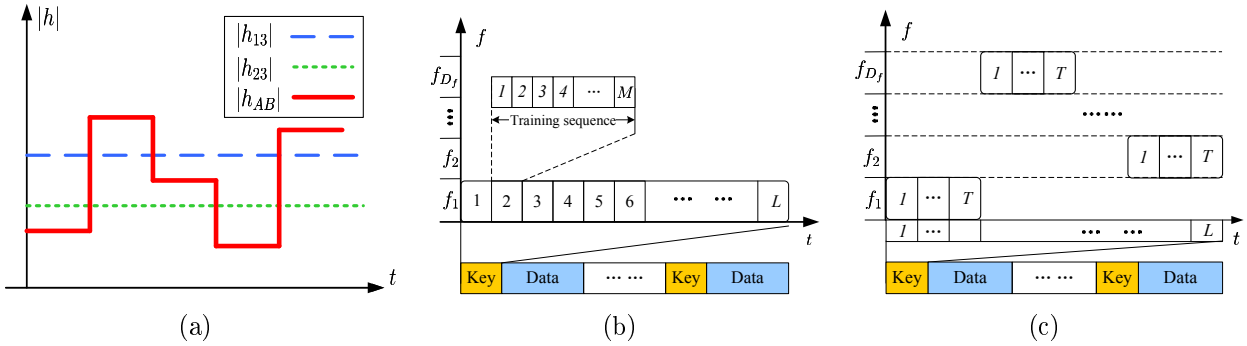
where d_{AB} is the distance between Alice and Bob, and γ is the pathloss exponent. h_{13} and h_{23} denote the channel fading gains between Alice and Bob, and are assumed identically and independently distributed as $\mathcal{CN}(0, \sigma_h^2)$. $w_{AB}[m]$ represents additive white Gaussian noise with distribution $\mathcal{CN}(0, \sigma_w^2)$. Considering that Alice leaks information to Eve, the received signal on antenna k of Eve is:

$$y_{AE^k}[m] = d_{AE}^{-\frac{\gamma}{2}}(\sqrt{\alpha}e^{j\theta_1}h_{1k} + \sqrt{1-\alpha}e^{j\theta_2}h_{2k})x[m] + w_{AE^k}[m], \tag{3.2}$$

where d_{AE} is the distance between Alice and Eve, $h_{1k} \sim \mathcal{CN}(0, \sigma_h^2)$, $h_{2k} \sim \mathcal{CN}(0, \sigma_h^2)$, and $w_{AE^k}[m] \sim \mathcal{CN}(0, \sigma_w^2)$. Without loss of generality, σ_h^2 and σ_w^2 are normalized to unity. Since $|\sqrt{\alpha}e^{j\theta_1}|^2 + |\sqrt{1-\alpha}e^{j\theta_2}|^2 = 1$, the total power of two antennas is constant. It also indicates that α of the total power is allocated to antenna 1 and $1-\alpha$ of the total power is allocated to antenna 2.

3.2.2 Design Principle of Our Novel Key Generation Scheme

In a wireless channel with long coherence time, we deliberately increase the channel variation with two antennas. From (3.1), the combined channel gain between the two antennas of Alice



(a) (b) (c)

Figure 3.2: Illustrations of our novel design for fast secret key generation in environments with long coherence time: (a) channel fluctuation with varied (α, θ_1, θ_2), (b) secret key generation without frequency diversity, and (c) secret key generation with frequency diversity

and the antenna of Bob can be expressed as:

$$h_{AB} = \sqrt{\alpha}e^{j\theta_1}h_{13} + \sqrt{1-\alpha}e^{j\theta_2}h_{23}. \tag{3.3}$$

We call h_{AB} the **virtual channel gain**. h_{AB} changes by varying $(\alpha, \theta_1, \theta_2)$. As shown in Figure 3.2(a), although h_{13} and h_{23} are unchanged within a coherence time, the virtual channel gain h_{AB} varies with different $(\alpha, \theta_1, \theta_2)$.

With this induced channel variation, the secret key can be generated as follows. First, Alice determines L 3-tuple $(\alpha, \theta_1, \theta_2)$ to achieve L virtual channel gains $\overrightarrow{h_{AB}}$ (i.e., $[h_{AB}(1), h_{AB}(2), \ldots, h_{AB}(L)]$) based on h_{13} and h_{23} (In an environment with sufficient long coherence time, it is easy for Alice to obtain accurate h_{13} and h_{23} with long training sequence). Second, for each $(\alpha, \theta_1, \theta_2)$, Alice transmits an M-symbol training sequence $\boldsymbol{x}$ (i.e., $\boldsymbol{x} \in \mathbb{C}^{M\times 1}$) to Bob and Bob estimates the virtual channel gain as $\hat{h}_{AB}$ with the least square (LS) estimation method [Kay (1993)], as discussed in Section 3.3.1. One time of this sending-and-receiving process is called a **channel probe**. The estimated virtual channel gain $\hat{h}_{AB}$ is a **sample** of a secret key at Bob. As shown in Figure 3.2(b), one key consists of L samples and each sample is estimated with an M-symbol training sequence. For each channel probe, (α, θ_1, θ_2) is kept unchanged. However, (α, θ_1, θ_2) varies from one channel probe to another.

Correspondingly, the sample $\hat{h}_{AB}$ at Bob changes. Finally, Bob obtains L samples $\overrightarrow{\hat{h}_{AB}}$ (i.e., $[\hat{h}_{AB}(1), \hat{h}_{AB}(2), \ldots, \hat{h}_{AB}(L)]$). Alice and Bob convert each sample of $\overrightarrow{h_{AB}}$ and $\overrightarrow{\hat{h}_{AB}}$ into bits to constitute a secret key with a proper quantization scheme and a well designed sample-to-key bit-mapping scheme as discussed in Section 3.3.2 and 3.3.5, respectively.

In our novel key generation scheme, $\overrightarrow{h_{AB}}$ is controlled by Alice, which brings two advantages for the secret key: high randomness (as discussed in Section 3.3.2) and high accuracy (as discussed in Section 3.3.3). Moreover, unlike two-way channel estimation approach in many papers [Ren et al. (2011)] [Mathur et al. (2008)], our scheme only needs one-way channel probe, i.e., Alice generates samples of the key on its own, and Bob extracts the samples of the shared key from the estimated virtual channels. Our one-way scheme is fit for static wireless networks where Alice can obtain fixed channel gains, and reduces the times of channel probing to improve the key generation rate.

Since channel variations are induced by Alice, there exists correlation between the legitimate virtual channel and eavesdropping virtual channel, which degrades the secrecy as discussed in Section 3.3.4. To ensure that secrecy matches the key size, merely increasing key size following Figure 3.2(b) is not effective. We need to exploit frequency diversity to generate different portions of the key. As shown in Figure 3.2(c), each portion of the key consists of T samples generated in one channel.

In the key generation phase shown in Figure 3.2(c), $(\alpha, \theta_1, \theta_2)$ on two antennas are controlled to induce virtual channel variations. However, in the data transmission phase, the antennas are tuned according to the data transmission techniques specified by the system.

3.2.3 Role of Frequency Diversity

Frequency diversity plays an important role in improving key secrecy. However, it should be noted that merely exploiting frequency diversity is impossible to achieve fast secret key generation, because only a limited number of independent channels are usually available in a

wireless communication system. Moreover, even if a large number of independent channels are available, key randomness cannot be achieved, due to static channels. As a result, exploiting more virtual channels in different independent frequencies is indispensable.

3.3 Secret Key Generation Based on Virtual Channel

In this section, we present a detailed design of our secret key generation scheme and analyze its performance.

3.3.1 Virtual Channel Estimation

Alice sends an M-symbol training sequence $\boldsymbol{x}$ to Bob with properly chosen $(\alpha, \theta_1, \theta_2)$, and Bob receives M-symbol signal $\boldsymbol{y} = \boldsymbol{x} d_{AB}^{-\frac{\gamma}{2}} h_{AB} + \boldsymbol{w}$. The least square (LS) estimation method [Kay (1993)] is adopted to estimate the virtual channel gain with $\boldsymbol{y}$ as:

$$\hat{h}_{AB} = \sqrt{\alpha} e^{j\theta_1} h_{13} + \sqrt{1-\alpha} e^{j\theta_2} h_{23} + N_{AB}, \tag{3.4}$$

where N_{AB} is the estimation error. Based on the LS estimation theory, $N_{AB} \sim \mathcal{CN}(0, (d_{AB}^{-\frac{\gamma}{2}} \boldsymbol{x}^* d_{AB}^{-\frac{\gamma}{2}} \boldsymbol{x})^{-1} \sigma_w^2)$. Since $d_{AB}^{-\frac{\gamma}{2}} \boldsymbol{x}^* d_{AB}^{-\frac{\gamma}{2}} \boldsymbol{x}$ is $M \cdot \mathbb{E}\big[|x[m]|^2\big] \cdot d_{AB}^{-\gamma}$ and SNR at Bob is $\mathbb{E}\big[|x[m]|^2\big] \cdot d_{AB}^{-\gamma} / \sigma_w^2$, the distribution of N_{AB} can be simplified as $\mathcal{CN}(0, \frac{1}{M \cdot SNR})$.

Thus, when SNR is $30dB$ and M is 20, the variance of the estimation error is 5×10^{-5}. The estimation error influences the sample agreement, which will be discussed in Section 3.3.3.

3.3.2 Sample Quantization and Selection

We design a 16-level quantization scheme to quantize each sample. The whole complex plane is divided into 16 quantization regions as shown in Figure 3.3(a). Regions 6, 7, 10 and 11 are 0.25×0.25 squares.

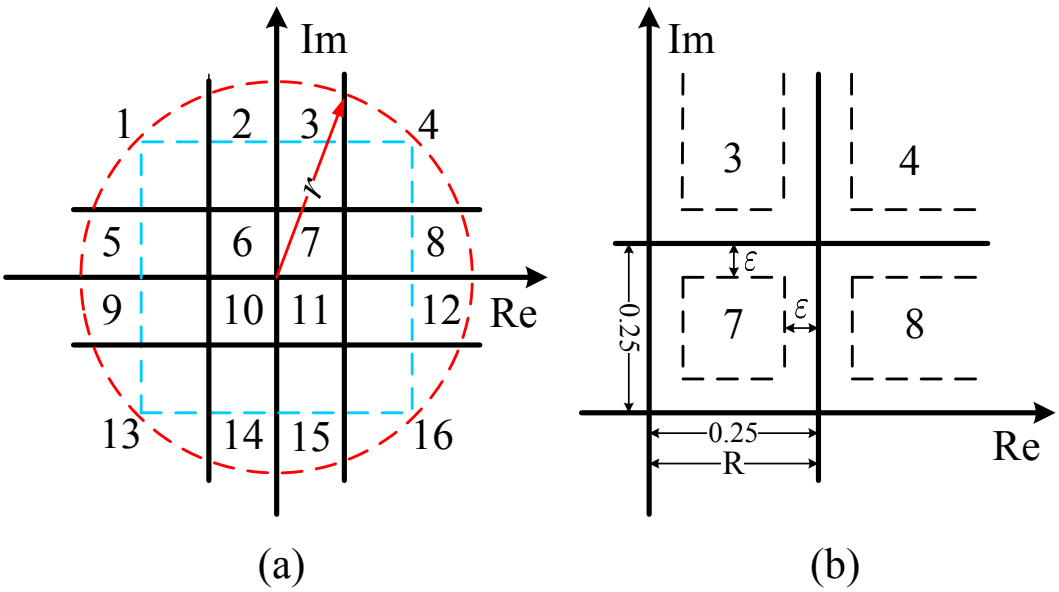


Figure 3.3: (a) The 16-level quantization scheme and (b) guardband ε for enhancement of sample agreement

With the design in Figure 3.3(a), quantization at Alice and Bob follows a different procedure: For Alice, a quantization region is first chosen randomly among all regions, and a point in this region is uniformly selected. Based on this point, Alice determines (α, θ_1, θ_2) to generate a controlled virtual channel gain. This procedure guarantees the randomness of key samples. If $(\alpha, \theta_1, \theta_2)$ are randomly chosen, several consecutive samples may fall into the same quantization region, which reduces the randomness of a secret key. For Bob, the quantization region is determined by the estimated virtual channel gain. For both Alice and Bob, Gray coding is adopted for mapping from a region to bits.

It should be noted that the quantization region that can be covered is limited by the channel gains between Alice and Bob, i.e., h_{13} and h_{23}. Given a particular value of h_{13} and h_{23}, by changing (α, θ_1, θ_2), it can be proved that the area which h_{AB} traverses in the complex plane is a disk, whose center is the origin and radius r is $|||[h_{13}, h_{23}]|||$, as shown in Figure 3.3(a). Thus, the quantization regions Alice can cover depends on h_{13} and h_{23}. For the Rayleigh fading, the probability that the disk can cover all the quantization regions can be calculated as $\text{Prob}(r > 0.25\sqrt{2}) = 99.28\%$. Thus, it is highly possible that Alice can control the virtual

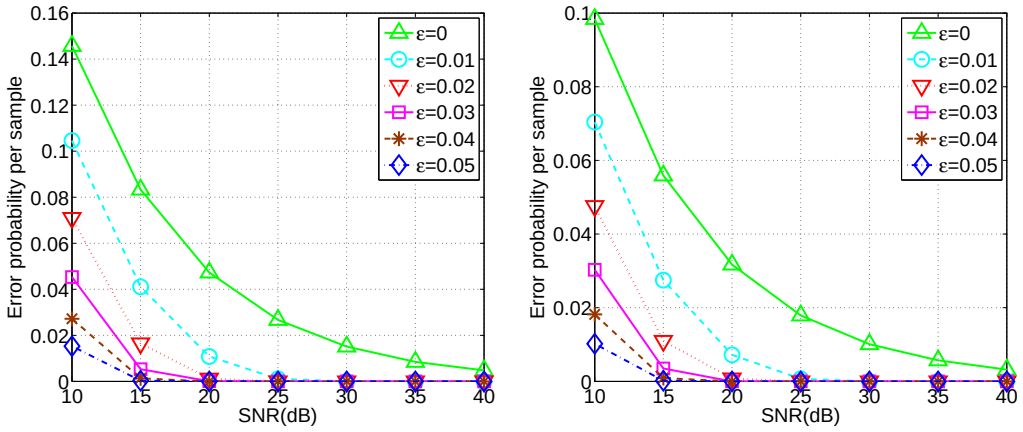
channel gain such that a sample is in any of 16 quantization regions. In case that the channel gains (h_{13} and h_{23}) do not ensure a full coverage of all regions, Alice can just randomly choose one from inner 4 regions. This approach does not degrade secrecy, because Eve has no way to know whether Alice can cover 16 regions or 4 regions.

3.3.3 Sample Disagreement: Analysis and Solution

For the sample disagreement analysis, we focus on the case that the disk of the virtual channel gain covers the dashed 0.5×0.5 square as shown in Figure 3.3(a). For the Rayleigh fading, the probability of this case is $\text{Prob}(r > 0.5\sqrt{2}) = 90.98\%$. Theoretical analysis of this highly probable case can represent the results of all scenarios, as validated by the simulation results in Section 3.5.1.

For a sample near the border of the quantization region at Alice's side, the estimated sample at Bob's side may fall in a different quantization region, leading to sample disagreement (i.e., sample error). To prevent this, sample h_{AB} at Alice is controlled in a guarded area which has a guardband ε to the border of the quantization region, as shown in Figure 3.3(b). The estimated sample $\hat{h}_{AB}$ by Bob is $h_{AB} + N_{AB}$, where $N_{AB} \sim \mathcal{CN}(0, \frac{1}{M \cdot SNR})$. To calculate the error probability, R is defined as 0.25, ε represents the guardband, and σ_e^2 is defined as $\frac{1}{2 \cdot M \cdot SNR}$. The error probability per sample varies with different quantization regions. We need to consider three categories: I (i.e., regions 1, 4, 13 and 16), II (i.e., regions 2, 3, 5, 8, 9, 12, 14 and 15), and III (i.e., regions 6, 7, 10 and 11). Since h_{AB} is controlled randomly in one of the quantization regions and is uniformly distributed in the guarded area of the selected region, the upper bound of the error probability, denoted as P_e^U, can be calculated as:

$$\begin{aligned} P_e^U =& \frac{1}{4} \times P_e^I + \frac{1}{2} \times P_e^{II} + \frac{1}{4} \times P_e^{III} \\ =& \frac{1}{4}(1 - P_1 P_1) + \frac{1}{2}(1 - P_1 P_2) + \frac{1}{4}(1 - P_2 P_2), \end{aligned} \tag{3.5}$$



(a) Upper bound (b) Lower bound

Figure 3.4: Error probability per sample for our 16-level quantization scheme: (a) theoretical upper bound and (b) theoretical lower bound

where $P_1 = \frac{1}{R-2\varepsilon}\int_{\varepsilon}^{R-\varepsilon}\int_{-\infty}^{y}\frac{1}{\sqrt{2\pi}\sigma_e}e^{-\frac{x^2}{2\sigma_e^2}}dxdy$, and $P_2 = \frac{1}{R-2\varepsilon}\int_{\varepsilon}^{R-\varepsilon}\int_{y-R}^{y}\frac{1}{\sqrt{2\pi}\sigma_e}e^{-\frac{x^2}{2\sigma_e^2}}dxdy$.

Correspondingly, the lower bound of the error probability, denoted as P_e^L, can be calculated with the following equation:

$$\begin{aligned} P_e^L =& \frac{1}{4}\times P_e^I + \frac{1}{2}\times P_e^{II} + \frac{1}{4}\times P_e^{III} \\ =& \frac{1}{2}(1-P_2) + \frac{1}{4}(1-P_2P_2). \end{aligned} \tag{3.6}$$

The theoretical error probability for different guardbands are shown in Figure 3.4, where the length of the training sequence M is fixed to be 50. The results indicate that for each fixed SNR, the error probability becomes smaller with the increment of guardband ε. When ε is 0.05, even in low SNR regime ($15dB$), the error probability reaches 0.

3.3.4 Key Secrecy Analysis

Eve can directly quantize its estimated virtual channel from Alice to form the key or guess the channel gains between Alice and Bob to crack the key.

Direct Key Generation (DKG) Scheme by Eve

In this case, Eve directly uses the samples from one of the receiving antennas to generate a key. Since all the antennas are the same, we take samples from antenna 4 for illustration. For a key consists of L samples, we assume Eve can accurately estimate each sample on antenna 4, i.e., $h_{AE}(l) = \sqrt{\alpha(l)}e^{j\theta_1(l)}h_{14} + \sqrt{1-\alpha(l)}e^{j\theta_2(l)}h_{24}$, where $l \in \{1, \cdots, L\}$. Eve can successfully crack all L samples when $h_{AE}(l)$ is in the same quantization region with $h_{AB}(l)$ for any l.

One condition for cracking the key is that h_{14} and h_{24} are near h_{13} and h_{23} respectively, i.e., $|h_{13} - h_{14}| \leq \delta$ and $|h_{23} - h_{24}| \leq \delta$, which provides a lower bound of the success probability of cracking a key. It can be derived that $|h_{AB}(l) - h_{AE}(l)| = |\sqrt{\alpha(l)}e^{j\theta_1(l)}(h_{13} - h_{14}) + \sqrt{1-\alpha(l)}e^{j\theta_2(l)}(h_{23} - h_{24})| \leq |\sqrt{\alpha(l)}e^{j\theta_1(l)} + \sqrt{1-\alpha(l)}e^{j\theta_2(l)}| \cdot |\delta| \leq \sqrt{2}|\delta|$. If $\delta = \frac{\varepsilon}{\sqrt{2}}$, then $|h_{AB}(l) - h_{AE}(l)| \leq \varepsilon$, i.e., $h_{AB}(l)$ and $h_{AE}(l)$ are always in the same quantization region for any l and any $(\alpha(l), \theta_1(l), \theta_2(l))$. Thus, under this condition, Eve can successfully crack a key with arbitrary length L.

For Rayleigh fading channels, the lower bound of the success probability of cracking a key using this DKG scheme, denoted as P_d^L, is:

$$\begin{aligned} P_d^L =& Pr\{|h_{13} - h_{14}| \leq \frac{\varepsilon}{\sqrt{2}}\} \cdot Pr\{|h_{23} - h_{24}| \leq \frac{\varepsilon}{\sqrt{2}}\} \\ =& (1 - e^{-\frac{\varepsilon^2}{4\sigma_h^2}})^2, \end{aligned} \tag{3.7}$$

where $|h_{13} - h_{14}|$ and $|h_{23} - h_{24}|$ are Rayleigh distributions. For $\varepsilon = 0.05$, $P_d^L = 3.90 \times 10^{-7}$.

However, even if h_{14} and h_{24} are not near h_{13} and h_{23}, it is possible that $h_{AE}(l)$ and $h_{AB}(l)$ are in the same quantization region for all L samples. To obtain a general success probability of cracking an L-length key, extensive simulations are carried out. As shown in Figure 3.5(a), when L is small, the success probability of cracking a key decreases dramatically as the key length increases. However, when L is more than 20, the success probability stays around $(1 \sim 3) \times 10^{-5}$.

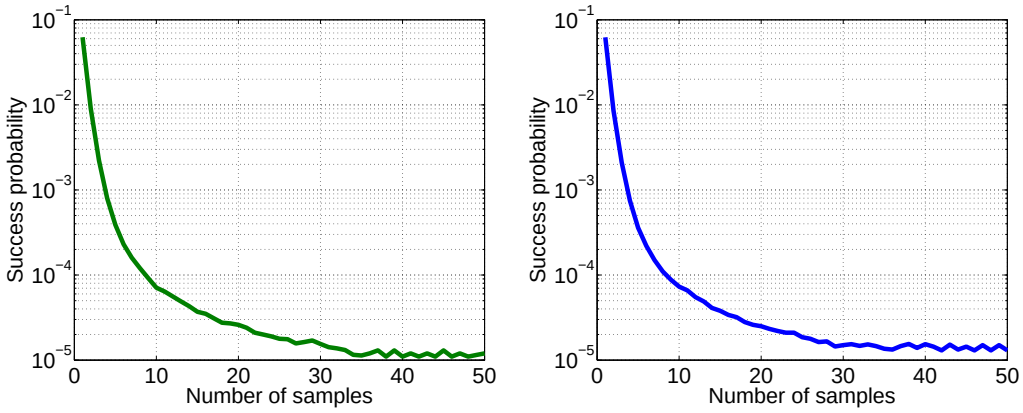


Figure 3.5: Success probability of cracking a key with different samples using (a) DKG scheme and (b) CG scheme

Channel Guessing (CG) Scheme by Eve

One straightforward scheme of cracking the key is to guess the key sample by sample independently. However, this scheme is inefficient. For example, if L is 32, each sample has 4 bits (16-level quantization), the success probability per guessing is as low as 2^{-128}. A better scheme for Eve is to rely on the correlation between the legitimate virtual channel and the eavesdropping virtual channel. More specifically, Eve can derive the 3-tuple $(\alpha, \theta_1, \theta_2)$ used by Alice, and then guesses the legitimate channel gains. Thus, Eve generates a secret key, which is usually different from the legitimate key.

It should be noted that Eve needs at least two antennas to estimate $(\alpha, \theta_1, \theta_2)$. With two antennas (e.g., antenna 4 and 5), Eve estimates virtual channel gains between Alice and Eve as follows.

$$\hat{h}_{AE^4} = \sqrt{\alpha} e^{j\theta_1} h_{14} + \sqrt{1-\alpha} e^{j\theta_2} h_{24} + N_{AE^4}, \tag{3.8}$$

$$\hat{h}_{AE^5} = \sqrt{\alpha} e^{j\theta_1} h_{15} + \sqrt{1-\alpha} e^{j\theta_2} h_{25} + N_{AE^5}. \tag{3.9}$$

From (3.8) and (3.9), Eve can estimate $\sqrt{\alpha}e^{j\theta_1}$ and $\sqrt{1-\alpha}e^{j\theta_2}$ with $\hat{h}_{AE^4}$ and $\hat{h}_{AE^5}$:

$$\widehat{\sqrt{\alpha}e^{j\theta_1}} = \frac{h_{25}\hat{h}_{AE^4} - h_{24}\hat{h}_{AE^5}}{h_{14}h_{25} - h_{15}h_{24}} = \sqrt{\alpha}e^{j\theta_1} + N_{\alpha,\theta_1}, \tag{3.10}$$

$$\widehat{\sqrt{1-\alpha}e^{j\theta_2}} = \frac{h_{15}\hat{h}_{AE^4} - h_{14}\hat{h}_{AE^5}}{h_{15}h_{24} - h_{14}h_{25}} = \sqrt{1-\alpha}e^{j\theta_2} + N_{\alpha,\theta_2}. \tag{3.11}$$

With $\widehat{\sqrt{\alpha}e^{j\theta_1}}$ and $\widehat{\sqrt{1-\alpha}e^{j\theta_2}}$, and guessed channel gains between Alice and Bob (h_{13}^g, h_{23}^g) according to the zero-mean circularly symmetric complex Gaussian distribution, Eve gets a guessed sample, i.e., $h_{AB}^g = (\widehat{\sqrt{\alpha}e^{j\theta_1}})h_{13}^g + (\widehat{\sqrt{1-\alpha}e^{j\theta_2}})h_{23}^g$. Based on guessed samples, Eve obtains a guessed key.

Similar to the analysis of the DKG scheme, we assume Eve can obtain accurate $\sqrt{\alpha}e^{j\theta_1}$ and $\sqrt{1-\alpha}e^{j\theta_2}$. When $|h_{13} - h_{13}^g| \leq \frac{\varepsilon}{\sqrt{2}}$ and $|h_{23} - h_{23}^g| \leq \frac{\varepsilon}{\sqrt{2}}$, Eve can always crack the key with arbitrary length. This lower bound of success probability of cracking a key, denoted as P_g^L, can be calculated as:

$$P_g^L = Pr\{|h_{13} - h_{13}^g| \leq \frac{\varepsilon}{\sqrt{2}}\} \cdot Pr\{|h_{23} - h_{23}^g| \leq \frac{\varepsilon}{\sqrt{2}}\}. \tag{3.12}$$

For the fixed h_{13} and h_{23}, guessed h_{13}^g and h_{23}^g are generated according to $\mathcal{CN}(0, \sigma_h^2)$. Thus, $|h_{13} - h_{13}^g|$ and $|h_{23} - h_{23}^g|$ are Rician distributions. For $\varepsilon = 0.05$, $h_{13} = 1$ and $h_{23} = 1$, P_g^L=2.11×10^{-7}. The maximum of P_g^L is 1.56×10^{-6}, achieved when $h_{13} = 0$ and $h_{23} = 0$.

Similar to the DKG scheme, to obtain a general success probability per channel guessing for cracking an L-length key, extensive simulations are carried out. The result in Figure 3.5(b) shows that the success probability per channel guessing drops dramatically with the increment of the key length, when L is small. However, when L is more than 20, the success probability per channel guessing stays around $(1 \sim 3) \times 10^{-5}$.

Success Probability of Cracking a Key

As shown in Figure 3.5, the success probabilities of cracking a key by two schemes are similar. However, the probability of each scheme has a different implication. In the DKG scheme, the probability indicates how many keys Eve needs to get before the legitimate key is cracked. In the CG scheme, Eve only needs one key, and then uses different guessed channel gains to crack the legitimate key. The probability in the CG scheme indicates how many times the channel gains need to be guessed. In either scheme, the success probability of cracking a key is too high to provide sufficient secrecy of the legitimate key. As a result, frequency diversity is exploited to improve the secrecy.

3.3.5 Secrecy Enhancement with Frequency Diversity

Frequency diversity provides independent fading channels, which can be utilized to increase key secrecy.

To exploit frequency diversity, each portion of a secret key is generated over independent fading channels. Suppose the success probability of cracking each portion of a key is P_c, and the number of channels with independent fading is D_f, then the success probability of cracking a whole key is $(P_c)^{D_f}$.

If each portion needs 4 samples, based on Figure 3.5, we know that P_c in two schemes are both around 0.0008. Then the success probability of cracking a key with 16 portions becomes 2.81×10^{-50}, which is lower than a 128-bit key (secrecy is 2.94×10^{-39}) and higher than a 256-bit key (secrecy is 8.63×10^{-78}). However, with 16 channels, 4 samples per channel, and 4 bits per sample, the key length is 256 bits.

This example shows that, if we simply apply frequency diversity, the key size does not match the secrecy. Therefore, we need to consider the tradeoff between the key size and the secrecy. Since the number of independent channels is critical to secrecy, it cannot be changed in tradeoff. However, we can consider the tradeoff between number of bits in each portion of a key and

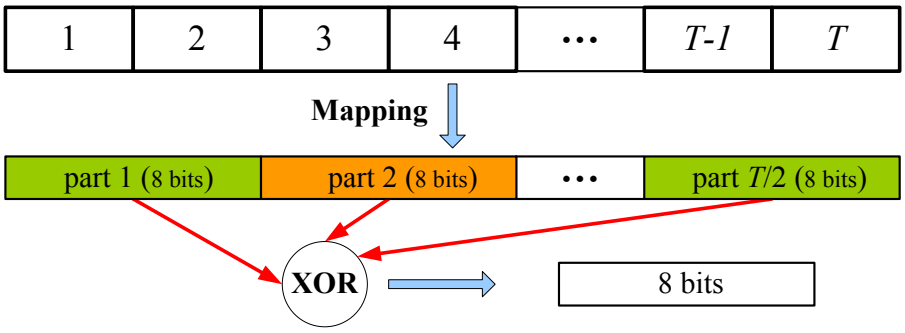


Figure 3.6: The XOR operation with T samples on one frequency channel

Table 3.1: Success probability for cracking 8 bits with different number of samples used in XOR operation

Scheme	T=4	T=8	T=12	T=16
DKG	0.00953	0.00496	0.00429	0.00386
CG	0.00836	0.00472	0.00421	0.00388

the secrecy of the portion. A scheme of such a tradeoff is proposed as follows. As shown in Figure 3.6, on one frequency channel, T samples are divided into $T/2$ parts, and all parts are combined together to form 8 bits with XOR operation. However, XOR operation also increases the success probability, so T is an important parameter in design. As shown in Table 3.1, when the number of samples is 4, the success probability for cracking 8 bits is around 0.009, which is higher than randomly guessing 8 bits, i.e., 3.91×10^{-3} (2^{-8}). Thus, we increase the number of samples for XOR operation to enhance the secrecy. From Table 3.1, 16 samples is a proper number (3.88×10^{-3}) for achieving perfect secrecy.

With the above design, if we need a 128-bit secret key, we require 16 channels, 16 samples per channel, and 4 bits per sample. Moreover, 16 samples have to be split into 8 parts and form 8 bits by XOR operation.

3.4 Application of Secret Key Generation

In this section, we discuss how the previous secret key generation scheme is applicable to both narrowband systems (e.g., GSM) and wideband systems (e.g., WiFi). The applications are

focused on a 128-bit key.

3.4.1 Narrowband Systems

We design a secret key generation protocol for a narrowband system, as shown in Algorithm 3.1. To secure a 128-bit key, the required frequency diversity D_f is 16 as discussed in Section 3.3.5. In a narrowband system, one channel can provide one frequency diversity. Thus, the required independent channel number N is 16. Taking typical narrowband system GSM as an example, the total bandwidth W is 25MHz and each channel bandwidth W_{ch} is 200KHz. Thus, the total channel number N_{ch} is 125. The typical delay spread T_d of this system is $1\sim2us$ [Tse and Viswanath (2005)]. According to formula $W_c=\frac{1}{2T_d}$ [Tse and Viswanath (2005)], the coherence bandwidth W_c is 0.25∼0.5MHz, i.e., if two channels are $0.25 \sim 0.5$MHz apart in the frequency domain, they are independent. Thus, 50∼100 independent channels are available, which is enough to obtain a frequency diversity of 16. Frequency-hopping on selected 16 independent channels is adopted and each portion of a key is generated on one channel.

To generate a 128-bit key, in Algorithm 3.1, 16 channels are adopted ($N = 16$) and 16 samples are transmitted per channel ($T = 16$). First, Alice selects 16 samples and determines corresponding $(\alpha, \theta_1, \theta_2)$ with known h_{13} and h_{23} on each channel. Then, Alice sends each sample to Bob, and Bob estimates the corresponding sample. Alice and Bob extract 8 bits on each channel with XOR operation, and then combine the bits from 16 channels to form a 128-bit key.

In a narrowband system, a channel probe on each channel can only generate one sample. Neglecting channel-hopping time, with symbol duration T_s, the sample rate is:

$$R^N_{sample} = \frac{1}{T_s \cdot M}(samples/s). \tag{3.13}$$

If $T_s = 5us$ and $M = 50$, then $R^N_{sample}=4 \times 10^3$ (samples/s). Such a high sample rate indicates

Algorithm 3.1

Input:
Frequency-hopping sequence: $[ch_1, ch_2, \ldots, ch_N]$.
$h_{13}(i)$, $h_{23}(i)$, $i \in [ch_1, ch_2, \ldots, ch_N]$.
Output: A 128-bit secret key.
Alice determines:
3-tuple $(\alpha, \theta_1, \theta_2)$ for T samples on each channel i:
$\overrightarrow{\alpha(i)} = [\alpha^1(i), \alpha^2(i), \ldots, \alpha^T(i)]$,
$\overrightarrow{\theta_1(i)} = [\theta_1^1(i), \theta_1^2(i), \ldots, \theta_1^T(i)]$,
$\overrightarrow{\theta_2(i)} = [\theta_2^1(i), \theta_2^2(i), \ldots, \theta_2^T(i)]$,
$i \in [ch_1, ch_2, \ldots, ch_N]$.
Alice sending and Bob receiving:

1: **for** i=ch_1 to ch_N **do**
2: **for** k=1 to T **do**
3: Alice transmits an M-symbol training sequence $\boldsymbol{x}$ with controlled $(\alpha^k(i), \theta_1^k(i), \theta_2^k(i))$.
4: Bob receives: $\boldsymbol{y} = d_{AB}^{-\frac{\gamma}{2}} h_{AB}^k(i)\boldsymbol{x} + \boldsymbol{w}$, and estimates: $\hat{h}_{AB}^k(i)$.
5: **end for**
6: **end for**
7: **Stop**

Samples-to-key mapping by Alice and Bob: 16 samples from one same channel form 8 bits with XOR operation. Combine the bits from 16 channels to constitute a 128-bit key.
Notation: $h_{AB}^k(i) = \sqrt{\alpha^k(i)} e^{j\theta_1^k(i)} h_{13}(i) + \sqrt{1-\alpha^k(i)} e^{j\theta_2^k(i)} h_{23}(i)$.

fast secret key generation is feasible in a static narrowband system.

3.4.2 Wideband Systems

For the wideband system, one channel is larger than the coherence bandwidth W_c. Thus, OFDM technique is adopted such that one channel can be seen as a set of parallel narrowband subchannels in the frequency domain. Taking the typical wideband system 802.11a in 5GHz as an example, the total available orthogonal channel number N_{ch} is 12. One channel width W_{ch} is 20MHz. There are 64 subchannels per channel and each subchannel bandwidth W_{sch} is 312.5KHz. In the application scenario of 802.11a, the typical delay spread T_d is $100 \sim 300ns$ [Hashemi (1993)]. Correspondingly, the coherence bandwidth W_c is $1.67 \sim 5$MHz. Thus, the independent fading subchannel number N_s per channel is $4 \sim 12$. Therefore, to provide a

frequency diversity of 16, the required channel number N is $2 \sim 4$. Particularly, if delay spread T_d is $400ns \sim 800ns$, a single channel is enough to support a frequency diversity of 16.

To generate a 128-bit key, in Algorithm 3.2, it is assumed 2 channels are adopted ($N = 2$), 8 independent subchannels are available per channel ($N_S = 8$), and 16 samples are transmitted per subchannel ($T = 16$). First, Alice determines $(\alpha, \theta_1, \theta_2)$ for 16 randomly selected samples with known subchannel gains $\tilde{h}_{13}$ and $\tilde{h}_{23}$ on each subchannel. Alice transmits samples on two channels. For each channel, Alice calculates 16 M-symbol training sequences with determined $(\alpha^k(i,j), \theta_1^k(i,j), \theta_2^k(i,j))$ for 16 samples in each subchannel j and transforms these training sequences from each subchannel to 16 M-OFDM-symbol training sequences with IFFT. Then, Alice sends out 16 M-OFDM-symbol training sequences to Bob. Bob receives all these sequences and obtains 16 samples on each independent subchannel through FFT. Finally, Alice and Bob extract 8 bits on each subchannel with XOR operation, and then combine the bits from 16 subchannels to form a 128-bit key.

In a wideband system, a channel probe on one channel can generate N_s samples. Neglecting channel switch time, with OFDM symbol duration T_s, the sample generation rate is:

$$R^W_{sample} = \frac{N_s}{T_s \cdot M}(samples/s). \tag{3.14}$$

If $T_s = 4us$ and $M = 50$, then R^W_{sample}=$5 \times N_s \times 10^3$ (samples/s). As compared to narrowband systems, the sample rate of wideband systems is much higher and fewer channel switch times are needed.

3.5 Performance Evaluation

The performance evaluation metrics for our secret key generation protocols are as follows. 1) Key disagreement probability: it measures how many different bits between the key on Alice's side and that on Bob's side prior to error correction procedure. 2) Key generation rate: it

Algorithm 3.2

Input:
Channel switch sequence: $[ch_1, ch_2, \ldots, ch_N]$.
$\tilde{h}_{13}(i,j)$, $\tilde{h}_{23}(i,j)$, $i \in [ch_1, ch_2, \ldots, ch_N]$, $j \in [sc_1(i), sc_2(i), \ldots, sc_{N_s}(i)]$.
Output: A 128-bit secret key.
Alice determines:
3-tuple $(\alpha, \theta_1, \theta_2)$ for T samples on each subchannel:
$\overrightarrow{\alpha(i,j)} = [\alpha^1(i,j), \alpha^2(i,j), \ldots, \alpha^T(i,j)]$,
$\overrightarrow{\theta_1(i,j)} = [\theta_1^1(i,j), \theta_1^2(i,j), \ldots, \theta_1^T(i,j)]$,
$\overrightarrow{\theta_2(i,j)} = [\theta_2^1(i,j), \theta_2^2(i,j), \ldots, \theta_2^T(i,j)]$,
$i \in [ch_1, ch_2, \ldots, ch_N]$, $j \in [sc_1(i), sc_2(i), \ldots, sc_{N_s}(i)]$.
Alice sending and Bob receiving:

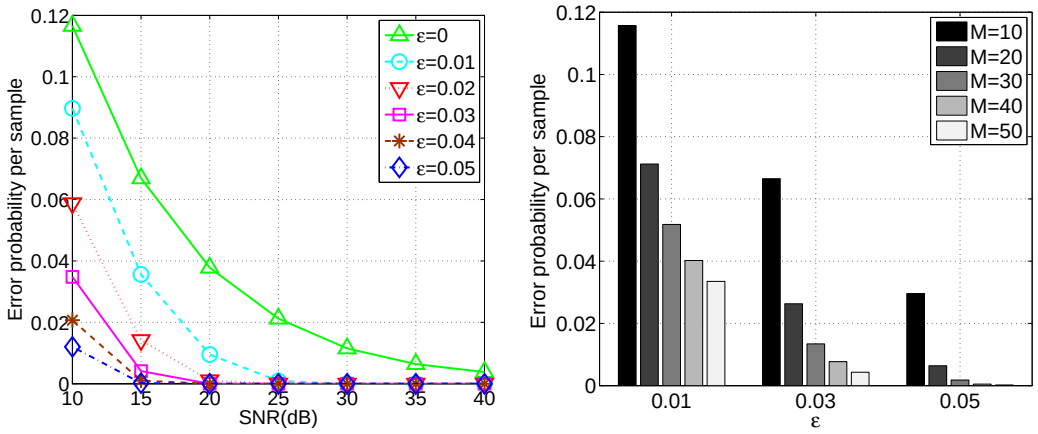
1: **for** i=ch_1 to ch_N **do**
2: **for** k=1 to T **do**
3: Alice transmits an M-OFDM-symbol training sequence with controlled $(\alpha^k(i,j), \theta_1^k(i,j), \theta_2^k(i,j))$ of N_s subchannels.
4: Bob receives the M-OFDM-symbol training sequence and transforms it with FFT. On subchannel j, Bob obtains: $\boldsymbol{y}(j) = d_{AB}^{-\frac{\gamma}{2}} \tilde{h}_{AB}^k(i,j)\boldsymbol{x} + \boldsymbol{w}$, and estimates: $\hat{\tilde{h}}_{AB}^k(i,j)$.
5: **end for**
6: **end for**
7: **Stop**

Samples-to-key mapping by Alice and Bob: 16 samples from one same subchannel form 8 bits with XOR operation, and combine the bits from 16 subchannels to constitute a 128-bit secret key.
Notation: $\tilde{h}_{AB}^k(i,j) = \sqrt{\alpha^k(i,j)} e^{j\theta_1^k(i,j)} \tilde{h}_{13}(i,j) + \sqrt{1-\alpha^k(i,j)} e^{j\theta_2^k(i,j)} \tilde{h}_{23}(i,j)$.

measures how fast the key can be generated. 3) Key bit randomness: the randomness of a bit sequence is measured using the NIST test suite [Rukhin et al. (2001)] before privacy amplification. 4) Key secrecy: the success probability that Eve guesses h_{13} and h_{23} to crack the secret key.

3.5.1 Study on Design Parameters through Simulations

We study the error probability per sample with 16-level quantization scheme under different conditions. For each condition, the error probability per sample is averaged over 1000 simulations. In each simulation, the channel gains h_{13} and h_{23} are generated according to Rayleigh fading, and Alice determines every sample as in Section 3.3.2. The error probability per sample



(a) $M = 50$ (b) $SNR = 15dB$

Figure 3.7: (a) Error probability per sample versus different guardband ε and SNR, and (b) error probability per sample versus different guardband ε and training sequence length M is calculated with 10000 samples.

Guardband ε

In Figure 3.7(a), the training sequence length M is fixed to be 50. It shows that for certain guardband ε, when SNR increases, the error probability is dramatically reduced. Similarly, for the fixed SNR, when guardband ε is larger, the error probability is smaller. The simulation results are between the upper bound and lower bound of the theoretical results in Section 3.3.3, which validate our theoretical analysis. Figure 3.7(a) also shows that when guardband ε is 0.05, even for low SNR ($15dB$), the error probability per sample nearly reaches 0.

Training Sequence Length M

In Figure 3.7(b), the SNR is fixed to be $15dB$. It indicates that, for the fixed guardband ε, when the training sequence length M is longer, the error probability per sample is smaller. Similarly, for the fixed M, when guardband ε is larger, the error probability per sample is smaller. It also shows even for low SNR ($15dB$), $M = 50$ and $\varepsilon = 0.05$ are sufficient to achieve extremely low error probability. From (3.13), when M is 50, the sample rate for narrowband system can achieve 4K (samples/s), which is fast enough for key generation.

Table 3.2: NIST statistical tests

TEST	p-value (N^a)	p-value (W^b)
DFT	0.5503	0.5868
Monobit Frequency	0.5986	0.5612
Approximate Entropy	0.9912	0.9953
Block Frequency	0.6063	0.6280
Runs	0.5975	0.5987
Cumulative Sums (Forward)	0.6139	0.5872
Cumulative Sums (Reverse)	0.6355	0.5953

[a]Narrowband system
[b]Wideband system

3.5.2 Key Generation for Narrowband and Wideband Systems

We test our scheme in both a narrowband system and a wideband system. For the narrowband system, 16 independent fading channels are used to provide 16 frequency diversity. The frequency-hopping sequence of 16 channels is randomly generated. On each channel, 16 samples are transmitted. Thus, there are total 256 samples. To constitute a 128-bit shared secret key, 16 samples on each channel are mapped to 8 bits of the key with XOR operation. For the wideband system, one channel is 20MHz, and the corresponding sampling rate of the system is $50ns$. The delay spread T_d of the environment is assumed to be $200ns$. Thus, we can extract 8 independent subchannels in each channel, i.e., one channel probe can generate 8 samples. Thus, two channels are adopted to satisfy 16 frequency diversity. 16 randomly selected samples are transmitted on each subchannel and are mapped to 8 bits of the key with XOR operation. The detailed key generation procedure follows Algorithm 3.1 and Algorithm 3.2. In the simulation, the guardband ε is fixed to be 0.05, SNR is fixed to be $20dB$, and training sequence length M is fixed to be 50.

Key Randomness

We use NIST test suite [Rukhin et al. (2001)] to verify the randomness of the key. In the test, we randomly select 100 key sequences that are generated from our simulations in both

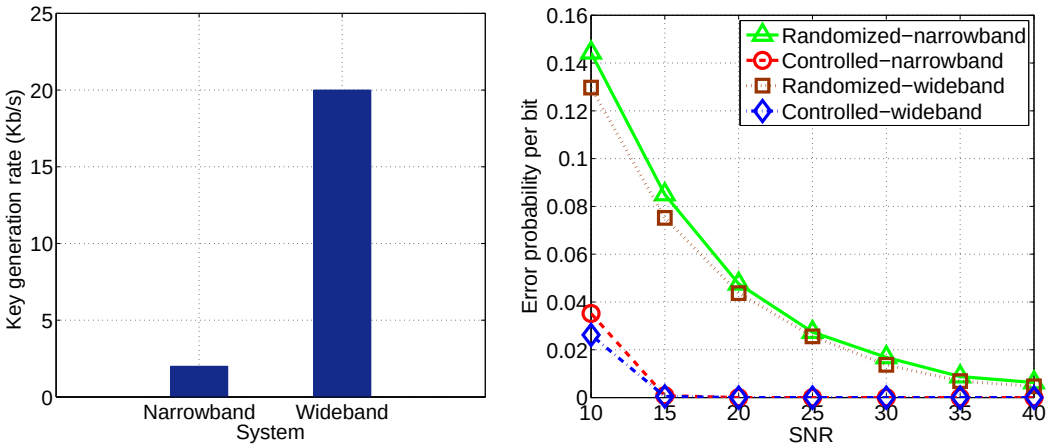


Figure 3.8: (a) Key generation rate and (b) error probability per bit for narrowband and wideband systems

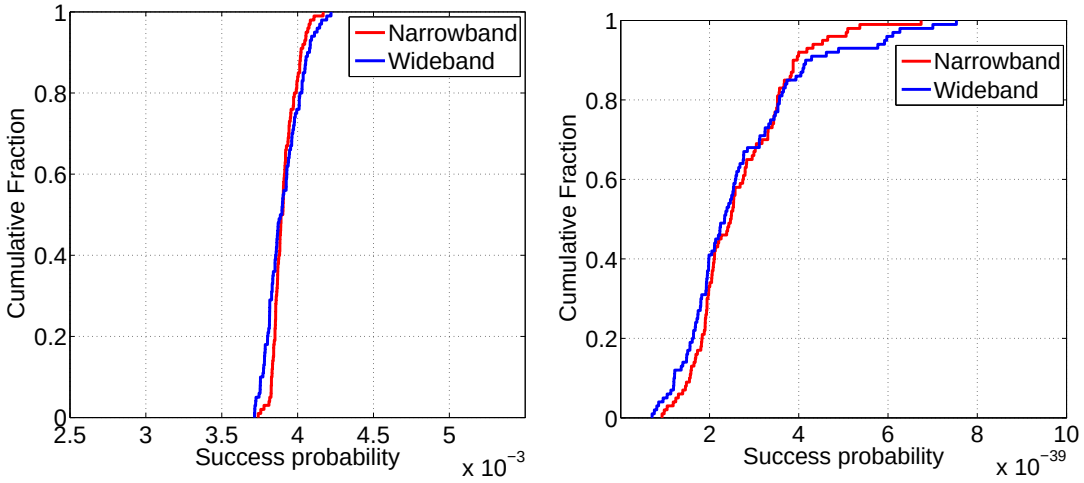
narrowband and wideband systems, and calculate their p-values. The averaged p-values for different tests are shown in Table 3.2. To pass each test, the p-value must be greater than 0.01. From Table 3.2, the averaged p-value for each test is greater than 0.01, indicating the generated key is random.

Key Generation Rate

As described before, for a 128 bits long secret key, 256 samples are transmitted. The transmission time for these 256 samples is different for the narrowband system and the wideband system. As shown in Figure 3.8(a), the key generation rate is 2 Kb/s for the narrowband system and 20 Kb/s for the wideband system. Such a high secret key generation rate can adapt to fast key changes.

Key Disagreement

In this test, SNR is varied from $10dB$ to $40dB$. The error probability per bit measures how many bits are different between the shared 128-bit key at Alice side and that at Bob side. In Figure 3.8(b), each point is averaged over 10000 simulations. It shows for both narrowband and



(a) (b)

Figure 3.9: (a) Cumulative distribution of success probability per channel guessing for cracking 8 bits and (b) cumulative distribution of success probability for cracking a secret key with 128 bits

wideband systems, given with the same SNR, the error probability per bit of our scheme (i.e., controlled (α, θ_1, θ_2)) is much lower than that of a scheme with randomly chosen (α, θ_1, θ_2). This gap is much larger in the low SNR regime. For our controlled (α, θ_1, θ_2) scheme, even in low SNR ($15dB$) regime, the error probability can reach 0. This result proves the benefits of controlling $(\alpha, \theta_1, \theta_2)$.

Key Secrecy

The cumulative distribution function (CDF) of success probability per channel guessing of cracking 8 bits for narrowband (wideband) system is shown with 100 rounds of simulations. In each simulation for narrowband (wideband) system, the success probability per channel guessing for cracking 8 bits is averaged over 16 channels (subchannels). On each channel (subchannel), 100000 experiments with channel-gain guessing by Eve are conducted. Figure 3.9(a) shows that the success probability per channel guessing for cracking 8 bits is between $(3.72 \sim 4.23) \times 10^{-3}$ with median 3.88×10^{-3}, which is near 3.91×10^{-3}(i.e., 2^{-8}). Thus, our key generation scheme achieves nearly perfect secrecy. In Figure 3.9(b), CDF curve for narrowband (wideband) is

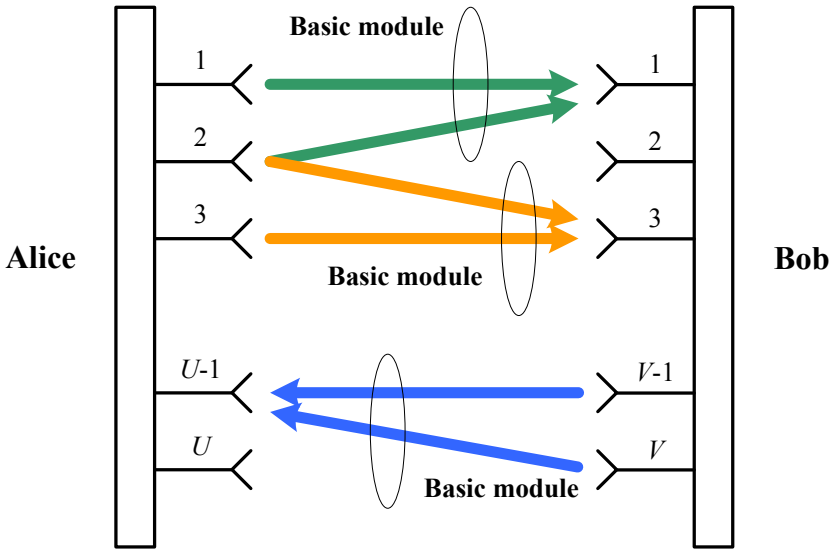


Figure 3.10: Extension to a $U \times V$ MIMO secure communication system

shown for the case of 128-bit key with 100 rounds of simulations. In each simulation, the success probability for cracking 128 bits is a product of the success probabilities for 16 independent channels (subchannels). As shown in Figure 3.9(b), the success probability for cracking 128 bits is between $(0.71 \sim 7.53) \times 10^{-39}$ with median 2.42×10^{-39}, which is less than 2.94×10^{-39}(i.e., 2^{-128}). Thus, our scheme of generating a 128-bit key has successfully achieved perfect secrecy.

3.6 Discussions

This chapter is focused on the key generation scheme. For information reconciliation, which is used to correct bit errors, we can resort to the existing schemes, e.g., error correcting codes [Dodis et al. (2004)] or some interactive information reconciliation protocols [Brassard and Salvail (1994)]. For privacy amplification, which is used to extract randomness, we can adopt some popular methods based on the leftover hash lemma, a well known technique to extract randomness from imperfect random sources [Impagliazzo et al. (1989)]. Since the key generated by our scheme has high agreement probability and high randomness, the information exchanged by Alice and Bob in the information reconciliation and privacy amplification phases is reduced.

The key secrecy can be further reinforced by a MIMO system, because spatial diversity improves security of wireless communications. For a general $U \times V$ MIMO system, several basic 2×1 MISO modules can be embedded in this MIMO system, as shown in Figure 3.10. Thus, the spatial diversity, i.e., the number of different virtual channels, for securing communications is $D_s = \binom{U}{2}V + \binom{V}{2}U$. If the frequency diversity for securing the communication is D_f, then Eve's success probability of cracking a key is reduced to $(P_c)^{D_s \cdot D_f}$, where P_c is the success probability of cracking a portion of a key in a virtual channel with no frequency diversity.

3.7 Summary

In this chapter, a novel secret key generation scheme was proposed for environments with long coherence time. It integrated opportunistic beamforming and frequency diversity to combat the shortage of time diversity. With controlled virtual channel fluctuations, secret keys were generated at a high rate with low bit-error probability and high randomness. By exploiting virtual channels on different frequencies, the secrecy was guaranteed. Applications of our scheme in both narrowband and wideband systems were investigated, and the results of the simulations validated the effectiveness of our scheme.

Chapter 4

Secrecy Enhancement with Artificial Noise in Decentralized Wireless Networks

4.1 Motivation

Artificial noise has been considered as an effective and efficient way to improve the secrecy of wireless communications. However, most existing artificial noise based approaches are analyzed in the scenario of a single legitimate transmitter-receiver communication link with some eavesdroppers. Therefore, how effective artificial noise can be in a large scale wireless network remains an unsolved problem. In contrast to the case of a point-to-point link, secrecy of a wireless network heavily relies on the spatial distributions of both legitimate and eavesdropping nodes. To study large scale wireless networks, papers [Ozan Koyluoglu et al. (2010)] [Liang et al. (2009)] [Vasudevan et al. (2010)] are focused on deriving scaling laws of the secrecy capacity, i.e., how the secrecy capacity grows with the number of nodes. However, we still need a concrete insight on the relationship between network secrecy capacity and system parameters (e.g., the number of antennas or the fraction of power allocated for generating artificial noise), because physical layer design parameters have an evident effect on the network secrecy capacity

rather than just a scaling behavior.

To this end, a notion of secrecy transmission capacity [Zhou et al. (2011)] is developed based on the concept of transmission capacity [Weber et al. (2010)]. It is derived using the stochastic geometry which is a proper and effective tool to study a large scale wireless network with randomly distributed nodes. Based on [Zhou et al. (2011)], the secrecy transmission capacity under the broadcast scenario is studied in [Ao and Chen (2011)]. How the secrecy transmission capacity is improved by cooperative jamming is characterized in [Zhou et al. (2012)].

In this chapter, we study the secrecy transmission capacity considering artificial noise in a wireless network. However, different from [Zhou et al. (2012)], we consider a more practical and interesting scenario where data and artificial noise are delivered simultaneously by the same transmitter. The theoretical relationship between the secrecy transmission capacity versus system parameters is then derived. The analytical results provide an insight on how the network secrecy capacity can be improved by properly designing system parameters.

The remainder of this chapter is organized as follows. The system model is introduced in Section 4.2. The secrecy transmission capacity with artificial noise is derived in Section 4.3. Numerical results are presented in Section 4.4, and this chapter is concluded in Section 4.5.

4.2 System Model

We consider a large scale decentralized wireless network which has both legitimate and eavesdropping nodes. The spatial distribution of legitimate transmitters is modeled as a homogeneous Poisson point process Φ_l with density λ_l. Each transmitter in the network has N_t ($N_t > 1$) antennas, and employs transmitting data by beamforming with ε of the total power and generating the artificial noise with the rest $(1 - \varepsilon)$ of the total power. Each transmitter has a corresponding receiver who has only one antenna. The eavesdroppers are distributed as another homogeneous Poisson point process Φ_e with density λ_e. Each eavesdropper uses a sin-

gle antenna for reception. Furthermore, it is assumed that the eavesdroppers are non-colluding and decode messages individually.

For the signal propagation in the wireless medium, we consider a path loss exponent $\alpha > 2$ and Rayleigh fading channels. The whole wireless network is considered as an interference-limited system, i.e., the thermal noise at a certain receiver is assumed to be negligible as compared to the aggregate interference from other transmitting nodes in the network.

4.2.1 Signal Representation for Beamforming and Artificial Noise

We give channel models of the legitimate link and the eavesdropping link with beamforming and artificial noise. For the legitimate link between Alice and Bob, the symbol that the legitimate receiver Bob receives from the legitimate transmitter Alice follows

$$\begin{aligned} y_b &= \mathbf{h}\mathbf{x} + n_b \\ &= \mathbf{h}\mathbf{z}_1 u + \mathbf{h}\mathbf{Z}_2\mathbf{v} + n_b \\ &= ||\mathbf{h}||u + n_b. \end{aligned} \tag{4.1}$$

For the eavesdropping link between Alice and Eve, the symbol that the eavesdropper Eve receives from the legitimate transmitter Alice is

$$\begin{aligned} y_e &= \mathbf{g}\mathbf{x} + n_e \\ &= \mathbf{g}\mathbf{z}_1 u + \mathbf{g}\mathbf{Z}_2\mathbf{v} + n_e. \end{aligned} \tag{4.2}$$

In (4.1) and (4.2), $\mathbf{x}$ is the $N_t \times 1$ symbol vector transmitted by Alice. $\mathbf{h}$ is the channel gain between Alice and Bob, and it is a $1 \times N_t$ vector whose elements are independent and identically distributed (i.i.d) complex Gaussian random variables. $\mathbf{g}$ is the channel gain between Alice and Eve. It is a $1 \times N_t$ vector, and its elements are i.i.d complex Gaussian random variables. n_b and n_e are the additive white Gaussian noises at the legitimate receiver and the eavesdropper.

With beamforming and artificial noise [Goel and Negi (2008)] [Zhou and McKay (2010)], Alice generates an $N_t \times N_t$ matrix $\mathbf{Z} = [\mathbf{z}_1\ \mathbf{Z}_2]$, where $\mathbf{z}_1 = \frac{\mathbf{h}^*}{||\mathbf{h}||}$ and $\mathbf{Z}_2$ is the null space matrix of $\mathbf{h}$. The $N_t \times 1$ transmitted symbol vector by Alice is given as $\mathbf{x} = \mathbf{z}_1 u + \mathbf{Z}_2 \mathbf{v}$, where scalar u has variance σ_u^2 and vector $\mathbf{v}$ has $N_t - 1$ elements which are i.i.d complex Gaussian random variables, each with variance σ_v^2. u and $\mathbf{v}$ represent the data and the artificial noise. The total power for data and artificial noise is P, where $P = \sigma_u^2 + (N_t - 1)\sigma_v^2$. We denote the fraction of the total power allocated to the data is ε. Thus, $\sigma_u^2 = \varepsilon P$, and $\sigma_v^2 = \frac{(1-\varepsilon)P}{N_t - 1}$.

4.2.2 Secrecy Transmission Capacity

The secrecy transmission capacity is proposed in [Zhou et al. (2011)] to depict the area spectral efficiency of secure communication in decentralized wireless networks. Specifically, the secrecy transmission capacity τ is defined as the achievable confidential messages transmission rate per unit area, satisfying a required connection outage probability $\mathrm{P_{co}} = \phi$ and a required secrecy outage probability $\mathrm{P_{so}} = \eta$:

$$\tau = R_s(1 - \phi)\lambda_l. \tag{4.3}$$

The secrecy rate R_s can be calculated as $[R_t - R_e]^+$, where $[x]^+ = \max\{0, x\}$. R_t is the transmission rate of the legitimate link with connection outage constraint ϕ, and R_e is the rate for securing the messages against the eavesdroppers with secrecy outage constraint η.

4.3 Secrecy Transmission Capacity with Artificial Noise

In this section, we give the derivation of the secrecy transmission capacity of a large scale decentralized wireless network where each transmitter sends data by beamforming with part of total power and generates artificial noise with the rest of the total power. For each transmitter,

the total power is fixed as P. Our analysis depends on the typical transmitter-receiver pair [Zhou et al. (2011)].

4.3.1 The Legitimate Link

Consider the typical transmitter-receiver pair (node a to node b). Receiver b experiences the interference from other transmitting nodes in Φ_l. Hence, at the typical receiver b, the signal-to-interference ratio (SIR) is denoted as SIR_b

$$SIR_b = \frac{S_{[a,b]} r_{[a,b]}^{-\alpha} (\varepsilon P)}{I_b}, \tag{4.4}$$

where $S_{[a,b]}$ and $r_{[a,b]}$ represent the channel fading and the distance between transmitter a and receiver b, respectively. εP is the power for data. I_b is the aggregate interference from other transmitting nodes in the network at receiver b. Receiver b is not interfered by the artificial noise from node a, as shown in (4.1).

With a threshold SIR value β_t, the connection outage probability $\mathrm{P_{co}}$ is defined as

$$\begin{aligned} \mathrm{P_{co}} =& \mathbb{P}(SIR_b < \beta_t) \\ =& \mathbb{P}\Big(\frac{S_{[a,b]} r_{[a,b]}^{-\alpha} (\varepsilon P)}{I_b} < \beta_t\Big). \end{aligned} \tag{4.5}$$

Theorem 4.1. *The connection outage probability* $\mathrm{P_{co}}$ *is calculated as*

$$\begin{aligned} \mathrm{P_{co}} =& 1 - \sum_{k=0}^{N_t-1} \Big[\frac{1}{k!} e^{-\lambda_l \beta_t^{\frac{2}{\alpha}} r_{[a,b]}^2 (C_\alpha + (\frac{1-\varepsilon}{\varepsilon(N_t-1)})^{\frac{2}{\alpha}} C_{\alpha,N_t-1})} \\ & \sum_{i=1}^{k} \big(\lambda_l \beta_t^{\frac{2}{\alpha}} r_{[a,b]}^2 \big(C_\alpha + \big(\frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{\frac{2}{\alpha}} C_{\alpha,N_t-1}\big) \frac{2}{\alpha}\big)^i (-1)^i \gamma_{k,i} \Big], \end{aligned} \tag{4.6}$$

where $C_\alpha = \frac{2\pi}{\alpha}\Gamma(\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})$, $C_{\alpha,N_t-1} = \frac{2\pi}{\alpha}\sum_{k=0}^{N_t-2}\binom{N_t-1}{k} B(\frac{2}{\alpha}+k; N_t-1-(\frac{2}{\alpha}+k))$, *and* $\gamma_{k,i}$ *is*

a constant defined as

$$\gamma_{k,i} = \sum_{\delta_q \in comb\binom{k-1}{k-i}} \prod_{l_{pq}\in\delta_q} \left(\frac{2}{\alpha}(l_{pq}-p+1)-l_{pq}\right),$$
$$p = 1,2,\ldots,|\delta_q|,\ q = 1,2,\ldots,\binom{k-1}{k-i},$$

where comb $\binom{m}{n}$ *is the set of all subsets of the natural numbers* $\{1,2,\ldots,m\}$ *of cardinality* n *with distinct elements, and* $\gamma_{k,k} = (-1)^k$.

Proof: For receiver b, we define

$$\begin{aligned} \mathrm{P_b} =& \mathbb{P}(SIR_b > \beta_t) \\ =& \mathbb{P}\left(\frac{S_{[a,b]} r_{[a,b]}^{-\alpha}(\varepsilon P)}{I_b} > \beta_t\right), \end{aligned} \tag{4.7}$$

where $S_{[a,b]} = \left|\mathbf{h}_{[a,b]} \frac{\mathbf{h}^*_{[a,b]}}{||\mathbf{h}_{[a,b]}||}\right|^2$, and $\mathbf{h}_{[a,b]}$ is the $1\times N_t$ Rayleigh fading channel between node a and node b, so $S_{[a,b]}$ has the gamma distribution with shape N_t and scale 1, i.e., $S_{[a,b]} \sim \Gamma(N_t,1)$. Its complementary cumulative distribution function is $F^c_{S_{[a,b]}}(x) = e^{-x}\sum_{k=0}^{N_t-1}\frac{1}{k!}x^k$. Applying Theorem 1 in [Hunter et al. (2008)], (4.7) can be calculated as

$$\mathrm{P_b} = \sum_{k=0}^{N_t-1} \left[\frac{1}{k!}(-\xi)^k \frac{d^k}{d\xi^k}\mathcal{L}_{I_b}(\xi)\right]\Big|_{\xi=\beta_t r^{\alpha}_{[a,b]}\frac{1}{\varepsilon P}}, \tag{4.8}$$

where $\mathcal{L}_{I_b}(\xi)$ represents the Laplace transform of I_b. Aggregate interference I_b consists of two parts I_{b1} and I_{b2}. Since $I_b = I_{b1} + I_{b2}$, $\mathcal{L}_{I_b}(\xi) = \mathcal{L}_{I_{b1}}(\xi)\mathcal{L}_{I_{b2}}(\xi)$.

I_{b1} is the interference from the data part of other transmitting nodes in Φ_l,

$$I_{b1} = \sum_{l\in\Phi_l} S_{[l(a),b]1}|X_{[l(a),b]}|^{-\alpha}(\varepsilon P),$$

where $S_{[l(a),b]1} = \left|\mathbf{h}_{[l(a),b]}\frac{\mathbf{h}^*_{[l(a),l(b)]}}{||\mathbf{h}_{[l(a),l(b)]}||}\right|^2$, $\mathbf{h}_{[l(a),b]}$ is the $1\times N_t$ Rayleigh fading channel between the

l-th transmitter and node b, and $\mathbf{h}_{[l(a),l(b)]}$ is the $1 \times N_t$ Rayleigh fading channel of the l-th transmitter-receiver pair, so $S_{[l(a),b]1}$ has the exponential distribution $f(x) = e^{-x}$. $|X_{[l(a),b]}|$ is the distance between the l-th transmitter and node b. The Laplace transform of I_{b1} is given as

$$\begin{aligned}\mathcal{L}_{I_{b1}}(\xi) =& e^{-\lambda_l \int_{\mathbb{R}^2} 1-\mathbb{E}[e^{-\xi S_{[l(a),b]1}|X_{[l(a),b]}|^{-\alpha}(\varepsilon P)}]dX_{[l(a),b]}} \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}}(\varepsilon P)^{\frac{2}{\alpha}} C_\alpha},\end{aligned} \tag{4.9}$$

where $C_\alpha = \frac{2\pi}{\alpha}\Gamma(\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})$.

I_{b2} is the interference from the artificial noise part of other transmitting nodes in Φ_l,

$$I_{b2} = \sum_{l \in \Phi_l} S_{[l(a),b]2}|X_{[l(a),b]}|^{-\alpha}(\frac{(1-\varepsilon)P}{N_t - 1}),$$

where $S_{[l(a),b]2} = \mathbf{h}_{[l(a),b]}\mathbf{Z}_{2[l(a),l(b)]}\mathbf{Z}^*_{2[l(a),l(b)]}\mathbf{h}^*_{[l(a),b]}$, $\mathbf{h}_{[l(a),b]}$ is the $1 \times N_t$ Rayleigh fading channel between the l-th transmitter and node b, and $\mathbf{Z}_{2[l(a),l(b)]}$ is the $N_t \times (N_t - 1)$ null space matrix of the channel $\mathbf{h}_{[l(a),l(b)]}$, so $S_{[l(a),b]2} \sim \Gamma(N_t - 1, 1)$. The Laplace transform of I_{b2} is given by

$$\begin{aligned}\mathcal{L}_{I_{b2}}(\xi) =& e^{-\lambda_l \int_{\mathbb{R}^2} 1-\mathbb{E}[e^{-\xi S_{[l(a),b]2}|X_{[l(a),b]}|^{-\alpha}(\frac{(1-\varepsilon)P}{N_t-1})}]dX_{[l(a),b]}} \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}}(\frac{(1-\varepsilon)P}{N_t-1})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}},\end{aligned} \tag{4.10}$$

where $C_{\alpha,m} = \frac{2\pi}{\alpha}\sum_{k=0}^{m-1}\binom{m}{k}B(\frac{2}{\alpha}+k; m-(\frac{2}{\alpha}+k))$.

Thus, $\mathcal{L}_{I_b}(\xi)$ is given by

$$\begin{aligned}\mathcal{L}_{I_b}(\xi) =& \mathcal{L}_{I_{b1}}(\xi)\mathcal{L}_{I_{b2}}(\xi) \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}}\tilde{C}},\end{aligned} \tag{4.11}$$

where $\tilde{C} = (\varepsilon P)^{\frac{2}{\alpha}} C_\alpha + (\frac{(1-\varepsilon)P}{N_t-1})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}$.

Substituting (4.11) into (4.8), we can obtain

$$\begin{aligned}
\mathrm{P_b} &= \sum_{k=0}^{N_t-1} \big[\frac{1}{k!}(-\xi)^k \frac{d^k}{d\xi^k}\mathcal{L}_{I_b}(\xi)\big]\big|_{\xi=\beta_t r_{[a,b]}^{\alpha}\frac{1}{\varepsilon P}} \\
&= \sum_{k=0}^{N_t-1} \big[\frac{1}{k!}(-\xi)^k \frac{e^{-\lambda_l \xi^{\frac{2}{\alpha}}\tilde{C}}}{(-\xi)^k} \sum_{i=1}^{k} (\lambda_l \xi^{\frac{2}{\alpha}}\tilde{C}\frac{2}{\alpha})^i (-1)^i \gamma_{k,i}\big]\big|_{\xi=\beta_t r_{[a,b]}^{\alpha}\frac{1}{\varepsilon P}} \\
&= \sum_{k=0}^{N_t-1} \Big[\frac{1}{k!} e^{-\lambda_l \beta_t^{\frac{2}{\alpha}} r_{[a,b]}^2 (C_\alpha + (\frac{1-\varepsilon}{\varepsilon(N_t-1)})^{\frac{2}{\alpha}} C_{\alpha,N_t-1})} \sum_{i=1}^{k} \big(\lambda_l \beta_t^{\frac{2}{\alpha}} r_{[a,b]}^2 \big(C_\alpha + \big(\frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{\frac{2}{\alpha}} C_{\alpha,N_t-1}\big)\frac{2}{\alpha}\big)^i (-1)^i \gamma_{k,i}\Big].
\end{aligned}$$

Thus, the connection outage probability $\mathrm{P_{co}}$ is $1 - \mathrm{P_b}$, which is the result in (4.6).

With the connection outage constraint given by $\mathrm{P_{co}} = \phi$, we can obtain the corresponding β_t with (4.6), and the transmission rate R_t can be obtained using

$$R_t = log_2(1 + \beta_t). \tag{4.12}$$

4.3.2 The Eavesdropping Link

Consider the eavesdropping link between the typical transmitter a and an eavesdropper e. Eve e suffers from the interference from transmitting nodes in Φ_l. Hence, the SIR at e is denoted as SIR_e,

$$SIR_e = \frac{S_{[a,e]} r_{[a,e]}^{-\alpha}(\varepsilon P)}{I_e}, \tag{4.13}$$

where $S_{[a,e]}$ and $r_{[a,e]}$ represent the channel fading and the distance between transmitter a and eavesdropper e, respectively. εP is the power allocated for data. I_e is the aggregate interference from transmitting nodes in the network at node e, including the artificial noise from node a, as shown in (4.2).

With a threshold SIR value β_e, the secrecy outage probability $\mathrm{P_{so}}$ is defined as the probability that there exists at least one Eve $e \in \Phi_e$, such that $SIR_e > \beta_e$.

Theorem 4.2. *The secrecy outage probability is bounded by*

$$\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}} = 1 - exp\Big[- \frac{\pi\lambda_e}{\lambda_l \beta_e^{\frac{2}{\alpha}} \big(C_\alpha + \big(\frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{\frac{2}{\alpha}} C_{\alpha,N_t-1}\big)} \frac{1}{\big(1+\beta_e \frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{N_t-1}} \Big]. \tag{4.14}$$

Proof: The secrecy outage occurs when there exists at least one Eve in Φ_e whose SIR is larger than β_e. Thus, the secrecy outage probability is expressed as

$$\begin{aligned} \mathrm{P}_{\mathrm{so}} =& 1 - \mathbb{E}_{\Phi_l}\Big\{ \mathbb{E}_{\Phi_e}\big\{ \prod_{e\in\Phi_e} (1 - \mathbb{P}(\frac{S_{[a,e]} r_{[a,e]}^{-\alpha}(\varepsilon P)}{I_e} > \beta_e | \Phi_e, \Phi_l)) \big\} \Big\} \\ =& 1 - \mathbb{E}_{\Phi_l}\big\{ e^{-2\pi\lambda_e \int_0^\infty \mathbb{P}(\frac{S_{[a,e]} r_{[a,e]}^{-\alpha}(\varepsilon P)}{I_e} > \beta_e | \Phi_l) r_{[a,e]} dr_{[a,e]}} \big\} \\ \leq& 1 - e^{-2\pi\lambda_e \int_0^\infty \mathbb{P}(\frac{S_{[a,e]} r_{[a,e]}^{-\alpha}(\varepsilon P)}{I_e} > \beta_e) r_{[a,e]} dr_{[a,e]}}, \end{aligned} \tag{4.15}$$

where the second equation is from the generating functional of the Poisson point process Φ_e and the third inequality is using the Jensen's inequality [Zhou et al. (2011)].

For Eve e, we define

$$\begin{aligned} \mathrm{P}_{\mathrm{e}} =& \mathbb{P}(SIR_e > \beta_e) \\ =& \mathbb{P}(\frac{S_{[a,e]} r_{[a,e]}^{-\alpha}(\varepsilon P)}{I_e} > \beta_e), \end{aligned} \tag{4.16}$$

where $S_{[a,e]} = |\mathbf{g}_{[a,e]} \frac{\mathbf{h}_{[a,b]}^*}{||\mathbf{h}_{[a,b]}||}|^2$, $\mathbf{g}_{[a,e]}$ is the $1 \times N_t$ Rayleigh fading channel between node a and node e, and $\mathbf{h}_{[a,b]}$ is the $1 \times N_t$ Rayleigh fading channel between node a and node b, so $S_{[a,e]}$ has the exponential distribution $f(x) = e^{-x}$. Its complementary cumulative distribution function is $F_{S_{[a,e]}}^c(x) = e^{-x}$. Thus, $\mathrm{P}_{\mathrm{e}} = \mathcal{L}_{I_e}(\xi)|_{\xi=\beta_e r_{[a,e]}^\alpha \frac{1}{\varepsilon P}}$, where $\mathcal{L}_{I_e}(\xi)$ is the Laplace transform of I_e. Aggregate interference I_e consists of three parts I_{e1}, I_{e2} and I_{e3}. Since $I_e = I_{e1} + I_{e2} + I_{e3}$, $\mathcal{L}_{I_e}(\xi) = \mathcal{L}_{I_{e1}}(\xi)\mathcal{L}_{I_{e2}}(\xi)\mathcal{L}_{I_{e3}}(\xi)$.

I_{e1} is the interference from the data part of other transmitting nodes in Φ_l,

$$I_{e1} = \sum_{l \in \Phi_l} S_{[l(a),e]1} |X_{[l(a),e]}|^{-\alpha} (\varepsilon P),$$

where $S_{[l(a),e]1} = \left| \mathbf{g}_{[l(a),e]} \frac{\mathbf{h}^*_{[l(a),l(b)]}}{||\mathbf{h}_{[l(a),l(b)]}||} \right|^2$, $\mathbf{g}_{[l(a),e]}$ is the $1 \times N_t$ Rayleigh fading channel between the l-th transmitter and node e, and $\mathbf{h}_{[l(a),l(b)]}$ is the $1 \times N_t$ Rayleigh fading channel of the l-th transmitter-receiver pair, so $S_{[l(a),e]1}$ has the exponential distribution $f(x) = e^{-x}$. $|X_{[l(a),e]}|$ is the distance between the l-th transmitter and node e. The Laplace transform of I_{e1} is given as

$$\begin{aligned} \mathcal{L}_{I_{e1}}(\xi) =& e^{-\lambda_l \int_{\mathbb{R}^2} 1 - \mathbb{E}[e^{-\xi S_{[l(a),e]1} |X_{[l(a),e]}|^{-\alpha} (\varepsilon P)}] dX_{[l(a),e]}} \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}} (\varepsilon P)^{\frac{2}{\alpha}} C_\alpha}. \end{aligned} \tag{4.17}$$

I_{e2} is the interference from the artificial noise part of other transmitting nodes in Φ_l,

$$I_{e2} = \sum_{l \in \Phi_l} S_{[l(a),e]2} |X_{[l(a),e]}|^{-\alpha} \left(\frac{(1-\varepsilon)P}{N_t - 1}\right),$$

where $S_{[l(a),e]2} = \mathbf{g}_{[l(a),e]} \mathbf{Z}_{2[l(a),l(b)]} \mathbf{Z}^*_{2[l(a),l(b)]} \mathbf{g}^*_{[l(a),e]}$, $\mathbf{g}_{[l(a),e]}$ is the $1 \times N_t$ Rayleigh fading channel between the l-th transmitter and node e, and $\mathbf{Z}_{2[l(a),l(b)]}$ is the $N_t \times (N_t - 1)$ null space matrix of the channel $\mathbf{h}_{[l(a),l(b)]}$, so $S_{[l(a),e]2} \sim \Gamma(N_t - 1, 1)$. The Laplace transform of I_{e2} is given by

$$\begin{aligned} \mathcal{L}_{I_{e2}}(\xi) =& e^{-\lambda_l \int_{\mathbb{R}^2} 1 - \mathbb{E}[e^{-\xi S_{[l(a),e]2} |X_{[l(a),e]}|^{-\alpha} \left(\frac{(1-\varepsilon)P}{N_t - 1}\right)}] dX_{[l(a),e]}} \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}} \left(\frac{(1-\varepsilon)P}{N_t - 1}\right)^{\frac{2}{\alpha}} C_{\alpha, N_t - 1}}. \end{aligned} \tag{4.18}$$

I_{e3} is the interference from the artificial noise part of the typical transmitter a,

$$I_{e3} = S_{[a,e]3} r^{-\alpha}_{[a,e]} \left(\frac{(1-\varepsilon)P}{N_t - 1}\right),$$

where $S_{[a,e]3} = \mathbf{g}_{[a,e]} \mathbf{Z}_{2[a,b]} \mathbf{Z}^*_{2[a,b]} \mathbf{g}^*_{[a,e]}$, $\mathbf{g}_{[a,e]}$ is the $1 \times N_t$ Rayleigh fading channel between node

a and node e, and $\mathbf{Z}_{2[a,b]}$ is the $N_t \times (N_t - 1)$ null space matrix of the channel $\mathbf{h}_{[a,b]}$, so $S_{[a,e]3} \sim \Gamma(N_t - 1, 1)$. The Laplace transform of I_{e3} is given by

$$\begin{aligned}\mathcal{L}_{I_{e3}}(\xi) =& \mathbb{E}[e^{-\xi S_{[a,e]3} r_{[a,e]}^{-\alpha} (\frac{(1-\varepsilon)P}{N_t-1})}] \\ =& \frac{1}{\big(1 + \xi r_{[a,e]}^{-\alpha} (\frac{(1-\varepsilon)P}{N_t-1})\big)^{N_t-1}}.\end{aligned} \tag{4.19}$$

Thus,

$$\begin{aligned}\mathrm{P_e} =& \mathcal{L}_{I_e}(\xi)|_{\xi=\beta_e r_{[a,e]}^{\alpha} \frac{1}{\varepsilon P}} \\ =& \mathcal{L}_{I_{e1}}(\xi)\mathcal{L}_{I_{e2}}(\xi)\mathcal{L}_{I_{e3}}(\xi)|_{\xi=\beta_e r_{[a,e]}^{\alpha} \frac{1}{\varepsilon P}} \\ =& e^{-\lambda_l \xi^{\frac{2}{\alpha}} [(\varepsilon P)^{\frac{2}{\alpha}} C_\alpha + (\frac{(1-\varepsilon)P}{N_t-1})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}]} \frac{1}{\big(1 + \xi r_{[a,e]}^{-\alpha} (\frac{(1-\varepsilon)P}{N_t-1})\big)^{N_t-1}} \Big|_{\xi=\beta_e r_{[a,e]}^{\alpha} \frac{1}{\varepsilon P}} \\ =& e^{-\lambda_l (\beta_e r_{[a,e]}^{\alpha} \frac{1}{\varepsilon P})^{\frac{2}{\alpha}} [(\varepsilon P)^{\frac{2}{\alpha}} C_\alpha + (\frac{(1-\varepsilon)P}{N_t-1})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}]} \frac{1}{\big(1 + (\beta_e r_{[a,e]}^{\alpha} \frac{1}{\varepsilon P}) r_{[a,e]}^{-\alpha} (\frac{(1-\varepsilon)P}{N_t-1})\big)^{N_t-1}} \\ =& e^{-\lambda_l \beta_e^{\frac{2}{\alpha}} r_{[a,e]}^2 [C_\alpha + (\frac{1-\varepsilon}{\varepsilon(N_t-1)})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}]} \frac{1}{\big(1 + \beta_e \frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{N_t-1}}.\end{aligned} \tag{4.20}$$

Substituting (4.20) into (4.15), we can obtain

$$\begin{aligned}\mathrm{P_{so}^{UB}} =& 1 - \exp\Big[- 2\pi\lambda_e \int_0^{\infty} \mathrm{P_e} r_{[a,e]} dr_{[a,e]}\Big] \\ =& 1 - \exp\Big[- 2\pi\lambda_e \int_0^{\infty} \Big[e^{-\lambda_l \beta_e^{\frac{2}{\alpha}} r_{[a,e]}^2 [C_\alpha + (\frac{1-\varepsilon}{\varepsilon(N_t-1)})^{\frac{2}{\alpha}} C_{\alpha,N_t-1}]} \frac{1}{\big(1 + \beta_e \frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{N_t-1}}\Big] r_{[a,e]} dr_{[a,e]}\Big] \\ =& 1 - \exp\Big[- \frac{\pi\lambda_e}{\lambda_l \beta_e^{\frac{2}{\alpha}} \big(C_\alpha + \big(\frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{\frac{2}{\alpha}} C_{\alpha,N_t-1}\big)} \frac{1}{\big(1 + \beta_e \frac{1-\varepsilon}{\varepsilon(N_t-1)}\big)^{N_t-1}}\Big],\end{aligned} \tag{4.21}$$

which is the result in (4.14). The bounding technique used in (4.15) to derive the upper bound $\mathrm{P_{so}^{UB}}$ is adopted in [Zhou et al. (2011)][Zhou et al. (2012)][Ganti and Haenggi (2007)]. From [Zhou et al. (2011)][Zhou et al. (2012)][Ganti and Haenggi (2007)], it is known this

bounding technique gives a tight approximation of the exact value. Therefore, we use $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}$ as an approximation of P_{so}.

For the secrecy outage requirement given by $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}} = \eta$, we can obtain the corresponding β_e with (4.14). The rate R_e for securing the messages can be computed using

$$R_e = log_2(1 + \beta_e). \tag{4.22}$$

Having R_t from (4.12) and R_e from (4.22), we compute the rate of confidential messages as $R_s = [R_t - R_e]^+$. Thus, with (4.3), the secrecy transmission capacity can be calculated.

4.4 Numerical Results and Discussions

In this section, we present numerical results to illustrate how the number of transmitting antennas N_t and power allocation ratio ε affect the secrecy transmission capacity.

In Figure 4.1, the secrecy transmission capacity versus the power allocation ratio ε are plotted for four cases (i.e., N_t=2, 4, 6 and 8). For each case, ε varies from 0 to 1. The system parameters are set as λ_l=0.01, λ_e=0.001, ϕ=0.2, η=0.01, α=4, and $r_{[a,b]}$=1. Figure 4.1 shows that: 1) For each fixed N_t, when ε is near 0 or 1, the secrecy transmission capacity is small, e.g., when ε=1 and N_t=2, no artificial noise is generated to confuse eavesdroppers, and the secrecy transmission capacity is 0.0061. When ε is near 0.5, the secrecy transmission capacity achieves its maximum value, e.g., when ε=0.5 and N_t=2, the secrecy transmission capacity reaches maximum value 0.0227. Thus, the secrecy transmission capacity is significantly improved by using the artificial noise, and the system parameter ε needs to be carefully designed to maximize the secrecy transmission capacity. 2) For the same ε, when the number of antennas is increased, the secrecy transmission capacity is evidently improved, e.g., for $\varepsilon = 0.5$, the secrecy transmission capacities are 0.0227 and 0.0337 for $N_t = 2$ and $N_t = 4$ cases, respectively. Thus, N_t is also an important system parameter, which needs to be chosen properly.

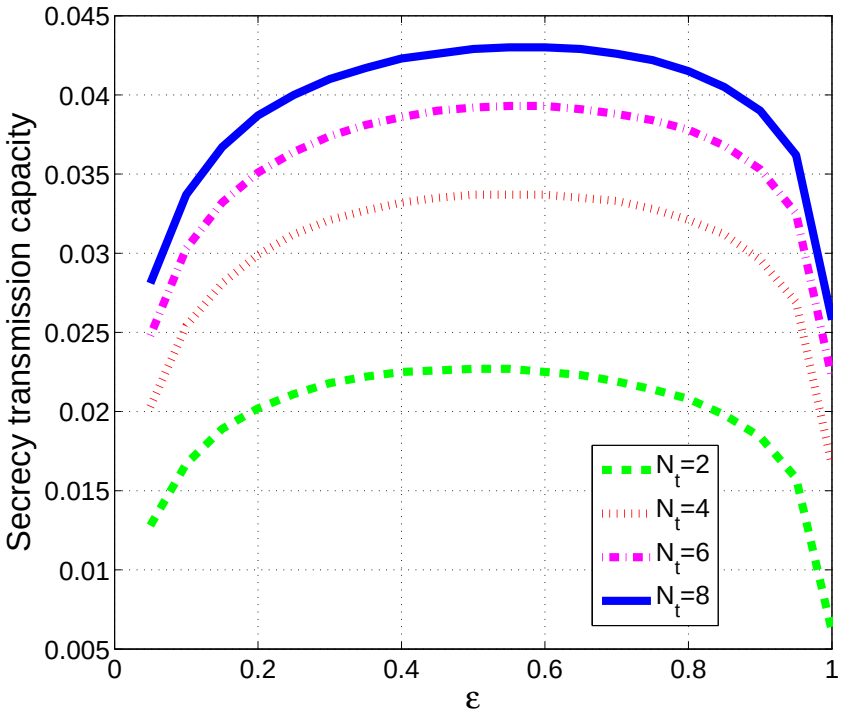


Figure 4.1: Secrecy transmission capacity versus power allocation ratio ε

In Figure 4.2, two scenarios that only beamforming (OB) and artificial noise (AN) are considered. In the OB scenario, the total power is used to transmit data with beamforming. In the AN scenario, the total power is optimally allocated to send data with beamforming and to generate artificial noise, so that the secrecy transmission capacity is maximized. The secrecy transmission capacity versus the eavesdropper density λ_e are plotted for four cases (i.e., N_t=2, 4, 6 and 8) under OB and AN scenarios. For each case, λ_e varies from 0.001 to 0.1. The system parameters are set as λ_l=0.01, ϕ=0.2, η=0.03, α=4 and $r_{[a,b]}$=1. Figure 4.2 illustrates that: 1) In the OB scenario, the secrecy transmission capacity drops dramatically with the increment of the eavesdropper density λ_e. When λ_e is larger than 10^{-2}, the secrecy transmission capacity becomes 0. It means when there are enough eavesdroppers, secrecy transmission can not be achieved. 2) In the AN scenario, the secrecy transmission capacity decreases slowly as λ_e increases. Even in the zero secrecy transmission capacity region in the OB scenario, positive secrecy transmission capacity can be obtained with the help of the artificial noise. 3) Increasing the number of antennas can evidently enhance the secrecy transmission capacity in both OB

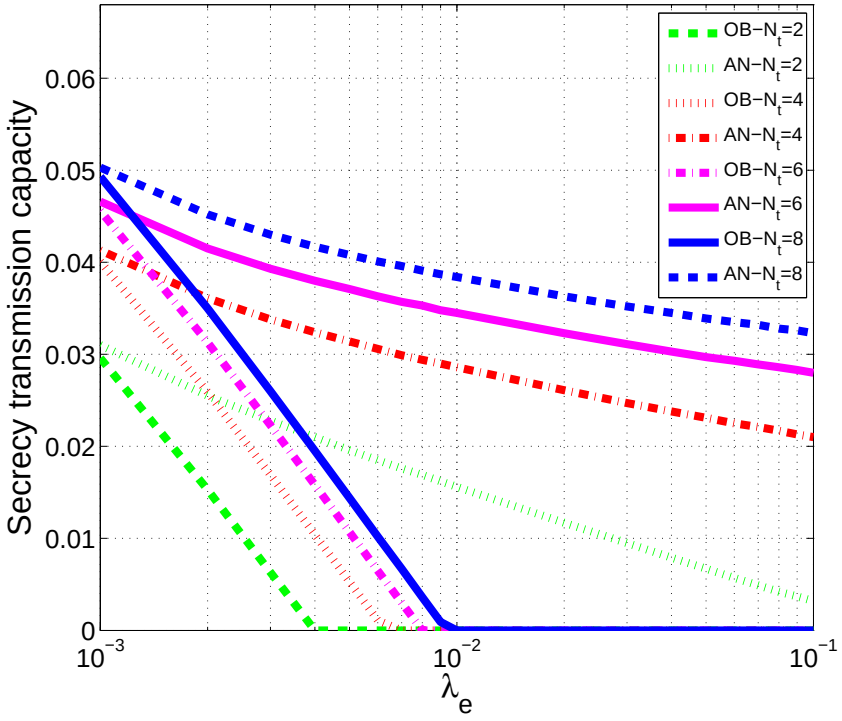


Figure 4.2: Secrecy transmission capacity versus eavesdropper density λ_e

and AN scenarios.

In Figure 4.3, the OB and the AN scenarios are considered. The secrecy transmission capacity versus the secrecy outage probability η are plotted for four cases (i.e., N_t=2, 4, 6 and 8) under OB and AN scenarios. For each case, η varies from 0.001 to 0.1. The system parameters are set as λ_l=0.01, λ_e=0.001, ϕ=0.2, α=4, and $r_{[a,b]}$=1. Figure 4.3 demonstrates that: 1) The secrecy transmission capacity decreases more quickly in the OB scenario than in the AN scenario as the secrecy requirement increases (i.e., η becomes smaller). It means the secrecy transmission capacity is more sensitive to the secrecy requirement without using the artificial noise. 2) When η is smaller than 0.003, the secrecy transmission capacity is zero for the OB scenario. Under so strict secrecy requirement condition, with the help of the artificial noise, positive secrecy transmission capacity can be achieved, as shown in the AN scenario. When η is larger than 0.04, the secrecy transmission capacities of OB and AN scenarios are the same. This observation indicates the secrecy requirement is so loose that the aggregate interference from other transmitting nodes in the network is enough to satisfy the secrecy outage constraint.

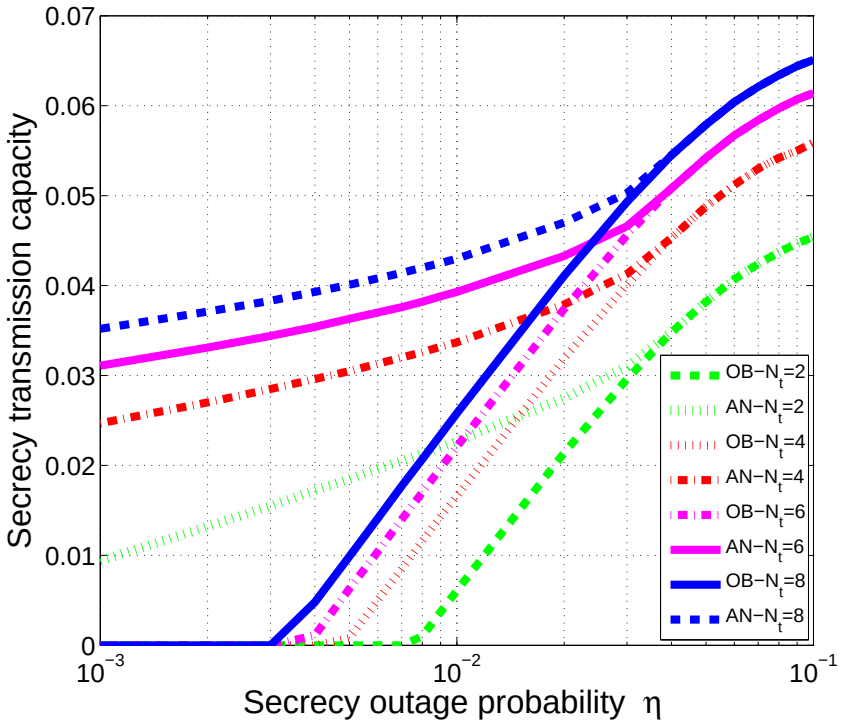


Figure 4.3: Secrecy transmission capacity versus secrecy outage probability η

Thus, it is better to use the total power for strengthening the legitimate channel than to allocate part of the power for generating artificial noise to degrade the eavesdropping channel. 3) In both OB and AN scenarios, the secrecy transmission capacity is improved with the increment of the number of antennas.

4.5 Summary

In this chapter, secrecy capacity under artificial noise was studied for a large scale wireless network. Influence of artificial noise to the network throughput was depicted using the secrecy transmission capacity. Our numerical results showed that significant network throughput enhancement could be obtained by properly designing number of transmitting antennas and power allocation ratio between data and artificial noise.

Chapter 5

Conclusions

Ubiquitous applications of wireless networks have brought great convenience to our daily life. However, with diverse data applications, demands for high quality of service, e.g., high data rate and security, are dramatically increased. In this thesis, throughput enhancement and security for the next generation wireless networks were studied. Along this direction, three topics were researched. We first studied channel-width adaptation in wireless mesh networks. We proposed a novel OFDMA-based scheme and developed relevant algorithms and protocols to improve network throughput. Our research results are instrumental to a wideband OFDMA-based multihop wireless network, which has become a key architecture for the next generation wireless networks. Our channel-width adaptation scheme is highly adaptive to dynamic network conditions such as topology change or traffic variations, and can be operated distributedly in a mesh network. Performance results show that our scheme significantly outperforms existing schemes and improves throughput by about 20%.

In the second topic, we studied fast secret key generation in static wireless networks with long coherence time. Our research plays a critical role in many applications, because there exist many scenarios where wireless communication nodes are static but the secrecy requirement is stringent, e.g., wireless monitoring nodes in the smart grid and enterprise wireless networks. In

these scenarios, our virtual-channel based secret key generation scheme can be easily adopted to generate secret keys to guarantee confidential data transmissions among different communication nodes.

In the third topic, stochastic geometry was adopted to analyze secrecy transmission capacity when artificial noise was employed as a security measure in wireless networks. Our analytical results provide insights for node deployment and are useful for the design of system parameters of a large scale wireless network with physical-layer security.

5.1 Contributions

The following contributions are made in this thesis:

- In Chapter 2, we proposed an OFDMA-based channel-width adaptation mechanism to improve the network throughput of wireless mesh networks. To analyze this scheme, we formulated a subchannel and time slot allocation problem and proved it to be NP-complete. A greedy algorithm was also derived to obtain a suboptimal solution to subchannel and time slot allocation. Based on the greedy algorithm, we designed a distributed MAC protocol to leverage channel-width adaptation to improve the network throughput of a wireless mesh network. Simulations proved the effectiveness of our algorithms and protocols. Our research work is the first result that leverages channel-width adaptation for resource allocation in wireless mesh networks, and has led to a paper [Huang et al. (2012)] and a patent [Wang and Huang (2012)].

- In Chapter 3, we developed a novel fast secret key generation scheme for wireless channels with long coherence time. It exploits opportunistic beamforming to generate keys and frequency diversity to secure keys. Our scheme can be easily adopted in the existing narrowband systems (e.g., the GSM cellular system) and wideband systems (e.g., the WiFi system). Performance results validated randomness and secrecy of keys, and also

illustrated that the proposed scheme could generate secret keys at a rate of 2Kb/s for narrowband systems and 20Kb/s for wideband systems. Our scheme is one of the two schemes that can achieve fast secret key generation for static wireless networks, but it is the only scheme that is applicable to all wireless systems. Research work from this topic results in a paper [Huang and Wang (2013a)] to be published in *IEEE INFOCOM*, which is a prestigious conference in the area of wireless networks.

- In Chapter 4, stochastic geometry was adopted to analyze the secrecy transmission capacity of wireless networks with artificial noise. The secrecy of the network is impacted by the number of transmitting antennas and the power ratio between data and artificial noise. We found that, in a wireless network with multiple communication links, artificial noise is not necessary when the aggregate interference from other transmitting nodes exceeds a certain level. Research work from this topic will appear in *IEEE WCNC* [Huang and Wang (2013b)].

5.2 Future Work

In spite of many contributions that we have made so far, challenging problems still remain. They can be interesting topics for future research.

- In Chapter 2, we assume the traffic demand on each link is given in the MAC layer. In practice, traffic demand on each link needs to be scheduled considering MAC/routing cross-layer design. How to consider channel-width adaptation under the framework of MAC/routing cross-layer design is critical for OFDMA-based channel-width adaptation to be adopted practically.

- In Chapter 3, the proposed scheme has not been fully implemented and tested on a real system. Moreover, the key generation scheme can be extended to MIMO communication

systems where the spatial diversity can be utilized to further increase the secrecy. These unresolved issues are exciting research topics on wireless network security.

- In Chapter 4, we assume legitimate receivers and eavesdroppers are equipped with only one antenna. Future work is needed to analyze a more general scenario where all the nodes are equipped with multiple antennas and eavesdroppers are colluding. Moreover, the gap between the actual secrecy transmission capacity and the theoretical bound needs further study.

Bibliography

Akyildiz, I., X. Wang, and W. Wang (2005). Wireless mesh networks: a survey. *Elsevier Computer Networks Journal 47*(4), 445–487.

Ao, W. and K. Chen (2011). Broadcast transmission capacity of heterogeneous wireless ad hoc networks with secrecy outage constraints. In *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–5.

Aryafar, E., O. Gurewitz, and E. Knightly (2008). Distance-1 constrained channel assignment in single radio wireless mesh networks. In *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, pp. 762–770.

Azar, Y., A. Madry, T. Moscibroda, D. Panigrahi, and A. Srinivasan (2011). Maximum bipartite flow in networks with adaptive channel width. *Elsevier Theoretical Computer Science Journal 412*(24), 2577–2587.

Bahl, P., R. Chandra, T. Moscibroda, S. Narlanka, Y. Wu, and Y. Yuan (2012, August 14). Dynamic channel-width allocation in wireless networks. US Patent 8,243,612.

Bai, S., W. Zhang, Y. Liu, and C. Wang (2011). Max-min fair scheduling in ofdma-based multi-hop wimax mesh networks. In *Proc. IEEE International Conference on Communications (ICC)*, pp. 1–5.

Bayan, A. and T. Wan (2010). A scalable qos scheduling architecture for wimax multi-hop relay networks. In *Proc. 2nd International Conference on Education Technology and Computer (ICETC)*, Volume 5, pp. V5–326.

Bloch, M., J. Barros, M. Rodrigues, and S. McLaughlin (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory 54*(6), 2515 –2534.

Bondy, J. and U. Murty (1976). *Graph Theory with Applications*. Macmillan.

Brassard, G. and L. Salvail (1994). Secret-key reconciliation by public discussion. In *Proc. Advances in Cryptology-Eurocrypt' 93*, pp. 410–423.

Chandra, R., R. Mahajan, T. Moscibroda, R. Raghavendra, and P. Bahl (2008). A case for adapting channel width in wireless networks. In *Proc. ACM Special Interest Group on Data Communication (SIGCOMM)*, pp. 135–146.

Cheng, H. and W. Zhuang (2009). Novel packet-level resource allocation with effective qos provisioning for wireless mesh networks. *IEEE Transactions on Wireless Communications 8*(2), 694–700.

Cheng, L., B. Henty, R. Cooper, D. Stancil, and F. Bai (2008). A measurement study of time-scaled 802.11 a waveforms over the mobile-to-mobile vehicular channel at 5.9 ghz. *IEEE Communications Magazine 46*(5), 84–91.

Csiszár, I. and J. Korner (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory 24*(3), 339–348.

Das, A., H. Alazemi, R. Vijayakumar, and S. Roy (2005). Optimization models for fixed channel assignment in wireless mesh networks with multiple radios. In *Proc. IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON)*, pp. 463–474.

Dodis, Y., L. Reyzin, and A. Smith (2004). Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In *Proc. Advances in Cryptology-Eurocrypt 2004*, pp. 523–540.

Ganti, R. K. and M. Haenggi (2007). Single-hop connectivity in interference-limited hybrid wireless networks. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 366–370.

Garey, M. and D. Johnson (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H.Freeman and Company.

Ghogho, M. and A. Swami (2011). Physical-layer secrecy of mimo communications in the presence of a poisson random field of eavesdroppers. In *Proc. IEEE International Conference on Communications (ICC)*, pp. 1–5.

Goel, S. and R. Negi (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications 7*(6), 2180–2189.

Gollakota, S. and D. Katabi (2011). Physical layer wireless security made fast and channel independent. In *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1125–1133.

Gopala, P., L. Lai, and H. El Gamal (2008). On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory 54*(10), 4687–4698.

Hashemi, H. (1993). The indoor radio propagation channel. *Proceedings of the IEEE 81*(7), 943–968.

Huang, J. and A. Swindlehurst (2011). Robust secure transmission in miso channels based on worst-case optimization. *IEEE Transactions on Signal Processing 60*(4), 1696–1707.

Huang, P. and X. Wang (2013a). Fast secret key generation in static wireless networks: a virtual channel approach. *Accepted by IEEE International Conference on Computer Communications (INFOCOM)*.

Huang, P. and X. Wang (2013b). Secrecy enhancement with artificial noise in decentralized wireless networks: a stochastic geometry perspective. *Accepted by IEEE Wireless Communications and Networking Conference (WCNC)*.

Huang, P., X. Wang, and M. Li (2012). Ofdma-based channel-width adaptation in wireless mesh networks. *Submitted to IEEE Transactions on Mobile Computing*.

Hunter, A., J. Andrews, and S. Weber (2008). Transmission capacity of ad hoc networks with spatial diversity. *IEEE Transactions on Wireless Communications 7*(12), 5058–5071.

Impagliazzo, R., L. Levin, and M. Luby (1989). Pseudo-random generation from one-way functions. In *Proc. ACM Symposium on Theory of Computing (STOC)*, pp. 12–24.

Jain, K., J. Padhye, V. Padmanabhan, and L. Qiu (2005). Impact of interference on multi-hop wireless network performance. *Springer Wireless Networks Journal 11*(4), 471–487.

Jana, S., S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 321–332.

Johnson, D. (1974). Worst case behavior of graph coloring algorithms. In *Proc. Utilitas Mathematica 5th Southeastern Conference on Combinatorics, Graph Theory and Computing*, pp. 513–527.

Kay, S. (1993). *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice Hall.

Kim, S., X. Wang, and M. Madihian (2008). Optimal resource allocation in multi-hop ofdma wireless networks with cooperative relay. *IEEE Transactions on Wireless Communications 7*(5), 1833–1838.

Koorapaty, H., A. Hassan, and S. Chennakeshu (2000). Secure information transmission for mobile radio. *IEEE Communications Letters 4*(2), 52–55.

Lee, K. and V. Leung (2006). Fair allocation of subcarrier and power in an ofdma wireless mesh network. *IEEE Journal on Selected Areas in Communications 24*(11), 2051–2060.

Leung-Yan-Cheong, S. and M. Hellman (1978). The gaussian wire-tap channel. *IEEE Transactions on Information Theory 24*(4), 451–456.

Li, Q. and W. Ma (2011). Optimal and robust transmit designs for miso channel secrecy by semidefinite programming. *IEEE Transactions on Signal Processing 59*(8), 3799 –3812.

Li, X., A. Nusairat, Y. Wu, Y. Qi, J. Zhao, X. Chu, and Y. Liu (2009). Joint throughput optimization for wireless mesh networks. *IEEE Transactions on Mobile Computing 8*(7), 895–909.

Liang, Y., H. Poor, and L. Ying (2009). Secrecy throughput of manets with malicious nodes. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 1189–1193.

Madiseh, M., M. McGuire, S. Neville, L. Cai, and M. Horie (2008). Secret key generation and agreement in uwb communication channels. In *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–5.

Maheshwari, R., H. Gupta, and S. Das (2006). Multichannel mac protocols for wireless networks. In *Proc. IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON)*, Volume 2, pp. 393–401.

Mai, Y. and K. Chen (2011). Design of zone-based bandwidth management scheme in ieee 802.16 multi-hop relay networks. *EURASIP Journal on Wireless Communications and Networking 2011*(1), 1–28.

Mathur, S., W. Trappe, N. Mandayam, C. Ye, and A. Reznik (2008). Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 128–139.

Moscibroda, T., R. Chandra, Y. Wu, S. Sengupta, P. Bahl, and Y. Yuan (2008). Load-aware spectrum distribution in wireless lans. In *Proc. IEEE International Conference on Network Protocols (ICNP)*, pp. 137–146.

Ozan Koyluoglu, O., C. Emre Koksal, and H. El Gamal (2010). On secrecy capacity scaling in wireless networks. In *Proc. IEEE Information Theory and Applications Workshop (ITA)*, pp. 1–4.

Ren, K., H. Su, and Q. Wang (2011). Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications 18*(4), 6–12.

Romero-Zurita, N., M. Ghogho, and D. McLernon (2011). Physical layer security of mimo frequency selective channels by beamforming and noise generation. In *Proc. European Signal Processing Conference (EUSIPCO)*, pp. 829 –833.

Romero-Zurita, N., M. Ghogho, and D. McLernon (2012). Outage probability based power distribution between data and artificial noise for physical layer security. *IEEE Signal Processing Letters 19*(2), 71 –74.

Rukhin, A., J. Soto, J. Nechvatal, M. Smid, and E. Barker (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications.

Sayeed, A. and A. Perrig (2008). Secure wireless communications: secret keys through multipath. In *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3013–3016.

Shafiee, S. and S. Ulukus (2007). Achievable rates in gaussian miso channels with secrecy constraints. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 2466–2470.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal 28*(4), 656–715.

So, J. and N. Vaidya (2004). Multi-channel mac for ad hoc networks: handling multi-channel hidden terminals using a single transceiver. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 222–233.

Subramanian, A., H. Gupta, S. Das, and J. Cao (2008). Minimum interference channel assignment in multiradio wireless mesh networks. *IEEE Transactions on Mobile Computing 7*(12), 1459–1473.

Tse, D. and P. Viswanath (2005). *Fundamentals of Wireless Communication*. Cambridge University Press.

Vasudevan, S., D. Goeckel, and D. Towsley (2010). Security-capacity trade-off in large wireless networks using keyless secrecy. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 21–30.

Viswanath, P., D. Tse, and R. Laroia (2002). Opportunistic beamforming using dumb antennas. *IEEE Transactions on Information Theory 48*(6), 1277–1294.

Wang, Q., H. Su, K. Ren, and K. Kim (2011). Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1422–1430.

Wang, X. and P. Huang (2012, December). Ofdma-based method for channel-width adaptation in wireless mesh networks. Patent Application Number: 201210514654.7.

Weber, S., J. Andrews, and N. Jindal (2010). An overview of the transmission capacity of wireless networks. *IEEE Transactions on Communications 58*(12), 3593–3604.

Wilson, R., D. Tse, and R. Scholtz (2007). Channel identification: secret sharing using reciprocity in ultrawideband channels. In *Proc. IEEE International Conference on Ultra-Wideband (ICUWB)*, pp. 270–275.

Wyner, A. (1975). The wire-tap channel. *Bell System Technical Journal 54*(8), 1355–1387.

Zeng, K., D. Wu, A. Chan, and P. Mohapatra (2010). Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9.

Zhou, X., R. Ganti, J. Andrews, and A. Hjørungnes (2011). On the throughput cost of physical layer security in decentralized wireless networks. *IEEE Transactions on Wireless Communications 10*(8), 2764–2775.

Zhou, X. and M. McKay (2010). Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. *IEEE Transactions on Vehicular Technology 59*(8), 3831–3842.

Zhou, X., M. Tao, and R. Kennedy (2012). Cooperative jamming for secrecy in decentralized wireless networks. In *Proc. IEEE International Conference on Communications (ICC)*, pp. 2339–2344.

Acknowledgments

I would like to express my gratitude to all who provide support to me during my master study.

First, I would like to thank my advisor, Prof. Xudong Wang. Under his guidance, I have made progress in many aspects, from identifying research problems to finding creative solutions, from writing papers to giving presentations, and from thinking independently to cooperating with others. Prof. Wang also instructs me on how to review papers submitted to top journals and conferences. This part of training encourages me to closely follow the state-of-the-art research and stimulates my critical thinking.

I also would like to thank Prof. Mian Li, who is patient and enthusiastic. Prof. Li provides me valuable suggestions on the theory of optimization.

It has been a great experience to work with my group members, Jun Wang, Pin Lv, Shanshan Wu, Wenguang Mao, Huaiyu Huang, Quan Liu, Yibo Pi, Yuhang Zhang, Rongguang Li, Zhongkai Xu, and Aimin Tang. Their friendship is a stimulus for my research work.

I am grateful to my roommates, Dong Qiu and Jiapin Guo. We help each other overcome difficulties, share ideas on different topics, and visit many places of interest. It has been a wonderful time to be with them.

I would like to express my deepest gratitude to my parents for their unconditional love, understanding, and encouragement.