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

---

Random Analog Network Coding

From Design to Applications

by

Wenguang Mao

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. Jun Zhang
Prof. Xinen Zhu

Shanghai
March, 2014

Abstract

Analog Network Coding (ANC) is a promising physical-layer technique which dramatically improves the spectrum efficiency of wireless communications. However, the applications of ANC in wireless networks remain very limited due to following facts:1) physical-layer limitations of current ANC schemes, such as requiring specific type of modulation or fine-grained synchronization; 2) lack of effective protocols and schemes to exploit the benefits of ANC. Therefore, to effectively apply ANC to wireless networks, both physical-layer design of ANC and protocols that creatively utilize ANC need to be investigated.

In this thesis, a new ANC scheme, called random analog network coding (RANC), is developed to eliminate physical layer limitations of existing ANC schemes. It incorporates several function blocks, including frame detection, joint channel estimation, waveform recovery, circular channel estimation, and frequency offset compensation, to support random concurrent transmissions with various linear modulation schemes. RANC is implemented and evaluated on USRP-based software-defined radio platforms. Extensive experiments demonstrate that RANC works effectively without being constrained by limitations of existing ANC schemes and the performance of RANC significantly outperforms these schemes.

Based on this new physical-layer scheme, two applications of ANC to wireless networks are studied. The first application is to incorporate ANC into wireless mesh/ad hoc networks to improve the network throughput performance. To achieve this goal without relying on complicated scheduling or network optimization algorithms, a new random medium access control protocol is proposed to dynamically form ANC cooperation groups. To evaluate the protocol performance, both theoretical analysis and network simulations are carried out. Performance results illustrate that our scheme can enhance the network throughput by 6%-115% compared to existing protocols in various network settings .

In the second application, RANC is utilized to support a new physical-layer security scheme designed for legacy wireless communication devices. In this scheme, a secrecy protector is introduced to: 1) generate jamming signals to prevent eavesdroppers from overhearing the messages sent by the legacy client; 2) securely share the jamming signals with the access point (AP). With RANC, the AP can effectively cancel the jamming interference and successfully receive the message from the client. To evaluate the performance of the scheme, it is implemented on the USRP-based platform. The experiment results demonstrate its effectiveness of ensuring the secure communications of the legacy client.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Analog network coding is an emerging physical-layer technique which supports concurrent transmissions from two different transmitters to the same receiver. When one frame (called *self frame* in this thesis) is known at the receiver, the other one (called *desired frame*) can be extracted from the superimposed signals by an ANC scheme. The assumption of knowing the self frame is valid in many scenarios of wireless networking, e.g., two-way relaying. Thus, it is highly beneficial to incorporate ANC into a wireless network to support concurrent transmissions and improve both spectrum efficiency and network capacity (Rankov and Wittneben, 2007). However, little progress has been made so far to practically apply ANC to wireless networks. The difficulty is mainly attributed to two factors explained as follows.

The first factor is the physical-layer limitations in existing ANC schemes. For instance, some ANC schemes (Popovski and Yomo, 2006; Rossetto and Zorzi, 2009; Li et al., 2009) demand a certain level of accuracy in frame-level synchronization between concurrent transmissions. Such ANC is only applicable to a wireless network where all nodes in the network are strictly synchronized and network-wide packet scheduling is adopted. However, for many wireless networks such as ad hoc networks and mesh networks, it is impractical to implement network-wide packet scheduling or achieve strict synchronization among nodes. In other ANC schemes, concurrent

transmissions can be totally asynchronous. However, the new limitations are introduced. For example, the design of ANC proposed by Katti et al. (2007) takes advantage of the features of minimum shift key (MSK) modulation, so it is inapplicable to other modulation schemes, including commonly used ones like BPSK, QPSK, and QAM.

The second factor which leads to limited applications of ANC is the lack of effective protocols to support ANC. So far, most of research results on how to apply ANC to wireless networks are limited to the networks with simple topologies such as layered topology (Maric et al., 2012), hierarchical topology (Jitvanichphaibool et al., 2009), and linear topology (Fu et al., 2010). However, for wireless networks with a general topology, there still remain many open problems. Particularly, there lacks an effective medium access control (MAC) protocol to coordinate nodes to form ANC cooperation in such type of networks.

Therefore, to apply ANC to wireless networks in a practical and effective manner, both physical-layer design of ANC and protocols that creatively utilize ANC need to be studied. In this thesis, we develop a new physical-layer scheme for ANC and propose two protocols for applying ANC to wireless networks: a MAC protocol to effectively support ANC cooperation in mesh networks or ad hoc networks and a security scheme to provide physical-layer security for legacy wireless communication devices.

In the rest of this chapter, the background, the motivation and the introduction of above research work are presented.

1.1 Physical-Layer Design of ANC

Analog network coding is first introduced in the two-way relay channel as shown in Fig. 1.1 (Zhang et al., 2006; Popovski and Yomo, 2006). In this channel model, each end user needs to send its data frames to the other one with the help of the relay node. With ANC technique, two end users can concurrently transmit their own data frames to the relay node and then the relay

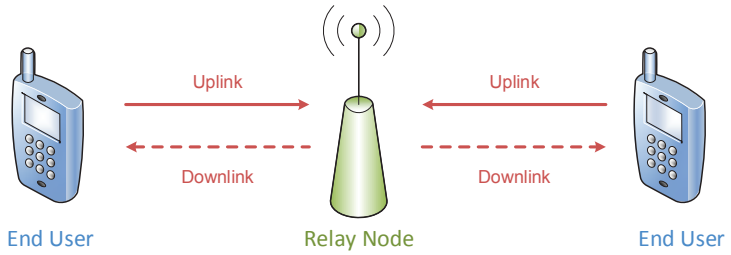


Figure 1.1: Two-way relay channel.

node amplifies (or performs some coding operations based on analog waveforms) and forwards superimposed signals to end users. Since one of frames in the superimposed signals is known, each end user can extract the other frame (the desired one) from the superimposed signals relying on an ANC scheme. By this means, the spectrum efficiency of wireless communications is significantly improved: ANC can enhance the throughput of a two-way relay channel by 100% compared to conventional bi-directional relaying technique, and 33% compared to digital network coding schemes (Popovski and Yomo, 2006).

However, the original ANC scheme proposed by Popovski and Yomo (2006) requires the strict synchronization between concurrent transmissions, which is highly demanding in many communications systems, such as mesh networks and ad hoc networks. To address this issue, several ANC schemes have been developed. ANC schemes designed by Rossetto and Zorzi (2009) and Li et al. (2009) relax the requirement of synchronization by taking advantage of cyclic prefix (CP) of orthogonal frequency division multiplexing (OFDM). As long as the misalignment of the two signals at the receiver does not exceed CP, there is no problem with frame reception. Unfortunately, if no global synchronization device like GPS is available, achieving synchronization accuracy of within one CP is still highly challenging. Some researchers assume that short signaling messages (e.g. request to send (RTS)/clear to send (CTS) in IEEE 802.11 (IEEE, 2007)) can be exchanged among nodes to achieve such synchronization accuracy. However, this approach is proved to be infeasible (Elson et al., 2002; Sommer and Wattenhofer, 2009). Katti et al. (2007) proposes another ANC scheme, which allows asynchronous concur-

rent transmissions. However, a certain level of asynchronization is required to guarantee an interference-free part at the beginning or the ending of a frame for the purposes of the baseband processing. To ensure such an interference-free part, frame sizes in concurrent transmissions need to be equal. Moreover, some random delay must be added by MAC before a transmission starts. Padding shorter frame degrades spectrum efficiency, and inserting random delay does not really guarantee the required level of asynchronization in concurrent transmissions. Also, the design of this ANC scheme takes advantage of the features of MSK modulation, so it is inapplicable to other modulation schemes, including commonly used ones like BPSK, QPSK, and QAM.

The limitations in existing ANC schemes severely limit the flexibility of incorporating ANC into a wireless network. To utilize the benefits of ANC, such limitations need to be eliminated. In this thesis, we propose a new ANC scheme to meet the following requirements: 1) frame transmissions from two transmitters do not have any requirement of frame-level synchronization or asynchronization; 2) it is applicable to any linear modulation schemes such as BPSK, QPSK, and QAM; 3) it supports concurrent transmissions with unequal frame sizes. Therefore, the new scheme eliminates all limitations in existing ANC schemes. With such a distinct advantage, it can be easily integrated with a *random* MAC protocol and can also be flexibly applied to many applications that demand *random* concurrent transmissions. As a result, this new ANC scheme is called **random** *analog network coding (RANC).*

With this new physical-layer technique that eliminates the constraints in existing ANC schemes, the applicability of analog network coding in wireless networks is significantly extended. To demonstrate this advantage, we study two applications of RANC. In the first application, RANC is applied to support a new relaying scheme called *multi-way relaying.* This scheme can achieve higher spectrum efficiency than two-way relaying when frames in a network have variable sizes. The second application of RANC is to enable effective random access in a wireless network with analog network coding. Due to the constraint-free characteristic of

RANC, a novel mechanism called *flow compensation* becomes feasible in such networks. This mechanism significantly improves the network throughput when traffic flows in the network are not symmetric. Both applications are greatly beneficial to boost network performance and only supported by RANC among all ANC schemes. Moreover, with the constraint-free feature, more creative applications of RANC in wireless networks can be expected.

The entire scheme of RANC and its network applications are implemented and evaluated on a USRP-based software-defined radio testbed. Firstly, each function block of RANC is validated. Experimental results are compared to the case without such a function block. Comparisons illustrate the significant performance gain achieved by each function block. Experiments also confirm that the constraints in existing ANC schemes are completely eliminated in RANC. Secondly, the bit error rate (BER) performance of the entire RANC scheme is measured on the testbed. Results show that BER of decoding the desired frame from superimposed signals is close to (within 0.3 dB) the case of interference-free communications. Thirdly, experiments for applications of RANC are conducted on real networks deployed in our laboratory where flexibility and efficiency of applying RANC in wireless networks are clearly demonstrated. Evaluation results show that the throughput performance of wireless networks can increase 47%-80% by applying RANC in different scenarios.

1.2 MAC Protocols for ANC

Medium access control (MAC) protocol is an essential mechanism to coordinate channel access when there exist multiple nodes sharing the same transmission medium. The primary objective of MAC protocol is to minimize collisions among different nodes in a network and maximize the transmission medium utilization (Leon-Garcia and Widjaja, 2003). In wireless communications, the transmission medium is intrinsically shared by all nodes. Hence MAC protocols are indispensable in wireless networks.

Since ANC involves multi-node cooperation and concurrent transmissions, MAC protocols proposed for traditional physical-layer transmission schemes (point-to-point transmission) cannot support ANC. Therefore, to effectively apply ANC to wireless networks, specifically designed MAC protocols are required. To date, a number of MAC protocols have been developed to support ANC in wireless networks with simple topologies such as layered topology (Maric et al., 2012), hierarchical topology (Jitvanichphaibool et al., 2009), and linear topology (Fu et al., 2010). However, for wireless networks with a general topology such as mesh networks and ad hoc networks, there still remain many research problems with regard to designing effective MAC protocols. Particularly, how to dynamically form ANC cooperation groups among network nodes poses the most important one. In [Su and Zhang (2009)], channel assignment and link scheduling for forming ANC cooperation groups in a wireless ad hoc network are formulated as an optimization problem, which is proved to be NP-hard. In general, the complexity of scheduling ANC cooperation groups in a wireless network is proved to be NP-complete by Goussevskaia and Wattenhofer (2008). Therefore, to ensure ANC technique to be practically applicable to a general wireless network, random access becomes a preferred approach.

To our best knowledge, only two papers (Khabbazian et al., 2011; Wang et al., 2013) have worked on random access MAC protocols for ANC. In the first paper (Khabbazian et al., 2011), an algebraic model is derived for MAC layer and a random access algorithm is designed for ANC at a theoretical level. However, no practical MAC protocol is actually developed. In the second paper (Wang et al., 2013), a distributed MAC protocol is proposed to support ANC in wireless mesh/ad hoc networks. However, this protocol does not develop any mechanism to hold the throughput performance in the scenario where bi-directional traffic flows in ANC cooperation groups are not always available. Since this scenario is very common in wireless networks, the applicability of the protocol is limited. Also, this protocol does not take the hidden nodes into consideration and no mechanism is proposed to mitigate the potential issues caused by the existence of hidden nodes. Thus, the performance of the protocol in a general

multi-hop network is negatively affected by these issues. So far, there still lacks an effective random access MAC protocol to support ANC.

In this thesis, a new random access MAC protocol, called *ANC-ERA*, is developed to dynamically form ANC cooperation groups in general-topology wireless networks. This protocol totally matches the mechanisms of IEEE 802.11 DCF. More importantly, it is characterized by several advantages: 1) an efficient mechanism of network allocation vector (NAV) significantly improves the throughput performance; 2) ANC cooperation is effectively protected with the channel occupation frame; 3) a reliable ACK mechanism dramatically reduces the negative impact of the loss of ACK frames due to the hidden-node problem in a network with ANC; 4) asymmetrical traffic flows from end nodes in an ANC cooperation group are compensated by traffic flows from neighboring nodes under the flow compensation mechanism, which highly increases the throughput performance of the networks where bi-directional traffic is not always present. The performance of ANC-ERA protocol is evaluated by the theoretical analysis and the network simulation. Results from derivations match those from simulations well, and both demonstrate that ANC-ERA can significantly enhance the network throughput in various scenarios as compared to existing random access schemes.

1.3 Physical-Layer Security Scheme Based on RANC

Different from wired networks where the transmission is enclosed in the cable, wireless communications are open in nature and easy to access. This characteristic of wireless communications leads to the transmission vulnerable to eavesdropping and also makes traditional encryption schemes less effective (Shiu et al., 2011). To protect wireless communications from eavesdropping, physical-layer security is introduced and developed.

Existing physical-layer security schemes can be classified into two categories according to the basic principles followed by these schemes. The fundamental of the first category schemes is

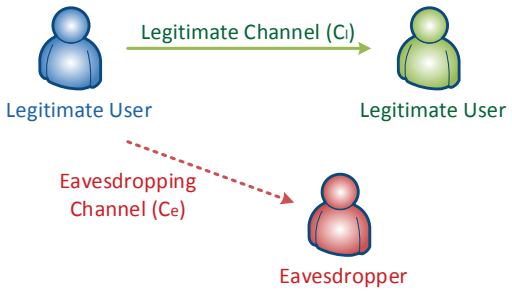


Figure 1.2: Wire-tap channel.

laid by Wyner (1975) and Csiszár and Korner (1978), who propose the wire-tap channel model and derive its secure capacity. As shown in Fig. 1.2, the secure capacity between legitimate users in a wire-tap channel is given by

$$C_{sec} = \max\{C_l - C_e, 0\}$$

According to this equation, if the eavesdropping channel has better link quality, no secure communication between legitimate users can be guaranteed. To avoid this situation, security schemes in the first category exploit some physical-layer technique, such as beamforming, imposing the interference, and generating artificial noise, to improve the secure capacity by enhancing C_l (Khisti and Wornell, 2010; Wang et al., 2012) or degrading C_e (Negi and Goel, 2005; Gollakota and Katabi, 2011; Tang et al., 2011). Further combining with special channel coding schemes (Popovski and Simeone, 2009; Thangaraj et al., 2007), security schemes in the first category can ensure the perfect secrecy of communications between legitimate users. The second category physical-layer security schemes exploit the channel magnitude reciprocity (Mathur et al., 2008; Jana et al., 2009), channel phase reciprocity (Koorapaty et al., 2000), or both (Pengfei Huang, 2013) to generate a common secret key for legitimate users. Since the eavesdropping channel is independent with the legitimate channel, the eavesdropper cannot extract any information about this key from its own channel and hence is not able to decipher the communications between legitimate users.

Most of current physical-layer security schemes in both categories require special physical-

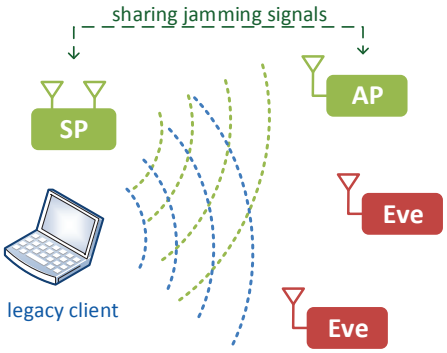


Figure 1.3: Schematic diagram for RANC-based physical-layer security protocol.

layer signal processing (e.g., applying superposition coding or generating artificial noise), and hence are not supported by existing commercial hardware. Therefore these schemes cannot be applied to provide secrecy protection for clients equipped with legacy wireless communication devices, since it is infeasible to modify the physical-layer hardware of legacy devices to adapt these schemes. A few schemes (Mathur et al., 2008; Jana et al., 2009) in the second category can run on the hardware of existing devices. However, the key generation speed of these schemes is very slow when channel coherence time is long and hence they are not applicable to semi-stationary networks (Gollakota and Katabi, 2011). Considering that a variety of legacy wireless devices such as laptops, tablets, and cell phones work in semi-stationary environments and require secrecy protection, a new physical-layer security scheme that can run on the hardware of these devices is highly needed.

To solve this problem, we propose the *collusion-resistant jamming* security scheme to provide secrecy protection on legacy wireless communication devices. In this scheme, a third-part device called *secrecy protector (SP)* is introduced to generate jamming signals to prevent the eavesdroppers from overhearing the transmission of the legacy client. To combat with the collusion among cooperative eavesdroppers, the mechanisms, such as multi-stream jamming, pseudo-preambles, and segment transmission, are designed to complicate the collusion process. Moreover, the seed generation mechanism is developed to allow the SP to share the jamming signals with the legitimate receiver of the data frames from the client, i.e., the access point

(AP). Based on this knowledge, the RANC technique is utilized to cancel the jamming signals at the AP, which effectively guarantees the successful reception of the frame sent by the client. To evaluate the effectiveness of the collusion-resistant jamming scheme, it is implemented on USRP software-defined radio platform and tested in the real network deployed in the laboratory. The performance results demonstrate that the scheme can effectively prevent the eavesdroppers from accessing the information sent by the client and the proper communication between the client and the AP is not affected. More importantly, the results confirm that the scheme does not impose any special requirement on the physical-layer of the legacy client.

1.4 Organization of the Thesis

The rest of the thesis is organized as follows. In Chapter 2, the physical-layer design of RANC is discussed in detail. In Chapter 3, ANC-ERA MAC protocol for applying ANC to wireless mesh/ad hoc networks is presented. In Chapter 4, the collusion-resistant jamming scheme based on RANC is described. In Chapter 5, the thesis is concluded.

Chapter 2

Random Analog Network Coding

In this chapter, the new physical-layer design of analog network coding (ANC) is investigated. Specifically, we first discuss the major constraints in existing ANC schemes. To remove these constraints and extend the applicability of ANC in wireless networks, we propose a new ANC scheme called *random analog network coding (RANC)*. This scheme includes several function blocks such as frame detection, joint channel estimation, waveform recovery, circular channel estimation, and frequency compensation. The algorithms in all these function blocks are specially designed to avoid the constraints on synchronization, frame size, modulation scheme, and so on. To evaluate its performance, the entire RANC scheme is implemented with USRP software-defined radio platform and tested in networks deployed in the laboratory. The results demonstrate that RANC effectively eliminates the limitations in existing ANC schemes and significantly outperforms these schemes.

2.1 Constraints in Analog Network Coding

The major constraints for limiting the applicability of ANC schemes in wireless networks are described in this section.

2.1.1 Synchronization

A simple ANC scheme is amplify-and-forward two-way relaying (Popovski and Yomo, 2006). It requires perfect synchronization to achieve optimal performance. However, in a wireless network, it is difficult to achieve strict synchronization unless GPS or other global reference clock is available. Even if the communication nodes are strictly synchronized, frame transmissions need to be scheduled in advance, which is not efficient for data networks where transmissions are bursty. This is even more challenging for ad hoc networks where distributed scheduling is still a challenging issue.

To mitigate the issue of strict synchronization, an OFDM-based physical layer network coding (PLNC) is proposed by Rossetto and Zorzi (2009). It requires the synchronization offset of two concurrent frames to be within cyclic prefix (CP) of an OFDM symbol. Such a scheme can be tailored for ANC. However, synchronization granularity within a CP is still a challenging requirement in many communication systems. For example, the CP of an OFDM symbol in an 802.11a transceiver is specified as 0.8μs (IEEE, 1999). As a result, two concurrent transmissions need to be synchronized within 0.8μs, which is a non-trivial task. Without a GPS module, communication nodes have to rely on signaling messages to synchronize their transmissions. However, synchronization accuracy is limited by a few factors such as disparate processing time of an arrival message, propagation delay, and multi-path effect. To the best of our knowledge, among all message-based synchronization schemes (Elson et al., 2002; Sundararaman et al., 2005; Sommer and Wattenhofer, 2009), the physical-layer reference broadcast scheme (Elson et al., 2002) achieves the highest accuracy, but the synchronization accuracy is only 1.85μs (mean) $\pm$ 1.28μs (deviation). Thus, satisfying the requirement of 0.8μs synchronization accuracy is not practically feasible. As the physical layer keeps increasing the rate, the CP becomes even smaller. For example, the CP of an OFDM symbol in 802.11ad is 48.4 ns (IEEE, 2012). Achieving such a synchronization accuracy is demanding even for GPS-based synchronization.

2.1.2 Asynchronization and Frame Size

The ANC scheme in [Katti et al. (2007)] requires an interference-free part (in the beginning or the end of a frame) for both frames. This is needed for identifying the start (or the end) of a frame and also for estimating frequency offset, sampling offset, and channel distortion due to sudden frequency change. Thus, two superimposed frames have to maintain a certain level of asynchronization. To this end, a frame with shorter length has to be padded to the same length as the longer one. Moreover, random delay must be inserted before a transmission starts. Padding frames leads to waste of transmission power and spectrum, and adding random delay increases overhead. Moreover, inserting random delay does not guarantee that two frames are asynchronous with each other.

Even if we assume that sufficient asynchronization can be guaranteed without padding frames, the requirement of interference-free part at the beginning or the end of the frames still leads to low spectrum utilization in some scenarios. Consider the example in Fig. 2.1, where Node A and Node C have frames to exchange with each other. We assume that traffic from Node A to Node C and that from Node C to Node A belong to different applications, and hence frames sent from two nodes may have significantly different frame sizes (McGregor et al., 2004; Roughan et al., 2004; Lin et al., 2009). Assuming a frame from Node A to Node C is longer, when ANC is applied, Node C finishes its transmission before Node A and then the channel from Node C to Node A becomes idle. In this case, even if this idle time is enough for Node D to send a frame to Node A, the transmission has to be delayed until Node B finishes broadcasting the superimposed signals. This is because, if Node D starts its transmission in this idle time, an interference-free part at the beginning (or the end) of each frame cannot be guaranteed: the frame from Node C can only have an interference-free part at the beginning , while the frame from Node D can only have an interference-free part at the end; if so, the frame from Node A does not have an interference-free part at either the beginning or the end.

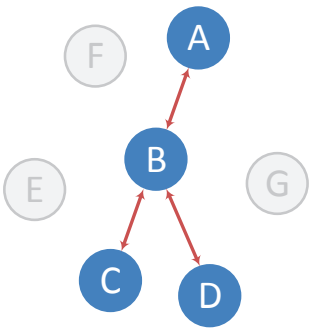


Figure 2.1: A typical communication scenario in wireless networks.

2.1.3 Modulation

Some ANC schemes are only applicable to a specific modulation scheme. The well known ANC scheme in [Katti et al. (2007)] relies on the property of MSK modulation (i.e., signals have constant amplitude). With this property, when two MSK-modulated signals are superimposed asynchronously with each other, the amplitude for each signal can be easily estimated. Based on the amplitude knowledge of each signal, the superimposed signals can be decomposed based on the parallelogram law, and possible phases for both signals can be determined (Katti et al., 2007). Since the receiver has knowledge on one of signals, it can select the right phase of the other signal from possible values. In MSK modulation, information is carried by the phase difference between consecutive samples, and channel phase shift has no impact on the phase difference. Thus, the ANC scheme in [Katti et al. (2007)] does not need a mechanism to track channel phase shift.

Considering many other modulation schemes (e.g., QAM), signal amplitude is not necessarily constant. Moreover, accurate phase tracking is needed for effectively demodulation. Therefore, ANC schemes like [Katti et al. (2007)] are not applicable to these modulations.

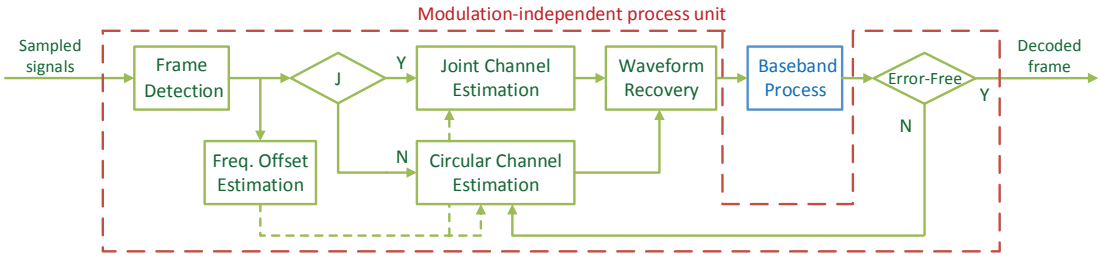


Figure 2.2: The block diagram of a RANC receiver.

2.2 Major Function Blocks in RANC

2.2.1 Overview

The physical-layer design of RANC takes a receiver-oriented approach, i.e., major functions are located in the receiver, as show in Fig. 2.2. Given the sampled superimposed signals, they are first forwarded to a frame detection module to locate the starting and ending points of two superimposed frames. The frame detection module also locates the samples that are helpful for channel estimation. To assist frame detection at the receiver, a transmitter needs to form a frame following a certain format, as discussed in Section 2.2.2. This is the only function that needs to be added to a RANC transmitter.

There are two channel estimation schemes in a RANC receiver: joint channel estimation and circular channel estimation. In the joint channel estimation module, channel coefficients for the self frame and the desire frame are estimated jointly by utilizing the samples located by the frame detection module.

When the samples located by the frame detection module are sufficient to obtain accurate channel coefficients, the interference to the desired frame can be cancelled by removing the signals of the self frame. However, to compensate the shift of optimal sampling points, a waveform recovery module is needed to recover the waveform of the desired frame and then resample it. The samples from the waveform recovery module are finally used by a standard

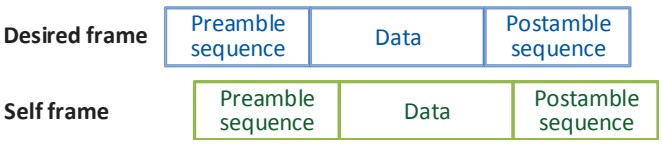


Figure 2.3: Frame format of RANC.

baseband module to reconstruct the desired frame.

When the samples located by the frame detection module are insufficient, the decision block J1 selects the circular channel estimation module. Circular channel estimation takes multiple rounds of channel estimation to successively mitigate interference until the desired frame is error-free. No function block in RANC needs any level of synchronization (or asynchronization), requires an interference free part of a frame, or exploits the property of a specific modulation scheme. Thus, modulation-independent concurrent transmissions can be started *randomly* with *arbitrary* frame sizes.

2.2.2 Frame Detection

The frame detection module detects the arrival of superimposed frames, finds the starting and ending points of each frame, and locates useful samples for channel estimation. To this end, a frame format is designed as shown in Fig. 2.3. In this design, two identical pseudo-random pilot sequences are attached to the header and the tail of a frame as the preamble and the postamble, respectively. The frame layout of our design looks similar to that in [Katti et al. (2007)]. However, there exist two major differences. First, our design does not need extra header information at the end of a frame. Second, how to utilize the frame layout is significantly different. Specifically, the scheme in [Katti et al. (2007)] requires an interference-free part at the preamble or the postamble of each frame in concurrent transmission for timing synchronization and channel distortion evaluation. Instead, our scheme allows any degree of overlapping in two concurrent transmitted frames. With our frame layout, we can effectively utilize overlapping parts to estimate channel coefficients.

With the new frame format, two transmitters of superimposed frames are required to adopt distinct pilot sequences, and both are known by the receiver. With distinct pilot sequences, the frames of concurrent transmissions can be detected via correlation. Let $\{p_s[n]\}$ and $\{p_d[n]\}$ denote two pilot sequences adopted by the self frame and the desired frame, respectively, and $\{s[n]\}$ stand for samples of superimposed signals. To detect frames, the receiver correlates samples with two pilot sequences to get correlation sequences $\{S_s[i]\}$ for the self frame and $\{S_d[i]\}$ for the desired frame, i.e.,

$$\begin{aligned} S_s[i] &= \sum_{k=0}^{L-1} s[i+k]p_s[k+1] \\ S_d[i] &= \sum_{k=0}^{L-1} s[i+k]p_d[k+1]. \end{aligned}$$

The value of correlation spikes only when sequence $\{p_s[n]\}$ or $\{p_d[n]\}$ perfectly aligns with the preamble or the postamble of the corresponding frame. Hence, frame detection can be fulfilled by checking the peaks of correlation: 1) the first peak indicates the arrival of superimposed frames; 2) the peaks of $\{S_s[i]\}$ locate the beginning and the end of the self frame; 3) the peaks of $\{S_d[i]\}$ tell the beginning and the end of the desired frame. Note that although the preamble (or the postamble) of one frame may be interfered by the other frame, the impact of the interference on the occurrence of correlation peaks is negligible. This observation has been verified by experiments in [Gollakota and Katabi (2008); Tan et al. (2009)].

Based on located points in each frame, we need to identify samples that can be utilized to estimate channel coefficients. For joint channel estimation, we need the samples of which the corresponding symbols from both frames are known by the receiver. We call these samples as *useful samples*. To this end, the superimposed frame is split into several parts as shown in Fig. 2.4: 1) $\mathbf{y_1}$ is aligned with the preamble of the desired frame; 2) $\mathbf{y_2}$ is in between the two starting points of the postamble of two frames; 3) $\mathbf{y_3}$ is the samples aligned with the postamble of the self frame; 4) $\mathbf{y_4}$ takes the remaining part. Whether these parts of the superimposed

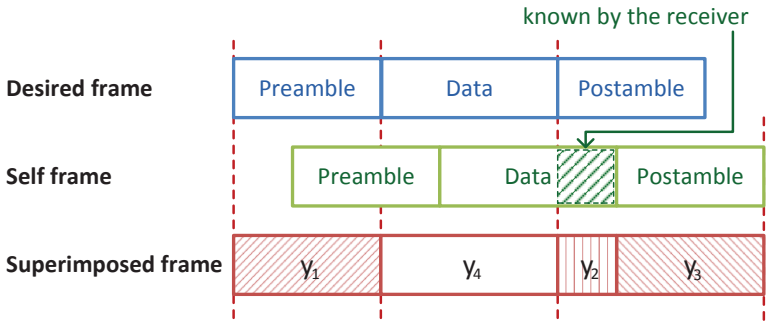


Figure 2.4: Different samples detected by the frame detection module.

frame can be utilized for joint channel estimation is analyzed as follows.

Considering samples $\mathbf{y_1}$ with length N_1, we have*

$$y_1[n] = h_{d,eqv}x_{1d}[n] + h_{s,eqv}x_{1s}[n] + w_1[n], \quad n = 1, \ldots, N_1,$$

where $h_{s,eqv}$ and $h_{d,eqv}$ are the equivalent channel coefficients in the discrete-time baseband model for the self frame and the desired frame, $x_{1d}[n]$ and $x_{1s}[n]$ are symbols in two frames, and $w_1[n]$ is noise. Note that $\{x_{1d}[n]\}$ is the preamble of the desired frame, so it is known. Moreover, $\{x_{1s}[n]\}$ is a sequence with a number of zeros followed by the truncated preamble sequence of the self frame. Since the receiver has located the starting point of each frame, the shift (in samples) between two frames, namely the number of zeros (denoted as N_{1z}) in $\{x_{1s}[n]\}$ before the truncated preamble sequence, is known. Thus, the receiver has full knowledge of sequence $\{x_{1s}[n]\}$. As a result, $\mathbf{y_1}$ is useful for estimating channel coefficients $h_{s,eqv}$ and $h_{d,eqv}$. A similar analysis on $\mathbf{y_3}$ indicates that $\mathbf{y_3}$ can also be utilized for channel estimation. Furthermore, samples in $\mathbf{y_2}$ can be expressed as

$$y_2[n] = h_{d,eqv}x_{2d}[n] + h_{s,eqv}x_{2s}[n] + w_2[n], \quad n = 1, \ldots, N_2,$$

where N_2 is the length of samples $\mathbf{y_2}$. Note that $\{x_{2d}[n]\}$ is the first N_2 symbols of the postamble

*For the sake of clarity, the items caused by multi-path effect are omitted in the following equations.

of the desired frame, and hence is fully known by the receiver. $\{x_{2s}[n]\}$ is a part of payload of the self frame, so it is still known by the receiver. Therefore, $\mathbf{y_2}$ is also useful for channel estimation. However, samples y_4 involve the unknown symbols in the data field of the desired frame, so they cannot be used for joint channel estimation.

As shown in Fig. 2.4, only partial preamble of the self frame is located in $\mathbf{y_1}$, but the entire preamble of the desired frame lies in this region. Thus, if $\mathbf{y_1}$ is used for channel estimation, a higher accuracy can be achieved for the channel coefficients of the desired frame, since the first N_{1z} samples in $\mathbf{y_1}$ make no contribution to the accuracy for estimating channel coefficients of the self frame. To quantify the quality of samples for channel estimation, we define *effective samples* as follows: considering a useful sample for channel estimation, if its component of the self frame (or the desired frame) is non-zero, then it is an *effective sample* for the self frame (or the desired frame). Given all useful samples, the number of effective samples for the desired frame is always equal to the total size of pilot sequences (i.e., N_p), since all samples aligning with the preamble and the postamble of the desired frame are *useful* and *effective* for estimating its channel coefficients. However, the number of effective samples for the self frame can be small. Thus, the number of effective samples in the self frame is a critical parameter for channel estimation. If it is greater than a threshold N_t (i.e., Condition J in Fig. 2.2) , then the useful samples are sufficient for jointly estimating channel coefficients of both the desired frame and the self frame. In this case, a joint channel estimation module is employed. Otherwise, another channel estimation scheme, called circular channel estimation, is adopted.

The threshold for selecting joint channel estimation or circular channel estimation is a system parameter and will be discussed in Section 2.5.

2.2.3 Joint Channel Estimation

As discussed before, if both the self frame and the desired frame have enough effective samples, the joint channel estimation scheme is adopted.

Considering two superimposed frames, if channel estimation is conducted individually for each frame, taking the other frame as interference, the estimation accuracy is low due to the existence of strong interference. One solution to this problem is to impose an interference-free part at the preamble (or the postamble) of each frame to guarantee that the channel estimation can be conducted without interference. However, this solution leads to some limitations as discussed in Section 2.1.2. In our scheme, instead of requiring interference-free samples, we utilize the overlapping part of two frames to jointly estimate their channel coefficients exploiting the frame layout and the knowledge of the self frame.

Assuming that both the self frame and the desired frame adopt linear modulations, the waveform of the superimposed frames at the receiver can be expressed as

$$\begin{aligned} y(t) &= \sum_{\substack{n>\frac{t}{T}-n_h+1,\\ n\leqslant\frac{t}{T}+1}} h_d x_d[n] g_d(t-(n-1)T) + \\ &\quad \sum_{\substack{n>\frac{t-T_d}{T}-n_h+1,\\ n\leqslant\frac{t-T_d}{T}+1}} h_s x_s[n] g_s(t-(n-1)T-T_d) + w(t), \end{aligned}$$

where T is the symbol time, h_d and h_s denote the channel gains of the desired frame and the self frame, respectively, $\{x_d[n]\}$ and $\{x_s[n]\}$ stand for the symbol sequences of two frames, $g_d(t)$ and $g_s(t)$ represent pulse shapes of the two frames, and T_d denote the time offset between the two frames. $w(t)$ is the noise process. Also, n_h captures inter-symbol interference (ISI) and multi-path effect and can be considered as the number of channel taps. Upon sampling, the signal of the i-th sample is given by

$$\begin{aligned} y[i] &= \sum_{\substack{n>\frac{\Delta}{T}-n_h+i,\\ n\leqslant\frac{\Delta}{T}+i}} h_d x_d[n] g_d((i-1)T+\Delta-(n-1)T) + \\ &\quad \sum_{\substack{n>i-n_h-\frac{T_d-\Delta}{T},\\ n\leqslant i-\frac{T_d-\Delta}{T}}} h_s x_s[n] g_s((i-1)T+\Delta-(n-1)T-T_d) + w((i-1)T+\Delta), \end{aligned}$$

where $(i-1)T+\Delta$ is the sampling position. In a conventional point-to-point communication mode, Δ is locked to a value that corresponds to the optimal sampling position via a time synchronization mechanism (Mengali and D'Andrea, 1997). However, in superimposed frames, time synchronization signals of one frame is interfered by the other frame. Tracking optimal sampling positions is infeasible, since Δ may vary from one round of transmissions to another. It is also difficult to precisely determine Δ.

For convenience, let $D = \lceil (T_d - \Delta)/T \rceil$ and $\delta = DT - (T_d - \Delta)$. Thus, a sample can be described as

$$\begin{aligned} y[i] &= \sum_{n=0}^{n_h-1} h_d x_d[i-n] g_d(\Delta + nT) + \\ &\quad \sum_{n=0}^{n_h-1} h_s x_s[i-n-D] g_s(\delta + nT) + w(iT - T + \Delta). \end{aligned} \tag{2.1}$$

In matrix form, it is

$$\mathbf{y} = [\mathbf{X_d}\ \mathbf{X_s}] \begin{bmatrix} \mathbf{h_{d,eqv}} \\ \mathbf{h_{s,eqv}} \end{bmatrix} + \mathbf{w}, \tag{2.2}$$

where $\mathbf{y}$ contains N samples of the entire superimposed frame, and $\mathbf{X_d}$ and $\mathbf{X_s}$ are $N \times n_h$ matrices whose columns are shift versions of $\{x_d[n]\}$ and $\{x_s[n]\}$ respectively. $\mathbf{w}$ is a N-dimension column vector that represents the noise. Moreover, the n_h-dimension vectors $\mathbf{h_{d,eqv}}$ and $\mathbf{h_{s,eqv}}$ are equivalent channel coefficients for the desired frame and the self frame in the discrete-time baseband model. It can be shown that,

$$\begin{cases} \mathbf{h_{d,eqv}} = h_d \left[g_d(\Delta)\ g_d(\Delta + T)\ \ldots\ g_d(\Delta + (n_h-1)T) \right]^{\mathsf{T}}, \\ \mathbf{h_{s,eqv}} = h_s \left[g_s(\delta)\ g_s(\delta + T)\ \ldots\ g_s(\delta + (n_h-1)T) \right]^{\mathsf{T}}. \end{cases}$$

The above equation indicates that the equivalent channel coefficients depend on both channel fading and pulse shape values at sampling points. Thus, equivalent channel coefficients

vary from time to time, even if channels are stationary. Thus, online channel estimation is indispensable.

Since samples $\mathbf{y_1}$, $\mathbf{y_2}$, and $\mathbf{y_3}$ in Fig. 2.4 are part of the N-dimension vector $\mathbf{y}$, a formula similar to Equation (2.2) can be written as

$$\begin{bmatrix} \mathbf{y_1} \\ \mathbf{y_2} \\ \mathbf{y_3} \end{bmatrix} = \mathbf{C_{est}} \begin{bmatrix} \mathbf{h_{d,eqv}} \\ \mathbf{h_{s,eqv}} \end{bmatrix} + \begin{bmatrix} \mathbf{w_1} \\ \mathbf{w_2} \\ \mathbf{w_3} \end{bmatrix}, \tag{2.3}$$

where the matrix $\mathbf{C_{est}}$ consists of sub-matrices of $[\mathbf{X_d}\ \mathbf{X_s}]$ that correspond to $\mathbf{y_1}$, $\mathbf{y_2}$, and $\mathbf{y_3}$. As discussed in Section 2.2.2, symbols of the desired frame and the self frame that are aligned with $\mathbf{y_1}$, $\mathbf{y_2}$, and $\mathbf{y_3}$ are known by the receiver, and hence the receiver has full knowledge of the matrix $\mathbf{C_{est}}$. Therefore, the Equation (2.3) can be utilized to jointly estimate channel coefficients of the desired frame and the self frame. Based on least square estimation, the equivalent channel coefficients are estimated as

$$\begin{bmatrix} \tilde{\mathbf{h}}_{\mathbf{d,eqv}} \\ \tilde{\mathbf{h}}_{\mathbf{s,eqv}} \end{bmatrix} = (\mathbf{C_{est}}^H \mathbf{C_{est}})^{-1} \mathbf{C_{est}}^H \begin{bmatrix} \mathbf{y_1} \\ \mathbf{y_2} \\ \mathbf{y_3} \end{bmatrix}.$$

Note that the inverse matrix of $\mathbf{C_{est}}^H \mathbf{C_{est}}$ exists if and only if the matrix $\mathbf{C_{est}}$ has full rank. This can be guaranteed by selecting different pilot sequences for two frames such that any column in the matrix $\mathbf{C_{est}}$ cannot be expressed as linear combinations of other columns.

2.2.4 Waveform Recovery and Resampling

After channel estimation, the samples are forwarded into the waveform recovery and resampling module. With the channel coefficients obtained from the previous module, the RANC receiver

removes the signals of the self frame from the superimposed frame as follows

$$\begin{aligned} \mathbf{y_d} &= \mathbf{y} - \mathbf{X_s}\tilde{\mathbf{h}}_{\mathbf{s,eqv}} \\ &= \mathbf{X_d}\mathbf{h}_{\mathbf{d,eqv}} + \mathbf{X_s}(\mathbf{h}_{\mathbf{s,eqv}} - \tilde{\mathbf{h}}_{\mathbf{s,eqv}}) + \mathbf{w} \\ &= \mathbf{X_d}\mathbf{h}_{\mathbf{d,eqv}} + \tilde{\mathbf{w}}, \end{aligned} \tag{2.4}$$

where $\tilde{\mathbf{w}}$ is the residual interference plus noise. The interference-canceled signal $\mathbf{y_d}$ cannot be directly used for demodulation, because the sampling points in $\mathbf{y_d}$ may shift from optimal positions for the desired frame. Thus, we first recover the waveform of the desired frame from y_d as

$$\tilde{y}_d(t) = \sum_{n=1}^{N} y_d[n]\text{sinc}(\frac{t-nT}{T}) \approx \sum_{n:|t-nT|\leqslant 6T} y_d[n]\text{sinc}(\frac{t-nT}{T}),$$

where the approximation is proper, since sinc signals outside an internal of $6T$ are negligible. To minimize the distortion of recovered waveform, oversampling mechanism is adopted, i.e., superimposed signals are oversampled before they are forwarded to frame detection module as shown in Fig. 2.2. If a root-raised-cosine pulse shape is adopted by two transmitters, an oversampling rate of twice of the symbol rate is sufficient. In this case, symbol time T in the above equation needs to be replaced by $T/2$.

After the waveform recovery, the resampling process is conducted. In this process, a timing synchronization algorithm (Mengali and D'Andrea, 1997) is applied to relocate optimal sampling points of the desired frame.

2.2.5 Circular Channel Estimation

When the size of the self frame is less than that of the desired frame, the number of effective samples for the self frame (marked by l_1 and l_2) can be small as shown in Fig.2.5. If the size of the self frame further reduces, it is possible that l_1 and l_2 in Fig. 2.5 approach zero. In

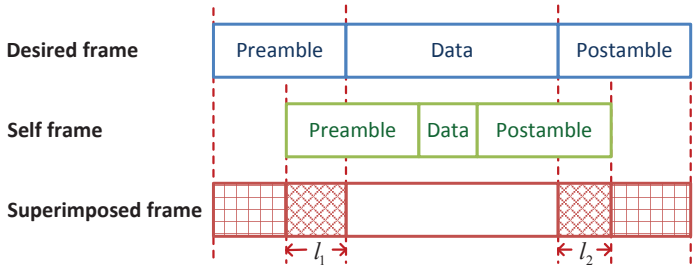


Figure 2.5: Insufficient effective samples for the self frame.

this case, channel coefficients cannot be accurately estimated through joint channel estimation. Considering arbitrary frame sizes in concurrent transmissions, such an event can easily occur.

To address the above issue, circular channel estimation is required. It is based on the concept of successive interference mitigation. In the first step, a preliminary channel estimation is performed for channel coefficients of the self frame. Since joint channel estimation is not effective for the self frame when its number of effective samples is low, a conventional approach is adopted, i.e., estimating the channel coefficients of the self frame by considering the desired frame as interference. In the second step, the joint channel estimation algorithm is applied to estimate the channel coefficients of the desired frame. We know that the number of effective samples for the desired frame is always sufficient (i.e., equal to the number of symbols in pilot sequences). Thus, joint channel estimation algorithm is always effective for estimating channel coefficients of the desired frame. In the third step, the receiver performs waveform recovery and resampling as described in Subsection 2.2.4. Since the channel coefficients of the self frame is not accurate, according to Eq. (2.4), the interference from the self frame cannot be fully removed. The remaining interference degrades the SINR for the desired frame and probably leads to decoding errors. However, the erroneous decoded data are useful. In fact, after decoding, the receiver obtains a symbol sequence, which is an approximation to the desired frame[†]. Instead of providing the decoded results to the upper layer, the receiver feed the approximate symbol sequence back to the circular channel estimation module, as shown in Fig. 2.2. In this new round of channel estimation, interference for estimating the channel coefficients of the self frame

[†]The proof is given by Appendix A

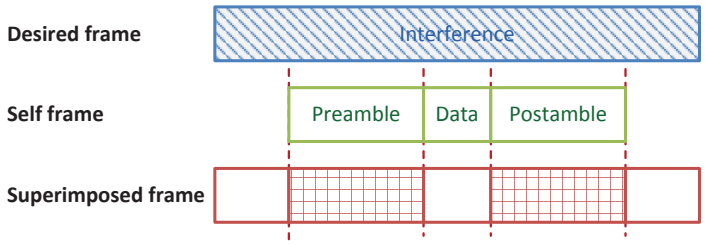
in samples $\mathbf{y}$ can be mitigated. The new samples $\mathbf{y_{s,est}}$ is equal to $\mathbf{y} - \tilde{\mathbf{X}}_\mathbf{d}\tilde{h}_{d,eqv}$, where $\tilde{\mathbf{X}}_\mathbf{d}$ are symbols (i.e. approximate ones of the desired frame) organized in a matrix format as defined in the channel model in (2.2). Since the receiver has accurately estimated the channel coefficients for the desired frame, we have

$$\begin{aligned}
\mathbf{y_{s,est}} &= \mathbf{X_s h_{s,eqv}} + \mathbf{X_d}(\mathbf{h_{d,eqv}} - \tilde{\mathbf{h}}_\mathbf{d,eqv}) + \\
&\quad \tilde{\mathbf{h}}_\mathbf{d,eqv}(\mathbf{X_d} - \tilde{\mathbf{X}}_\mathbf{d}) + \mathbf{w} \\
&\approx \mathbf{X_s h_{d,eqv}} + \tilde{\mathbf{h}}_\mathbf{d,eqv}(\mathbf{X_d} - \tilde{\mathbf{X}}_\mathbf{d}) + \mathbf{w} \\
&= \mathbf{X_s h_{s,eqv}} + \tilde{\mathbf{h}}_\mathbf{d,eqv}\mathbf{X_e} + \mathbf{w},
\end{aligned}$$

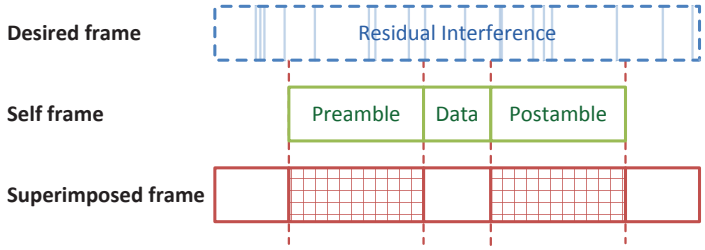
where the error sequence $\mathbf{X_e}$ is defined as $\mathbf{X_d} - \tilde{\mathbf{X}}_\mathbf{d}$. Although symbols from the decoded results are not perfect, they help dramatically mitigate the interference for estimating the channel coefficients for the self frame. An illustrative example showing the original interference and residual interference after mitigation is given in Fig. 2.6. Thus, based on samples $\mathbf{y_{s,est}}$, the performance for estimating channel coefficients of the self frame is highly improved. The procedure discussed previously may repeat several rounds, and the estimation accuracy of the channel coefficients of the self frame will be increased round by round, which eventually leads to accurate samples of the desired frame (i.e. $\mathbf{y_d}$). Based on these samples, the waveform recovery module ensures successful reception of the desired frame. According to the experiment results in Section 2.5.1, two rounds of circular channel estimation are sufficient to achieve successful decoding for low-order modulation schemes such as BPSK and QPSK. For higher-order modulations, more rounds are needed.

2.2.6 Frequency Offset

In either joint or circular channel estimation, the carrier frequency at the receiver is assumed to be the same as that in the transmitters. However, transceivers in commercial communications



(a) The first channel estimation for the self frame (the desired frame is the interference).



(b) The second channel estimation for the self frame (the interference from the desired frame is mitigated).

Figure 2.6: Circular channel estimation.

usually do not have such high performance in carrier frequency stability. As a result, there exist a frequency offset between the actual received signal and the original signal. Suppose f_s is the frequency offset between the receiver and the transmitter of the self frame and f_d is the frequency offset for the desired frame. Thus, given a sample $y[i]$ with symbol period T, we have

$$\begin{aligned} y[i] &= \sum_{k=0}^{n_h-1} h_{d,eqv}[k+1]x_d[i-k]e^{j2\pi f_d iT} + \\ &\quad \sum_{k=0}^{n_h-1} h_{s,eqv}[k+1]x_s[i-k-D]e^{j2\pi f_s iT} + w[n]. \end{aligned}$$

Frequency offset changes the equivalent channel coefficients in (2.1). If it is not compensated, the performance of interference cancellation drops. Moreover, the frequency offset between two devices varies from time to time. Thus, it needs to be estimated and compensated for each reception of superimposed frames. There exist frequency offset estimation schemes for

superimposed frames (Katti et al., 2007; Gollakota and Katabi, 2008; Fung et al., 2010), but they do not work for RANC. The reason is that schemes in [Katti et al. (2007); Gollakota and Katabi (2008)] rely on the existence of an interference-free part in a superimposed frame and the scheme in [Fung et al. (2010)] assumes frame synchronization. Thus, a new frequency offset estimation scheme is developed as follows.

Since the frequency offset estimation for both f_s and f_d follows the same approach, we take f_s as an example to describe our frequency offset estimation scheme.

Considering the preamble sequence $\{p_s[i]\}$ for the self frame, its length is L_p (i.e., $N_p/2$), and it starts from index i_1 in the sample sequence $\{y[i]\}$, which is determined in the frame detection module. Suppose the frequency offset used for compensating the self frame is $\tilde{f}_s$, then the correlation between the preamble and the samples that align with it is

$$\begin{aligned} V_1 &= \sum_{i=i_1}^{i_1+L_p-1} y[i] \times p_s[i-i_1+1] e^{-j2\pi \tilde{f}_s iT} \\ &\approx \sum_{i=i_1}^{i_1+L_p-1} h_{s,eqv}[1] x_s[i-D] e^{j2\pi(f_s-\tilde{f}_s)iT} p_s[i-i_1+1] \\ &= \sum_{i=i_1}^{i_1+L_p-1} h_{s,eqv}[1] (p_s[i-i_1+1])^2 e^{j2\pi(f_s-\tilde{f}_s)iT} \\ &= h_{s,eqv}[1] e^{j2\pi(f_s-\tilde{f}_s)i_1T} \sum_{i=0}^{L_p-1} e^{j2\pi(f_s-\tilde{f}_s)iT}. \end{aligned}$$

The approximation in above equations is valid, because the contribution from $x_d[n]$ and $w[n]$ can be neglected due to the pseudo-noise nature of preamble[‡]. If $\tilde{f}_s$ is close to f_s, for $i \leqslant L_p - 1$, we have $(f_s - \tilde{f}_s) \cdot iT \approx 0$. Hence, the correlation V_1 becomes

$$V_1 \approx L_p h_{s,eqv}[1] e^{j2\pi(f_s-\tilde{f}_s)i_1T}.$$

[‡]Multi-path and ISI items are also eliminated by correlating, since the correlation between the pseudo-random sequence and its shift version approaches zero.

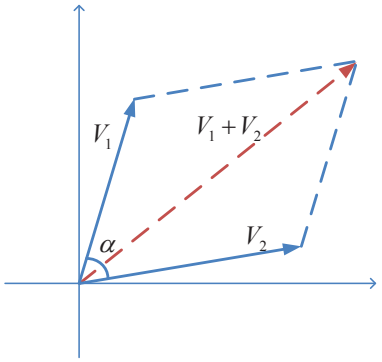


Figure 2.7: Relationship between correlations V_1 and V_2.

Similarly, the correlation between the postamble and samples which align with the postamble of the self frame has the following result:

$$V_2 \approx L_p h_{s,eqv}[1] e^{j2\pi(f_s - \tilde{f}_s) i_2 T},$$

where i_2 is the sample index where the postamble of the self frame starts. Based on above equations, V_1 and V_2 are actually two vectors with approximately equal amplitude, and their phase offset is $\alpha = 2\pi(f_s - \tilde{f}_s)(i_2 - i_1)T$, as shown in Fig. 2.7. When the phase offset is equal to zero, the amplitude of $V_1 + V_2$ reaches maximum. Since $i_2 - i_1$ is the number of symbols in the payload and is none-zero, the maximum amplitude of $V_1 + V_2$ is achieved when $\tilde{f}_s = f_s$. This condition means that we can vary the values of $\tilde{f}_s$ to search the real frequency offset f_s by checking if $V_1 + V_2$ reaches maximum. However, when $|f_s - \tilde{f}_s|$ equals multiple of $\Delta f = \frac{1}{(i_2 - i_1)T}$, $V_1 + V_2$ also reaches maximum. These cases cause confusion to the above approach of frequency offset searching. Fortunately, this confusion can be eliminated by narrowing the search range of frequency offset. Suppose we start from an initial frequency offset $f_{s,est}$, which is usually obtained through a preliminary frequency offset estimation scheme. If $|f_s - f_{s,est}| \leqslant \frac{\Delta f}{2}$ and the search range is $[f_{s,est} - \frac{\Delta f}{2}, f_{s,est} + \frac{\Delta f}{2}]$, then we know that $\tilde{f}_s - f_s$ can only vary within $(-\Delta f, \Delta f)$. Thus, $V_1 + V_2$ can only reach maximum when $\tilde{f}_s = f_s$. In other words, the frequency offset can be accurately determined without any confusion. The condition of $|f_s - f_{s,est}| \leqslant \frac{\Delta f}{2}$

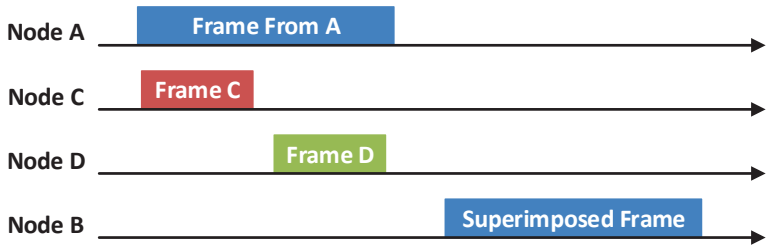


Figure 2.8: The flow diagram for multi-way relaying.

can be easily maintained in a practical system. We will validate this assumption in Section 2.5 through experimental results.

The above analysis leads to the following frequency offset estimation scheme. Initially, a preliminary frequency offset estimation $f_{s,est}$ is conducted with an interference-free frame during the signaling process. Upon RANC has been started, the frequency offset estimated in the previous transmission can be used as the preliminary frequency offset for the next transmission. Secondly, starting from $f_{s,est}$, $\tilde{f}_s$ varies by a step size of δ_f within $(-\frac{\Delta f}{2}, \frac{\Delta f}{2})$. When $V_1 + V_2$ reaches maximum, $\tilde{f}_s$ gives an accurate estimation of the real frequency offset for the self frame. The step size δ_f is much smaller than Δf, and it can be fine-tuned as a system parameter.

2.3 Network Applications of RANC

Without requiring frame synchronization, an interference-free part for each frame in concurrent transmission, or a specific modulation scheme, RANC significantly extends the applicability of analog network coding to wireless networks. In this section, two applications of RANC are provided. The first application is to support a new relaying strategy called *multi-way relaying*. Compared to two-way relaying, this strategy further improves the spectrum utilization when there are variable frame sizes in networks. The second application is to enable random access in a wireless network with ANC. Both applications become feasible because of the constraint-free feature of RANC.

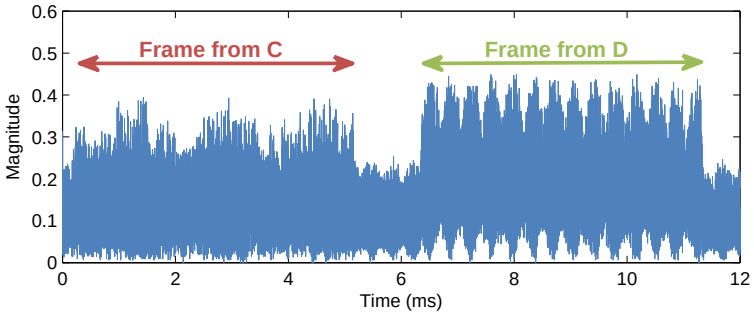


Figure 2.9: A snapshot of the superimposed signals at Node B during the transmission period of a frame from Node A. These signals are sampled by a USRP device.

2.3.1 Multi-Way Relaying in Wireless Networks

The example discussed in Section 2.1.2 indicates that current ANC schemes, which require synchronization or sufficient interference-free parts, only support two frames concurrently transmitted to the relay node (known as *two-way relaying*). This pattern of cooperation is not efficient when two frames have significantly different size as mentioned in the example.

To further improve the spectrum utilization of a relay network, we propose a new cooperation strategy called *multi-way relaying*, which is supported by RANC. With this strategy, Node D starts its transmission once the frame from Node C is completely transmitted as shown in Fig. 2.8 and Fig. 2.9. After the transmission of Node D is finished, the relay node (e.g. Node B) amplifies and forwards the superimposed signals to Node A and Node C. Since no synchronization or interference-free parts are required, RANC can be applied to decode the desired frames for Node A and Node C, respectively. Taking Node C as an example, the details of the decoding procedure are discussed as follows:

- To cancel all the interference for receiving the frame from Node A, Node C has to overhear the frame transmitted by Node D. Usually, if Node D is close to Node C, the signal from Node A, which is two-hop away from Node C, will be dominated by that from Node D. In this case, the probability for successful overhearing is high.

- For frame detection, frames from Node C and Node D can share the same pilot sequence,

but the frame from Node A needs to adopt a different one.

- The channel coefficients for the frame from A are estimated by utilizing the joint channel estimation method, while those for frames from Node C and Node D are determined by circular channel estimation.

Although there are two frames (from Node C and Node D) superimposing with the frame from Node A in our example, frames from more nodes can be involved if the length of the frame from Node A is longer, and the decoding procedure described above is still applicable. Since the frames concurrently transmitted to the relay node comes from multiple nodes, we call the scheme as *multi-way relaying*.

2.3.2 Random Access with RANC

Enhancing the throughput of a wireless network with random access is an important problem due to rapidly growing traffic demand. One effective solution to this problem is to integrate advanced physical-layer transmission technique into such networks. Since analog network coding can significantly improve the spectrum utilization and hence the network throughput, applying ANC to random access wireless networks is beneficial. However, the existing ANC schemes are difficult to be applied to random access networks. In contrast, RANC can be easily applied to such networks for the following reasons. First, most of ANC schemes, such as that in [Rossetto and Zorzi (2009)], require certain-level synchronization among different nodes. However, the accuracy of existing synchronization schemes for random access networks, including the reference broadcast technique (Elson et al., 2002) that exploits signaling messages (such as RTS, CTS) to synchronize two nodes, can hardly reach the requirement imposed by these ANC schemes. RANC supports fully asynchronous transmissions, and hence the synchronization requirement is completely removed. Second, some ANC schemes, such as that in [Katti et al. (2007)], require a specific modulation, while RANC supports multiple ones, including

those adopted by IEEE 802.11 (i.e. BPSK, QPSK, 16QAM, and 64QAM). This feature allows RANC to be easily applied to many scenarios such as IEEE 802.11 networks. Third, due to the constraint-free feature, RANC provides more freedom to design mechanisms for improving the network performance of random access networks. To demonstrate flexibility and efficiency of integrating RANC with random access networks, a simple MAC protocol supporting RANC in wireless networks is proposed below, which totally matches the mechanisms of IEEE 802.11 DCF. In this section, we only consider the network without hidden terminals. Solving hidden terminal issue in a network with analog network coding is an important problem but out of the scope of this paper.

Forming ANC Cooperation

The key issue for designing the random access protocol for RANC is how to dynamically form ANC cooperation groups among network nodes based on traffic demand. In our MAC protocol, we exploit signaling frames such as RTS, CTS to achieve this function. Consider that a frame from Node A (called *initiator*) needs to be transmitted to Node C (called *destination*) with the help of Node B (called *relay*) as shown in Fig. 2.1. Once the backoff counter of Node A reduces to zero, an RTS frame is sent to Node B as shown in Fig. 2.10. Beside original contents, this RTS frame also includes the address of the destination (e.g. Node C). After Node B receives this frame, it transmits a CTS frame to the destination (e.g. Node C) and the initiator (e.g. Node A) indicating that they can form ANC cooperation. When the CTS frame is received by Node A, it begins its frame transmission after waiting SIFS period. When Node C receives the CTS frame, it also initiates a transmission if there is a data frame to be sent to Node A. In this case, the frames from the destination and the initiator superimpose at the relay node, and then the relay node amplifies and forwards the superimposed signals to the destination and the initiator. With RANC, the destination and the initiator can decode their own desired frames, respectively.

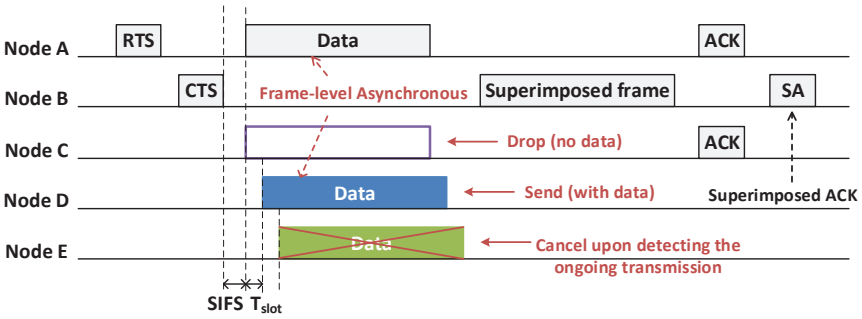


Figure 2.10: Flow diagram for our random access MAC protocol.

Flow Compensation

In many cases, Node C may not have a data frame to Node A in its transmission queue when the CTS frame is received. In this scenario, the ANC cooperation cannot form since the flow from the destination is absent. This situation may significantly reduce the probability of forming ANC cooperation and hence has a negative impact on the network performance. To address this issue, a novel mechanism called *flow compensation* is proposed. Under this mechanism, if Node C does not have a frame to Node A but one of its neighbors, e.g. Node D, coincidentally has one, the traffic from Node D (called *compensator*) can be used to compensate that from Node C to Node A, i.e., Node D begins to transmit its data frame after receiving the CTS frame. In this case, the data frames from the initiator (e.g. Node A) and the compensator (e.g. Node D) superimpose at the relay node. Following that, the relay node (e.g. Node B) amplifies and forwards the superimposed signals. With RANC technique, Node A can decode the data frame from Node D by cancelling the interference due to its own frame. Also, if the transmission of Node D is successfully overheard, Node C can utilize RANC to eliminate the interference of the frame from Node D and decode the frame from Node A.

To apply this mechanism, two problems need to be solved. First, given the destination, we need to determine all candidate nodes that can serve as its compensator. Second, given the destination and its compensator candidates, an effective mechanism is required to provide the ANC cooperation (with the initiator) opportunity to one of them that does have data frames

to the initiator in its transmission queue. Note that each node only has the knowledge about its own queue.

HQL Neighbor Table To decode the initiator's frames, the destination needs to overhear the transmission of its compensator successfully. For this purpose, each node maintains a special neighbor table called *HQL Neighbor Table*, which contains all neighbors that has high quality link[§] (HQL) with itself. Since the initiator is two-hop away from the destination, the signal from a node belonging to the HQL Neighbor Table of the destination is usually much stronger than that from the initiator. In this case, the destination can successfully overhear the transmission of this node with high probability. Hence, given the destination, all nodes in its HQL Neighbor Table can serve as its compensator. In addition, each node needs to periodically exchange its HQL Neighbor Table with all its neighbors.

Virtual Contention for Cooperation Opportunity The second problem for applying flow compensation can be solved with virtual contention mechanism as shown in Fig. 2.10. Specifically, before the transmission of CTS, the relay node randomly allocates sequence numbers from zero to N-1 to the destination and its compensator candidates[¶], where N is the total number of these nodes. The sequence number for each node indicates required "backoff time" for this node and is written in a specific field of the CTS frame. Once the CTS is received, the initiator simply starts the transmission of its data frame after waiting for SIFS period, while the destination and its compensator candidates need to contend the transmission opportunity according to their sequence numbers. If a node does not have any data frame to the initiator, it simply drops its transmission opportunity. Otherwise, the node will transmit its data frame after waiting for SIFS $+ n \cdot T_{slot}$, where n is the sequence number for the node and T_{slot} is the slot time. During the waiting time, the node needs to keep overhearing the channel. Once the

[§]The threshold of link quality is a design parameter depending on network environment.

[¶]Since the HQL Neighbor Table of each node has been broadcast to its neighbors, the relay node has the knowledge about all compensator candidates of the destination.

transmission from other node is detected, the node immediately cancels its own transmission attempt to avoid collision as shown in Fig. 2.10. In this way, the transmission opportunity is provided to one node (e.g. Node D) that has data frames to the initiator (e.g. Node A). Note that if the sequence number of such node is not equal to zero, two data frames from the node and the initiator will superimpose with the asynchonization of several slot time at the relay node. Since RANC allows fully asynchronous transmission, this mechanism can be effectively supported.

Replying ACKs

After decoding the desired frames, the initiator and the destination send ACK frames to report successful receptions. Note that the transmission of ACK frames are also conducted in ANC cooperation manner as shown in Fig. 2.10.

In summary, our protocol exploits signaling messages (e.g. RTS and CTS) to dynamically form ANC cooperation. In this process, no mechanism is required to maintain the synchronization among different nodes, since RANC can effectively support asynchronous transmission. This feature makes our protocol easy to implement in real systems. Also, due to the contraint-free characteristic of RANC, the flow compensation mechanism is supported. This mechanism significantly improves the network throughput when traffic flows between different nodes are not symmetric.

2.4 Implementation

2.4.1 Platform

All functions of RANC have been implemented in a Universal Software Radio Peripheral (USRP) software radio platform. In our platform, USRP N210 motherboard with WBX RF daughter-board operating at 1.26 GHz is used to transmit or receive signals. Via a gigabit

ethernet cable, the USRP device is connected to a general purpose computer. With National Instrument Labview software running on the computer, we implement functions to generate or process baseband signals.

USRP N210 in our experiment is configured as follows. For the transmitter, the onboard DAC chip has a fixed converting rate of 400 M samples per second. We set the interpolation rate to 100 and samples-per-symbol to 4. The resulting symbol rate is equal to 1 MBd/s. For the receiver, the ADC rate is fixed at 100 M and samples-per-symbol is set to 2, which corresponds to $2X$ oversampling in our experiments. To achieve the same symbol rate as that of the transmitter, we set the decimation rate to 50.

2.4.2 Communication Nodes

Three types of nodes are implemented for experiments: 1) RANC TX Node that generates frames following the format required by RANC; 2) RANC RX Node that is capable of superimposed frames decoding; 3) AF Node that simply amplifies and forwards received signals.

RANC TX Node

A RANC TX node generates frames following the format as mentioned in Section 2.2.2. The default payload size of each frame is 1500 bytes unless it is specified differently. Two same pilot sequences with length equal to 160 are attached at the head and the tail of the payload as preamble and postamble. The total number of pilot symbols is equal to 320, which is identical with that in an 802.11a frame (IEEE, 1999). Moreover, a frame is modulated by BPSK (default), QPSK, 16QAM, or 64QAM, and is pulse-shaped with a raised-cosine function. In addition, in network experiments, the 1/2 or 3/4 convolutional channel coding are applied.

RANC RX Node

A RANC RX node extracts and decodes the desired frame from superimposed frames. It implements all function blocks shown in Fig. 2.2, including frame detection module, joint channel estimation module, circular channel estimation module, waveform recovery module, and frequency offset module.

AF Node

An AF node oversamples received signals and stores the baseband samples without any processing. After receiving complete superimposed frames, the stored samples are re-interpolated with sinc function, up-converted to the radio frequency, and then transmitted.

Note that in network experiments, a single transceiver may play different roles at different time, namely it may serve as a RANC TX node in some time periods while work as a RANC RX node in other time periods.

2.5 Performance Evaluation

2.5.1 Evaluation on PHY-layer performance of RANC

In this section, physical-layer performance of RANC is evaluated under different scenarios. First, we conduct experiments to demonstrate the necessity and effectiveness of each function block of RANC. Then, the overall bit error rate (BER) performance of RANC at different SNR is measured.

In these PHY-layer experiments, three USRP nodes are involved. Two of them are RANC TX nodes and simultaneously transmit their own frames to a RANC RX node. The RANC RX node has the knowledge about the frame from one of RANC TX nodes and needs to receive the frame from the other one. For each received desired frame, decoding results and related

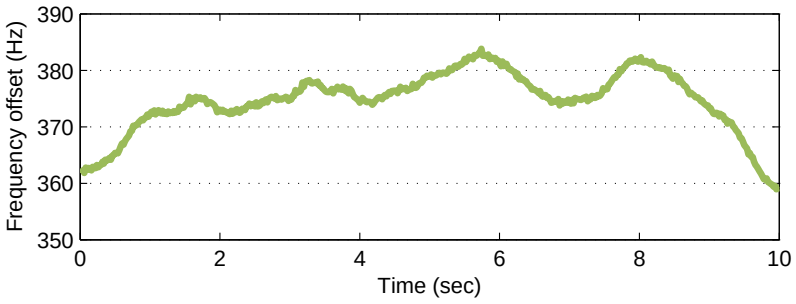


Figure 2.11: The variations of frequency offset between two USRP devices over 10 seconds.

Table 2.1: Bit error rate with frequency offset compensation

Frequency offset	**BER** ($\cdot 10^{-3}$)	
	Long frame (1500 bytes)	Short frame (600 bytes)
Non-existent	0.664	0.649
Compensated	0.682	0.636
Non-compensated	35.51	1.751

information such as SNR are recoded. If not explicitly specified, we collect the results when the SNR for the desired frame falls into the range of $7-8$ dB, which is the typical SNR for BPSK modulation.

Frequency Offset

The purpose of the first experiment is to demonstrate that the condition (i.e., $|f_s - f_{s,est}| \leqslant \frac{\Delta f}{2}$ derived in Section 2.2.6) for our frequency offset algorithm can be practically satisfied.

As discussed in Section 2.2.6, Δf is equal to $\frac{1}{(i_2-i_1)T}$, where $i_2 - i_1$ is the payload size in symbols and T is the symbol period. In our experiment, since the frame size is 1500 bytes (i.e., 12000 symbols for BPSK modulation) and the symbol rate is 1 MBd/s, we have

$$\frac{\Delta f}{2} = \frac{1 \times 10^6}{2 \times 12000} = 41.7 \text{ Hz}.$$

Thus, the condition for our frequency offset algorithm becomes $|f_{s,est} - f_s| < 41.7$Hz, where

$f_{s,est}$ is the frequency offset estimated in the initiate phase with an interference-free frame and f_s is the precise frequency offset to be estimated.

To check if the above condition can be satisfied, we measure the frequency offset between two USRP nodes over 10 seconds. Each measurement is conducted with an interference-free frame. The measurements are plotted in Fig. 2.11. The results show that frequency offset does not change significantly (much less than 41.7 Hz) within certain period (e.g., 2 second). Thus, as soon as the preliminary frequency offset is estimated (exploiting interference-free association frames or based on previous estimation results) within this period before the current reception, the condition for our frequency offset estimation algorithm can be easily satisfied.

To evaluate the necessity and effectiveness of our frequency offset estimation scheme, the BER performance of RANC with frequency offset compensation is compared to that under following two cases: 1) there exists no frequency offset between RANC TX nodes and RANC RX nodes; 2) there are frequency offsets, but only preliminary estimation on frequency offset is applied. To eliminate the frequency offsets in the first case, all USRP nodes are connected to a common external oscillator to replace their own onboard oscillators. In this experiment, the external oscillator we use is Thunderbolt E GPS disciplined clock (Trimble Inc., 2013).

The results are shown in Table 2.1. It can be found that the bit error rate with our frequency offset compensation algorithm is significantly lower than that without compensation, especially when the frame is long, where the phase error caused by residual frequency offset is even larger. This difference in BER performance indicates the necessity of our frequency offset compensation algorithm. In addition, according to the table, there does not exist evident difference in the BER performance between the case with our compensation scheme and the scenario where frequency offset does not exist. This result demonstrates that our compensation scheme has basically eliminated the influence of frequency offset.

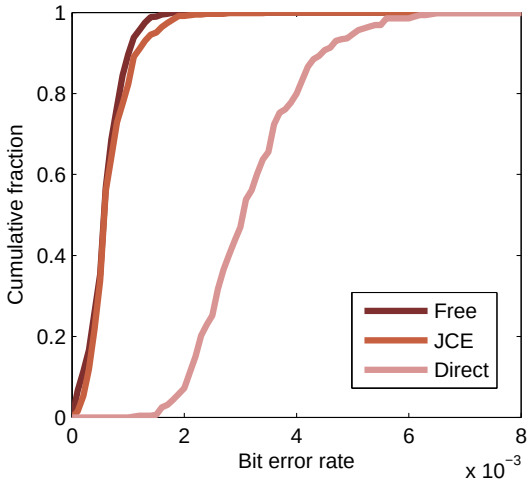


Figure 2.12: Bit error rate with joint channel estimation.

Joint Channel Estimation

To evaluate the accuracy of joint channel estimation (JCE), we compare the BER performance of our scheme with that under two other scenarios: 1) no joint channel estimation scenario (Direct): the receiver estimates the channel coefficients of the self frame directly, considering the desired frame as interference; 2) interference-free scenario (Free): the receiver decodes an interference-free frame. For fair comparison, we collect the results for three cases with SNR of the desired-frame falling into the same range. Also, in this experiment the self frame and the desired frame have the same length. In this case, the number of effective samples N_{eff} for the self frame is equal to N_p, i.e., the total number of pilot sequences. Moreover, the asynchronization between two frames is controlled within 30 symbol times to simulate a scenario where the interference-free part is not sufficient for channel estimation.

The cumulative density function (CDF) of BER for three scenarios are plotted in Fig. 2.12. It is clear that the BER performance with joint channel estimation closely approaches that under the interference-free scenario. This result indicates that the channel estimation for the self frame is sufficiently accurate so that the residual interference after subtracting the self frame from superimposed signals is negligible. From Fig. 2.12 we know that the BER of the joint

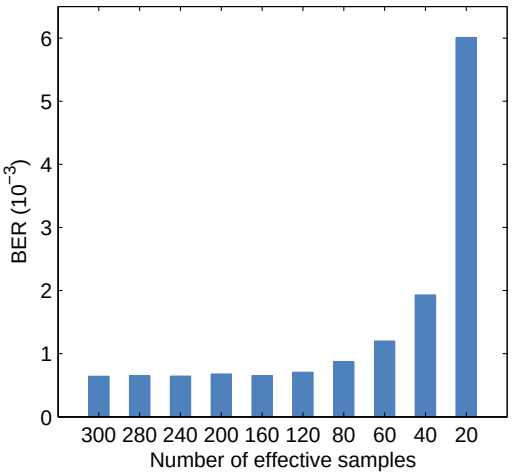


Figure 2.13: Bit error rate versus different N_{eff}

channel estimation scheme is much lower than that with direct channel estimation. Thus, joint channel estimation is necessary when the sufficient interference-free part cannot be guaranteed in a superimposed frame.

To study the impact of N_{eff} on the BER performance, we need to get superimposed frames with different N_{eff}. To this end, we vary the length of the self frames in a specific range and collect the results with N_{eff} close to (± 3) the values labelled on the x-axis of Fig. 2.13.

The BER performance for different N_{eff} is shown in Fig. 2.13. It can be observed that when the N_{eff} reduces to 80, the BER performance evidently degrades. As N_{eff} further decreases, the BER increases significantly. Based on this figure, the threshold N_t (see Section 2.2.2) for selecting joint or circular channel estimation can be determined according to the maximum tolerable BER performance degradation. If N_{eff} (which is measured by the frame detection module) is smaller than N_t, circular channel estimation is adopted.

Waveform Recovery

To examine the necessity of re-locating optimal sampling positions in the waveform recovery module, decoding performance for three cases of transmissions is measured. In the first case, the re-sampling is applied, and hence the decoding is based on samples at optimal positions. In

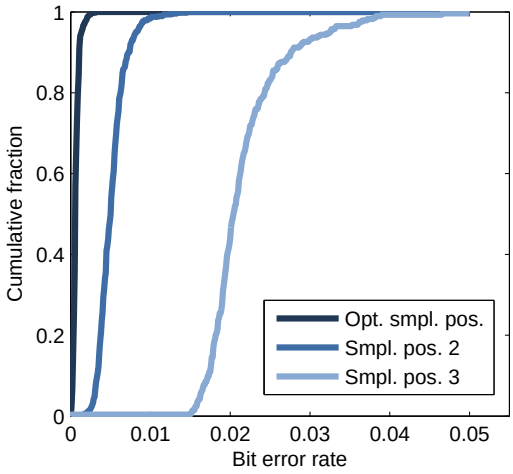


Figure 2.14: Bit error rate with or without re-locating optimal sampling positions.

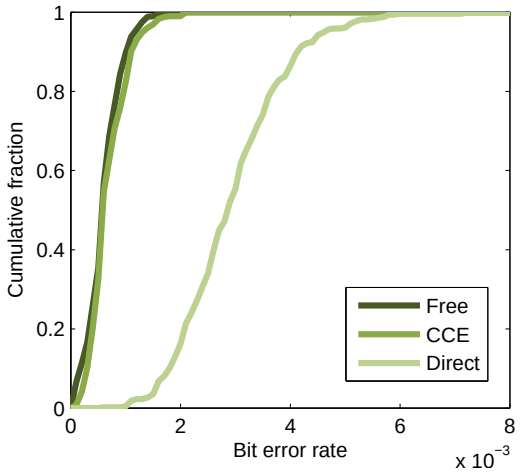


Figure 2.15: Bit error rate with circular channel estimation.

the other two cases, the re-sampling is disabled, and the decoding is conducted based on orignal samples (at smpl. pos. 2 and smpl. pos. 3) that deviate from optimal sampling positions . In each case, two Tx nodes consecutively transmit fixed-length frames with the equal interval time and the RX node keeps receiving the signals. In this scenario, the sampling positions for each frame in the same case are basically identical.

The BER performance for three cases are shown in Fig. 2.14. It can be found that the BER for the first case is significantly lower than that for the second case and the third case. The reason is that the sampling positions in the second case and the third case deviate from the

optimal positions, and without re-locating procedure the equivalent SNRs for these two groups significantly degrade.

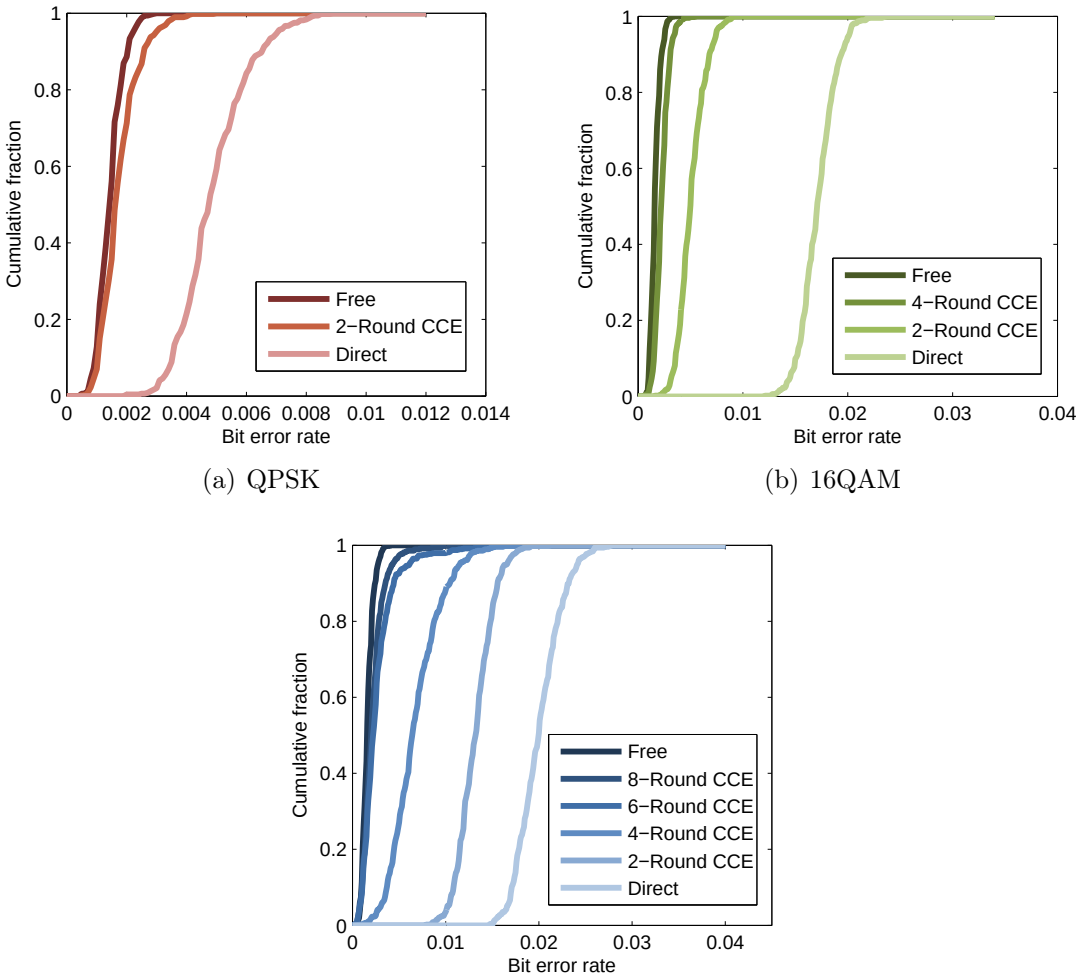
Circular Channel Estimation

Similar to the experiment for joint channel estimation, circular channel estimation (CCE) is evaluated by comparing the BER performance of RANC with CCE to that under two other cases: 1) no circular channel estimation scenario (Direct); 2) interference-free scenario (Free).

The experimental results for BPSK modulation are illustrated in Fig. 2.15. As shown in this figure, the BER performance significantly degrades if circular channel estimation is not applied. Moreover, the BER performance with circular channel estimation closely approaches that under interference-free scenario, which indicates that the circular channel estimation can provide accurate channel coefficients and with these coefficients the self frame can be completely removed from the superimposed signals. In this case, the desired frame is decoded under a near interference-free scenario. Also, note that the CCE scheme in this experiment includes two rounds of channel estimation.

Since the circular channel estimation utilizes the results of demodulation, its performance is influenced by a specific modulation scheme. To investigate this influence, we evaluate the BER performance of circular channel estimation under different modulation schemes. For each modulation, we consider the SNR range where an interference-free frame is decoded with BER around 0.001. To this end, we collect the decoding results when the SNR of the desired frame falls into the range of [9 dB, 10 dB] (QPSK), [15.5 dB, 16.5 dB] (16QAM), and [23 dB, 24 dB] (64QAM).

The experiment results are shown in Fig. 2.16. It can be observed that the maximum performance gain brought by circular channel estimation is more significant for higher order modulation schemes. The reason is that high order modulations have dense constellation and hence are more vulnerable to residual self-frame interference caused by inaccurate channel



(a) QPSK

(b) 16QAM

(c) 64QAM

Figure 2.16: Circular channel estimation for different modulations.

estimation. Thus, the BER performance for high order modulations degrades more if circular channel estimation is not applied. Also, from Fig. 2.16, we find that, for higher order modulations, more rounds of channel estimation are required to approach the performance of interference-free decoding. This is reasonable, because in each round, demodulation of the desired frame with a higher order modulation usually leads to more errors and these errors will degrade the accuracy of channel estimation as explained in Section 2.2.5. Hence more rounds are needed for high order modulations to get sufficiently accurate channel coefficients for the self frame.

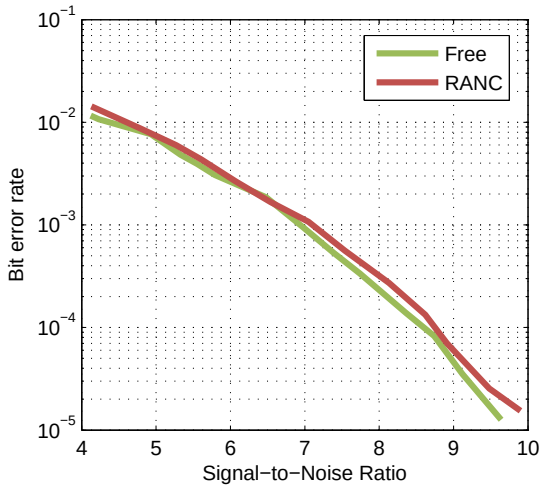


Figure 2.17: Bit error rate of RANC under different SNRs.

BER Performance of RANC

This experiment evaluates the overall BER performance of RANC at different SNR. To demonstrate a constraint-free RANC, we generate frames as follows: 1) frame size varies in the range of [600, 1500] bytes; 2) the relative delay between two concurrent frames varies from 0ms to 1ms. We set the threshold of effective samples for the self frame (i.e. N_t) to 160. Thus, if the number of effective samples is below 160, then circular channel estimation is selected; otherwise, joint channel estimation is adopted.

The experimental results are shown in Fig. 2.17, where the BER performance of the interference-free scenario is compared. In all SNR regions, the BER performance of RANC closely follows that of the interference-free decoding, and the performance gap is within 0.3 dB. Thus, the performance of RANC is not bounded to a specific SNR region.

2.5.2 Evaluation on Network Applications of RANC

Multi-Way Relaying

To demonstrate the advantages of multi-way relaying in wireless networks, the network throughput performance with this scheme is compared to that with two-way relaying in a network as

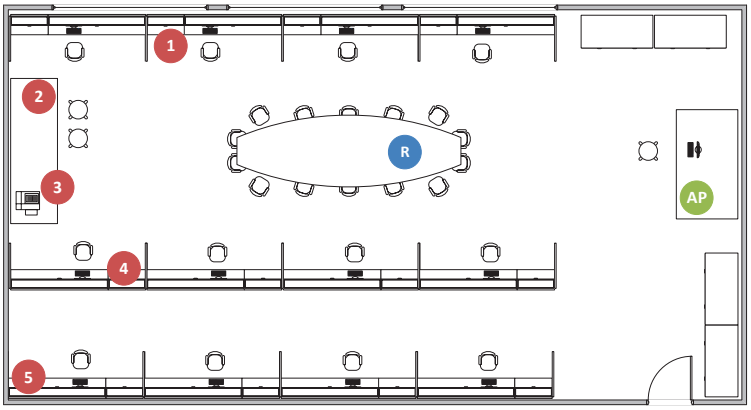


Figure 2.18: Node deployment in our laboratory for evaluating multi-way relaying.

shown in Fig. 2.18. In this network, there are an access point (AP), a relay node, and five users. AP needs to transmit data frames to each user, while each user also has traffic flows to AP. Moreover, we assume that the traffic from AP to users and that from users to AP are generated by different applications and hence the sizes of frames in two directions are different (McGregor et al., 2004; Roughan et al., 2004; Lin et al., 2009): the frame from AP contains the payload of 1500 bytes, while that from users has 600 bytes. All these frames are encoded with 1/2 convolutional channel coding and modulated with BPSK. Also, the transmission power of each node is adjusted such that its frames can be received by corresponding destinations with frame error rate (FER) less than 10%. With traditional ANC, such as that proposed by Katti et al. (2007), only two-way relaying is supported as discussed in Section 2.3.1. In this case, we pick each of user to exchange data frames with AP via the relay node in a two-way relaying manner for 400 rounds. We record the decoding results and calculate FERs for each user and AP. Then the throughput of each node (users or AP), which is defined as the number of frames that are successfully transmitted by this node, can be determined. With RANC, multi-way relaying can be effectively supported. In this case, one primary user and one secondary user (20 different combinations in total) are selected in each run. The primary user and AP exchange their data frames with the help of the relay node, and the secondary user takes the transmission opportunity once the transmission of primary user is finished. For a fair comparison, the frame

Table 2.2: Frame error rate for overhearing secondary users

Primary user	**Frame Error Rate** (%)				
	User 1	User 2	User 3	User 4	User 5
User 1	–	0.00	0.00	3.00	9.00
User 2	0.00	–	0.00	0.00	19.0
User 3	0.00	0.00	–	7.00	37.0
User 4	8.00	0.00	0.00	–	0.00
User 5	5.00	16.0	26.0	0.00	–

size, the modulation, and the channel coding for AP and users are set identically with those in the two-way relaying case. Also, for each combination of the primary user and the secondary user, 100 rounds[‖] of multi-way relaying are conducted. Decoding results for these transmissions are recorded.

The FER for Overhearing To decode the frame from AP, the primary user has to overhear the transmission of the secondary user. The frame error rates for overhearing secondary users by different primary users are shown in Table 2.2. It can be observed that except some combinations involving User 5, the FERs for overhearing are always low. This result confirms that when the primary user and the secondary user are close to each other, the signal at the receiver of the primary user is dominated by that from the secondary user and hence the overhearing will be successful with high probability.

Throughput with multi-way relaying The throughput performance of each node with two-way relaying (supported by traditional ANC) and that with multi-way relaying (supported by RANC) are shown in Fig. 2.19. The results indicate that the throughput of AP with multi-way relaying is slightly less (about 6%) than that with two-way relaying. This degradation is caused by the occasional failure of overhearing the secondary user. In this case, the

[‖]The total number of cooperation rounds is equal to 2000, which is identical with that in the case of two-way relaying.

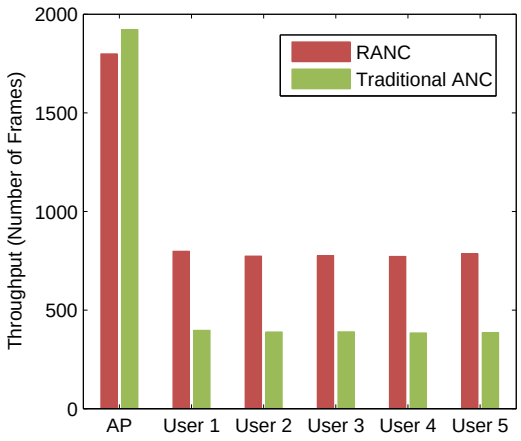


Figure 2.19: Throughput comparison between RANC (multi-way relaying) and ANC (two-way relaying).

frame from AP cannot be successfully received by the primary user. Also, it can be observed that the throughput of each user is almost doubled by adopting multi-way relaying technique. This significant enhancement on throughput attributes to more efficient spectrum utilization of multi-way relaying. For the system overall throughput, the gain from multi-way relaying scheme is about 47%.

Random Access with RANC

To evaluate the performance of RANC-based random access MAC protocol (denoted as *R-MAC*) proposed in Section 2.3.2, the throughput with this protocol is measured in a two-hop network as shown in Fig. 2.20 where the hidden terminal is absent. In this network, edge nodes (labeled by red dots) in one side (left or right) of the laboratory have traffic flows towards edge nodes at the other side. Since no direct links exist between edge nodes at different sides, their data frames need to be forwarded by internal nodes (labeled by green squares). Each data frame is coded with 1/2 or 3/4 convolutional coding, and modulated by BPSK or QPSK according to link quality**. In addition, the payload in a data frame contains 8000 symbols.

**The power of each node is set so that there exists no direct link between edge nodes at different sides and link SNRs between edge nodes and internal nodes are around 10dB. In this case, 16QAM and 64QAM cannot be supported by any link.

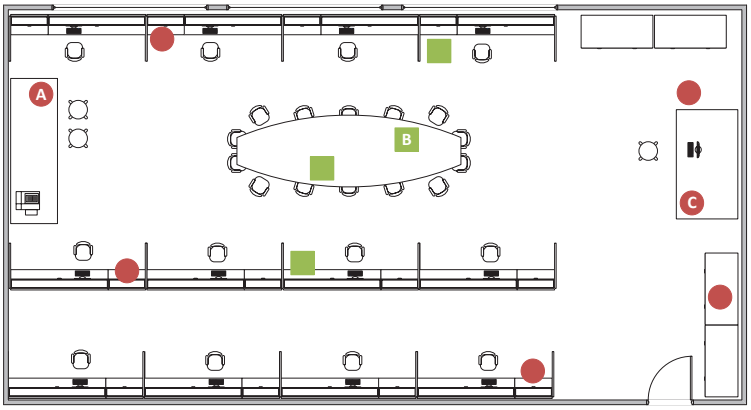


Figure 2.20: Node deployment in our laboratory for evaluating R-MAC.

Since USRP software radio devices cannot support the running of MAC protocol in real time, we evaluate the protocol performance with the trace-driven measurement. Specifically, we measure RANC-decoding results of different combinations of initiators, relays, and destinations and run off-line program to evaluate the network throughput with our protocol based on these results. For each combination, we try different coding rates and modulation schemes for the frames from initiator and the destination. Following that, the maximum supported transmission rates for two frames are selected by maintaining FER less than 10%. With selected rates, the initiator and the destination conduct ANC cooperation for 100 rounds, and decoding results with RANC are recorded. Also, for each compensator candidate of the destination, we repeat previous procedure. In this case, frames from the initiator and the compensator superimpose at the relay node, and decoding results at the receivers of the destination and the initiator are recorded. For comparison, we also measure decoding results for traditional point-to-point transmissions on the links between the initiator, the relay, and the destination with a similar procedure. With collected traces, we emulate the MAC behavior in Matlab programs. Once an ANC cooperation involving an initiator, a relay, and a destination (may also including a compensator) is formed following our MAC protocol, corresponding decoding results are retrieved and the protocol takes further steps according to the results. Similarly, IEEE 802.11 are also emulated with measured traces. The protocol parameter used in the

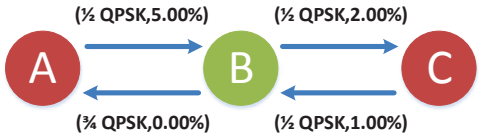
Table 2.3: Protocol parameters used in our experiments

Protocol Parameters			
Item	Value	Item	Value
symbol rate	1 MBd/s	payload	8 ms
PHY header (PH)	400 μs	SIFS	320 μs
RTS	20 bytes + PH	DIFS	680 μs
CTS	14 bytes + PH	slot time	180 μs
ACK	20 bytes + PH	init. window size	64 slots
RTS (R-MAC)	26 bytes + PH	max. backoff state	3
CTS (R-MAC)	33 bytes + PH		

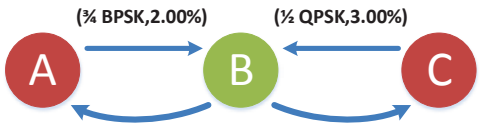
emulation are summarized in the Table 2.3. These parameters are selected according to IEEE 802.11a standard (IEEE, 1999). However, since the symbol rate of our experiment is 1/20 of that specified in [IEEE (1999)], we get our parameters by scaling 20 times as those in [IEEE (1999)]. Also, the RTS frame and CTS frame in our protocol contains more information and therefore the sizes of these frames are longer than that in IEEE 802.11a.

Noise accumulation Since ANC cooperation involves amplify-and-forward process, the influence of noise accumulation on the decoding performance needs to be considered. To illustrate this influence in our experiment, the decoding results for a combination of an initiator, a relay, and a destination is shown in Fig. 2.21, where the maximum supported transmission rate (expressed as the combination of modulations and coding schemes) and the frame error rate are labeled on each link. It can be observed that transmitters have to reduce their rates to utilize ANC cooperation due to the existence of noise accumulation. Taking this rate degradation into account, the throughput performance gain with ANC cooperation in a two-way relay channel is about 60% instead of 100% under ideal scenarios (i.e. no noise accumulation).

Saturation throughput To evaluate the maximum throughput that can be supported in a network with ANC cooperation, the saturation throughput with our MAC protocol is measured.



(a) Point-to-point transmission



(b) RANC

Figure 2.21: Transmission rates and FER for different physical-layer techniques. With these rates and FER, the average throughput for point-to-point transmission is 0.539 M/s, while that for RANC is 0.853 M/s.

Here, the network throughput is defined as the successfully transmitted payload bits on all links in a second, while the saturation scenario indicates that any edge node always in one side (left or right) of the laboratory has data frames to any edge nodes at the other side. The saturation throughput (sat. thr.) of our MAC protocol is shown in Fig. 2.22. For comparison, the saturation throughput of IEEE 802.11 DCF is also provided. It can be observed that the performance gain with our MAC protocol is close to 80%. This significant enhancement on the throughput is contributed by two factors. First, ANC cooperation improves the spectrum utilization compared to traditional point-to-point transmission. According to previous results, this brings about 60% throughput enhancement. Also, for each transmission round (i.e., from the start of an RTS to the finish of replying ACKs), effective data transmission time in our MAC protocol, including data transmission time of edge nodes and the amplify-and forwarding time of internal nodes, is much longer than that of IEEE 802.11 DCF . Therefore the overhead in each transmission round, caused by contention, backoff, and control frames such as RTS/CTS, accounts for a lower proportion in our MAC protocol.

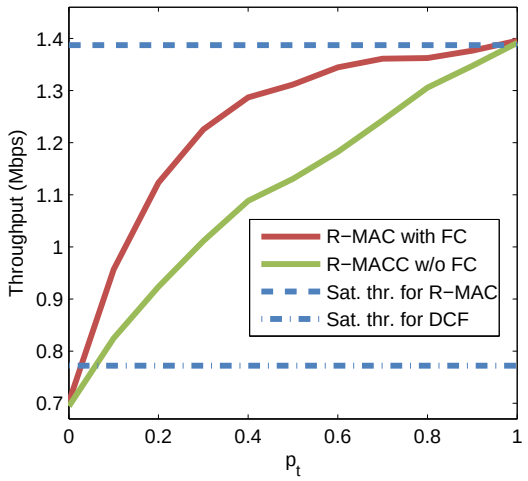


Figure 2.22: Throughput performance with R-MAC.

Flow compensation In more realistic scenarios, an edge node in one side of the laboratory does not always have data frames to each edge nodes at the other side. In this case, flow compensation mechanism is designed to improve the network performance as discussed in Section 2.3.2. To evaluate the effectiveness of this mechanism, the network throughput performance with the mechanism is compared to that without the mechanism under different cases, i.e., the probability (denoted as p_t) that an edge node has a frame to the initiator varies from zero to one. The results shown in Fig. 2.22 indicate that the improvement on the throughput with flow compensation mechanism is significant in middle p_t range. When p_t is close to zero, the ANC cooperation is hardly formed even with flow compensation mechanism. When p_t is close to 1, the ANC cooperation can be easily formed even if the mechanism is not applied. Except these two cases, the flow compensation mechanism can significantly enhance the probability of forming ANC cooperation and hence evidently improve the throughput performance.

In our network setting, the HQL Neighbor Table of an edge node only contains one or two members. If a node has more neighbors and hence a larger HQL Neighbor Table, there are more candidates that can compensate the traffic flows from the destination and the probability of forming ANC cooperation will further increase. In this case the performance gain brought by the flow compensation mechanism is even larger.

2.6 Summary

In this chapter, random analog network coding (RANC) was developed to allow fully asynchronous concurrent transmissions. It supports all linear modulation schemes, and concurrent transmissions with unequal frame sizes work perfectly in RANC. The advantages of RANC makes it highly flexible for a wireless network to adopt analog network coding. RANC was implemented on a software-defined radio testbed and extensive experiments proved that RANC worked gracefully without being constrained by synchronization, frequency offset, modulation, and frame size. In RANC, the performance of receiving the desired frame from superimposed signals is comparable as that of interference-free communications. Experiment results collected from real networks demonstrated that RANC significantly outperformed the existing ANC schemes. Due to the constraint-free nature, RANC is promising for creative applications of analog network coding to wireless networks.

Chapter 3

ANC-ERA: Effective Random Access of Analog Network Coding

In this chapter, ANC-ERA random access MAC protocol is proposed to apply RANC to wireless networks with general topologies such as mesh networks and ad hoc networks. Under this protocol, the short signaling messages such RTS/CTS are utilized to dynamically form analog network coding (ANC) cooperation. Moreover, several advanced mechanisms, such as NAV modification, channel occupation frame, ACK diversity, and flow compensation, are developed to combat the hidden-terminal issue and the asymmetrical flow problem. To evaluate the performance of ANC-ERA, the saturation throughput under this protocol is derived and the network simulation is conducted. The theoretical and experiment results demonstrate that the protocol is highly effective in various scenarios and leads to significant throughput improvement compared to existing schemes.

3.1 Overview

ANC-ERA random access MAC protocol is designed to dynamically form ANC cooperation among nodes in wireless networks. The ANC cooperation process in this protocol consists

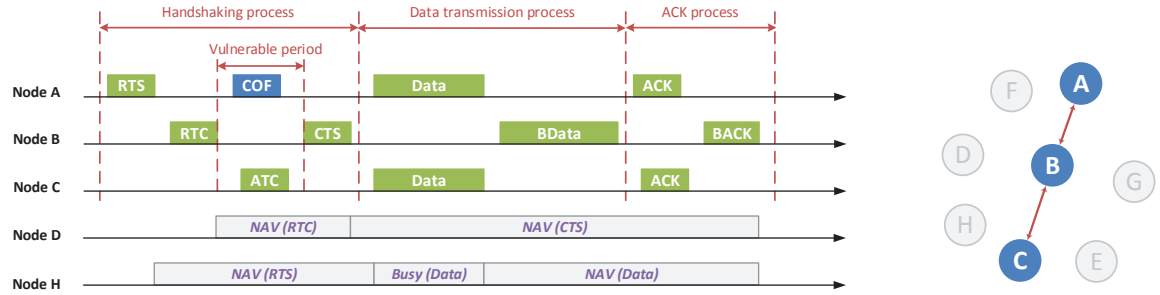
of three sub-processes: handshaking process, data transmission process and acknowledgement (ACK) process, as shown in Fig. 3.1(a). The handshaking process exploits short signaling messages (such as RTS/CTS) to form ANC cooperation groups. Following that end users in a cooperation group exchange their data frames with ANC technique in the data transmission process. Finally, the successful reception of data frames is reported in the ACK process. Note that this process also exploits ANC cooperation to improve the transmission efficiency.

On the basis of the cooperation process mentioned above, several advanced mechanisms are proposed to further improve the protocol performance: 1) the new NAV setting is developed to minimize the negative effect of over-blocking problem which is serious in a wireless network with ANC cooperation; 2) the channel occupation frame is introduced to protect ANC cooperation groups formed in the handshaking process and avoid the cooperation is interfered by hidden nodes; 3) the ACK diversity mechanism is proposed to reduce the loss of ACK frames due to the special hidden-terminal issue in wireless networks with ANC cooperation; 4) the flow compensation mechanism is designed to combat traffic asymmetry in an ANC cooperation group by exploiting traffic flows from neighboring nodes and significantly enhance the throughput performance of a network with asymmetrical traffic flows.

3.2 ANC-ERA Random Access Protocol

3.2.1 ANC Cooperation in ANC-ERA

In our protocol, we exploit signaling messages such as RTS and CTS to dynamically form ANC cooperation. Specifically, the cooperation can be divided into three processes as shown in Fig. 3.1(a). In the handshaking process, signaling messages are utilized to associate different nodes to form cooperation groups based on traffic flows. In the data transmission process, the nodes in the cooperation group send data frames following an analog network coding scheme. In the ACK process, successful receptions are reported. To support ANC cooperation as described



(a) Flow diagram (b) Cooperation group

Figure 3.1: ANC cooperation in ANC-ERA protocol

previously, each node also needs to maintain a special neighbor management module in ANC-ERA protocol.

Neighbor Management Module

Before a node transmit a data frame, it is necessary to determine its one-hop destination and two-hop destination on its routing path*, for the purpose of ANC cooperation. The one-hop destination information (e.g. MAC and IP address) is already indicated in the routing table, while the two-hop destination information is acquired by maintaining a special neighbor management module in ANC-ERA protocol. This module utilizes beacon frames to collect necessary neighbor information including routing entries on one-hop neighbors. Based on collected information, a node can gain the knowledge of MAC/IP address of its two-hop neighbors. Moreover, the management module of each node also maintains a HQL neighbor table, which will be discussed in detail in Section 3.2.5.

Handshaking Process

Consider Node A (called *initiator*) with a frame to be routed to Node B (called *relay*) and then sent to Node C (called *cooperator*), as shown in Fig. 3.1(b). As IEEE 802.11 distributed coordination function (DCF) (IEEE, 2007), when the channel is sensed idle and the backoff

*In this paper, we assume that the routing is given.

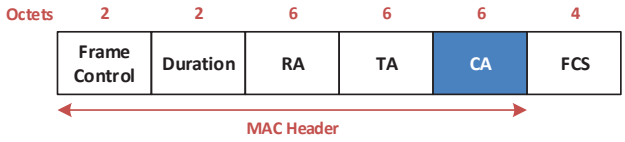


Figure 3.2: The format of an RTS frame.

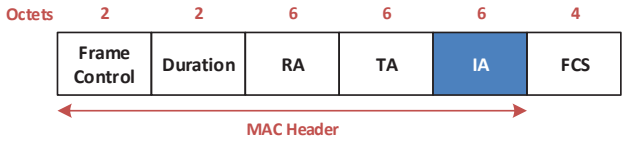


Figure 3.3: The format of an ATC frame.

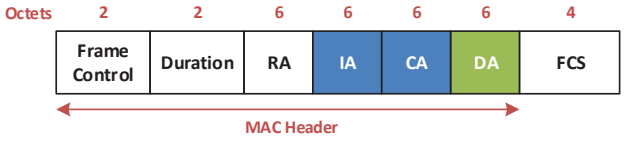


Figure 3.4: The format of a CTS frame.

time counter decreases to zero, Node A sends an RTS frame to initiate the handshaking process. To support ANC cooperation, the MAC address of the cooperator (e.g. Node C) is included in this RTS frame by adding a CA field as shown in Fig. 3.2.

Once the relay (e.g. Node B) successfully receives the RTS frame, it waits for SIFS period, and then transmits an Request-to-Cooperate (RTC) frame to the cooperator (e.g. Node C) as addressed by the RTS frame. The objective of the RTC frame is to request Node C to cooperate with the initiator (e.g. Node A) following an analog network coding scheme. If Node C has a data frame (called *backward frame*) to send back to the initiator in its transmission buffer, it replies an Answer-to-Cooperate (ATC) frame to the relay.

If the relay (e.g. Node B) receives the ATC frame from the cooperator before timeout, then it transmits a CTS frame to both the initiator (e.g. Node A) and the cooperator (e.g. Node C). This frame serves as the permission for the ANC cooperation between the initiator and the cooperator. To this end, their addresses are included in the CTS frame by adding an IA field

and a CA field as shown in Fig. 3.4.

In addition, as shown in Fig. 3.1(a), a channel occupation frame (COF) is sent by the initiator in handshaking process. This frame is designed to avoid channel recapture, which is discussed in detail in Section 3.2.3.

Data Transmission Process

If the CTS frame for the ANC cooperation is received by the initiator and the cooperator, both transmit their data frames to the relay after waiting SIFS time period. Following that, the relay amplifies and forwards the superimposed signals to the initiator and the cooperator as shown in Fig. 3.1(a). With an analog network coding scheme, they can decode the data frame from the other node based on the knowledge of their own frames. To support the decoding of superimposed signals, each node needs to format its data frame according to the adopted ANC scheme. If the scheme proposed in Chapter 2 is adopted, the initiator and the cooperator need to use different pilot sequences for their data frames.

ACK Process

If the initiator and the cooperator decode the data frames correctly, they send ACK frames to announce successful receptions. Note that ACK transmission is also conducted in an ANC manner as shown in Fig. 3.1(a). Following that, the initiator and the cooperator update their contention windows as IEEE 802.11 DCF (IEEE, 2007), depending on whether the corresponding ACK frames are received.

Special Cases

If the two-hop destination on routing path of a data frame does not exist, i.e. the data frame would reach its final destination after next hop, RTS/CTS and data transmission are exactly the same as IEEE 802.11 DCF.

Also, if the relay does not receive any ATC frame before timeout, it presumes that the cooperator does not have a backward frame in its transmission buffer. In this case, the relay sends a CTS to the initiator only. Following that, a standard data/ACK procedure is performed.

3.2.2 Network Allocation Vector Design

In IEEE 802.11 DCF, the network allocation vector (NAV) of a control frame, such as RTS or CTS, indicates deferring access until the end of entire transmission processes (IEEE, 2007). However, this design is not suitable for ANC-ERA protocol as explained below. On one hand, because the transmission process under ANC-ERA protocol involves analog network coding, as shown in Fig. 3.1(a), the NAV time duration in a control frame (e.g. RTS or CTS) can be about twice as large as that in IEEE 802.11 DCF. On the other hand, the handshaking process in ANC-ERA protocol involves three nodes and four control frames, and the collision of any control frame will lead to the failure of the process. Hence the probability of handshaking failure is higher comparing to IEEE 802.11 DCF. Therefore, if the NAV of a control frame in ANC-ERA protocol is set as IEEE 802.11 DCF, it will lead to much more serious *over-blocking* issue, i.e., the cooperation initiated by an RTS frame fails but all neighbors are still prevented from channel access for a long period. Since this issue can significantly degrade the network performance, we propose a new NAV setting for control frames in ANC-ERA protocol. The NAV of an RTS frame only defers the channel access of neighbor nodes in the period from the end of its transmission to the time when the data frame is to be transmitted as shown in Fig. 3.1(a). Similarly, the NAV of RTC and ATC frames terminates when data frame transmission starts. Since the CTS frame is the last control frame in the handshaking process and its transmission indicates highly likely channel capture, the NAV of this type of frame still lasts until the end of entire cooperation process. With this new NAV design, the over-blocking issue is significantly alleviated.

The above NAV design does not compromise the channel protection of the remaining period

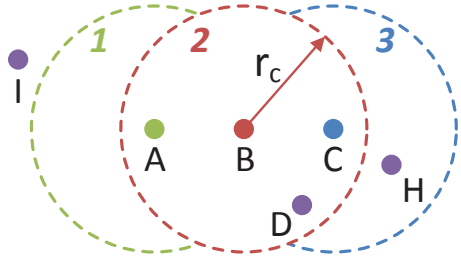


Figure 3.5: Channel protection.

of ANC cooperation. Without the modification on the NAV setting of control frames, the channel access of nodes in Region 1, 2, and 3, as shown in Fig. 3.5, are deferred by the NAV of RTS, RTC, ATC and CTS frames. The radii of dashed circles in the figure are equal to the communication ranges of corresponding nodes. With the new NAV design, we can demonstrate that all these nodes still cannot access channel before the end of the entire cooperation process. First, nodes (e.g. Node D) in Region 1 will be blocked by the NAV of RTC and CTS frames as shown in Fig. 3.1(a). Second, the channel access of nodes (e.g. Node H) in Region 3 will be deferred by the NAV of the RTS frame first, as shown in Fig. 3.5. Following that, Node H can sense the data transmission of Node C and hence further postpone the channel access. Since Node H (as other nodes in Region 3) is much closer to Node C, the received signal strength of the frame from Node C is much stronger than that from Node A. Thus, Node H can receive the data frame from Node C with high probability, in spite of concurrent transmissions from Node A and Node C. If so, the NAV in this frame can further defer the channel access of Node H as shown in Fig. 3.5. Similarly, nodes in Region 1 will be blocked by NAV carried by the ATC frame and the data frame from Node A.

3.2.3 Channel Occupation Frame

In a wireless network with analog network coding, the cooperator (e.g. Node C) is two-hop away from the initiator (e.g. Node A). Thus, nodes (e.g. Node I) at the left side the initiator

as shown in Fig. 3.5 is even farther from the cooperator and hence may not be able to sense its transmission. In this case, if the initiator takes no action after receiving a RTC frame, both the initiator and the relay have no transmission until a CTS frame is sent, as shown in Fig. 3.1(a). In this period, nodes such as Node I may sense a idle channel. If Node I locates in the interference range of the initiator, but not in its communication range, Node I cannot receive the RTS frame from the initiator and hence are not blocked by its NAV. In this case, it is possible that Node I send a RTS frame to capture the channel for new cooperation. If so, the transmission of Node I will interfere the frame reception of Node A and hence may lead to the failure of the ongoing ANC cooperation formed by Node A, Node B, and Node C.

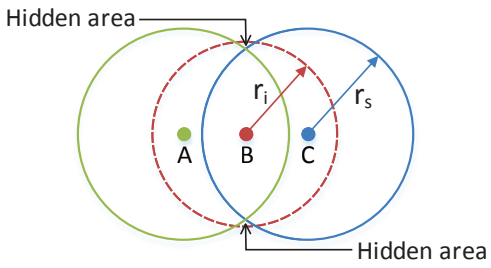
To combat this channel re-capture issue, we utilize a channel occupation frame (COF) to protect the vulnerable period as shown in Fig. 3.1(a). After the initiator receives an RTC frame, it transmit a COF, which is actually the RTS frame transmitted previously. In this way, nodes (e.g Node I) that is hidden from the cooperator (but not from the initiator and the relay) will not sense an idle channel until the end of entire cooperation process.

Note that this COF will superimpose with the ATC frame at the relay. However, since this COF is the RTS frame transmitted previously and hence is known by the relay, it can utilize an analog network coding scheme to cancel the COF frame from the superimposed signals and extract the ATC frame.

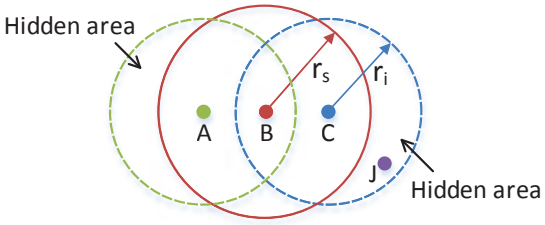
3.2.4 ACK Diversity

The Loss of ACKs

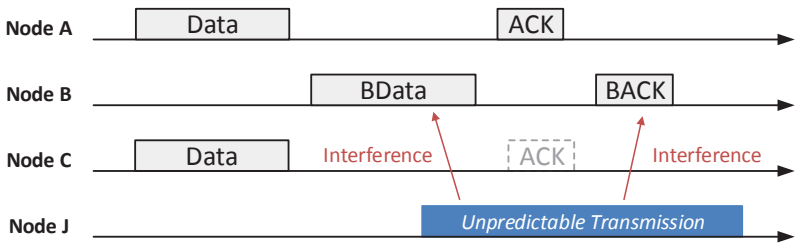
The ANC cooperation process after successful transmission of an RTS frame includes two alternate stages, i.e., multiple access stages and broadcast stages. In a multiple access stage, the initiator and the cooperator concurrently transmit their own frames (e.g. COF/ATC, Datas, ACKs) to the relay, while in a broadcast stage, the relay sends signals (e.g. RTC, BData, BACK) to the initiator and the cooperator. The hidden-terminal issues for two stages



(a) Multiple access stage



(b) Broadcast stage



(c) The interference from hidden nodes

Figure 3.6: Hidden nodes in a wireless network with ANC

are illustrated in Fig .3.6(a) and Fig .3.6(b), respectively. In both figures, r_i stands for the interference radius, and r_s denotes the sensing range. A region in the interference range of the receiver but not in the sensing range of the transmitter(s) is a hidden area, where a node cannot sense the ongoing transmission(s) and may interfere the reception of corresponding receiver with its own transmission. With larger hidden areas, a broadcast stage has relatively severe hidden-terminal issue. Moreover, the issue gets worse as the increase of transmission

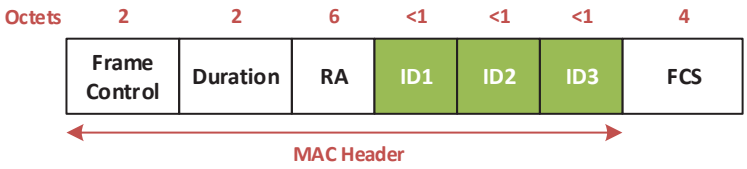


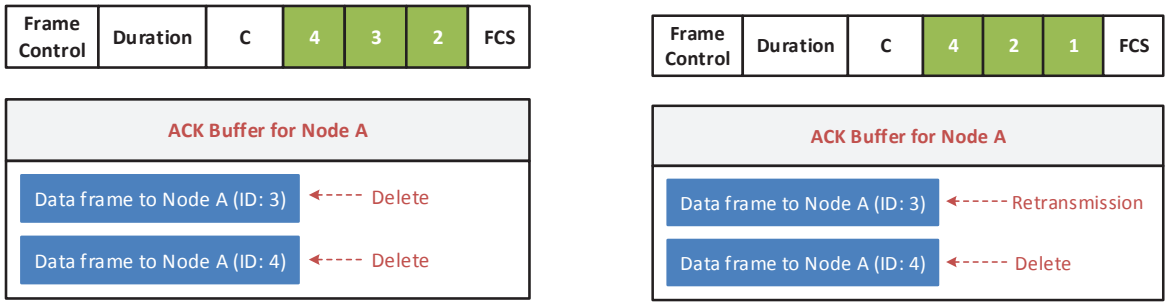
Figure 3.7: The format of an ACK frame.

time in a broadcast stage, since nodes in hidden areas have more opportunities to start new transmissions. Therefore, the stage where the relay amplifies and forwards the superimposed data frames (e.g. BData) is vulnerable to hidden nodes. If a hidden node (e.g. Node J) starts its transmission in this stage as shown in Fig. 3.6(c) , it will cause Node C to fail to receive the BData. Moreover, it is possible that the transmission process involving Node J lasts and further causes the failure of the reception of BACK at Node C. In this case, although the data frame from Node C is successfully received by Node A, the ACK (i.e., BACK) is lost. Since the stage of forwarding BData is vulnerable to hidden nodes, the ACK loss situation is not scarce. According to simulation results, when the sensing range is relatively small, about 15% ACK will be lost. This situation leads to lots of unnecessary retransmissions and hence significantly degrades the network performance.

ACK Diversity Mechanism

To minimize the impact of the loss of ACKs, we design a scheme providing ACK diversity. In this scheme, an ACK frame acknowledges not only the data frame in the current ANC cooperation but also several data frames that are recently received from the same sender. To support this mechanism, we need to adopt the new format for an ACK frame, allocate IDs for each data frames, and manage a new type of buffers called *ACK-waiting buffer* as explained below.

Frame Format. The new format for an ACK frame in ANC-ERA protocol is shown in Fig. 3.7. In this frame, ID fields are added, and each field takes N_{id} bits that depends on the



(a) Case 1 (b) Case 2

Figure 3.8: Buffer management.

maximum ID number, i.e., N_{ID}. The number of ID fields is equal to N_{ACK}. In these fields, IDs for N_{ack} most recently received data frames from the node specified by RA field are recorded. In this way, ID of each received data frame will be carried by N_{ACK} ACKs, i.e. each frame will be acknowledged by N_{ACK} times. This provides N_{ACK} diversity for receiving ACK and hence effectively combats the ACK-loss issue.

Data Frame ID Management. For each data frame, an ID is allocated. This ID is specified in the MAC header of the frame by adding a new field. To minimize the overhead in ACK frames and data frames for carrying IDs, the maximum ID (i.e., N_{ID}) is controlled as small as possible. To this end, an different ID is only allocated for data frames with the same two-hop destination. Without the ambiguity, the same ID can be used by data frames towards different destinations.

For each two-hop destination, a node needs to manage the mapping between IDs and data frames towards this destination. To avoid the ambiguity, an ID cannot be allocated to another date frame until the previous date frame with this ID is successfully acknowledged by its receiver, or discarded due to the reach of the maximum retransmission number.

Buffer Management. Under the new ACK scheme, a node needs to manage an ACK-waiting buffer for each two-hop destination. If a transmitted data frame is not acknowledged, it remains in the ACK-waiting buffer instead of being retransmitted immediately. The next

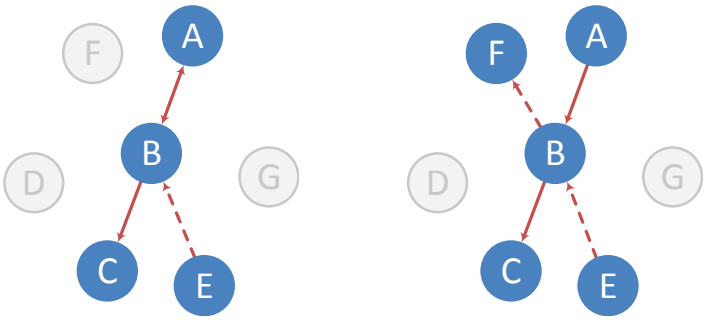
data frame in the transmission buffer is selected to be sent. Once the ACK for a new transmission is received, the receiver extracts all frame IDs from the ACK. These IDs indicates that corresponding data frames are most recently received by the sender of the ACK. Thus, if the ID for a data frame in the ACK-waiting buffer for this two-hop destination (i.e., the sender of the ACK) appears in the ACK, this frame has been successfully received and can be deleted from the buffer without retransmission. Otherwise, a data frame needs to be moved to the transmission buffer for retransmission.

An example is illustrated in Fig. 3.8. Consider the ACK-waiting buffer for a two-hop destination (e.g. Node A) maintained by Node C. In this buffer, there are two data frames: one of date frames is sent in the current ANC cooperation process and has the ID equal to 4; the other one with ID equal to 3 is not acknowledged in the previous cooperation process and hence remains in the buffer. Once the ACK in the current cooperation process is received, Node C knows that the data frame sent in this round (i.e. the frame with ID equal to 4) has successfully reached its two-hop destination. Moreover, Node C needs to determine whether the data frame with ID 3 is acknowledged by detecting ID fields in this ACK. If ID 3 appears in the ACK as shown in Fig. 3.8(a), Node C knows that the data frame has been successfully received by Node A and deletes it from the buffer directly. Otherwise, as shown in Fig. 3.8(b), Node C knows that the frame is not received and hence moves the frame to the transmission buffer for retransmission.

Moreover, in the following two cases, a data frame in the ACK-waiting buffer will be scheduled for retransmission without continuing waiting for future ACKs:

- The capacity of an ACK-waiting buffer is reached. In this case, the data frame with the earliest arrival time is moved to the transmission buffer for retransmission.

- The time for which a data frame stays in the buffer reaches the upper limit. If so, this data frame is scheduled for retransmission.



(a) FC (b) Enhanced FC

Figure 3.9: Flow compensation mechanism (FC).

3.2.5 Flow Compensation

In many cases, the cooperator may not have a data frame to the initiator in its transmission queue when an RTC frame is received, i.e., the traffic between the initiator and the cooperator is not symmetric. In this scenario, the ANC cooperation cannot form since the flow from the cooperator is absent. This situation may significantly reduce the probability of forming ANC cooperation and hence has a negative impact on the network performance. More importantly, the asymmetric-traffic scenario is very common in wireless networks. Thus, an effective strategy that can hold the performance gain introduced by ANC under such scenarios is highly needed.

To this end, a mechanism called *flow compensation* is proposed. Under this mechanism, if the cooperator does not have a frame to the initiator but one of its neighbors (e.g. Node E) coincidentally has one, the traffic from Node E (called *compensator*) can be used to compensate that from the cooperator (e.g. Node C) to the initiator (e.g. Node A), as shown in Fig. 3.9(a). For this purpose, Node E begins to transmit its data frame after receiving the CTS frame. In this case, the data frames from the initiator (e.g. Node A) and the compensator (e.g. Node E) superimpose at the relay node. Following that, the relay node (e.g. Node B) amplifies and forwards the superimposed signals. With an ANC scheme, Node A can decode the data frame from Node E by cancelling the interference due to its own frame. Also, if the transmission

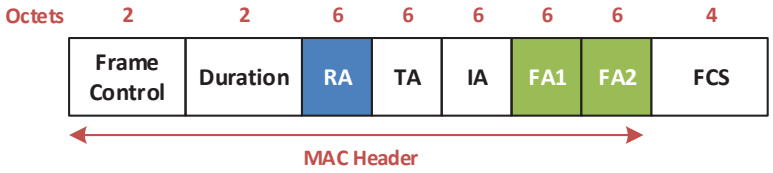


Figure 3.10: The format of an RTC frame.

of Node E is successfully overheard, Node C can utilize the ANC scheme to eliminate the interference of the frame from Node E and decode the frame from Node A.

To apply this mechanism, two problems need to be solved. First, given the cooperator, we need to determine all candidate nodes that can serve as its compensator. Second, given the cooperator and all its compensator candidates, an effective mechanism is required to provide the ANC cooperation opportunity (with the initiator) to one of them that does have data frames to the initiator in its transmission queue. Since each node only has the knowledge about its own queue, the predetermined-based solution is not feasible.

HQL Neighbor Table. In the flow compensation mechanism, to decode the initiator's frames, the cooperator needs to overhear the transmission of its compensator successfully. For this purpose, each node maintains a special neighbor table called *HQL Neighbor Table*, which contains all neighbors that has high quality link[†] (HQL) with itself. Since the initiator is two-hop away from the cooperator, the signal from a node in the HQL Neighbor Table of the cooperator is usually much stronger than that from the initiator. In this case, the cooperator can successfully overhear the transmission of this node with high probability. Hence, given the cooperator, all nodes in its HQL Neighbor Table can serve as its compensator. Note that the HQL neighbor table is managed by our neighbor management module mentioned in Section 3.2.1. As routing entries, the module utilizes beacon frames to collect the HQL neighbor tables of its adjacent nodes.

Virtual Contention for Cooperation Opportunity The second problem for applying

[†]The threshold of link quality is a design parameter depending on network environment.

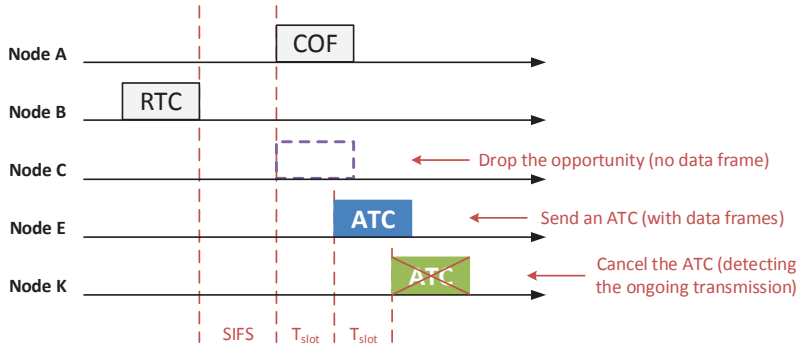


Figure 3.11: Virtual contention for cooperation opportunity.

flow compensation can be solved with virtual contention mechanism. Specifically, after receiving an RTS frame from the initiator, the relay node randomly allocates sequence numbers from 1 to N_c to the compensator candidates, where N_c is the total number of these nodes. The allocation information is carried by the RTC frame by writing the address of candidates following the order of their sequence numbers in the FA fields, as shown in Fig. 3.10. If N_c is greater than the number of FA fields in an RTC frame, the addresses of extra candidates are not written in the RTC frame and hence these nodes are not allowed for transmission in the current cooperation process. In addition, the sequence number for the cooperator is always allocated as zero.

The sequence number for each node indicates extra required waiting time for this node before it can starts its ATC frame transmission. Once the RTC is received, the initiator simply starts the transmission of the COF frame after waiting for SIFS period, while the cooperator and its compensator candidates need to contend the cooperation opportunity according to their sequence numbers. If a node does not have any data frame to the initiator, it simply drops its transmission opportunity. Otherwise, the node will transmit its ATC frame after waiting for $\text{SIFS} + n \cdot T_{\text{slot}}$, where n is the sequence number for the node and T_{slot} is the slot time. During the waiting time, the node needs to keep overhearing the channel. Once the transmission from the cooperator or other candidates is detected, the node immediately cancels its own transmission attempt to avoid collision as shown in Fig. 3.11. In this way, only one ATC frame can be successfully sent to the relay and the transmission opportunity is provided to the

corresponding node (e.g. Node E), which has data frames to the initiator.

Two issues related to the physical-layer design are discussed as follows. First, the transmission of the ATC frame starts at (SIFS $+ n \times T_{\text{slot}}$) after the end of transmission of the RTC frame. However, the COF frame is sent by the initiator after SIFS period upon receiving the RTC frame. Hence the COF frame and the ATC frame may superimpose at the relay with relative delay as large as several slot times, as shown in Fig. 3.11. To support this situation, ANC schemes that allow frame-level asynchronous transmissions, such as those proposed in Chapter 2 and by Katti et al. (2007), are required.

Second, for effectively detecting the transmission from the cooperator or the compensator under the interference (i.e. the COF frame) from the initiator, an ATC frame needs to adopt a different preamble sequence. By correlating this sequence (or the part of this sequence if the whole preamble is longer than a time slot) and detecting the correlation peak, a node can determine whether there exists the transmission from these nodes (Gollakota and Katabi, 2008; Tan et al., 2009).

3.2.6 Enhanced Flow Compensation

In the scenario shown in Fig. 3.9(a), it is possible that the cooperator and all compensator candidates have no data frames to the initiator, which leads to the failure of forming ANC cooperation. To further increase the probability of forming cooperation, an enhanced flow compensation mechanism is proposed. Under this mechanism, if the cooperator or a compensator candidate (e.g. Node E) has a data frame with the two-hop destination (e.g. Node F) whose HQL-neighbor table includes the initiator, as shown in Fig. 3.9(b), it also schedules to send an ATC frame, following the virtual contention procedure described in Section 3.2.5. In this ATC frame, the address of the two-hop destination is carried in the CA field as shown in Fig. 3.3. To help a node determine if the initiator is included in the HQL neighbor of the two-hop destinations of its data frames, a node needs to know HQL-neighbor tables of nodes

that are two-hop away. This can be done by our neighbor management module.

Upon such an ATC frame is received by the relay, it broadcasts a CTS frame including the addresses of the initiator (in the IA field), the cooperator (in the CA field), the compensator (in the RA field), and the two-hop destination of the frame from the compensator (in the DA field), as shown in Fig. 3.4. In this way, an ANC cooperation is formed by two crossing flows as shown in Fig. 3.9(b). To decode the data frame from the compensator, the two-hop destination follows the same strategy with the cooperator as discussed in Section 3.2.5.

3.3 Performance Analysis

In this section, we derive the saturation throughput of the network under ANC-ERA protocol to evaluate its performance and understand its throughput improvement over IEEE 802.11 DCF. As in [Bianchi (2000)], we define the throughput as the successfully transmitted payload bits on all links in a second. In this paper, saturation means two conditions are satisfied: 1) when the channel is sensed idle, a node always has data frames to send to its two-hop destinations; 2) when a cooperation request (i.e., an RTC frame) is received, a node always has frames to send back to the initiator.

The following proposition is derived for a network without hidden terminals (e.g. typical two-hop networks). The derivation for a network with hidden terminals is highly complicated and suject to the future research.

Proposition 3.3.1. Under ANC-ERA protocol, the saturation throughput of a network with n nodes that can sense each other is given by

$$\frac{4P_{\text{succ}}L_p}{(1-\frac{1}{W_0})T_{\text{slot}}+P_{\text{succ}}T_s+(1-\frac{1}{W_0})P_{\text{col}}T_c},$$

where

$$\begin{cases} P_{\text{succ}} = np_t(1-p_t)^{n-1} \\ P_{\text{col}} = 1-(1-p_t)^n - np_t(1-p_t)^{n-1} \\ T_s = \text{RTS} + \text{SIFS} + \delta + \text{RTC} + \text{SIFS} + \delta + \text{ATC} \\ \qquad +\text{SIFS} + \delta + \text{CTS} + \text{SIFS} + \delta + \text{BData} \\ \qquad +\text{SIFS} + \delta + \text{BData} + \text{SIFS} + \delta + \text{BACK} \\ \qquad +\text{SIFS} + \delta + \text{BACK} + \text{SIFS} + \delta + \text{DIFS} \\ T_c = \text{RTS} + \text{DIFS} + \delta. \end{cases}$$

T_{slot}, L_p, δ are defined as slot time, the length of payload bits in a data frame, and propagation delay, respectively. Also, p_t represents the probability that a node initiates an ANC cooperation process by sending an RTS frame in a given time slot. The determination of p_t and the proof of the proposition can be found in Appendix B.

Based on Proposition 3.3.1, the saturation throughput can be expressed as

$$\begin{aligned} & \frac{4L_p}{T_s} \cdot \frac{P_{\text{succ}}T_s}{(1-\frac{1}{W_0})T_{\text{slot}} + P_{\text{succ}}T_s + (1-\frac{1}{W_0})P_{\text{col}}T_c} \\ = \; & R_{\text{ANC}} \cdot \gamma_{\text{ANC}}, \end{aligned} \tag{3.1}$$

where R_{ANC} can be interpreted as the effective transmission rate that counts the overhead introduced by control frames (e.g. RTS and ACK) and frame header, and γ_{ANC} represents the percentage of time in which the channel is occupied by the successful ANC cooperation process. For comparison, we arrange the expression of the saturation throughput for IEEE 802.11 DCF derived in [Bianchi and Tinnirello (2005)] into the similar form, i.e., $R_T \cdot \gamma_T$. In this equation, R_T is given by $\frac{L_p}{T_s'}$, where T_s' denotes the time from the start of sending RTS to the finish of replying ACK under DCF, and γ_T is the counterpart of γ_{ANC} in the DCF case and can be represented in a similar formula.

Based on the previous discussion, the throughput gain of ANC-ERA protocol can be di-

vided into two components, i.e., the physical-layer gain (R_{ANC}/R_T) and the MAC-layer gain ($\gamma_{\text{ANC}}/\gamma_T$). The physical-layer gain attributes to the higher spectrum utilization of ANC. If the data transmission rates under ANC-ERA protocol and IEEE 802.11 DCF are equal, the time of a successful transmission round in ANC-ERA, i.e. T_s, is about twice as larger as its counterpart $T_s^{'}$ in the DCF case. In this scenario, the physical-layer gain, which can be expressed as $4T_s^{'}/T_s$, is close to 2. However, due to the existence of noise accumulation in amplify-and-forward process, the transmission rate with ANC will degrade by a factor α ($\alpha \leqslant 1$), which depends the SNR and the adopted modulation. Based on the experiments in Chapter 2, α is approximately 0.8 in the settings of that paper. If the rate degradation is considered, the time for transmitting the same amount payload increases and this leads to a larger T_s. As a result, the physical-layer gain is about 2α. The other source for the throughput improvement is MAC-layer gain. If the probability P_{succ} that an RTS successfully captures the channel in a given time slot under ANC-ERA protocol and its counterpart under IEEE 802.11 DCF are comparable, the ratio γ_{ANC} is greater than γ_T according to their expressions, since T_s is much larger than $T_s^{'}$. Thus, we can expect a MAC-layer gain that is larger than 1, i.e., under ANC-ERA protocol, the medium is occupied by successful transmissions in higher proportion of time. This is confirmed by our simulation, where the MAC-layer gain is approximately 1.1.

3.4 Performance Evaluation

In this section, the performance of ANC-ERA random access MAC protocol is evaluated through simulation programs built on Matlab platform. To investigate the protocol performance in various scenarios, two type of networks are considered: 1) two-hop networks where the hidden nodes do not exist; 2) general multi-hop networks. In both types of networks, several communication nodes are uniformly distributed in the corresponding areas. The link SNR between one-hop neighboring nodes is assumed high enough, and hence the decoding error is

Table 3.1: Parameters used in the simulation.

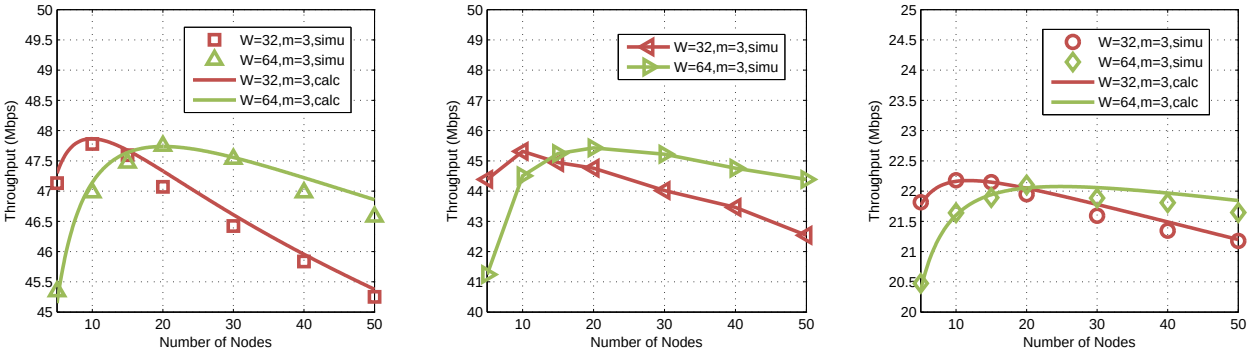
Parameter	**Value**	**Parameter**	**Value**
MAC header	34 bytes	RTS	26 bytes + PH
PHY header (PH)	20 μs	RTC	38 bytes + PH
Payload (default)	1023 bytes	ATC	26 bytes + PH
Link rate	54 Mbps	CTS	32 bytes + PH
Slot time	9 μs	ACK	15 bytes + PH
SIFS	16 μs	α	1
DIFS	34 μs	Comm. range	1 (normalized)
Max. backoff state	3	Interference range	1.78
Init. backoff window (default)	64	Sensing range (default)	2.7

neglected even with the existence of the noise accumulation caused by ANC (i.e., the factor α mentioned in Section 3.3 is equal to 1). Moreover, we consider the traffic model that there exist the data flows from one node to each of its two-hop neighbors.

To compare ANC-ERA with existing schemes, the performance of PNC-MAC proposed by Wang et al. (2013) and IEEE 802.11 DCF (IEEE, 2007, 1999) are also evaluated. For fair comparison, all the protocol parameters used in the simulation except control frame sizes are identical for three schemes. The common parameters and the control frame sizes for our protocol is summarized in Table 3.1, while those for PNC-MAC and DCF are specified in [Wang et al. (2013)] and [IEEE (2007)] respectively.

3.4.1 Performance in Two-Hop Networks

In this part, the throughput performance of ANC-ERA protocol are evaluated in a two-hop network where no hidden node exists.



(a) ANC-ERA (b) PNC-MAC (c) DCF

Figure 3.12: Saturation throughput in a two-hop network.

Saturation Throughput

In this experiment, the throughput performance of ANC-ERA, PNC-MAC, and DCF is compared in a two-hop network with various numbers of nodes, as shown in Fig. 3.12. Moreover, the theoretical saturation throughput of ANC-ERA calculated based on equations in Section 3.3 and that of DCF derived by Bianchi (2000) are also plotted in the figure. It can be observed that the theoretical results and simulation results for ANC-ERA match well with each other, and the error is less than 1% in all cases.

In addition, the comparison results indicate that the performance gain of ANC-ERA protocol over DCF approaches to 115%. As discussed in Section 3.3, this significant gain attributes to two factors. The first factor is the higher spectrum utilization of ANC, which leads to approximately 100% throughput improvement[‡]. The second factor is the MAC-layer gain: for each successful channel contention, effective data transmission time in ANC-ERA, including data transmission time of the initiator/the cooperator and the amplify-and-forwarding time of the relay, is much longer than that in IEEE 802.11 DCF. Therefore the overhead caused by contention and backoff accounts for a lower proportion in our MAC protocol, which is beneficial to improve the throughput performance.

Also, compared to PNC-MAC protocol, ANC-ERA also has approximate 6% performance

[‡]Note that we assume that α is equal to 1.

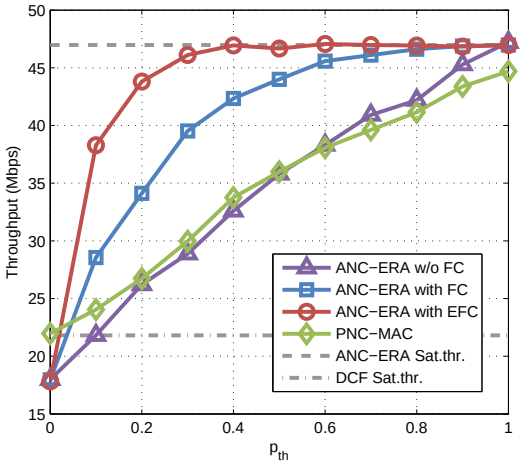


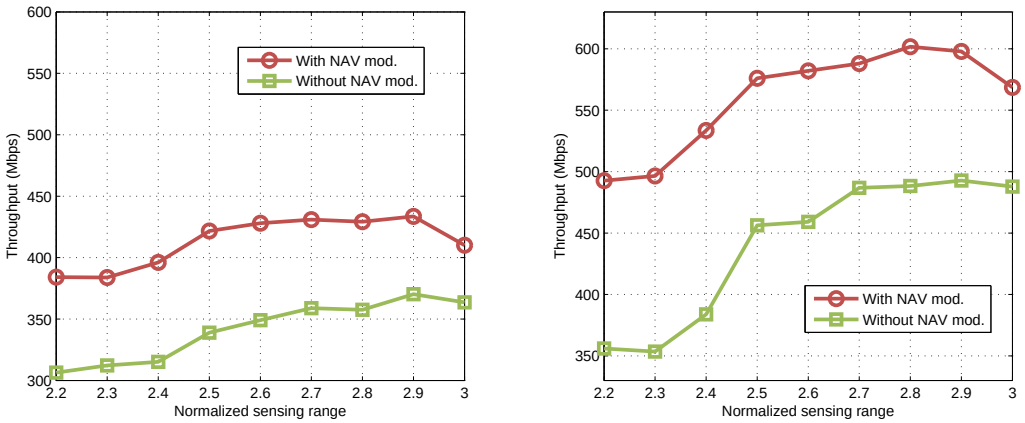
Figure 3.13: Unsaturated throughput performance of different schemes.

advantage. This advantage is due to the more efficient ACK process in our protocol: the transmission of ACK is also conducted in an ANC cooperation manner.

Performance in Unsaturated Cases

In unsaturated cases, the cooperator does not necessarily have a data frame toward the initiator when the ANC cooperation request (the RTC frame) arrives, i.e., the bi-directional traffic flow is not always available. To characterize this situation, we define p_{th} as the probability that one node has date frames to its certain two-hop neighbor (e.g. the initiator). The throughput performance of different protocols under various p_{th} is evaluated in a two-hop network with 40 nodes. The results are shown in Fig. 3.13.

It can be observed that the throughput performance of ANC-ERA is slightly worse than that of DCF when p_{th} is close to zero. In this case, no ATC frame will be received by the relay, and thus traditional data/ACK procedure is conducted by the initiator and the relay as mentioned in Section 3.2.1. If so, our protocol degrades to a traditional CSMA protocol but with longer handshaking process. Hence its performance is lower than that of DCF. For PNC-MAC, if there is no cooperation opportunity, only traditional transmission procedure is triggered. Hence when p_{th} is close to zero, its performance is identical with that of DCF.



(a) 1023 Bytes (b) 2047 Bytes

Figure 3.14: Throughput performance with/without NAV modification.

Moreover, when p_{th} is greater than zero, the throughput performance of ANC-ERA with the flow compensation mechanism (FC) and the extended mechanism (EFC) increase more rapidly compared to ANC-ERA without the mechanism and PNC-MAC. When p_{th} is equal to 0.2, the performance gain of ANC-ERA (with EFC) over PNC-MAC approaches to 70%. This significant enhancement is due to the fact that under the FC mechanism, the backward flow can be provided not only by the cooperator but also by all potential compensators. Thus this mechanism is greatly beneficial to increase the ANC cooperation opportunities and improve the throughput performance.

When p_{th} is close to 1, the network throughput of all the schemes approach their saturation performance. Therefore, the performance gain of ANC-ERA with FC/EFC over PNC-MAC diminishes.

3.4.2 Performance in General Multi-Hop Networks

In this part, several experiments are conducted in a general multi-hop network deployed in the area with the size 10×10 (normalized to the communication range). In this network, there exist hidden nodes which have significant impact on the protocol performance.

Table 3.2: ACK loss rates under various schemes.

Sensing range	**DCF**	**ANC-ERA** w/o ACK diversity	**ANC-ERA** with ACK diversity
2.2	~ 0	8.50%	0.19%
2.4	~ 0	7.73%	0.13%
2.6	~ 0	4.51%	~ 0
2.8	~ 0	2.92%	~ 0
2.9	~ 0	1.15%	~ 0

NAV modification

To evaluate the effectiveness of new NAV setting, we compare the performance of ANC-ERA protocol with and without the NAV modification. The results are given in Fig. 3.14. It can be observed that the ANC-ERA protocol with NAV modification significant outperforms the protocol without the NAV modification. Also, for the frame with larger payload (i.e., 2047 bytes), the performance gap between two cases becomes larger. This can be explained as follows. In a network with ANC, if the data frame increases by 1024 bytes , the entire cooperation period is increased by the time of transmitting 2048 bytes. Hence, without new NAV setting, the increase of payload bytes in data frames will lead to more serious over-blocking issue.

ACK Diversity

In this experiment, the ACK loss issue is investigated. The ACK loss rates under various schemes are summarized in Table 3.2. From the table, it can be observed that the DCF scheme is free from the ACK loss issue. In contrast, in a network with ANC cooperation, a fraction of ACK frames are not received, although the corresponding data frames have arrived at their destinations. Moreover, the issue becomes even worse as the decrease of the sensing range. This degradation attributes to the fact that under short sensing range scenarios, the hidden-node

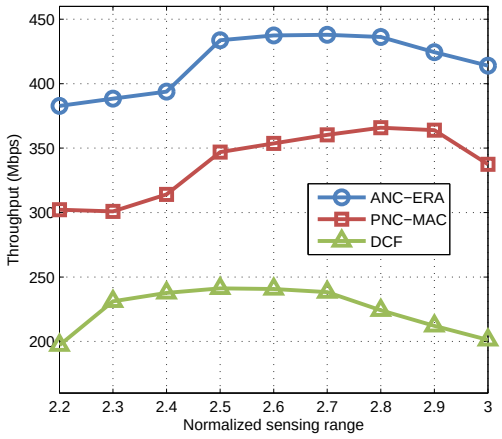


Figure 3.15: Saturation throughput in general multi-hop wireless networks.

problem that leads to the loss of ACK frames becomes more severe. To address the ACK loss issue, the ACK diversity mechanism is applied. The results in the Table 3.2 indicate that the probability that a successfully transmitted data frame is not acknowledged is dramatically reduced with the mechanism.

Saturation Throughput

The throughput performance of ANC-ERA protocol in a general multi-hop network is evaluated, as shown in Fig. 3.15. For comparison, the performance of PNC-MAC and DCF is also provided. From the comparison results, it can be observed that the throughput performance of ANC-ERA protocol is approximately 85% better than that of DCF scheme, which is lower than the performance gain in two-hop network case. This is because a network with ANC cooperation is more vulnerable to hidden nodes as compared to a network with traditional point-to-point transmission. Thus, when hidden nodes exist, the performance degradation of ANC-ERA is more evident.

Also, the comparison results indicate that the throughput of ANC-ERA is 20%-25% higher than that of PNC-MAC. This performance gap attributes to the issues caused by the existence of hidden nodes, such as the over-blocking issue, the channel recapture issue, and the ACK loss

issue as discussed in Section 3.2.2, 3.2.3, and 3.2.4, respectively. Note that all these issues are present in a network with PNC-MAC protocol. However, no mechanism is proposed to mitigate these issues in PNC-MAC.

3.5 Summary

In this chapter, we proposed ANC-ERA random access MAC protocol to apply RANC (or other practical ANC schemes) to wireless networks with general topologies. The protocol exploited the signaling messages to dynamically form ANC cooperation. More importantly, it incorporated several novel mechanisms to effectively combat issues such as over-blocking, channel recapture, ACK loss, and asymmetrical flows. To evaluate the protocol performance, both theoretical analysis and network simulation were conducted. The performance results indicated that ANC-ERA protocol significantly enhanced the throughput performance of wireless networks as compared to existing random access schemes.

Chapter 4

Collusion-Resistant Jamming for Securing Legacy Wireless Clients

The application of RANC is not limited to enhancing the network throughput. With its constraint-free feature, RANC can also be creatively utilized for other purposes. In this chapter, we propose a new physical-layer security scheme based on RANC. This scheme is designed to secure legacy communication devices where the hardware cannot be modified to support physical-layer signal processing as required by existing schemes. In our scheme, the specially designed jamming signals are generated by a third-part device called *secrecy protector* (SP) to prevent the cooperative eavesdroppers from overhearing the information sent by the client. Moreover, RANC is utilized to remove the jamming signals at the access point (AP) and hence enable the secure communication between the AP and the legacy client. To verify the effectiveness of the proposed scheme, it is implemented the on USRP software-defined radio platform. Evaluation results demonstrate that the scheme can effectively guarantee the secure communications between the AP and the client without imposing any special requirement on the physical-layer hardware of the client.

4.1 Design Challenges

Signal jamming is an important technique to prevent the eavesdropping in wireless communications and is actively investigated in recent years. Different from previous research (Negi and Goel, 2005; Gollakota and Katabi, 2011; Dong et al., 2010; Tekin and Yener, 2008), our scheme is aimed to provide secrecy protection on legacy communication devices where the physical-layer hardware cannot be modified to adapt a security scheme. To this end, our design faces several unique challenges. In this section, we discuss these design challenges in detail.

4.1.1 Channel Independence

When the jamming signals are generated by the same antenna that transmits the information, these signals experience the identical channel fading and attenuation with those of the information signals before arriving at the receiver of an eavesdropper. However, since the legacy client itself cannot generate jamming noises, a third-part device, i.e., SP, has to be introduced to send these signals. Therefore, in our scheme, different antennae are used to transmit information signals and jamming noises respectively. In this scenario, the channel gain between the jammer and the eavesdropper is not necessarily identical with that between the client and the eavesdropper. Actually, according to Tse and Viswanath (2005), if two antennae are separated by half carrier wavelength, the channel fading experienced by the signals from these two antenna can be considered as independent. The carrier frequency of commonly used Wi-Fi communication systems is 2.4G/5G, and the corresponding half wavelength is equal to 6.25 cm and 3 cm. In many cases, it is highly demanding to guarantee the distance between the SP and the client less than these lengths. Thus, to support secure Wi-Fi communication, we cannot assume any correlation between the jammer channel and the information channel. The independence between two channels leads to the feasibility of the collusion among eavesdroppers to access the information of the client.

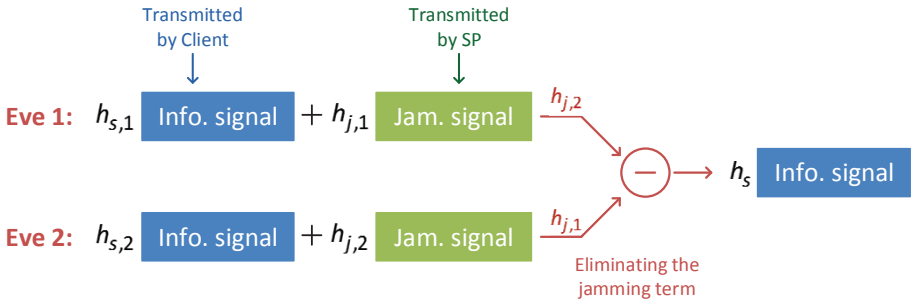


Figure 4.1: Elimination-type collusion.

4.1.2 Elimination-Type Collusion

The first type of collusion among the eavesdroppers that may cause traditional jamming noneffective is the *elimination-type collusion*. Under this type of collusion, two or more eavesdroppers can cooperatively eliminate the jamming signals. As shown in Fig. 4.1, two eavesdroppers receive two different copies of information signals (denoted by $\mathbf{S}$), which are severely interfered by the jamming signals (denoted by $\mathbf{J}$). The received signals can be expressed as

$$\begin{aligned} \mathbf{y_1} &= h_{s,1}\mathbf{S} + h_{j,1}\mathbf{J} + \mathbf{w_1}, \\ \mathbf{y_2} &= h_{s,2}\mathbf{S} + h_{j,2}\mathbf{J} + \mathbf{w_2}, \end{aligned}$$

where $h_{s,i}$ and $h_{j,i}$ are channel coefficients for the eavesdropper i ($i \in \{1, 2\}$), and $\mathbf{w_i}$ denotes the channel noises. If both $h_{j,1}$ and $h_{j,2}$ are known by eavesdroppers, they can cooperatively eliminate the jamming signals following

$$\mathbf{y} = h_{j,2}\mathbf{y_1} - h_{j,1}\mathbf{y_2} = (h_{j,2}h_{s,1} - h_{j,1}h_{s,2})\mathbf{S} + (h_{j,2}\mathbf{w_1} - h_{j,1}\mathbf{w_2}) = h_s\mathbf{S} + \mathbf{w}.$$

Since channel coefficients $h_{s,i}$ and $h_{j,i}$ are not correlated, h_s is not necessarily close to zero. In this case, the eavesdroppers can decode the information signals $\mathbf{S}$ relying on $\mathbf{y}$.

In many scenarios, the jamming signals do not include a preamble sequence. If so, the eaves-

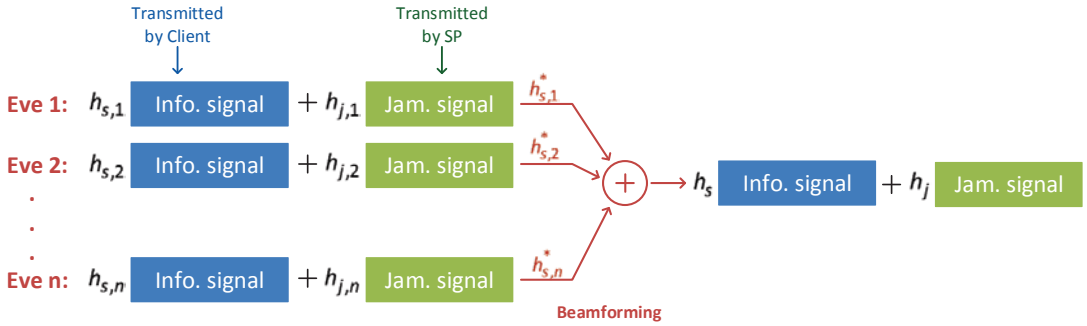


Figure 4.2: Beamforming-type collusion.

droppers cannot conduct channel estimation and hence have no way to gain precise knowledge about the channel coefficients $h_{j,i}$. Nevertheless, the eavesdroppers can still cooperate to estimate the ratio between $h_{j,1}$ and $h_{j,2}$. For example, since it is demanding to precisely synchronize the jamming signals and the information signals, it is possible to locate some samples at the beginning or the end of the received signals where the information signals are absent. These samples can be expressed as

$$\begin{aligned} \mathbf{y_1'} &= h_{j,1}\mathbf{J}' + \mathbf{w_1'}, \\ \mathbf{y_2'} &= h_{j,2}\mathbf{J}' + \mathbf{w_2'}, \end{aligned}$$

where $\mathbf{J}'$ and $\mathbf{w_i'}$ are corresponding jamming signals and noises. By calculating the ratio between $\mathbf{y_1'}$ and $\mathbf{y_2'}$, the eavesdroppers can estimate the ratio between $h_{j,1}$ and $h_{j,2}$. With this knowledge, the previous elimination scheme can still be applied, and the eavesdropper may access the information signals. To avoid this case, some measures must be taken to prevent the elimination-type collusion.

4.1.3 Beamforming-Type Collusion

Another type of collusion among the eavesdroppers is the *beamforming-type collusion*. In this case, several eavesdroppers cooperatively conduct receiver beamforming to mitigate the inter-

ference of jamming signals. As shown in Fig. 4.2, n eavesdroppers receive n different copies of jammed information signals. The received signals are given by

$$\begin{aligned} \mathbf{y_1} &= h_{s,1}\mathbf{S} + h_{j,1}\mathbf{J} + \mathbf{w_1}, \\ \mathbf{y_2} &= h_{s,2}\mathbf{S} + h_{j,2}\mathbf{J} + \mathbf{w_2}, \\ ... \quad &... \quad ... \\ \mathbf{y_n} &= h_{s,n}\mathbf{S} + h_{j,n}\mathbf{J} + \mathbf{w_n}, \end{aligned}$$

If $h_{s,i}$ ($i \in [1, n]$) are known by the eavesdroppers, they can conduct beamforming as

$$\begin{aligned} \mathbf{y} &= \sum_i h_{s,i}^* \mathbf{y_i} \\ &= (\sum_i |h_{s,i}|^2)\mathbf{S} + (\sum_i h_{s,i}^* h_{j,i})\mathbf{J} + \mathbf{w}. \end{aligned}$$

Without loss of generality, we can assume that $[|h_{s,i}|^2] = 1$ and $[|h_{j,i}|^2] = \sigma_j^2$. Since $h_{s,i}$ and $h_{j,i}$ are independent, it can be shown that

$$E[|\sum_i h_{s,i}^* h_{j,i}|^2] = n\sigma_j^2.$$

The the SINR of the signal $\mathbf{y}$ is given by

$$\mathrm{SINR_y} = \frac{n^2}{n\sigma_j^2 + \sigma_w^2}, \tag{4.1}$$

where σ_w is the noise strength. It can be observed that as soon as the number of eavesdroppers that participate in the cooperative beamforming, i.e., n, is large enough, the signal SINR after beamforming can always be enhanced to the level where the successful decoding of the information signals is possible, no matter how large the jamming signal strength σ_j is. Moreover, since a data frame always includes a preamble sequence, the eavesdropper can easily obtain the

channel coefficients $h_{s,i}$ even if there exists strong jamming signals (Gollakota and Katabi, 2008; Sen et al., 2012). Hence, to achieve secure communications, measures must be taken to prevent the beamforming-type collusion.

4.1.4 Removing the Jamming Signals at AP

Jamming signals not only prevent the eavesdroppers from overhearing the transmission from the client, but also cause the severe interference at the legitimate receiver, i.e., the access point (AP). To guarantee that the AP can successfully receive the transmitted information, the jamming signals at the AP needs to be removed. To this end, the device that generates jamming signals, i.e., the secrecy protector (SP), needs a mechanism to share these signals with the AP. Moreover, the sharing process itself must be secure, i.e., the information about jamming signals should not be obtained by the eavesdropper.

With the knowledge of the jamming signals, the AP needs to remove them from the received samples. Since it is demanding to precisely synchronize the legacy client and the SP, the jamming signals and the information signals may be asynchronous with each other. Moveover, jamming signals themselves may be quite complicated to combat two types of collusion mentioned previously. Therefore, an effective scheme is required to cancel these jamming signals at the receiver of AP.

4.2 Collusion-Resistant Jamming Scheme

In this section, we present our collusion-resistant jamming scheme to guarantee the secure communications between the legacy wireless communication device and the access point. In this scheme, several effective mechanisms are designed to address the issues mentioned in the previous section.

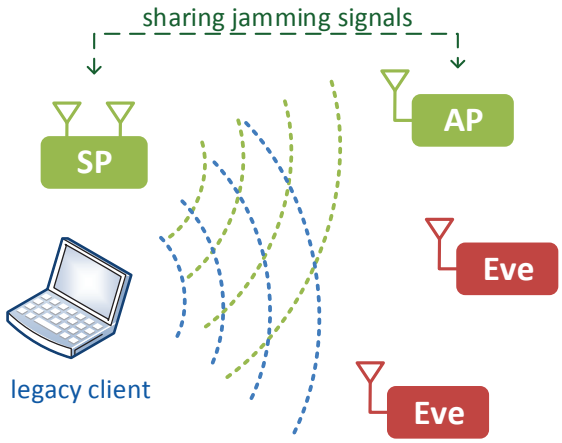


Figure 4.3: The schematic diagram for the collusion-resistant jamming.

4.2.1 Overview

The collusion-resistant jamming scheme is designed to build secure connections between the legacy client and the access point (AP). Since the physical-layer hardware of these devices cannot be modified to adapt a specific security scheme, we introduce a third-part device called secrecy protector (SP)* to undertake the task of security protection. As shown in Fig. 4.3, once the client begins to send its data frames, the SP generates some jamming signals to prevent the eavesdroppers from overhearing the messages. By securely sharing these jamming signals with the AP, it can utilize the RANC technique to effectively remove the interference of jamming signals and then receive the information transmitted by the client.

Specifically, the collusion-resistant jamming scheme includes three parts. The first part is the jamming scheme that is mainly implemented by the SP. In this jamming scheme, several mechanisms, such as multi-stream jamming, pseudo-preamble, and segment transmission, are designed to combat the collusion among the eavesdroppers and dramatically complicate the process for hacking the client's information. The second part is the sharing scheme. This task is cooperatively conducted by the SP and the AP to guarantee that the AP can gain the full

*The SP is placed close to the client. Thus the space attenuation from the client to an eavesdropper and that from the SP to the same eavesdropper is assumed identical. However, the fading for two channels is independent.

knowledge about jamming signals while keep the eavesdroppers from knowing it. To reduce the overhead of sharing process, the seed generation mechanism is proposed to enable the SP and the AP to securely share the seeds from which the jamming signals are generated pseudo-randomly, instead of jamming signals themselves. The third part is the cancellation scheme. In this scheme, the AP utilizes RANC technique to remove the interference of jamming signals.

Moreover, physical-layer security will inevitably degrade the information transmission rate (Wyner, 1975; Csiszár and Korner, 1978). To guarantee the transmission throughput, the previous scheme is only applied when transmitting the secret key. Once the key is successfully distributed, the AP and the client communicates with each other by enciphering their messages with the key. In this chapter, we will demonstrate that , with the collusion-resistant jamming scheme, the complexity for the eavesdroppers hacking this key based on their received signals is no less than that of blindly guessing what the key is.

Also, note that the whole security scheme is mainly undertaken by the SP and the AP, and does not impose any special requirement on the physical-layer of the legacy client.

4.2.2 Jamming Scheme

Multi-Stream Jamming

To combat the elimination-type collusion, we propose the multi-stream jamming mechanism. In this mechanism, multiple independent jamming signal streams are transmitted by different antennae of the SP. Each jamming stream consists of pseudo-randomly generated noise-like signals that follow the complex Gaussian distribution. As soon as the different antennae of the SP are sufficiently separated, the channel gains from different SP antennae to different eavesdroppers are independent (Tse and Viswanath, 2005). In this case, the jamming signals received by various eavesdroppers are different combinations of several independent jamming streams, instead of the same jamming stream multiplied by different coefficients in traditional jamming scenarios. Therefore, it is more complicated to conduct elimination-type of collusion

to hack the client's information.

Consider n eavesdroppers and a SP equipped with m antennae. Then the received signals at the i-th eavesdropper can be expressed as

$$\mathbf{y_i} = h_{s,i}\mathbf{S} + \sum_{k=1}^{m} h_{j,i}^{k}\mathbf{J_k} + \mathbf{w_i}, \tag{4.2}$$

where J_k is the k-th jamming stream and $h_{j,i}^{k}$ is the channel gain from the k-th antenna of the SP to the i-th eavesdropper. Consider the best scenario (for eavesdroppers), i.e. there exist samples where the information signal terms are absent and the noise terms are negligible. In this case, for the i-th eavesdropper, the received signals can be denoted by

$$\mathbf{y_i} = \sum_{k=1}^{m} h_{j,i}^{k}\mathbf{J_k}. \tag{4.3}$$

To conduct elimination-type collusion as discussed in Section 4.1.2, the eavesdroppers need to gain the knowledge of the coefficients $\frac{h_{j,i}^{k}}{h_{j,1}^{k}}$ based on Eq. (4.3), where $i \in [2, n]$ and $k \in [1, m]$. Since the channels are independent, all these coefficients are not correlated with each other. Thus, there are mn unknowns in n equations such as (4.3), i.e., $m(n-1)$ different coefficients $\frac{h_{j,i}^{k}}{h_{j,1}^{k}}$ and m jamming streams $h_{j,1}^{k}\mathbf{J_k}$. When m is greater than 1, no matter how large the number of cooperative eavesdroppers, the number of the equations that can be utilized to calculate coefficients $\frac{h_{j,i}^{k}}{h_{j,1}^{k}}$ is always less than unknown variables. Hence, with multi-stream jamming mechanism, the eavesdroppers cannot acquire enough knowledge about channel coefficients to conduct elimination-type collusion based on received signals.

Beside relying on the received signals, the eavesdroppers can also guess the channel coefficients by bruteforce. To eliminate m independent jamming streams, at least $m+1$ eavesdroppers are needed. Hence, the eavesdroppers need to guess at least m^2 coefficients $\frac{h_{j,i}^{k}}{h_{j,1}^{k}}$. Assume the number of guesses that is required to obtain sufficiently accurate approximation of one such coefficient is c_e. Then, the total complexity for getting all required coefficients is $(c_e)^{m^2}$.

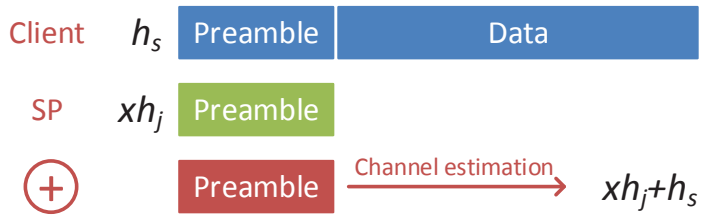


Figure 4.4: Pseudo-preamble.

By considering this case, we further enhance the multi-stream jamming mechanism. Instead of sending a single jamming stream, each antenna of the SP transmits a pseudo-random combination of all jamming streams, i.e., the signals transmitted by k-th antenna is given by

$$\sum_{i=1}^{m} \alpha_{k,i}\mathbf{J_i},$$

where $\alpha_{k,i}$ is pseudo-randomly generated power allocation coefficient and varies from transmission to transmission. In this case, the received signals at the eavesdroppers can still be denoted by Eq. (4.2), but the equivalent channel coefficients $h^k_{j,i}$ vary for each transmission, even if the physical channels are stationary. Therefore, the eavesdroppers have to guess the coefficients $\frac{h^k_{j,i}}{h^k_{j,1}}$ for each transmission from the client. This dramatically enhances the complexity for hacking the client messages.

Pseudo-Preamble

To combat the beamforming-type collusion, we propose the pseudo-preamble mechanism. As discussed in Section 4.1.3, the central task for avoiding the beamforming-type collusion is to prevent the eavesdroppers from knowing the gains of the channels between the client and them. However, traditional jamming signals cannot achieve this function. Generally, a data frame always contains a preamble for the purpose of channel estimation. Since the physical-layer of the client cannot be modified, removing the preamble involves the change of physical-layer

frame format and hence is not feasible. Relying on this preamble, the eavesdroppers can estimate the channel gains from the client to them by correlating received samples with this preamble. Considering the samples received by a eavesdropper i, we have

$$y_i[n] = h_{s,i}S[n] + h_{j,i}J[n] + w[n].$$

By correlating the preamble sequence $\{p[n]\}$ that consists of 1 and -1, we have

$$\begin{aligned} C[n] &= \sum_{k=1}^{L_p} p[k] \cdot y_i[n+k-1] \\ &= h_{s,i}\sum_{k=1}^{L_p} p[k]S[n+k-1] + h_{j,i}\sum_{k=1}^{L_p} p[k]J[n+k-1] + \sum_{k=1}^{L_p} p[k]w[n+k-1]. \end{aligned}$$

where L_p is the length of the preamble sequence. When $\{p[n]\}$ aligns with the preamble of the data frame from the client, it can be shown that

$$\begin{aligned} C[n] &= h_{s,i}\sum_{k=1}^{L_p} (p[k])^2 + h_{j,i}\sum_{k=1}^{L_p} p[k]J[n+k-1] + \sum_{k=1}^{L_p} p[k]w[n+k-1] \\ &= h_{s,i}L_p + h_{j,i}\sum_{k=1}^{L_p} p[k]J[n+k-1] + \sum_{k=1}^{L_p} p[k]w[n+k-1]. \end{aligned}$$

Due to the pseudo-noise nature of the preamble, if a sequence is independent with the preamble, then the correlation between the preamble and the sequence is close to zero. Hence, with traditional jamming signals, the second and the third terms in the above equation vanish after correlating, and the channel coefficients can be estimated by $\frac{C[n]}{L_p}$.

To effectively prevent the eavesdroppers from channel estimation, we design the pseudo-preamble mechanism. As shown in Fig. 4.4, beside multi-stream jamming signals, the SP also transmit a pseudo-preamble (multiplied by a random coefficient x) when the client begins to send its data frame. If the pseudo-preamble aligns with the preamble of the data frame,

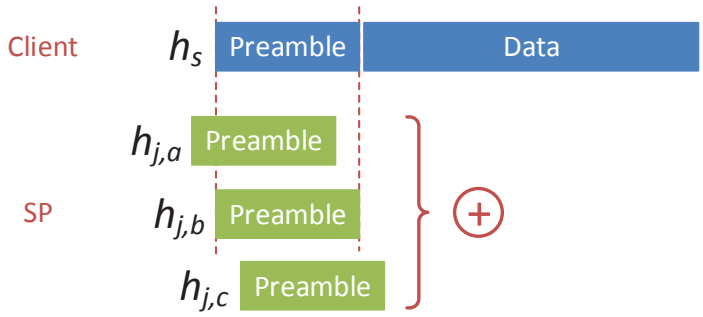


Figure 4.5: Successive pseudo-preambles.

two preambles superimpose at the receivers of the eavesdroppers. In this case, the channel estimation result based on correlating the preamble sequence becomes the sum of the channel gain from the client to the eavesdropper and that from the SP to the eavesdropper multiplied by x. Since xh_j is random and the eavesdroppers cannot separate it with h_s, the channel estimation result provides no useful information about h_s. With pseudo-preamble, the eavesdroppers cannot gain the knowledge of h_s based on the channel estimation, which is indispensable for beamforming-type collusion.

To ensure that the pseudo-preamble aligns with the preamble of the data frame sent by the client, the fine-grained synchronization between the SP and the client is required, which is highly demanding since it is difficult to precisely control the physical-layer of the legacy client. To address this issue, the SP is designed to transmit N_p successive pseudo-preambles, instead of only one, as shown in Fig. 4.5. In this case, as soon as one of these pseudo-preambles aligns with the preamble of the frame from the client, the channel estimation at the eavesdroppers will be effectively prevented. To guarantee this situation, the course synchronization is sufficient, which is easy to achieve.

Beside relying on the channel estimation, the eavesdropper can also guess the channel gains by bruteforce. Assume that the number of guesses that is required to obtain sufficiently accurate approximation of the channel gain from the client to one eavesdropper is c_b. When there are n cooperative eavesdropper, the total complexity for getting all channel gains required by

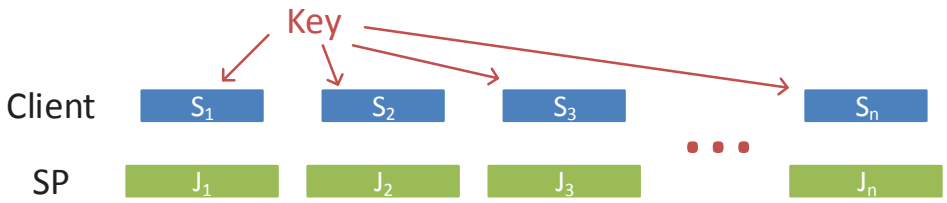


Figure 4.6: Segment Transmission.

beamforming is $(c_b)^n$. Although the large number of eavesdroppers can enhance the SINR of the client's signals by beamforming, the complexity of acquiring necessary information for beamforming also exponentially increases. Therefore, with pseudo-preamble mechanism, the beamforming among large number of eavesdroppers is effectively suppressed.

Moreover, since a receiver needs to conduct the frame synchronization (i.e., precisely determine the beginning of a frame) by correlating the preamble and detecting the correlation peak, the successive pseudo-preambles can also confuse the eavesdroppers about the beginning of the client's data frame. If there are N_p successive pseudo-preambles, the complexity for the eavesdroppers guessing the beginning of the data frame sent by the client is N_p.

Segment Transmission

To further increase the complexity for the eavesdroppers hacking the client's transmission, we design the segment transmission mechanism. As mentioned in Section 4.2.1, our scheme is used to transmit the secret key. Thus, we divide the secret key into L_k segments, and encapsulate each segment into a data frame. Therefore, to transmit a key to the AP, the client needs to send L_k frames and the SP needs to generate L_k groups of jamming signals to protect these frames, as shown in Fig. 4.6.

To acquire the secret key, the eavesdroppers have to hack each transmission for getting all segments. If the elimination-type collusion is adopted, the coefficients $\frac{h^k_{j,i}}{h^k_{j,1}}$ are required. With multi-stream jamming mechanism, the eavesdroppers have to guess these coefficients for

each transmission. Hence the total complexity for conducting elimination-type collusion is $(c_e)^{m^2 L_k}$. If the beamforming-type collusion is used, the channel gains from the client to each eavesdropper need to be known. With the pseudo-preamble mechanism, the eavesdroppers need to guess each of these channel gains for at least once, assuming that the physical channels remain unchanged among L_k transmissions. The complexity for this task is $(c_b)^n$ (n is the number of eavesdroppers). Also, different from the elimination-type collusion, the beamforming-type collusion does not directly cancel the jamming signals. Thus, the pseudo-preambles in the jamming signals will deactivate the frame synchronization which is based on correlating the preamble. Hence, for each transmission, the eavesdroppers need to guess the starts of the frames. The complexity for this task is $(N_p)^{L_k}$. Thus, the total complexity for beamforming-type collusion is $(c_b)^n (N_p)^{L_k}$.

Based on these results, the complexity of hacking the key under our scheme can be estimated. For example, consider that the client transmits a 128-bit key with BPSK modulation and divides it into 16 segments. Also, the SP is equipped with 4 antennae and generates 4 independent jamming streams, each of which has 3 times power as that of the information signals. The number of successive pseudo-preambles is 16. Moreover, we make a conservative assumption that both c_e and c_b are equal to 4, i.e., 4 guesses are sufficient to get the corresponding coefficients. For decoding the transmission of the client (BPSK modulation), the SINR needs to be enhanced to 6 dB. According to Eq. (4.1), this requires at least 36 eavesdroppers to cooperatively conduct beamforming. Based on these conditions, under our jamming scheme, the complexity for the elimination-type collusion is 2^{512}, and that for beamforming-type of collusion is 2^{136}, both of which are larger than the complexity of directly guessing the key (i.e., 2^{128}). This demonstrates the effectiveness of our scheme. To further enhance the complexity, we can increase the jamming signal power, the number of successive pseudo-preambles, the number of segments, and the number of antennae at the SP.

Note that the complexity analysis in this chapter is an approximate one. The rigorous

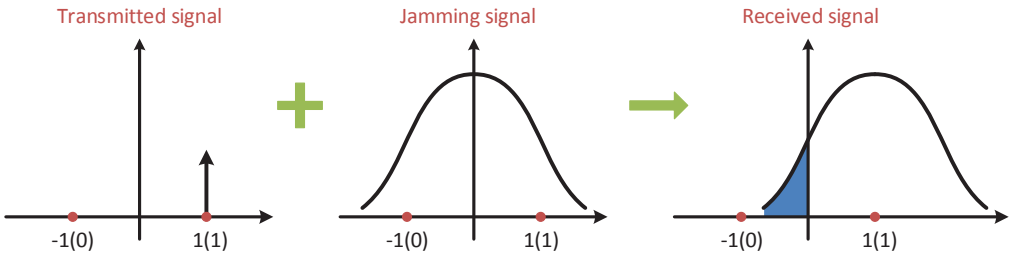


Figure 4.7: The signals after jamming.

analysis of the hacking complexity is high challenging and left for the future research.

Bit Compression

Jamming may not guarantee that the information signals are fully concealed from the eavesdroppers, i.e., from the received signals, the eavesdropper can gain some knowledge about the transmitted information. This can be explained with Fig. 4.7. Assume that a "1" is sent by the client, and the SP generates a noise-like jamming signal that follow the complex Gaussian distribution. Then the received signals at an eavesdropper follows the distribution as shown in Fig. 4.7. Only when the received signal is less than zero, the eavesdropper will make wrong decision about the transmitted bit, and the corresponding probability is equal to the area of the shadow region in the figure. This probability may be not close enough to 0.5. In this case, the received signal is not independent with the transmitted bit, and will leak some information to the eavesdropper. If the key is directly transmitted without any processing, the eavesdroppers can gain some knowledge about the key, which reduces its secrecy.

To address this issue, we propose the bit compression mechanism. Under this mechanism, instead of sending the key directly, the client transmits a sequence based on which the key is generated. When the AP receives the sequence, it compresses every successive L_c bits into one secret bit by performing GF-2 addition as shown in Fig. 4.8. Hence, if a 128-bit key is adopted, the length of the sequence used for generating the key is equal to $128 \cdot L_c$.

For the eavesdropper, assume that its bit error probability under jamming is p_e. Then after performing bit compression, the error probability for a bit in the generated key is $p_{k,e}$. It can

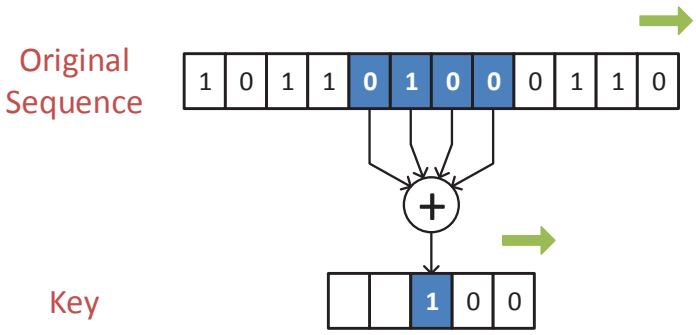


Figure 4.8: Bit compression.

be shown that

$$p_{k,e} = \frac{1-(1-2p_e)^{L_c}}{2}.$$

Under the most of cases, $p_{k,e}$ is sufficiently close to 0.5. For example, consider that p_e is about 0.45 as measured in our experiments and L_c is equal to 4. According to the above equation, $p_{k,e}$ is 0.49995. In this scenario, the key generated based on the received signals of the eavesdropper is basically independent with the true key. Hence, the secrecy of the key is guaranteed.

Note that the above equation is also applied to the AP. However, since the jamming signals are removed at the AP, the decoding error probability p_e for the AP is very small (usually $10^{-3} \sim 10^{-5}$). Hence, after the bit compression, the error probability $p_{k,e}$ is still small, and the bit error can be easily corrected with the channel coding[†].

With the bit compression mechanism, the eavesdropper cannot gain any knowledge about the secret key based on received signals. Also, with the mechanisms proposed in previous sections, the eavesdroppers cannot obtain any benefit from colluding. The whole jamming scheme effectively guarantees the secrecy of the key transmitted by the client. Moreover, the speed of the key distribution under our scheme is very fast. With 802.11a physical-layer specifications, only about 500 μs is required to transmit a 128-bit key (with 16 segments) to

[†]The channel coding introduces some redundance and hence may degrade the secrecy of the key. To remove this negative impact, the method proposed by Jana et al. (2009) can be utilized.

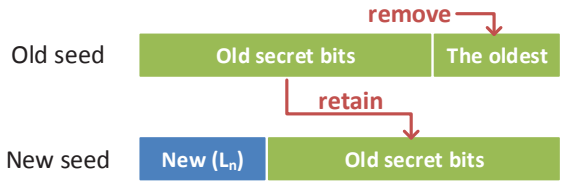


Figure 4.9: The seed updating.

the AP. In contrast, about 3 s is needed to share a 128-bit key between the transmitter and the receiver for the key generation scheme based on RSSI (Mathur et al., 2008; Jana et al., 2009; Liu et al., 2013).

4.2.3 Sharing Scheme

To remove the jamming signals, the AP needs to gain the full knowledge about these signals. For this purpose, the seed generation mechanism is designed. Under this mechanism, instead of sharing the jamming signals directly, the AP and the SP use a common seed to generate all pseudo-random signals or coefficients mentioned in the previous section following a specific rule. Each bit in the seed is generated based on the characteristic (e.g. phase, magnitude, and fading) of the channel between the SP and the AP. The detailed procedure for generating a common bit sequence for two wireless devices are studied by Mathur et al. (2008) and Patwari et al. (2010). Note that this generating process is secure, since the channel between the SP and the AP is independent with those between eavesdroppers and the SP/AP, and hence the eavesdroppers cannot extract any information about the channel characteristics between the SP and the AP. By this mean, the seed is shared by the AP and the SP, but concealed from the eavesdroppers.

For the sake of the security, it is necessary to keep updating the seed, as shown in Fig. 4.9. Once L_n new secret bits are generated exploiting the channel characteristic between the SP and the AP, they are added to the beginning of the seed, while the oldest bits at the end of the seed is removed.

4.2.4 Cancellation Scheme

With the full knowledge about the jamming signals, the AP needs to effectively cancel them[‡] for decoding the frame transmitted by the client. To this end, RANC proposed in Chapter 2 can be utilized.

Since the jamming signals are fully known, we can treat the beginning and the end of each jamming stream as the preamble and the postamble respectively. Thus, we consider that all jamming streams follow the format required by RANC. Also, because the jamming signals can be designed longer than the client's frame, RANC is still applied even if the frame does not contain a postamble.

By applying RANC, the jamming signals can be effectively removed: 1) the frame detection module can accurately locate the beginning and the end of each jamming stream; 2) with joint channel estimation module, the channel coefficients for all jamming streams can be determined, which is necessary for the jamming signal cancellation; 3) with waveform recovery and re-sampling model, the negative impact of the asynchrony between the jamming signals from the SP and the data frame from the client can be minimized.

After remove the jamming signals, the AP is able to decode the frames transmitted by the client, and successfully extract the secret key.

4.3 Implementation

4.3.1 Platform

To evaluate the performance of our collusion-resistant jamming security scheme, we implement it on the Universal Software Radio Peripheral (USRP) software-defined radio platform. In our platform, USRP N210 motherboards combined with WBX radio-frequency daughterboard (operating at 1.26 GHz) are utilized to transmit or receive wireless signals. With gigabit

[‡]Include the pseudo-preambles, which can be considered as a special jamming stream.

Ethernet cables, USRP devices are connected to general purpose computers, where the signal generating and baseband processing are performed with National Instrument Labview software.

The N210 motherboard in this implementation is configured as follows. At the transmitter side, the onboard digital-to-analog converter (DAC) has a fixed converting rate equal to 400 M samples per second. By setting the interpolation rate to 400 and samples-per-symbol to 8, we get the transmission symbol rate equal to 125 kBd/s. At the receiver side, the analog-to-digital converting (ADC) rate is fixed at 100 M samples per second. To achieve the equal symbol rate with the transmitter, we set the decimation rate to 100 and samples-per-symbol to 8.

4.3.2 Communication Nodes

In our experiments, we implement four types of communication nodes: 1) the secrecy protector; 2) the access point; 3) the legacy client; 4) the eavesdropper.

The Secrecy Protector (SP)

The SP is in charge of jamming the transmission of the client to prevent the eavesdroppers from overhearing it. To combat the collusion among eavesdroppers, the SP jams the information signals sent by the client following the multi-jamming stream mechanism and pseudo-preamble mechanism. All the pseudo-random signals and coefficients used by these mechanisms are generated based on a seed. This seed should have been generated based on seed generation mechanism proposed in Section 4.2.3. However, since generating a common bit sequence for two wireless devices based on channel characteristic has been studied in several papers (Mathur et al., 2008; Patwari et al., 2010), its performance is well understood. Therefore, in our experiment, the seed generation and update are not implemented, and the SP simply uses a given sequence as the seed.

Moreover, in our experiment, the SP is equipped with 4 antennae. This is implemented with 4 USRP devices and each of them has one antenna.

The Access Point (AP)

The AP needs to receive the secret key sent by the client under the jamming environments. To this end, two main functions are implemented for the AP: 1) bit-compression mechanism that is used to extract the secret key from the received bit sequence; 2) RANC-processing capability for cancelling the jamming signals from received samples. Also, the seed by which the SP generates the jamming signals is shared by the AP. Hence the AP has the full knowledge about the jamming signals.

The Legacy Client

The main task for the client is to generate and transmit the secret key. As a legacy device, the client only needs to generate a bit sequence based on which the secret key can be extracted, and divide it into several segments for transmissions. All these operations can be completed by the upper-layer at the client. The physical-layer of the client is a standard transmitter and does not include any specific modification: 1) the device is equipped with a single antenna; 2) the modulation scheme is BPSK; 3) a physical-layer frame consists of a 64-bit preamble and payload bits.

The Eavesdroppers

Since it has been demonstrated in the previous sections that the eavesdroppers cannot benefit from the collusion, in this implementation, each eavesdropper individually hacks the secret key transmitted by the client exploiting received signals. Also, the eavesdroppers have no knowledge about the seed shared by the SP and the AP, and hence they are not able to remove the jamming signals from the received samples. In addition, due to the existence of pseudo-preambles, the eavesdroppers cannot estimate the channel coefficients from the client to them. However, we assume that they are capable of gaining the knowledge about the channel

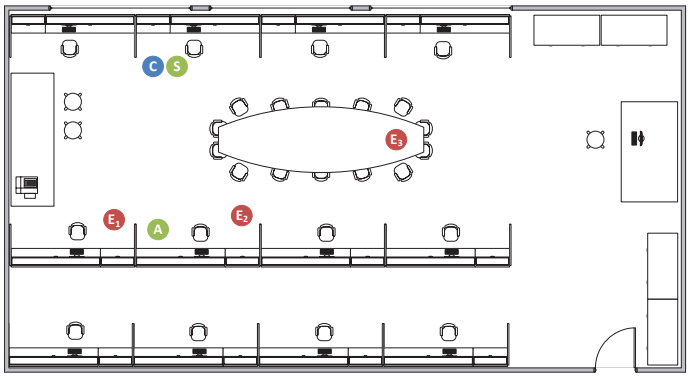


Figure 4.10: Node placement for the experiment.

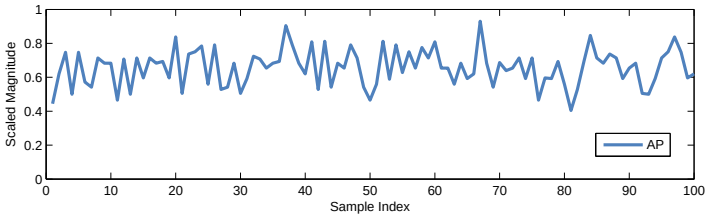
coefficients by guessing[§].

4.4 Evaluation

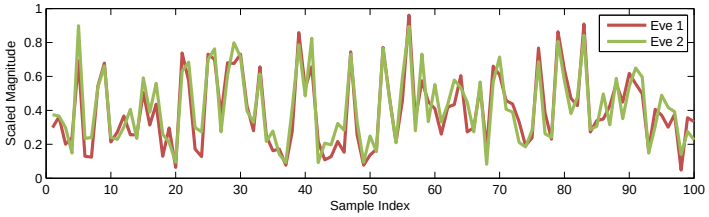
4.4.1 Experiment Setup

To evaluate the proposed scheme, we conduct several experiments with the network deployed in our laboratory building, as shown in Fig. 4.10. In this network, there are a legacy client, a secrecy protector (SP) that is placed 30 cm away from the client, an access point (AP), and three eavesdroppers. The transmission power gain (TX gain) of the client is adjusted so that the link SNR between the client and the AP is around 7 dB, which is a typical range for BPSK transmission. Also, the SP is equipped with four antennae, and the TX gain for each of antenna is 4.7 dB higher than that of the client. Under these settings, the client sends a 128-bit secret key to the AP. This is achieved by generating a 512-bit sequence (i.e., $L_c = 4$) based on which the key can be extracted, dividing the sequence into 16 segments, and transmitting each segment with a data frame. This key transmission procedure is repeated for 400 rounds, and the receiving results of the AP and the eavesdroppers are recorded.

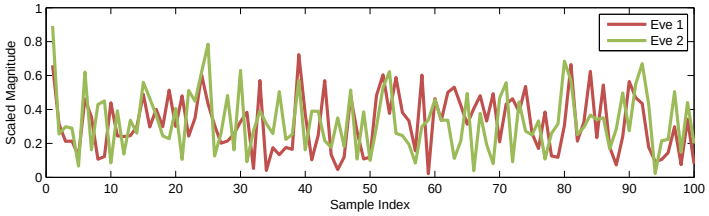
[§]In our implementation, this knowledge is actually gained from channel estimation with a interference-free frame sent by the client instead of guessing.



(a) Without jamming



(b) Traditional jamming



(c) Multi-stream jamming

Figure 4.11: The signal waveforms with/without jamming.

4.4.2 Multi-Stream Jamming

To illustrate the effect of multi-stream jamming, the received samples with and without jamming signals are shown in Fig. 4.11. Since BPSK modulation scheme is adopted by the client to transmit data frames, the received samples without jamming signals have constant magnitude with small fluctuations caused by the noises, as shown in Fig. 4.11(a). When the traditional jamming (single-stream) is applied, the magnitude of the received samples changes significantly and irregularly, and the information signals are fully overwhelmed, as shown in Fig. 4.11(b). However, it can be also observed that the magnitude of received signals at different eavesdropper has high-level similarity. As discussed in Section 4.1.2, this similarity can be exploited by the cooperative eavesdroppers to eliminate the jamming signals. With the multi-stream jamming mechanism, this similarity is effectively avoided, and the magnitude variation of received

Table 4.1: Channel estimation under various jamming schemes.

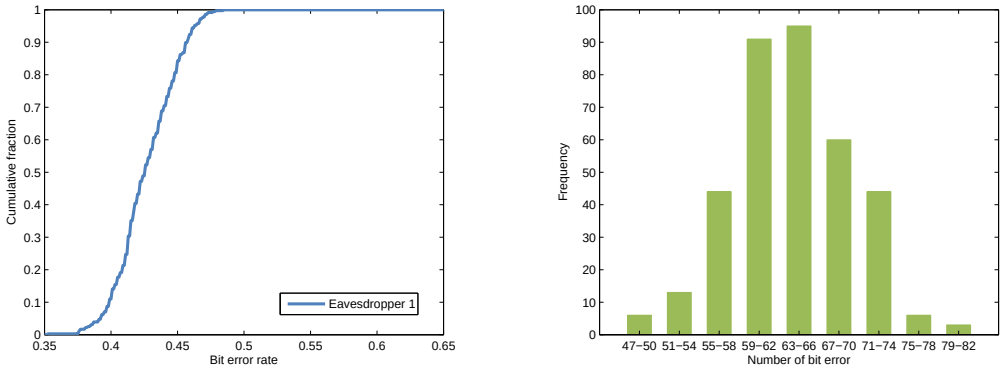
Index	**Channel Coef.**	**Trad. Jamming**		**Pseudo-Preambles**	
	($\cdot 10^{-4}$)	Value ($\cdot 10^{-4}$)	Error	Value ($\cdot 10^{-4}$)	Error
1	2.019-0.620i	2.039-0.715i	4.561%	-0.798-0.958i	134.3%
2	-1.936-0.581i	-2.205-0.300i	19.23%	0.516+0.328i	129.4%
3	-0.498-1.899i	-0.496-2.282i	19.48%	-2.529+2.428i	243.3%
4	-1.290+1.060i	-1.028+1.839i	49.16%	2.134-1.949i	272.9%
5	-0.854-1.699i	-0.803-1.646i	3.850%	0.312-2.719i	81.45%
6	2.230+0.872i	2.683+1.091i	21.01%	-0.990+2.999i	161.2%

signals at different eavesdroppers are significantly different, which is beneficial to prevent the elimination-type collusion among different eavesdroppers.

4.4.3 Pseudo-Preambles

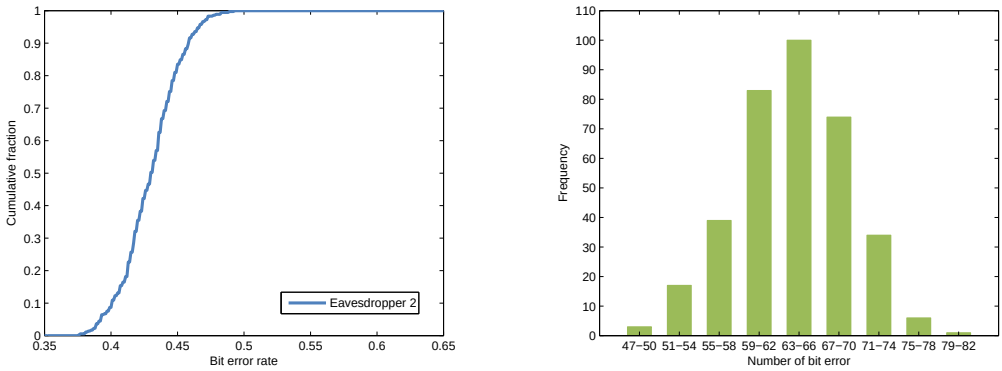
To evaluate the effectiveness of the pseudo-preamble mechanism, we compare the channel estimation results of different eavesdroppers under various scenarios: 1) without jamming signals (in this case, the estimation can accurately reflect the channel conditions); 2) with traditional jamming signals (i.e., the artificial noise); 3) with pseudo-preamble jamming. For the fair comparison, the SP generates the pseudo preamble and the traditional jamming signals with the same transmission power. Also, for each eavesdropper, the channel estimation experiment is repeated for twice with one minute separation (much larger than the channel coherence time). The results, including the estimated value of the main channel tap and the estimation error, are summarized in Table 4.1.

In this table, it can be observed that the eavesdroppers can gain the approximate knowledge about the channel condition through channel estimation under traditional jamming signals. As discussed in Section 4.2.2, this is due to the fact that the channel estimation based on the preamble is robust to the interference of noise-like signals. However, with the pseudo-preambles,



(a) Before bit compression (b) After bit compression

Figure 4.12: Reception bit error (Eavesdropper 1).



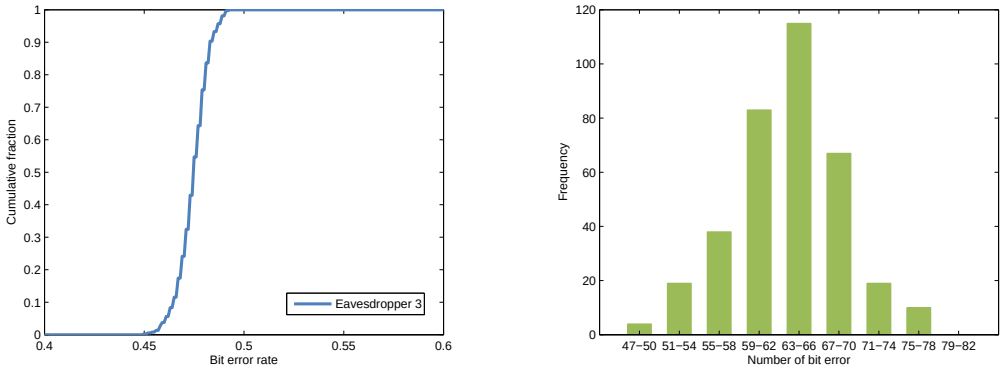
(a) Before bit compression (b) After bit compression

Figure 4.13: Reception bit error (Eavesdropper 2).

the estimated results are significantly deviated from the true values. Therefore, under this mechanism, the eavesdroppers cannot acquire the channel coefficients by estimating. Since these coefficients are indispensable for the beamforming-type collusion, the pseudo-preamble mechanism significantly complicates the beamforming-type collusion among the eavesdroppers.

4.4.4 Key Reception (Eavesdroppers)

The decoding results for different eavesdroppers are present in Fig. 4.12, Fig. 4.13, and Fig. 4.14. Due to the existence of strong jamming signals, the bit error rate (BER) of the received



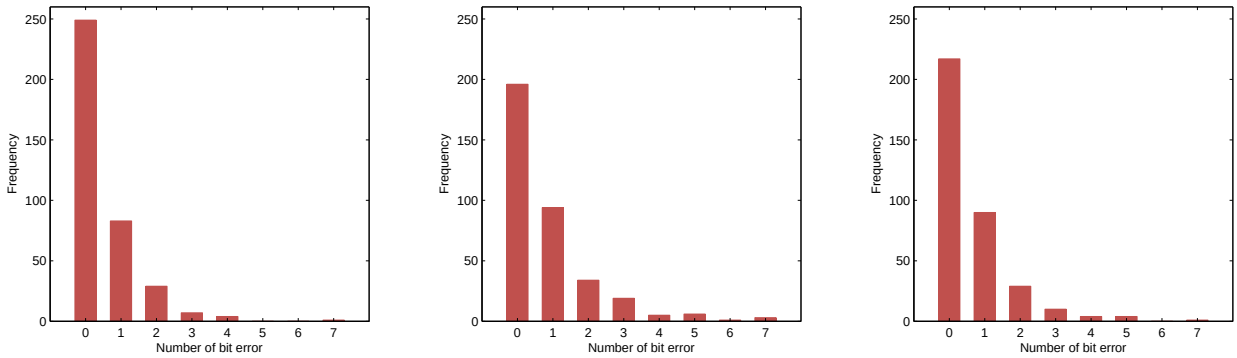
(a) Before bit compression (b) After bit compression

Figure 4.14: Reception bit error (Eavesdropper 3).

sequence (before bit compression) for each eavesdropper is much higher than the upper bound for successful reception, as shown in Fig. 4.12(a), Fig. 4.13(a), and Fig. 4.14(a). However, the mean bit error probabilities of the raw received sequence for three eavesdroppers (0.426, 0.429, and 0.474, respectively) are still not sufficiently close to 0.5. To avoid the leakage of the information of the secret key, the bit compression mechanism is applied. As shown in Fig. 4.12(b), Fig. 4.13(b), and Fig. 4.14(b), after the bit compression, the number of bit errors in the received secret key is approximate to half its length in most cases, and the mean error probabilities of a bit in the key are equal to 0.495, 0.499, and 0.499, for three eavesdroppers respectively. These results demonstrate that the eavesdroppers cannot gain any information about the secret key transmitted by the client under our security scheme.

4.4.5 Key Reception (AP)

The decoding results for the AP are given in Fig. 4.15. Since the RANC decoding algorithm is applied, the jamming signals are effectively removed at the receiver of the AP. Hence the number of bit errors in the received secret key is very low. In most cases, the key is received without any error. In other cases, the low number of errors can be easily corrected with the channel coding. Note that the negative effect of the channel coding on the secrecy of the key



(a) Group 1 (b) Group 2 (c) Group 3

Figure 4.15: Reception bit error (AP).

can be eliminated following the scheme proposed by Jana et al. (2009).

4.5 Summary

In this chapter, a new physical-layer security scheme, i.e., the collusion-resistant jamming, was proposed. This scheme was designed to provide secrecy protection on the legacy wireless communication devices where the physical-layer hardware cannot be modified to support existing physical-layer security schemes. In this scheme, several mechanisms, such as the multi-stream jamming and the pseudo-preamble, were developed to combat the collusion among different eavesdroppers. Also, the RANC decoding algorithm was utilized to cancel the jamming signals at the access point. To evaluate the performance of the scheme, it was implemented in USRP software-defined radio platform. The experiment results demonstrated that the scheme can effectively prevent the eavesdroppers from overhearing the transmission of the client while guarantee the proper communication between the legacy client and the AP.

Chapter 5

Conclusions

Analog network coding (ANC) significantly improves the spectrum utilization of wireless communications by allowing concurrent transmissions from different nodes. Thus, applying ANC to wireless networks is greatly beneficial to enhance the network performance. However, the applicability of ANC is severely limited by two factors: 1) the physical-layer constraints in existing ANC schemes; 2) the lack of effective protocols or schemes to support ANC in wireless networks. Therefore, in this thesis, the new physical-layer design of ANC and the protocols for applying ANC in wireless networks were investigated to significantly extend the applicability of ANC. Specifically, we first proposed a new ANC scheme called random analog network coding that effectively eliminates the physical-layer limitations in existing ANC schemes such as the requirement on the synchronization, the frame size, and the modulation. This scheme is beneficial to dramatically reduce the complexity for applying ANC in wireless networks and simplify the upper-layer protocol design. For instance, by applying RANC, the network synchronization procedure, which is required by many existing ANC schemes but highly demanding in many communication scenarios, can be fully removed. Performance results collected from the real network deployed in the laboratory demonstrated the constraint-free feature of RANC and its performance advantage over existing schemes.

Furthermore, a new random access MAC protocol called ANC-ERA was developed to support RANC (or other practical ANC schemes) in wireless networks with general topologies. This protocol is greatly helpful to enhance the throughput performance of mesh/ad hoc networks, which play a significant role in the next generation wireless networks. Results from the theoretical analysis and the network simulation indicated that ANC-ERA protocol can enhance the network throughput by 6%-115% in various scenarios as compared to existing random access schemes.

Moreover, the RANC decoding algorithm is utilized to support a new physical-layer security scheme. Relying on a third-part device called secrecy protector, this scheme can provide secrecy protection on the legacy wireless communication devices, such as existing cell phones, tablets, and laptops, without modifying the physical-layer hardware of these devices. The experiment results on USRP platform demonstrated that the scheme can effectively guarantee the secure communication between the legacy client and the access point.

5.1 Contributions

The contributions made in this thesis are summarized as follows:

- A new physical-layer scheme called random analog network coding was developed in this thesis. With several specially designed function blocks, such as frame detection, joint channel estimation, circular channel estimation, waveform recovery and re-sampling, and fine-grained frequency offset compensation, RANC supports random concurrent transmissions with arbitrary frame sizes and various modulation schemes. By eliminating constraints in existing ANC schemes, RANC enables the effective, flexible, and creative application of analog network coding in wireless networks.

- A new random access MAC protocol called ANC-ERA was proposed to support practical ANC schemes such as RANC in general-topology wireless networks. In this protocol,

several mechanisms, such as the NAV modification, the channel occupation frame, and the ACK diversity, were designed to combat special issues caused by hidden nodes in a network with ANC cooperation. More importantly, the protocol includes an effective mechanism to enable ANC cooperation even if bi-directional traffic flows are absent. This distinct feature dramatically reduces the dependence of ANC on traffic patterns, and significantly extends the application scope of ANC.

- Combining the physical-layer design and MAC-layer protocol development, we provided a framework for applying complicated physical-layer techniques to general wireless networks in a scalable manner. This framework is beneficial to accelerate the progress of effective application of these advanced techniques.

- The collusion-resistant jamming scheme was designed to provide the secrecy protection on the legacy wireless communication devices where the hardware cannot be modified to support existing physical-layer security schemes. In our scheme, the RANC decoding algorithm was utilized to guarantee the proper communication between the legacy client and the AP. Moreover, several mechanisms, such as multi-stream jamming and the pseudo-preamble, were developed to combat the collusion among eavesdroppers. This scheme not only provides a feasible solution to protect the legacy clients, but also serves as an example of diverse application of RANC.

5.2 Future Work

Although several critical problems related to the application of ANC are solved in this thesis, there remain a few challenging topics for the future research, which are summarized as follows:

- In Chapter 3, we assumed that routing path of a traffic flow was given. However, a routing scheme considering the features of our physical-layer scheme and MAC protocol brings

more benefits to the performance of a network with ANC cooperation. Thus, the design of such a routing scheme needs to be studied.

- With the constraint-free feature, more novel applications of RANC, such as being creatively incorporated into an upper-layer protocol or supporting a new transmission pattern (e.g. multi-way relaying), deserve to be investigated to improve the network performance.

Acknowledgements

My sincere gratitude goes to all who give me generous help in my master study.

First, I would like to express my deepest gratitude to my advisor, Prof. Xudong Wang. During my master study, he provides me considerable support in various aspects, including how to identify interesting research topics, how to conduct solid research work, and how to improve my technical communication skills. Also, Prof. Wang usually provides insightful suggestions for my future career path. Under his guidance, I have gradually become an experienced and dedicated researcher in communications and networking domain.

Also, I am genuinely grateful to my thesis committee members, Prof. Jun Zhang, Prof. Xinen Zhu, and Prof. Weikang Qian. They provide valuable comments and helpful suggestions to my master thesis.

In addition, I would like to thank my research group members, Shanshan Wu, Yibo Pi, Longguang Li, Jun Wang, Huaiyu Huang, Yuhang Zhang, Aimin Tang, Jiawei Chen, Pengfei Huang, Lv Pin, and Quan Liu. We usually discuss and solve research problems together. It is a great experience to cooperate with them.

Finally, I would like to express my most sincere gratitude to my parents. They keep providing me solid support in my life and study and encouraging me to make more progress.

Appendix A

Proof of Proposition 2.2.1

Proposition 2.2.1 Assume that channel coefficients for the desired frame are accurately estimated, while channel gains for the self frame are estimated considering the desired frame as the interference. Then due to the residual interference caused by inaccurate channel estimation for the self frame, SINR for decoding the desired frame will degrade by the factor $\frac{\alpha \mathrm{SNR_d}+1}{N_p}+1$ comparing to the interference-free scenario, where $\mathrm{SNR_d}$ is the signal-to-noise ratio for the desired frame when the self-interference is fully removed, N_p is the total length of pilot sequence including both preamble and postamble and α is a scaling factor determined by the modulation scheme and the pulse shape.

Proof. First of all, we consider the scenario where ISI is absent. For each sample, we have

$$y[n] = h_{d,eqv}x_d[n] + h_{s,eqv}x_s[n] + w[n].$$

To estimate channel coefficients for the self frame, we select samples which align with its preamble and postamble. Then we have

$$\mathbf{Y} = \mathbf{C_s}h_{s,eqv} + \mathbf{C_d}h_{d,eqv} + \mathbf{W},$$

where $\mathbf{Y}$ is the column vector which consists of selected samples, $\mathbf{C_s}$ is the column vector which is filled with pilot sequence of the self frame including both preamble and postamble, and $\mathbf{C_d}$ and $\mathbf{W}$ are corresponding vectors for symbols of the desired frame and noise. If the desired frame is simply considered as the interference, $h_{s,eqv}$ will be estimated as

$$\tilde{h}_{s,eqv} = (\mathbf{C_s^H C_s})^{-1}\mathbf{C_s^H} \cdot \mathbf{Y}.$$

The estimation error can be expressed as

$$\begin{aligned}
\tilde{h}_{s,eqv} - h_{s,eqv} &= (\mathbf{C_s^H C_s})^{-1}\mathbf{C_s^H} \cdot \mathbf{Y} - h_{s,eqv} \\
&= (\mathbf{C_s^H C_s})^{-1}\mathbf{C_s^H} \cdot (\mathbf{C_s} h_{s,eqv} + \mathbf{C_d} h_{d,eqv} + \mathbf{W}) - h_{s,eqv} \\
&= (\mathbf{C_s^H C_s})^{-1}\mathbf{C_s^H} \cdot (\mathbf{C_d} h_{d,eqv} + \mathbf{W}) \\
&= \frac{1}{N_p}\mathbf{C_s^H} \cdot (\mathbf{C_d} h_{d,eqv} + \mathbf{W}) \\
&= \frac{1}{N_p}(\sum\ c_s[i](h_{d,eqv} c_d[i] + w[i])) \\
&= \frac{1}{N_p}(h_{d,eqv} \sum\ c_s[i] c_d[i] + \sum\ c_s[i] w[i]),
\end{aligned}$$

where $c_s[i]$, $c_d[i]$ and $w[i]$ are elements of corresponding column vector. Due to asynchronous superposition between the self frame and the desired frame, $c_d[i]$ could be pilot symbol or data symbol. For the sake of simplicity, we can assume that $c_d[i]$ is a random variable, which takes the value from the symbol alphabet with equal probability, and is independent with each other. Then we have

$$\begin{aligned}
E[c_d[i]] &= 0, \\
V[c_d[i]] &= M^2,
\end{aligned}$$

where the value of M depends on the modulation scheme adopted by the desired frame. For

PSK modulations, M is equal to 1, while for 4-PAM and 16-QAM, M is equal to 0.75. Also, note that $c_d[i]$ has the same distribution with $-c_d[i]$. In addition, $c_s[i]$ is a pilot symbol of the self frame and hence takes the value 1 or -1. Then we have

$$\tilde{h}_{s,eqv} - h_{s,eqv} = \frac{1}{N_p}(h_{d,eqv} \sum\ c_d[i] + \sum\ w[i]).$$

According to central limit theorem, we have

$$\tilde{h}_{s,eqv} - h_{s,eqv} = h_{d,eqv}c_d + w_1,$$

where c_d, w_1 are Gaussian random variables with the deviation equal to $M/\sqrt{N_p}$ and $\sigma_n/\sqrt{N_p}$ respectively. Furthermore, the error of channel estimation can be expressed as

$$\tilde{h}_{s,eqv} - h_{s,eqv} = w_2,$$

where w_2 is a Gaussian random variable with the deviation equal to $\sqrt{\frac{h_{d,eqv}^2 M^2 + \sigma_n^2}{N_p}}$. With the knowledge of the estimation error, the SINR for decoding the desired frame after removing the self-interference can be calculated. We have

$$y_d[n] = h_{d,eqv}x_d[n] + (h_{s,eqv} - \tilde{h}_{s,eqv})x_s[n] + w[n].$$

With the waveform recovery, we have

$$\tilde{y}_d(t) = x_d(t) + \sum_i\ (h_{s,eqv} - \tilde{h}_{s,eqv})x_s[i]\text{sinc}\left(\frac{t - iT}{T}\right) + w(t).$$

After relocating sampling positions, we have

$$y_{d,opt}[n] = h_{d,opt}x_d[n] + \sum_i\ (h_{s,eqv} - \tilde{h}_{s,eqv})x_s[i]\text{sinc}\left(\frac{t_{opt} - iT}{T}\right) + w[n],$$

where t_{opt} corresponds to the optimal sampling position. Then the SINR for decoding the desired frame can be expressed as

$$\begin{aligned}
\text{SINR} &= \frac{h_{d,opt}^2 \cdot M^2}{E\left[\left(\sum_i (h_{s,eqv} - \tilde{h}_{s,eqv}) x_s[i] \text{sinc}\left(\frac{t_{opt}-iT}{T}\right)\right)^2\right] + \sigma_n^2} \\
&= \frac{h_{d,opt}^2 \cdot M^2}{E\left[(h_{s,eqv} - \tilde{h}_{s,eqv})^2\right] E\left[\left(\sum_i x_s[i] \text{sinc}\left(\frac{t_{opt}-iT}{T}\right)\right)^2\right] + \sigma_n^2} \\
&= \frac{h_{d,opt}^2 \cdot M^2}{\frac{E[h_{d,eqv}^2]M^2+\sigma_n^2}{N_p} E\left[\left(\sum_i x_s[i] \text{sinc}\left(\frac{t_{opt}-iT}{T}\right)\right)^2\right] + \sigma_n^2}.
\end{aligned}$$

Note that when $|x_s[n]| = \pm 1$, the self frame causes the maximum interference. Also, we assume that $x_s[i]$ is independent with each other. Then the SINR can be further simplified as

$$\begin{aligned}
\text{SINR} &= \frac{h_{d,opt}^2 \cdot M^2}{\frac{E[h_{d,eqv}^2]M^2+\sigma_n^2}{N_p} E\left[\sum_i \left(x_s[i] \text{sinc}\left(\frac{t_{opt}-iT}{T}\right)\right)^2\right] + \sigma_n^2} \\
&= \frac{h_{d,opt}^2 \cdot M^2}{\frac{E[h_{d,eqv}^2]M^2+\sigma_n^2}{N_p} \sum_i \left(\text{sinc}\left(\frac{t_{opt}-iT}{T}\right)\right)^2 + \sigma_n^2 \cdot M^2} \\
&= \frac{h_{d,opt}^2 \cdot M^2}{\frac{E[h_{d,eqv}^2]M^2+\sigma_n^2}{N_p} + \sigma_n^2}.
\end{aligned}$$

The value of $E[h_{d,eqv}^2]$ depends on the pulse shape of the desired frame, and can be expressed as $\alpha h_{d,opt}^2$. Then we have

$$\begin{aligned}
\text{SINR} &= \frac{h_{d,opt}^2 \cdot M^2}{\frac{\alpha h_{d,opt}^2 M^2+\sigma_n^2}{N_p} + \sigma_n^2} \\
&= \frac{\text{SNR}_\text{d}}{\frac{\alpha \text{SNR}_\text{d}+1}{N_p} + 1}.
\end{aligned}$$

Thus, the SINR degrades by a factor $\frac{\alpha \mathrm{SNR_d}+1}{N_p}+1$ comparing to the interference-free scenario.

As discussed previously, sampling errors (not sampling at the optimal positions) for the self frame and the desired frame cannot not be avoided, which may lead to the inter-symbol interference. If the inter-symbol interference is taken into consideration, let

$$\mathbf{h_{s,eqv}} = \begin{bmatrix} h_{s,1} \\ h_{s,2} \\ \vdots \\ h_{s,l_s} \end{bmatrix} \quad \text{and} \quad \mathbf{h_{d,eqv}} = \begin{bmatrix} h_{d,1} \\ h_{d,2} \\ \vdots \\ h_{d,l_d} \end{bmatrix},$$

and

$$\mathbf{C_S} = \begin{bmatrix} \mathbf{C_{s,1}} & \mathbf{C_{s,2}} & \cdots & \mathbf{C_{s,l_s}} \end{bmatrix} \quad \text{and} \quad \mathbf{C_D} = \begin{bmatrix} \mathbf{C_{d,1}} & \mathbf{C_{d,2}} & \cdots & \mathbf{C_{d,l_d}} \end{bmatrix},$$

where $\mathbf{C_{i,j}}$ $(i \in \{S, D\},\ j \in [1, l_i])$ is the column vector equal to $\begin{bmatrix} \mathbf{0}_{j-1} & \mathbf{C_{f_i}} & \mathbf{0}_{\,l_i-j.} \end{bmatrix}$ ($\mathrm{f}_S = s,$ and $\mathrm{f}_D = d$). Here, $\mathbf{0}_n$ is defined as the column vector with the length equal to n and all entries equal to zero. Then we have

$$\begin{aligned} \tilde{\mathbf{h}}_{\mathbf{s,eqv}} - \mathbf{h_{s,eqv}} &= (\mathbf{C_S^H C_S})^{-1} \mathbf{C_S^H} \cdot (\mathbf{C_D h_{d,eqv}} + \mathbf{W}) \\ &= \left(\begin{bmatrix} \mathbf{C_{s,1}^H} \\ \mathbf{C_{s,2}^H} \\ \vdots \\ \mathbf{C_{s,l_s}^H} \end{bmatrix} \begin{bmatrix} \mathbf{C_{s,1}} & \mathbf{C_{s,2}} & \cdots & \mathbf{C_{s,l_s}} \end{bmatrix} \right)^{-1} \begin{bmatrix} \mathbf{C_{s,1}^H} \\ \mathbf{C_{s,2}^H} \\ \vdots \\ \mathbf{C_{s,l_s}^H} \end{bmatrix} \left(\sum_k \mathbf{C_{d,k}} h_{d,k} + \mathbf{W} \right). \end{aligned}$$

Note that

$$\mathbf{C_{s,i}^H C_{s,i}} = N_p,$$

and when $i \neq j$

$$\mathbf{C_{s,i}^H C_{s,j}} \ll N_p.$$

Hence, the estimation error can be further simplified as

$$\begin{aligned}
\tilde{\mathbf{h}}_{\mathbf{s,eqv}} - \mathbf{h}_{\mathbf{s,eqv}} &\approx \begin{bmatrix} N_p & 0 & 0 & \cdots & 0 \\ 0 & N_p & 0 & \cdots & 0 \\ 0 & 0 & N_p & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & N_p \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{C}_{\mathbf{s,1}}^{\mathbf{H}} \\ \mathbf{C}_{\mathbf{s,2}}^{\mathbf{H}} \\ \vdots \\ \mathbf{C}_{\mathbf{s,l_s}}^{\mathbf{H}} \end{bmatrix} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \\
&= \begin{bmatrix} \frac{1}{N_p}\mathbf{C}_{\mathbf{s,1}}^{\mathbf{H}} \\ \frac{1}{N_p}\mathbf{C}_{\mathbf{s,2}}^{\mathbf{H}} \\ \vdots \\ \frac{1}{N_p}\mathbf{C}_{\mathbf{s,l_s}}^{\mathbf{H}} \end{bmatrix} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \\
&= \begin{bmatrix} \frac{1}{N_p}\mathbf{C}_{\mathbf{s,1}}^{\mathbf{H}} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \\ \frac{1}{N_p}\mathbf{C}_{\mathbf{s,2}}^{\mathbf{H}} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \\ \vdots \\ \frac{1}{N_p}\mathbf{C}_{\mathbf{s,l_s}}^{\mathbf{H}} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \end{bmatrix}.
\end{aligned}$$

Then

$$\begin{aligned}
\tilde{h}_{s,j} - h_{s,j} &= \frac{1}{N_p}\mathbf{C}_{\mathbf{s,j}}^{\mathbf{H}} \left(\sum_k \mathbf{C}_{\mathbf{d,k}} h_{d,k} + \mathbf{W} \right) \\
&= \frac{1}{N_p} \sum_i c_{s,j}[i] \left(\sum_k c_{d,k}[i] h_{d,k} + w[i] \right).
\end{aligned}$$

Similar with previous discussion, it can be shown that

$$\tilde{h}_{s,j} - h_{s,j} = w_{eqv,j},$$

where $w_{eqv,j}$ is a Gaussian random variable with the variance equal to $\frac{M^2 \sum_k h_{d,k}^2 + \sigma_n^2}{N_p}$. After

removing the components due to the self frame and relocating optimal sampling positions, we have

$$\begin{aligned} y_{d,opt}[n] &= h_{d,opt}x_d[n] + \sum_i (h_{s,1} - \tilde{h}_{s,1})x_s[i]\text{sinc}\left(\frac{t_{opt} - iT}{T}\right) \\ &\quad + \sum_i (h_{s,2} - \tilde{h}_{s,2})x_s[i-1]\text{sinc}\left(\frac{t_{opt} - iT}{T}\right) + \ldots + w[n]. \end{aligned}$$

Note that the inter-symbol interference of the desired frame can be removed after sampling at optimal positions if the pulse shape of the desired frame satisfies the Nyquist criterion. With the similar derivation as the non-ISI case, the SINR can be given as

$$\text{SINR} = \frac{h_{d,opt}^2 \cdot M^2}{\frac{l_s E\left[\sum_k h_{d,k}^2\right] M^2 + \sigma_n^2}{N_p} + \sigma_n^2}.$$

Let $E\left[\sum_k h_{d,k}^2\right] = n_{eqv} h_{d,opt}^2$. The value of n_{eqv} depends on the pulse shape adopted by the desired frame. If the sinc function is adopted, it can be shown that $n_{eqv} = 1$. Also, if the raised cosine function is selected as the pulse shape, the value of n_{eqv} is also close to 1. Hence we can use 1 as an approximation for n_{eqv}, and then we have

$$\begin{aligned} \text{SINR} &= \frac{h_{d,opt}^2 \cdot M^2}{\frac{l_s M^2 h_{d,opt}^2 + \sigma_n^2}{N_p} + \sigma_n^2} \\ &= \frac{\text{SNR}_\text{d}}{\frac{l_s \text{SNR}_\text{d} + 1}{N_p} + 1}. \end{aligned}$$

If let $\alpha = l_s$, the SINR degrades by a factor $\frac{\alpha \text{SNR}_\text{d} + 1}{N_p} + 1$ comparing to the interference-free scenario. □

Comments This theorem can be used to evaluate the error performance of preliminary decoding in the circular channel estimation scheme and determine whether the preliminary decoding results are sufficient to be exploited to mitigate the interference for estimating channel coef-

ficients of the self frame. Consider that $\mathrm{SNR_d}$ belongs to the region of 8dB-25dB, which is a typical range for wireless communications. The theorem indicates that under common conditions*, the residual self-interference will degrades the decoding SINR for the desired frame by 1dB-9dB comparing to the scenario where the self-interference is fully removed. This degradation of SINR will evidently increase the bit error rate. However, the result SINR (7dB-16dB) is still enough to guarantee that the bit error rate of preliminary decoding is less than 10^{-1}, meaning that most of symbols are corrected decoded. Also, for high-order modulation scheme such as 64-QAM, even if a symbol is incorrectly decoded, it is highly possible that the decoded result is close to the correct value. Therefore, the preliminary decoding results are helpful to mitigate the interference for estimating channel coefficients of the self frame.

*The number of channel taps is about 7. The number of pilot symbols in a frame is equal to 320. The common modulation schemes (e.g. BPSK, QPSK, 16-QAM and 64-QAM) are adopted according to the value of $\mathrm{SNR_d}$.

Appendix B

Proof of Proposition 3.3.1

Consider a network with n nodes that can sense each other. For each node, it may stay in different backoff stages. The contention window for i-th backoff stage is denoted by W_i, where i is a non-negative integral and bounded by a constant m. A node in the i-th backoff stage has a value of backoff-time counter in the range $[0, W_i - 1]$. To characterize the backoff situation of each node, we use $S_{i,j}$ to denote the state that a node entries to the ith backoff stage and has a backoff-time counter equal to j.

There exist two important probabilities affecting transitions between different states $\{S_{i,j}\}$. One of them is the transmission failure probability p_f defined as the probability that collision happens in an ANC cooperation process and leads to the failure of the cooperation. As mentioned in Bianchi (2000), it is reasonable to assume that p_f is independent with the number of retransmissions. The other key probability is the cooperation probability p_c, defined as the probability that one node receives a cooperation request (i.e., an RTC frame) when it stays in a backoff state and forms ANC cooperation with the initiator. Note that the cooperation probability is independent from backoff stages and counters.

Based on above definitions, we can model the transitions between states $\{S_{i,j}\}$ as a discrete-

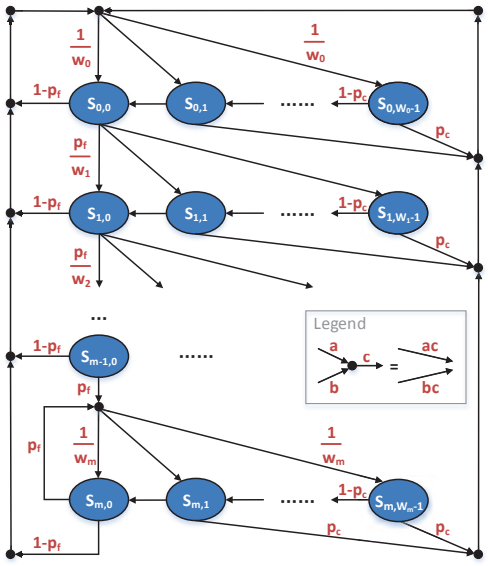


Figure B.1: The Markov chain for backoff state transitions in ANC-ERA protocol

time Markov chain. As shown in Fig. B.1, all of non-zero state transition probabilities are:

$$\begin{cases} p\{S_{0,j}|S_{i,0}\} = \frac{1-p_f}{W_0}, \ i \in [0,m], j \in [0,W_0) \\ p\{S_{i+1,j}|S_{i,0}\} = \frac{p_f}{W_{i+1}}, \ i \in [0,m), j \in [0,W_{i+1}) \\ p\{S_{m,j}|S_{m,0}\} = \frac{p_f}{W_m}, \ j \in [0,W_m) \\ p\{S_{0,k}|S_{i,j}\} = \frac{p_c}{W_0}, \ i \in [0,m], j \in [0,W_i), k \in [0,W_0) \\ p\{S_{i,j-1}|S_{i,j}\} = 1-p_c, \ i \in [0,m], j \in [1,W_i), \end{cases} \tag{B.1}$$

The first three equations in (B.1) represent backoff behaviors after collisions or successful transmissions, which is similar to the case in IEEE 802.11 DCF. The fourth equation describes the state transitions due to the data transmission as a cooperator. Specifically, if a node receives an RTC frame, under saturation condition, it always has a data frame to the initiator and ANC cooperation will be formed. Since the channel has been captured by the RTS frame and all nodes can sense the ongoing transmission, the data frames sent by the initiator and the node

(i.e. the cooperator) will be free from collisions and successfully received* by each other. In this case, the node resets its backoff stage to zero and takes a random backoff time, i.e. the backoff state will be changed following the probability described by the fourth equation. The last equation represents that if a node does not receive any cooperation request, it will reduce its backoff counter once the channel is sensed idle for DIFS period.

Let $\{v_{i,j}\}$ denote the stationary distribution of $\{S_{i,j}\}$. It can be shown that

$$\begin{cases} v_{0,j} = v_{0,j+1}(1-p_c) + \frac{v_c p_c}{W_0} + v_t \frac{1-p_f}{W_0}, \ j \in [0, W_0) \\ v_{i,j} = v_{i,j+1}(1-p_c) + \frac{v_{i-1,0} p_f}{W_i}, \ i \in [1, m), j \in [0, W_i) \\ v_{m,j} = v_{m,j+1}(1-p_c) + \frac{v_{m-1,0} p_f}{W_m} + \frac{v_{m,0} p_f}{W_m}, j \in [0, W_m) \\ \sum_{i=0}^{m} \sum_{j=0}^{W_i - 1} v_{i,j} = 1, \end{cases} \tag{B.2}$$

where

$$v_c = \left(\sum_{i=0}^{m} \sum_{j=1}^{W_i - 1} v_{i,j} \right), \quad v_t = \sum_{i=0}^{m} v_{i,0}. \tag{B.3}$$

Based on recursive relations in Eq. (B.2), we can show that

$$v_{i,0} = \frac{p_f^i [v_c p_c + v_t (1-p_f)]}{p_c^{i+1} \delta_i} \prod_{k=0}^{i} \frac{1-(1-p_c)^{W_k}}{W_k},$$

where δ_i is given by

$$\begin{cases} \dfrac{p_c W_m - p_f [1-(1-p_c)^{W_m}]}{p_c W_m}, & i = m \\ 1, & \text{otherwise.} \end{cases}$$

Then, according to Eq. (B.3), v_t can be expressed as

$$v_t = [v_c p_c + v_t (1-p_f)] \left\{ \sum_{i=0}^{m} \frac{p_f^i}{p_c^{i+1} \delta_i} \prod_{k=0}^{i} \frac{1-(1-p_c)^{W_k}}{W_k} \right\}.$$

*The transmission error is not considered in this paper.

We define the expression included by braces in the above equation as $c(p_f, p_c)$. With Eq. (B.3) and Eq. (B.2), we can conclude that $v_c + v_t = 1$. Thus, based on the above equation, it can be shown that

$$v_t = \frac{c(p_f, p_c)p_c}{1 - c(p_f, p_c)(1 - p_c - p_f)}.$$

Furthermore, the transmission probability p_t is defined as the probability that a node initiates an ANC cooperation process in a given time slot. Thus, it can be expressed as

$$p_t = \sum_{i=0}^{m} v_{i,0} = v_t = \frac{c(p_f, p_c)p_c}{1 - c(p_f, p_c)(1 - p_c - p_f)}. \tag{B.4}$$

For the sake of simplicity, we consider a symmetric setting where each node has an equal opportunity to be requested to participate in an ANC cooperation. In this case, we can assume that the cooperation probability p_c is the same for all nodes in the network. Also, as mentioned in Bianchi (2000), it is reasonable to assume that p_f keeps invariant for different nodes. Furthermore, since the transmission probability is determined by the cooperation probability p_c and the transmission failure probability p_f, we can conclude that the transmission probability p_t is also invariable over nodes.

Let D_X denote the set of nodes that have data frames with Node X as their two-hop destination and T_X represent the set of nodes which are two-hop destinations of data frames from Node X. Also, p^t_{XY} stands for the probability that Node X transmits an RTS frame with Node Y as the two-hop destination in a given time slot, and p^s_{XY} denotes the probability that such RTS frame is free from collision (and hence captures the channel). Thus, for a specific station A, the cooperation probability is given by

$$p_c = \sum_{X \in D_A} p^t_{XA} p^s_{XA} = (1 - p_t)^{n-2} \sum_{X \in D_A} p^t_{XA}.$$

Adding the cooperation probabilities of all nodes together, we have that

$$\begin{aligned}\sum_{Y} p_c &= (1-p_t)^{n-2} \sum_{Y} \sum_{X \in D_Y} p^t_{XY} \\ &= (1-p_t)^{n-2} \sum_{X} \sum_{Y \in T_X} p^t_{XY} \\ &= (1-p_t)^{n-2} \sum_{X} p_t.\end{aligned}$$

We know that p_c and p_t are same for all nodes, hence it can be shown that

$$p_c = p_t(1-p_t)^{n-2}. \tag{B.5}$$

The transmission failure probability can be expressed as

$$p_f = 1-(1-p_t)^{n-1}. \tag{B.6}$$

Combining Eq. (B.4) (B.5) (B.6), we can solve p_t, p_f and p_c with numerical methods. Although the previous derivation is based on symmetric setting assumption, our theoretical framework is not limited to this case. In fact, it can be applied to various scenarios. In a general case, p_t, p_f and p_c are different for different nodes, and we need to solve $3n$ equations to obtain these probabilities.

Based on previous results, the saturation throughput can be calculated following similar steps in Bianchi and Tinnirello (2005). The main difference is that in each successful ANC cooperation, two data frames are received by their two-hop destinations. This is equivalent to four transmissions in a network following IEEE 802.11 DCF. Therefore the saturation throughput can be expressed as

$$\frac{4P_{\text{succ}}L_p}{(1-\frac{1}{W_0})T_{\text{slot}} + P_{\text{succ}}T_s + (1-\frac{1}{W_0})P_{\text{col}}T_c}, \tag{B.7}$$

where

$$\begin{cases} P_{\text{succ}} = np_t(1-p_t)^{n-1} \\ P_{\text{col}} = 1-(1-p_t)^n - np_t(1-p_t)^{n-1} \\ T_s = \text{RTS} + \text{SIFS} + \delta + \text{RTC} + \text{SIFS} + \delta + \text{ATC} \\ \qquad +\text{SIFS} + \delta + \text{CTS} + \text{SIFS} + \delta + \text{BData} \\ \qquad +\text{SIFS} + \delta + \text{BData} + \text{SIFS} + \delta + \text{BACK} \\ \qquad +\text{SIFS} + \delta + \text{BACK} + \text{SIFS} + \delta + \text{DIFS} \\ T_c = \text{RTS} + \text{DIFS} + \delta. \end{cases}$$

T_{slot}, L_p, δ are defined as slot time, the length of payload bits in a data frame, and propagation delay, respectively.

Bibliography

Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function. *Selected Areas in Communications, IEEE Journal on 18*(3), 535–547.

Bianchi, G. and I. Tinnirello (2005). Remarks on IEE 802.11 DCF performance analysis. *IEEE Communications Letters 9*(8), 765–767.

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

Dong, L., Z. Han, A. P. Petropulu, and H. V. Poor (2010). Improving wireless physical layer security via cooperating relays. *Signal Processing, IEEE Transactions on 58*(3), 1875–1888.

Elson, J., L. Girod, and D. Estrin (2002). Fine-grained network time synchronization using reference broadcasts. *ACM SIGOPS Operating Systems Review 36*(SI), 147–163.

Fu, S., K. Lu, T. Zhang, Y. Qian, and H.-H. Chen (2010). Cooperative wireless networks based on physical layer network coding. *Wireless Communications, IEEE Transactions on 17*(6), 86–95.

Fung, P. H. W., S. Sun, and C. K. Ho (2010). Preamble design for carrier frequency offset estimation in two-way relays. In *Proceedings of IEEE Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5. IEEE.

Gollakota, S. and D. Katabi (2008). Zigzag decoding: combating hidden terminals in wireless networks. In *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM)*, pp. 159–170. ACM.

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

Goussevskaia, O. and R. Wattenhofer (2008). Complexity of scheduling with analog network coding. In *Proceedings of the ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing (FOWANC)*, pp. 77–84. ACM.

IEEE (1999). IEEE Std 802.11a-1999-part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 Ghz band. pp. 24.

IEEE (2007). IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2007*, 72–74.

IEEE (2012). IEEE Std 802.11ad-2012-part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 3: Enhancements for very high throughput in the 60 Ghz band. pp. 1–628.

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

Jitvanichphaibool, K., R. Zhang, and Y.-C. Liang (2009). Optimal resource allocation for two-way relay-assisted OFDMA. *Vehicular Technology, IEEE Transactions on 58*(7), 3311–3321.

Katti, S., S. Gollakota, and D. Katabi (2007). Embracing wireless interference: analog network coding. In *ACM SIGCOMM Computer Communication Review*, Volume 37, pp. 397–408. ACM.

Khabbazian, M., F. Kuhn, N. Lynch, M. Médard, and A. ParandehGheibi (2011). MAC design for analog network coding. In *Proceedings of ACM International Workshop on Foundations of Mobile Computing*, pp. 42–51. ACM.

Khisti, A. and G. W. Wornell (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel. *Information Theory, IEEE Transactions on 56*(7), 3088–3104.

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

Leon-Garcia, A. and I. Widjaja (2003). *Communication Networks: Fundamental Concepts and Key Architectures*. McGraw-Hill, Inc.

Li, Z., X.-G. Xia, and B. Li (2009). Achieving full diversity and fast ML decoding via simple analog network coding for asynchronous two-way relay networks. *Communications, IEEE Transactions on 57*(12), 3672–3681.

Lin, Y.-D., C.-N. Lu, Y.-C. Lai, W.-H. Peng, and P.-C. Lin (2009). Application classification using packet size distribution and port association. *Journal of Network and Computer Applications 32*(5), 1023–1030.

Liu, H., Y. Wang, J. Yang, and Y. Chen (2013). Fast and practical secret key extraction by exploiting channel response. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 3048–3056. IEEE.

Maric, I., A. Goldsmith, and M. Médard (2012). Multihop analog network coding via amplify-and-forward: the high SNR regime. *Information Theory, IEEE Transactions on 58*(2), 793–803.

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

McGregor, A., M. Hall, P. Lorier, and J. Brunskill (2004). Flow clustering using machine learning techniques. *Passive and Active Network Measurement*, 205–214.

Mengali, U. and A. N. D'Andrea (1997). *Synchronization Techniques for Digital Receivers*. Springer.

Negi, R. and S. Goel (2005). Secret communication using artificial noise. In *Proceedings of IEEE Vehicular Technology Conference*, Volume 62, pp. 1906. IEEE.

Patwari, N., J. Croft, S. Jana, and S. K. Kasera (2010). High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *Mobile Computing, IEEE Transactions on 9*(1), 17–30.

Pengfei Huang, X. W. (2013). Fast secret key generation in static wireless networks: A virtual channel approach. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*. IEEE.

Popovski, P. and O. Simeone (2009). Wireless secrecy in cellular systems with infrastructure-aided cooperation. *Information Forensics and Security, IEEE Transactions on 4*(2), 242–256.

Popovski, P. and H. Yomo (2006). Bi-directional amplification of throughput in a wireless multi-hop network. In *Proceedings of IEEE Vehicular Technology Conference*, Volume 2, pp. 588–593. IEEE.

Rankov, B. and A. Wittneben (2007). Spectral efficient protocols for half-duplex fading relay channels. *Selected Areas in Communications, IEEE Journal on 25*(2), 379–389.

Rossetto, F. and M. Zorzi (2009). On the design of practical asynchronous physical layer network coding. In *Proceedings of IEEE Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 469–473. IEEE.

Roughan, M., S. Sen, O. Spatscheck, and N. Duffield (2004). Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification. In *Proceedings of ACM IMC*.

Sen, S., R. Roy Choudhury, and S. Nelakuditi (2012). CSMA/CN: carrier sense multiple access with collision notification. *Networking, IEEE/ACM Transactions on 20*(2), 544–556.

Shiu, Y.-S., S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen (2011). Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications 18*(2), 66–74.

Sommer, P. and R. Wattenhofer (2009). Gradient clock synchronization in wireless sensor networks. In *Proceedings of International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 37–48. IEEE.

Su, H. and X. Zhang (2009). Modeling throughput gain of network coding in multi-channel multi-radio wireless ad hoc networks. *Selected Areas in Communications, IEEE Journal on 27*(5), 593–605.

Sundararaman, B., U. Buy, and A. D. Kshemkalyani (2005). Clock synchronization for wireless sensor networks: a survey. *Ad Hoc Networks 3*(3), 281–323.

Tan, K., H. Liu, J. Fang, W. Wang, J. Zhang, M. Chen, and G. M. Voelker (2009). SAM: enabling practical spatial multiple access in wireless LAN. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 49–60. ACM.

Tang, X., R. Liu, P. Spasojevic, and H. Poor (2011). Interference assisted secret communication. *Information Theory, IEEE Transactions on 57*(5), 3153–3167.

Tekin, E. and A. Yener (2008). The general gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming. *Information Theory, IEEE Transactions on 54*(6), 2735–2751.

Thangaraj, A., S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla (2007). Applications of LDPC codes to the wiretap channel. *Information Theory, IEEE Transactions on 53*(8), 2933–2945.

Trimble Inc. (2013). Thunderbolt E GPS disciplined clock.

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

Wang, H.-M., Q. Yin, and X.-G. Xia (2012). Distributed beamforming for physical-layer security of two-way relay networks. *Signal Processing, IEEE Transactions on 60*(7), 3532–3545.

Wang, S., Q. Song, X. Wang, and A. Jamalipour (2013). Distributed MAC protocol supporting physical-layer network coding. *Mobile Computing, IEEE Transactions on 12*(5), 1023–1036.

Wyner, A. D. (1975). The wire-tap channel. *Bell Syst. Tech. J. 54*(8), 1334–1387.

Zhang, S., S. C. Liew, and P. P. Lam (2006). Hot topic: physical-layer network coding. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 358–365. ACM.